Response to SEC Crypto Roundtable on Asset Tokenization

AUTHORS:

Raj Mukherjee
Special Advisor, Global Regulatory Affairs, Finternet

Abhishek Sankritik
Director– Programs & Policy, Finternet

Finternet

Executive Summary

Digital asset markets have evolved rapidly in a fragmented landscape of inhibitive platforms and patchwork regulations. This paper is a response to the recent Securities and Exchange Commission's ("SEC") Crypto Task Force roundtable discussions on regulating tokenized assets. This paper proposes adopting universal technical standards and regulatory approaches for such digital assets. Grounded in the U.S. context and informed by the EU and Singapore, we outline how an open, interoperable architecture can coexist with smart, *flow-based* regulation to foster innovation while protecting users. Key insights and recommendations include:

1. Baseline Technical Standards: We advocate for a *common set* of protocols enabling interoperability and programmability of digital assets without presupposing the asset's legal nature. The *Finternet* model introduces open, internet-like standards, such as a *Unified Interledger Protocol (UILP),* allowing disparate ledgers and token systems to transact seamlessly. By focusing on standardizing transaction flows like issuance, transfer and settlement rather than rigid asset container formats, regulators and industry can better future-proof the ecosystem for evolving asset types. Core technical building blocks like token managers, proof claims, and portable credentials enable any token (stablecoin, security token or commodity token etc.) to seamlessly integrate into a shared secure financial internet. By grounding digital asset regulation in technology-neutral standards and flow-aware policies, we can unlock the benefits of tokenization (efficiency, financial inclusion, new financial products) while upholding market integrity and consumer protection.

2. Global Regulatory Best Practices: Despite differing regulatory regimes, we identify universal principles for digital asset oversight. These include a user-centric designs that ensure consumer protection and access, flow-based regulation focusing on activities and transactions rather than asset labels, and principles-based accountability that aim to set broad obligations for fairness, transparency, and risk management. We recommend regulators converge on risk-based rules for digital asset flows (for example, higher scrutiny for larger

more complex transactions, simplified rules for low-value or experimental use) applied consistently across jurisdictions.

3. Custodial Architecture: *Self-Custody and Third-Party Custody*: The *Finternet* vision is neutral to whether users self-custody assets or entrust them to intermediaries. Both models can be supported on a unified ledger infrastructure provided there are common safeguards that cover operational controls, cybersecurity standards, key management protocols, disclosures communicating clear risk, rights and obligations, and technical safeguards such as multi-signature or smart contract-based custody, audit trails, and recovery mechanisms. For *self-custody*, the system should empower users with tools to securely manage private keys (or mnemonic credentials) and enable social recovery or registrar-assisted recovery for lost access without compromising autonomy. For *third-party custody*, stricter standards are needed to ensure segregation of client assets and greater remoteness from bankruptcy through qualified custodian or trust account usage to shield customer tokens in circumstances of provider failure. It is important to acknowledge that despite *Finternet's* inherent flexibility, certain cases will necessitate third-party custody despite. Institutional investors and fiduciaries are often legally required to use regulated custodians.[1] Similarly, large-scale capital flows and tokenized securities settlements may demand intermediary custody to provide settlement finality, compliance monitoring, and legal accountability in case of disputes or insolvency. As such, viable policy framework must accommodate both models, recognizing self-custody as a legitimate choice for retail users while mandating third-party custody for situations of high risk or public interest (pension funds, collective investment schemes, etc.).

4. Flow-Based Regulation of Digital Asset Transactions: We suggest that regulators focus on regulating the movement and usage of digital assets (the "flows") rather than solely the containers or wallets that hold them. Focus on how a token moves through the system, who the counterparties are, whether transaction types (public offering, a private transfer, a payment, a derivatives trade) should trigger

[1] For example, the Security and Exchange Commission's ("SEC") proposed rule would require investment advisers to custody crypto with qualified custodians

contingent requirements. Embedding compliance into transaction protocols and token standards make oversight more effective and automated. For instance, permissioned token standards (such as Ethereum's ERC-3643 for regulated

tokens) allow transfer rules to be encoded directly into smart contracts, such that only eligible, KYC-verified parties can transact. KYC can be achieved with regulator agnostic, user based tokenized identity usable across transactions and token types – setting higher standards for approved tokenized identity. This *flow-centric* approach mirrors traditional securities regulation precedence on monitoring trading activity and money flows. For example, the U.S. Bank Secrecy Act's "Travel Rule" attaches information to fund transfers above specific thresholds.[2] From tokenized securities that only trade among whitelisted investors, to stablecoins that carry identity attestations, to DeFi protocols with built-in controls, several examples exist where programmable compliance logic in tokens can enforce regulations in real-time. *Flow-based* regulation, enabled by *Finternet*'s smart technology, results in more targeted and dynamic policy goals of preventing illicit finance and enhancing investor protection than asset-classification. We recommend policymakers reframe legislative mandates to recognize "regulated digital tokens" with embedded compliance and permit activity-based oversight that travels with the asset across platforms. A regulated digital token is defined as is a digitally represented unit of value or rights that operates on a distributed ledger or blockchain and is subject to oversight by a financial regulatory authority under applicable laws. The classification of a token as "regulated" depends on its function, legal characterization, and associated risks, rather than its technological features alone.[3] Regulatory oversight includes, but is not limited to issuance, custody, trading, marketing, disclosure, capital

[2] The *BSA Travel Rule* is a regulatory requirement under the U.S. Bank Secrecy Act (BSA) that mandates certain financial institutions to transmit specific information about fund transfers along with the payment itself. Specifically, when a funds transfer (domestic or international) exceeds $3,000, financial institutions must include and retain originator and beneficiary information. *See* Federal Code of Regulations, 31 CFR § 1010.410(f).

[3] U.S. Securities and Exchange Commission (SEC) (2019). *Framework for "Investment Contract" Analysis of Digital Assets* – applies securities law to certain digital tokens. Available at: https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets

requirements, consumer protection and anti-money laundering (AML) compliance.

To implement these ideas, this paper suggests a phased pathway to addressing key challenges through a four part framework. It remains our belief that standard setting should emerge through market-driven collaboration on (a) identity

credentials, (b) open interoperability standards for token transfers and (c) compliance data exchange. Regulators should coordinate globally to harmonize baseline principles and taxonomy. In the U.S., a unified legislative approach clarifying digital asset definitions and regulating core functions (issuance, custody, exchange, payments) on a *functional flow* basis would fill current gaps. Sandbox programs and pilot projects[4] through the *Finternet* architecture could allow controlled content testing. Further, below we outline the four-part framework for challenge resolution:

1. Technical Standards for a Finternet Architecture: We outline foundational technical standards for *Finternet* — a unified, secure digital asset infrastructure designed to support interoperability, safety, and scalability.
2. Comparative Regulatory Best Practices: Next, we examine global regulatory models across the U.S., EU, and Singapore to extract cross-jurisdictional principles that can inform harmonized policymaking.
3. Custody Models and Risk Mitigation: We then analyze custody structures, outlining how the Finternet can support both custodial and self-custody models, while embedding safeguards to manage operational and regulatory risks.
4. The Case for Flow-Based Regulation: Finally, we advocate for a shift from static, asset container-based regulation to dynamic, transaction flow-based approaches. We demonstrate how programmable compliance mechanisms can meet regulatory frameworks and objectives more effectively.

[4] Such as a cross-border pilot between jurisdictions to transact tokenized assets under shared rules.

Throughout, we integrate comparative insights such as MiCA's approach to token issuance and MAS's sandbox experiments to illustrate how our proposals align with emerging global standards and offer practical pathways toward implementation.

A. Introduction

The rise of digital assets and distributed ledgers has prompted a re-imagination of financial infrastructure. Today, the digital asset ecosystem is at an inflection point: technological innovation is outpacing regulatory frameworks, and markets remain fragmented into "walled gardens" of blockchain networks, exchanges, and token standards. *Finternet* – a financial internet, is a response to these challenges, proposing *a unified architecture for digital assets* analogous to how the Internet unified information networks. *Finternet* envisions open protocols and common standards that enable any asset to transact across platforms, coupled with supportive regulatory environments that transcend jurisdictional silos. This paper lays out a blueprint for realizing that vision, with a focus on the United States and comparative insights from the European Union and Singapore.

B. Key Challenges in the Ecosystem

Several challenges motivate the need for Finternet-based approaches:

1. Interoperability and Fragmentation: Most digital asset systems do not natively interoperate. A token issued on one blockchain cannot easily move to another; a user's identity or credentials are not portable across services. This is akin to the pre-internet era of isolated networks. The lack of baseline technical standards hinders efficiency and innovation. For instance, liquidity is fragmented across multiple exchanges and chains, and compliance checks must be repeated in each silo. There is a clear need for *common standards that enable interoperability* of ledgers and wallets, much as TCP/IP enabled different networks to communicate.

2. Regulatory Uncertainty and Inconsistency: In the U.S., despite recent progress on legislative actions, digital assets face regulatory uncertainty. Regulators apply decades-old statutes designed for traditional finance instruments (like securities, commodities, etc.) and not for crypto. Whether a token is deemed a security (and thus regulated by the SEC) often hinges on nuanced interpretations of the

   Howey investment contract test, leading to inconsistent outcomes.[5] Meanwhile, activities that fall outside those definitions may evade clear oversight or fall into gaps. Other jurisdictions, like the EU and Singapore, have moved toward bespoke regimes (e.g. MiCA in Europe) or adaptive measures under existing law (Singapore's Payment Services Act and sandbox), creating a patchwork of rules globally. This fragmentation can lead to *regulatory arbitrage*, compliance burdens for cross-border activity, and difficulty in coordinating enforcement against illicit uses. A set of global best-practice principles and greater harmonization is needed to guide national regulatory strategies.

3. User Risks in Custody and Access: Digital assets represent a fundamental shift in financial autonomy by enabling individuals to exercise direct ownership and control over their assets through self-custody mechanisms. This model aligns with principles of financial self-empowerment but simultaneously introduces novel risks, including the potential for irreversible loss of assets due to mismanagement of private keys, susceptibility to cybersecurity breaches, and the absence of established avenues for redress. Conversely, the delegation of asset custody to centralized intermediaries such as cryptocurrency exchanges and other custodians mitigates some operational risks but exposes users to counterparty risk, as evidenced by numerous high-profile institutional failures resulting in significant customer losses. A balanced regulatory framework must

[5] The *Howey Test*, is a legal standard established by the US Supreme Court n *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946), used to determine whether a particular arrangement constitutes an "investment contract"—and therefore a security—under U.S. federal securities law. According to the Howey Test, a transaction is deemed an investment contract if the following are involved: (i) an investment of money (ii) in a common enterprise (iii) with an expectation of profits (iv) solely from the efforts of others. Note that this test is function based and technology neutral which means it applies to both traditional securities or a digital asset token. U.S. Supreme Court. (1946). *SEC v. W.J. Howey Co.*, 328 U.S. 293. Available at: https://supreme.justia.com/cases/federal/us/328/293/

therefore aim to protect users in both self-custody and third-party custody arrangements, without implicitly endorsing any particular technological model. This dual mandate requires the development of safeguards that uphold asset security and operational integrity across custody modalities, while simultaneously advancing policy objectives such as financial inclusion and user-centric access to digital asset markets. Achieving this balance between security, accessibility, and technological neutrality constitutes a material challenge for contemporary digital asset regulation.

4. Compliance and Illicit Finance: Policymakers have expressed sustained concerns that digital assets, if left inadequately regulated, could facilitate illicit financial activities like money laundering, sanctions evasion, and fraud. Conventional regulatory frameworks predominantly target centralized intermediaries (like custodial digital asset exchanges) by imposing obligations related to customer due diligence (Know your customer or KYC procedures), anti-money laundering (AML) compliance, and sanctions screening. Additionally, these frameworks often rely on the classification of certain digital tokens as regulated financial instruments to establish jurisdictional oversight. However, the emergence of decentralized networks and peer-to-peer (P2P) protocols fundamentally challenges these paradigms by enabling asset transfers independent of traditional intermediaries, thereby circumventing established regulatory checkpoints. This evolution raises a critical policy question: how can regulatory objectives be effectively enforced within decentralized systems, particularly "on-chain," at the level of transactions, protocols, or smart contracts? The answer lies in emerging concepts such as *flow-based* regulation that purport to embed compliance mechanisms directly into the transactional architecture of digital assets, shifting regulatory focus from static classification of assets to dynamic oversight of asset flows. However, implementing such frameworks, poses complex challenges in balancing regulatory effectiveness with the imperative to preserve technological innovation and the open-source ethos of decentralized finance. Addressing this tension is a central task for the next generation of digital asset regulation and supervisory technology.

C. Technical Standards for Finternet – An Open, Interoperable Digital Asset Network

A foundational step toward a *Finternet* is defining baseline technical standards that enable interoperability and programmability of digital assets across platforms and

jurisdictions. These standards are conceived to be agnostic to an asset's legal classification or type, i.e. the network would not hard-code whether a token is a security, commodity, currency, or utility token. Instead, it's aim is to provide a flexible infrastructure where any of these assets can operate with appropriate rules layered on top. The key components of such a technical architecture are outlined below, drawing from the *Finternet* vision papers and industry developments.

1. Unified Ledgers and Common Protocols: The core concept introduced by Carstens & Nilekani in 2024[6] is the idea of a *unified ledger*, a shared, programmable infrastructure that can host numerous asset types and execute transactions among them. Importantly, a unified ledger is not necessarily a single global monolithic ledger, but rather where multiple unified ledgers could exist for different jurisdictions or use cases, but each possess common interfaces that allow inter-ledger connectivity. To enable this, a *Unified Interledger Protocol (UILP)* has been proposed as a suite of open messaging standards for transactions. The UILP defines how different participants like communicate to achieve a transaction that spans networks. This is analogous to how the Internet's TCP/IP allows different networks to route packets to each other.

   Under the UILP, when a token transfer or trade is initiated between two ledgers, a series of steps ensures both sides agree on the transaction details, verify each other's identity and permissions, and achieve atomic finalization (so that either both ledgers update or none do). A central feature is the use of "proof chains", cryptographic evidence chains that carry all relevant information about a transaction across ledgers. These proof chains link the token's data, any credentials or attestations (for identity, compliance, etc.), and the transaction

[6] Carstens, A., & Nilekani, N. (2024). *Finternet: The financial system for the future* (BIS Working Paper No. 1178). Bank for International Settlements. Available at: https://www.bis.org/publ/work1178.pdf

metadata into a signed package. Because the proof chain is transferable and verifiable by the receiving party, it creates an *immutable audit trail* of the transaction's flow. This has a number of important implications for regulatory compliance; it could include a certificate with the sender's and receiver's verified identities and risk scores fulfilling automated travel rule requirements for cross-border payments. The receiving institution could locally verify upstream completion of required AML/KYC checks without needing to trust an

intermediary. This is a significant transaction flow standardization process, allowing every transfer to carry both the asset and pertinent compliance and context data enabling regulation through protocol.

2. Token Managers and Asset Abstraction: In a *Finternet* architecture, token managers are entities or smart contracts that administer specific tokens (or sets of tokens). They issue and redeem tokens, enforce the rules attached to those tokens, and interface with the unified ledger. A key design principle is that token managers can operate their own internal ledgers (on a private blockchain, database, or a sub-ledger) yet remain interoperable with the broader network via UILP. This allows, for instance, a regulated financial institution to maintain its own ledger of tokenized assets (for privacy or performance) while still participating in the open network. The unified ledger does not replace all ledgers, but rather synchronizes them. Further, *Finternet's* design permits users to act as their own token manager for assets they create and hold, empowering self-custody and innovation, but with action limitations to prevent abuse; for instance, users can issue tokens *for themselves* but not for others, unless they become an authorized token manager. This ensures no rogue actor can create counterfeit tokens on behalf of someone else.

   The role of token managers is closely tied to ensuring compliance and integrity. They implement controls such as token creation permissions, supply management, and embedding of required credentials. A token manager for a stablecoin might enforce that each token has an associated attestation of reserve (from a bank or auditor), while a token manager for securities could require that any transfer includes an accreditation check for investor eligibility. In the *Finternet*

ecosystem, token managers are complemented by registrars and other trust service providers who help secure the system by offering identity verification, escrow (locker) services, or recovery mechanisms for lost keys. Under agreed upon terms or contingencies, these registrars might maintain a registry of legitimate token issuers or provide emergency rollback of transactions in case of proven fraud. These building blocks create a flexible infrastructure where *different asset types (and regulatory requirements) can be accommodated without changing the underlying transaction protocol*. Whether a token represents a user-created loyalty point or a strictly regulated stock, the same UILP handshake and proof chain concepts apply; the difference lies in what the token manager and credentials demand for a valid transaction.

3. Verifiable and Portable Credentials: User Identity and credentials are crucial to any regulated financial system. To address the dynamic nature of proposed asset transaction system, Finternet envisions portable digital credentials and attestations that a user or entity can carry across the network rather than relying on static account identifiers tied to one platform. These could include government-issued IDs, KYC verifications, credit scores, professional certifications, or any attribute relevant to transactions. Using standards akin to W3C Verifiable Credentials, these credentials are digitally signed by trusted issuers and can be shared peer-to-peer. For example, before engaging in a large-value trade, a user could present a verifiable credential proving they are an accredited investor or not sanctioned entity. Finternet would incorporate this by allowing credentials to attach to transactions (as part of the proof chain or alongside it) while also preserving privacy.

   A critical aspect is the *portability across ledgers* – i.e. credential issued in one context recognized in another, just as a passport from one country is accepted at foreign borders. Open standards ensure that, for instance, a digital ID issued by Singapore's national ID system could be used to satisfy a U.S. exchange's customer verification, if both adhere to prior agreed common international standards. Moreover, credentials could either be *dynamic or static*; some (like a business license status) may need to be updated periodically or revoked for cause , while others (like a birthdate or biometric) are permanent. Credential

status are intended to be verified via the *Finternet's* technical architecture during a transaction (e.g. querying an issuer's registry). The concept of a proof chain is particularly valuable here: each transaction can include hashed references to credentials, enabling the receiving party to verify that required credentials were presented and valid at the time of execution. By standardizing credential formats and exchange protocols, we can move from fragmented, siloed KYC processes to a "write once, use anywhere" model of identity, laying the groundwork for more efficient, interoperable financial systems.

4. Standardizing Transaction Flows vs Asset Containers: Traditional approaches to token standardization have focused on the token as a *container*. For example, the ERC-20 standard defines how a token contract keeps track of balances and transfers, or ERC-721 defines NFTs. *Finternet's* approach focuses on *flows*: the sequence of actions and messages that constitute a financial transaction (*transaction initiation ⊠ required checks or escrow steps ⊠ to completion and settlement*). By standardizing flows, interoperability can be achieved even if the underlying tokens have different rules or run on different technologies. In practice, this would require defining *common transaction types and stages*. For instance, a token transfer might universally involve: (1) a discovery phase (find recipient and exchange capabilities), (2) a negotiation phase (check rules, reserve funds), (3) an execution phase (transfer token and update ledger), and (4) a finalization phase (both parties log the outcome). Conceivably, should all systems adhere to this standardized flow, a token on a U.S. bank's ledger could be sent to a wallet on a European blockchain seamlessly with each party's full awareness of the process standards, even though the internal ledger mechanics may differ between counterparties.

   This flow-oriented standardization acknowledges that while financial workflows can vary widely (payments vs. trades vs. lending etc.), they can be built from a common set of *primitive actions*.[7] Ultimately, most complex workflows (For example, a decentralized exchange trade or a coupon payment on a bond) can be segmented down to these primitives, executable in a specific sequence to

[7] The *Finternet* architecture defines primitives like "Create," "Read," "Update," "Transfer" for assets, as well as the roles of actors ("Holder," "Issuer," "Guarantor," etc.).

achieve desired outcomes. This is analogous to how internet data can be broken into packets regardless of content. By standardizing primitives and message formats, regulators and industry bodies can ensure the application of *standard compliance checks and records across platforms*.[8] A *Finternet* transaction flow standard would similarly define how a token transfer is represented (perhaps in a JSON or similar message including sender, receiver, asset ID, credential proofs,

etc.), enabling a global "financial packet" format for token movements.

5. Enabling Programmability and Composability: A benefit of unified standards is greater *composability*, the ability to combine financial actions and assets like Lego bricks to create new products and services. On a unified ledger with common standards, one could orchestrate multi-step transactions that currently require separate systems. For example, at present, a token swap with delivery-vs-payment that might involve two exchanges and a clearinghouse could become a single flow: trade asset A for asset B and ensure payment is simultaneous. In a *Finternet* world, a smart contract or protocol would coordinate the exchange in one unified process (atomic swap). Similarly, ease of cross-asset conditional transactions could be enhanced by the following programmed transaction contingency: *If stock index > X by expiry, automatically sell tokenized bond and purchase stablecoins*.[9]

   These arrangements rely on underlying interoperability and programmability, both of which are enabled by the proposed standards through the removal of existing barriers between disparate distributed ledger technologies (DLTs) and legacy financial systems
   The end result is an infrastructure that can support a richer, more complex set of financial services (not feasible today) within a framework of *embedded oversight* (given the flows are designed to carry their proofs and comply with the

[8] A real-world parallel is the ISO 20022 messaging standard for payments which defines common data fields and process steps for payments globally, allowing banks and payment companies to interoperate.
[9] Should all assets reside or interface on the unified network, the code would execute directly.

global protocols). The technical architecture of the *Finternet* provides the *substrate upon which sensible regulation can be built*. Establishing clear standards for ledgers (unified but not monolithic), identity (portable credentials), and transaction flows (UILP and proof chains) creates a level playing field. Innovation accelerates because entrepreneurs can build new services that plug into a shared network without having to reconstruct compliance and interoperability layers from scratch. At the same time, regulators benefit from enhanced visibility and control at the transaction flow level—surpassing the fragmented oversight of the current system.

D. Global Regulatory Best Practices & Jurisdictional Comparative Frameworks

The regulation of digital assets necessitates a careful balance between fostering innovation and ensuring robust consumer protection, a complex task that jurisdictions have addressed through varied regulatory approaches. Despite these differences, certain common themes and emerging best practices can be observed across regulatory regimes. In this section, we delineate a set of universal regulatory principles that may serve as foundational pillars for effective oversight of digital asset ecosystems. Specifically, we undertake a comparative analysis of the United States' regulatory approach, the European Union's Markets in Crypto-Assets ("MiCA") regulation, and the Monetary Authority of Singapore's ("MAS") framework. Our analysis focuses on four key dimensions: user-centric design, flow-based regulatory mechanisms, principles-based accountability, and risk-proportional tailoring of rules. We examine how these principles are operationalized (or in some cases insufficiently addressed) within the policy architectures of these leading jurisdictions.

1. User-Centric Design: A *user-centric* regulatory approach means crafting rules and systems that prioritize the needs, rights, and safety of the end-users (consumers). Key to this structure are principles of *transparency, access, and redress*. Users should receive clear information about digital asset products (e.g. fees, risks, rights), have fair access to services, and be protected against fraud or

loss. It also means reducing unnecessary friction, making compliance largely invisible to the user experience whenever possible (e.g. using digital IDs to avoid repetitive paperwork). In the *Finternet* context, user-centric design aligns with "privacy by design and compliance by design." Instead of burdening users with complex steps to meet regulatory requirements, the system bakes those into the background. For example, using portable credentials approach, a user could complete one robust KYC process and then seamlessly meet that requirement on any platform thereafter, making for a frictionless compliance feel. Another aspect

is *inclusion*: regulators and architects should ensure the digital asset ecosystem is accessible (e.g. low-cost accounts, mobile-friendly interfaces etc.). The BIS has noted that fast payment systems like India's UPI[10] or Brazil's Pix[11] succeeded through a *user-centric, inclusive design* that brought millions into the digital economy. A global best practice would be to extend similar principles to crypto and tokenization.

2. Flow-Based Regulation: *Flow-based* regulation refers to focusing oversight on the *activities and transactions* occurring, rather than on static classification of an asset or on siloed entities. This functional approach to regulation is gaining

[10] India's *Unified Payments Interface (UPI)* is a notable example of a state-supported, interoperable, and real-time retail payment system that has transformed the country's digital payment landscape. Launched in 2016 by the National Payments Corporation of India (NPCI), UPI enables instantaneous peer-to-peer (P2P) and person-to-merchant (P2M) payments through mobile devices, integrating multiple bank accounts into a single mobile application. UPI's design emphasizes interoperability, allowing seamless transactions across different banks and payment service providers without the need for proprietary platforms. Its open API architecture, coupled with zero-merchant discount rates (MDR) for small transactions, has contributed to rapid adoption, financial inclusion, and the formalization of the economy, particularly among underbanked populations. Bharadwaj, P. (2023). Digital public infrastructure and financial inclusion: Lessons from India's UPI. *Journal of Payments Strategy & Systems*, 17(1), 35–47.

[11] Brazil's *Pix* system, launched in 2020 by the Banco Central do Brasil, is a real-time payment system within a public digital infrastructure model. Pix enables instant, 24/7 payment transfers between individuals, businesses, and government entities, offering low-cost, interoperable, and immediate settlement via mobile phones, QR codes, or social identification keys (e.g., email, phone number). Developed and operated by the central bank, Pix aims to promote financial inclusion, reduce reliance on cash, and lowers entry barriers for fintech and payment service providers. Duarte, M., Martins, M., & Rocha, F. (2023). Instant payment systems and financial inclusion: Evidence from Brazil's Pix. *Journal of Financial Market Infrastructures*, 11(1), 1–26.

prominence as policymakers increasingly recognize that similar risks should be subject to equivalent regulatory treatment, irrespective of the underlying technological form. For instance, an unbacked crypto token that exhibits the economic characteristics of a speculative investment may warrant regulatory interventions analogous to those applied to securities or gambling products, particularly with respect to consumer disclosures and risk warnings, not because the token is formally designated as a security, but due to its *comparable financial flows and risk profile* to consumers. Contemporary regulatory frameworks increasingly advocate for classifying digital assets based on their functional use (payment tokens, stablecoins, utility tokens etc.) with corresponding regulatory obligations calibrated to each category. In parallel, these frameworks often define and regulate crypto-asset services (e.g., trading, custody, exchange operations)

as distinct licensable activities, regardless of the specific tokens involved. This represents an *activity-centric regulatory model*, contrasting with regimes that rely predominantly on asset classification to determine regulatory scope. Furthermore, a risk-based threshold can be employed to exempt certain limited-purpose tokens such as closed-loop loyalty points or in-game tokens for example, from burdensome regulation, recognizing that tokens which are neither freely tradable nor widely utilized pose minimal systemic or consumer risk.

Flow-based regulation is particularly salient in the context of anti-money laundering and countering the financing of terrorism (AML/CFT) enforcement. Internationally, the Financial Action Task Force ("FATF") has established global standards (most notably the "travel rule")[12] which mandate that identifying information on the payer and payee must accompany fund transfers exceeding specified thresholds. This framework does not categorically prohibit anonymous

[12] The FATF Travel Rule refers to a global anti-money laundering (AML) and countering the financing of terrorism (CFT) standard established by the Financial Action Task Force (FATF), formally known as *Recommendation 16*. The rule requires that financial institutions (including Virtual Asset Service Providers (VASPs)) transmit specific identifying information about the originator (payer) and beneficiary (payee) when transferring funds or digital assets above a certain threshold. Financial Action Task Force (FATF). (2019). *Guidance for a risk-based approach to virtual assets and virtual asset service providers*. Paris: FATF/OECD. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/RBA-VA-VASPs.pdf

crypto transactions but requires traceability once value moves beyond certain limits, particularly when intermediaries are involved. A regulatory best practice involves embedding such flow requirements directly into the technical architecture of digital asset systems, for example, through the use of on-chain mechanisms such as "proof chains" that integrate travel rule compliance data.

The principal advantage of flow-based regulation lies in its *precision and adaptability*. Rather than applying blanket classifications where all tokens of a certain type are subjected to uniform regulatory treatment regardless of context, flow-based approaches enable regulators to *tailor* oversight to the specific use case and transaction type. For example, low-value peer-to-peer transfers could be subject to minimal regulation, akin to cash transactions, whereas high-risk flows, such as large-scale corporate fundraising events (e.g., initial coin offerings or ICOs), could trigger heightened disclosure and anti-fraud obligations irrespective of the token's nominal classification. This perspective also supports a

more nuanced approach to the lifecycle of digital assets, recognizing that a token may initially constitute a security during its fundraising phase, but subsequently lose that designation as it becomes widely decentralized and used in secondary markets. Under this model, the regulatory focus is placed on the capital-raising activity (where investor protection concerns are most acute) without necessarily extending onerous requirements to all downstream transactions where risks may be materially different. Current regulatory frameworks may not be fully prepared to oversee the growing variety of digital asset transactions, but the rapid pace of innovation makes it essential for global regulators to anticipate and address these emerging oversight needs to ensure effective and balanced regulation.

3. Principles-Based Accountability vs. Rules-Based Prescription: An important dimension in regulatory design lies in the distinction between *principles-based* and *rules-based* approaches. *Principles-based* regulation establishes broad, outcome-oriented requirements, allowing firms flexibility in determining how best to achieve compliance. In contrast, *rules-based* regulation relies on prescriptive, detailed mandates specifying exact procedures or prohibitions. Within the context of digital assets, a principles-based accountability framework offers

distinct advantages, particularly given the rapid pace of technological evolution. Under such a regime, regulators would articulate fundamental principles, such as ensuring cusumer asset integrity, fair treatment, robust cybersecurity standards, and preventing illicit use of platforms, without prescribing rigid operational methods. Market participants would be obligated to implement effective controls and could be subject to supervisory audits or enforcement actions should they fail to meet these overarching principles. This flexible approach is particularly well-suited to the digital asset sector, where inflexible, rules-based regimes risk becoming outdated or inadvertently stifling innovation by prohibiting emerging models that may, in practice, deliver equivalent or superior consumer protection outcomes.

A widely utilized regulatory innovation tool is the *regulatory sandbox*, which provides a structured environment to test novel financial products, services, or business models under regulator oversight, with certain requirements temporarily

relaxed to encourage responsible experimentation.[13] Crucially, participation in such sandboxes does not constitute a wholesale exemption from regulation, but allows for selective waivers or modifications of prescriptive rules while preserving adherence to non-negotiable core regulatory principles. These principles typically include protection of sensitive customer information, proper segregation of client funds, maintenance of sound governance through fitness and propriety assessments of key personnel, and prevention of illicit activities such as fraud,

[13] *Regulatory sandboxes* have emerged as a widely adopted tool among financial regulators to foster responsible innovation and maintain supervisory oversight. One of the earliest examples is the UK's *Financial Conduct Authority (FCA)* sandbox, launched in 2016, which allows fintech firms to test products in a controlled environment with tailored regulatory relief. Similarly, the *Monetary Authority of Singapore (MAS)* operates both a standard and express sandbox, the latter providing expedited approvals for low-risk experiments, supporting developments in financial inclusion and cross-border payment solutions. In the Middle East, the *Abu Dhabi Global Market (ADGM)* established RegLab, targeting fintech and blockchain innovations, particularly in cross-border payments and Islamic finance. Australia's *Australian Securities and Investments Commission (ASIC)* also launched an enhanced sandbox in 2020, offering fintech startups a two-year testing window with exemptions from certain licensing requirements (ASIC, 2020). Finally, the *Central Bank of Bahrain (CBB)* operates a sandbox with a focus on digital assets, crypto exchanges, and open banking, which has facilitated the licensing of platforms such as *Rain*.

money laundering, or market abuse. Even where specific requirements (like minimum capital thresholds, disclosure formats, or operational licensing conditions) are adjusted or deferred, participants remain accountable for meeting these foundational safeguards.

Regulatory and supervisory bodies, including self-regulatory organizations (SROs), often complement sandbox regimes by developing technical standards, codes of conduct, and interpretative guidance that enable market participants to implement regulatory objectives with operational flexibility. This contributes to a more dynamic regulatory environment, facilitating *principles-based outcomes through rule-like mechanisms* that can evolve with technology advances. In jurisdictions where formal, sector-specific legislation for digital assets remains underdeveloped, supervisory authorities increasingly rely on broad statutory mandates, including general anti-fraud provisions, consumer protection laws, and financial market integrity statutes, to regulate digital asset activities on a case-by-case basis. This results in a de facto *principles-based regime*, where enforcement actions are grounded in overarching legal standards rather than detailed, asset-specific rules. Such approaches are evident in various jurisdictions where crypto-assets have not yet been comprehensively integrated into the

regulatory perimeter but are nonetheless subject to enforcement predicated on unfair practices, misrepresentation, and consumer harm prevention. While this approach can be instrumental in addressing regulatory gaps during periods of rapid market evolution, it also raises concerns regarding legal certainty, regulatory predictability, and the consistent application of supervisory oversight, all of which are critical factors for market stability and investor confidence.

Accountability constitutes a fundamental counterpart to principles-based regulation: the flexibility granted to firms is balanced by a heightened expectation of outcome-based compliance. This regulatory model necessitates that supervisory authorities possess robust tools for effective monitoring, auditing, and enforcement. The advent of transparent digital infrastructures, such as shared ledgers and immutable audit trails within initiatives like the *Finternet*, facilitates a paradigm shift from predominantly ex-ante rule-setting to more

dynamic, real-time supervisory practices. For example, regulators could integrate into the unified ledger infrastructure via supervisory nodes (permissioned access points that enable observation of on-chain activity) while maintaining appropriate privacy protections. This would allow regulators verification of ongoing compliance with key principles in practice, such as confirming that stablecoin issuers regularly update proof-of-reserves tokens or that transactions exceeding specified thresholds consistently include requisite identity verification markers. Globally, regulatory frameworks are increasingly converging towards ongoing, *data-driven supervision*, particularly for systemically significant token issuers and digital asset service providers. This evolution reflects a broader trend toward real-time, risk-sensitive oversight, rendered more feasible by the traceability and programmability of tokenized financial systems compared to traditional financial markets. The interplay between technological architecture and regulatory strategy thus emerges as a critical enabler of effective, adaptive supervision in digital asset ecosystems.

4. Risk-Based Regulation and Proportionality: Not all digital asset activities pose equal risk; as such, regulation should be *calibrated to the level of risk*. This concept is well accepted in AML (where higher-risk customers or transactions get enhanced scrutiny). It should also apply more broadly: for example, a small

   start-up project issuing a token to a handful of users might warrant lighter touch (perhaps just anti-fraud and basic disclosure), whereas a global stablecoin with millions of users must face strict operational and reserve requirements due to systemic risk. Whether it is a bank that is globally important or "significant" stablecoins (those reaching large scale of users or value), regulators can subject these entities to additional rules and oversight. This uses transaction flow volume as a *measure of risk* to scale regulation. In the U.S., risk-based adjustments have often been made through regulatory discretion or no-action letters. For instance, the SEC's 2020 no-action relief for broker-dealers dealing in digital securities had a series of conditions (to mitigate risk since the SEC was cautious), one of which was that the broker-dealer not mix traditional securities with crypto assets. In 2023, the SEC also proposed to broaden custody rules to all assets, but acknowledged given certain assets have different risk profiles, the Agency

needed public comments to tailor such rules. A more systematic risk-based framework in the U.S. would be beneficial. For example, regulators could categorize token projects by size and function: Tier 1 (experimental/small), Tier 2 (medium, some oversight), Tier 3 (large or critical, heavy oversight). Requirements like audits, capital, cybersecurity certifications, etc., could then scale up accordingly.

Not all digital asset activities present equivalent levels of risk, and as such, regulatory frameworks should be calibrated to reflect these differences in risk exposure. This *risk-proportional approach* is well established in anti-money laundering (AML) regulations, where transactions or customers assessed as higher risk are subject to enhanced due diligence. The same principle should be applied more broadly within digital asset regulations. For instance, a small-scale startup issuing a token to a limited user base may warrant a lighter regulatory touch, focused primarily on anti-fraud measures and basic disclosures while other more systemically significant actors (such as global stablecoin issuers) serving millions of users should be subject to stringent prudential requirements including robust operational safeguards, capital reserves, and liquidity management to mitigate systemic risk. This approach parallels existing regulatory models where risk tiering dictates oversight intensity. For example, the differentiated treatment of globally systemically important banks (G-SIBs). A similar tiered framework could be applied to "significant stablecoins" or high-volume digital asset platforms, using transaction flow volume, user base, and market impact as determinants of regulatory obligations. In the United States, risk-based calibration has often been operationalized through regulatory discretion or no-action relief mechanisms. For example, the SEC's 2020 no-action letter to broker-dealers dealing in digital asset securities mandated risk-mitigation contingencies including the segregation of digital asset activities from traditional securities. Similarly, the SEC's 2023 proposed amendments to custody rules acknowledged the need to differentiate based on asset class risk profiles and sought public comment to inform a tailored approach. A more systematic and transparent risk-tiering framework_would enhance regulatory *clarity* and *proportionality*. Such a framework could categorize digital asset projects into risk tiers—e.g., Tier 1 (experimental/small scale), Tier 2 (intermediate

oversight), and Tier 3 (systemically important or large-scale projects with heightened oversight requirements). Corresponding obligations, such as mandatory audits, capital buffers, cybersecurity certifications, and operational resilience standards, would be graduated in accordance with the tier classification. This approach would promote regulatory efficiency, support innovation at early stages, and ensure robust safeguards for projects with broader economic or systemic significance.

An additional dimension of risk-based regulatory design is the incorporation *sandbox frameworks and phased rollouts* that enable innovation to proceed within *predefined* risk-limiting parameters. Regulatory sandboxes allow firms to test novel products, services, or technologies with a restricted number of participants, transaction volumes, or over a limited timeframe, all under close supervisory oversight. This approach serves as a *risk containment mechanism*, mitigating the potential for broader market disruption or consumer harm during the experimentation phase. Sandboxing operates as a *proportionate regulatory concession*, acknowledging the lower systemic risk posed by small-scale, time-bound pilots, while facilitating real-world testing of emerging business models. Furthermore, phased rollouts where regulatory permissions or market access are expanded incrementally based on performance metrics, compliance standards, or risk assessments, allow for *adaptive supervision*. Such graduated

approaches ensure that regulatory burdens are commensurate with risk and scale in proportion with enhancements in complexity, market reach, or systemic importance. The *iterative learning process* generated through sandbox trials and phased expansions contributes to a feedback loop for regulatory refinement, whereby supervisors can also collect empirical data on operational risks, consumer behavior, and market impacts before finalizing comprehensive regulatory treatments. Sandboxing and phased rollouts also facilitate *regulatory harmonization* across jurisdictions by providing a structured pathway for *cross-border regulatory dialogues* and knowledge sharing. By generating data in controlled environments, regulators can better coordinate international

supervisory practices, align risk thresholds, and develop consistent compliance

benchmarks, especially critical in transnational digital asset markets. This risk-based, iterative model represents a pragmatic pathway to balance innovation enablement with regulatory prudence.

The table below summarizes key elements of the U.S., EU, and Singapore approaches in light of these principles:

[14]Aspect	United States (U.S.)	European Union (MiCA)	Singapore (MAS)
Regulatory Approach	Fragmented across agencies (SEC, CFTC, FinCEN, state regulators). Relies on existing laws: securities law (Howey test) for many token sales, commodities law for others, Bank Secrecy Act for AML. Lacks a unified crypto-specific statute, leading to regulation by enforcement and case-by-case interpretation.	Comprehensive single framework (MiCA) covering issuance of crypto-assets (except those already regulated as securities) and services (exchanges, custodians, etc.). Aims for uniform rules across all EU member states, reducing fragmentation.	Combination of *activity-based regulation* under various laws: Payment Services Act for digital payment tokens (mostly covering crypto exchanges, payments), Securities and Futures Act for tokenized securities, plus guidance and sandbox. MAS as sole regulator, providing clarity and agility.
User-Centric Measures	Investor protection mainly through securities law (disclosures for registered offerings, fraud enforcement for	Strong disclosure regime: mandatory *White Paper* for any public token offering with key info (protocol,	MAS emphasizes consumer education and risk warnings. Guidelines restrict mass marketing of crypto to retail. Upcoming rules

14

	all). If a token is not deemed a "security", users may have less formal protection beyond general anti-fraud provisions (FTC, state laws). Consumer financial protections (like FDIC insurance, etc.) generally do not cover crypto. Some officials advocate clearer disclosures even for non-securities.	project, rights, risks). Advertisements must be fair and not misleading. Custodians must segregate user assets and are liable for loss (except under force majeure). Users have the right of complaint and redress with service providers under MiCA rules. Overall, a protective stance.	(under consultation) propose retail customers pass a knowledge test and refrain from using credit for crypto trading to prevent over-leverage. Licensed firms must *segregate customer assets* and provide risk disclosures. Singapore also leverages its national e-ID (SingPass) to streamline secure onboarding (an example of user-centric infrastructure).
Principles vs. Rules	More rules-based – e.g. SEC and CFTC have detailed regs. for assets within domain (custody, exchange rules etc.). Grey areas create uncertainty rather than broad principles. Enforcement actions fill gaps (e.g. anti-fraud). Approach can feel punitive than advisory. Some movement seen toward principle-based thinking in guidance (e.g. OCC's letters on	Mix of rules & standards: MiCA has detailed provisions (e.g. stablecoin issuers must maintain 1:1 reserves, publish reserve reports, trading platforms must have market abuse monitoring, etc.), but also tasks European authorities to develop technical standards to allowing for principle-based adaptation over time. The EU codifies more detail in law than the U.S. or Singapore,	More principles-based and collaborative. MAS often issues broad guidelines and expects financial institutions to adhere to high-level outcomes (e.g. "ensure robust technology risk management"). Give firms implementation leeway. *Regulatory sandbox* explicitly allows specific rule waivers, trusting firms to manage risks under oversight. MAS's consistent stance is "same activity, same risk, same regulation," a

	stablecoin activities set broad risk management expectations).	providing certainty but less flexibility.	principle applies case-by-case.
Risk-Based Differentiation	Implicit and developing. Partial differentiation present, e.g. higher scrutiny for large ICOs vs small utility token projects (informally), special conditions for large stablecoins (PWG report recommended limiting stablecoin issuance to insured institutions for systemic risk reasons) but inconsistent execution. SEC's proposals to expand custody and trading rules to crypto signals intent to bring moderate-risk crypto activities under traditional safe frameworks (arguably treating all crypto as high-risk for now).	Explicit in MiCA: *Tiering of stablecoins* (significant tokens have higher oversight). Small offerings (<€1 million) exempt from full regulation. Also calibrates compliance requirements to service type (e.g. advisors vs trading venues). Outside MiCA, EU also launched a *DLT Pilot Regime* for market infrastructures to experiment under lighter rules for short term, exhibiting sandbox-like risk testing at market scale.	Very explicit: Payment Services Act with two license tiers (Standard vs Major Payment Institution) depending on transaction volumes with additional requirements for higher risk volumes. MAS can impose additional conditions on licensees with high risk profile. Sandbox approach risk-based (small scale tests). Has also shown willingness to ban or restrict clearly high-risk activities (e.g. MAS cracked down on retail crypto lending offerings after some global failures, viewing them as unsuitable for public).
International Alignment	U.S. isolated in approach, sticking largely to existing legal structure. Participates in global bodies (FATF, IOSCO) and has started	Trying to set global benchmark with MiCA. MiCA could serve as template for jurisdictional proliferation. Also aligns with global	Explicitly positions itself as hub with high standards. Often implements global guidelines early (FATF rules, IOSCO principles for digital assets) and

	bilateral dialogues (e.g. with EU on trade and tech which includes crypto regulatory discussions).	standards on AML (implementing FATF travel rule via Transfer of Funds Regulation in parallel). Regulators actively engaged in global fora to share model and best practices.	works with other regulators. Spearheaded the *Global Financial Innovation Network (GFIN)* which shares fintech regulatory lessons. Also collaborates through BIS Innovation Hub projects (Project Dunbar for multi-CBDC, etc.), indicating a commitment to interoperable solutions.

Global regulatory best practices are increasingly converging around activity-based (functional) regulation, technology-neutral definitions, strong consumer protections, and harmonized AML/CFT standards. We recommend that regulators adopt these core principles to promote consistent and effective oversight of digital assets. The *Finternet* model suggests going further by embedding compliance into technical infrastructure, such as proof chain protocols and programmable compliance tools. This approach would integrate key safeguards like travel rule enforcement and proof-of-reserves transparency directly into market systems, reducing regulatory arbitrage and enhancing cross-border regulatory alignment.

E. Self-Custody vs. Third-Party Custody in a Finternet Architecture

Currently, the central issue in crafting both regulatory policy and technology architecture within the digital asset sphere is contingent on digital asset private key ownership. A key strength of the *Finternet* model lies in its *architectural neutrality*, enabling the coexistence of self-custody and third-party custody arrangements within a unified network framework. Users retain the option to exercise autonomous control through self-custody or opt for delegated control via custodians or

exchanges, without compromising interoperability or access to market infrastructure. The regulatory challenge, therefore, is not to mandate one custody model over another, but to ensure that both options are safeguarded by appropriate operational standards, risk disclosures, and supervisory oversight.

This section of the paper examines how *Finternet* accommodates both custody models and proposes a framework of operational, disclosure, and technical safeguards tailored to each, while also identifying pertinent factors such as systemic risk, investor sophistication, or transaction scale where third-party custody may be advisable or required, notwithstanding self-custody availability.

1. Self-Custody in the Finternet: *Self-custody* is defined as direct control by individual or entity of asset private keys authorizing transactions. In *Finternet* terms, the user could be their own token holder and manager for assets they create. The unified ledger and protocols would treat a self-custody wallet like any other participant. For example, a user's *Finternet* wallet app might hold their identity credentials and keys locally, initiate UILP transactions, and interact with token managers directly via smart contracts or APIs. Self-custody offers several distinct benefits, particularly its alignment with the decentralization ethos of digital assets, enabling users to transact peer-to-peer without intermediaries, preserving autonomy and enhancing individual sovereignty over digital assets. From a security perspective, self-custody can reduce systemic vulnerabilities by eliminating centralized private key repositories often targeted as high-value attack vectors. Additionally, in jurisdictions characterized by institutional instability or low trust in financial intermediaries, self-custody provides a critical mechanism for individuals to maintain direct and uninhibited control over their assets.

   However, self-custody also imposes significant responsibility and risk on individual users. Security failures through loss of private keys, seed phrases, or social engineering attacks like phishing can lead to irreversible asset loss, as there is typically no institutional recourse mechanism. The *Finternet* framework seeks to mitigate these risks through the integration of technical safeguards

within its architectural design. One such mechanism involves introduction of registrars or recovery agents, which offer opt-in key recovery services. This model allows users to register their wallets with a registrar who, subject to pre-defined conditions (e.g., multi-factor authentication protocols, mandatory waiting periods, or identity adjudication processes) can assist in the secure restoration of access following key loss.

Furthermore, *Finternet's* unified identity layer ensures that *key loss does not equate to identity loss*. Users can leverage portable credentials, potentially linked to government issued identification or biometric data, to securely re-establish control via the issuance of a new cryptographic key upon successful verification and authorization through registrars. Regulatory frameworks can reinforce these mechanisms by establishing standards for emergency key recovery services, ensuring such systems are secure, transparent, and resistant to unauthorized access or abuse. Another foundational safeguard is the promotion of *multi-signature* (multisig) and *multi-party computation (MPC)* wallet architectures for self-custody. These approaches distribute control across multiple devices or trusted entities, reducing the risk associated with single-point key compromise. For example, a 2-of-3 multisig arrangement could allocate key shares between a user's personal device, a hardware backup, and a cloud-based recovery agent, ensuring continued access even if one component is compromised. *Finternet's* unified ledger architecture is designed to support such advanced account structures natively, aligning with emerging practices observed in leading blockchain protocols. Regulators can further strengthen these safeguards by recognizing multi-signature and MPC configurations as self-custody best practices, and by offering legal clarity and protection for such arrangements. For

instance, regulatory provisions could acknowledge that compromise of a single key does not constitute sufficient authorization for transactions, especially if tied to a digital notarization or verification process. This multi-layered approach, combining technical design, user choice, and regulatory endorsement, promotes a resilient and user-centric custody framework within digital asset ecosystems.

From a *disclosure and consumer education* perspective, it is essential that users opting for self-custody are adequately informed of the associated responsibilities and risks. We recommend that regulators, in collaboration with industry stakeholders, develop a standardized *Self-Custody Risk Disclosure Framework*, analogous to risk disclosures in securities and derivatives markets. Under this framework, wallet providers would be required to present clear and accessible disclosures outlining key risks, including the user's sole responsibility for safeguarding private keys, the irreversibility of transactions sent to incorrect addresses, and the critical importance of credential security. Such disclosures should also highlight best practice security measures, including the use of backup mechanisms, whitelisted addresses, and multi-factor authentication, thereby reinforcing prudent risk management among users. Enhanced transparency serves to clarify accountability boundaries, promoting informed decision-making and reducing consumer protection disputes. In certain jurisdictions, regulators may consider mandating explicit user acknowledgments, whereby individuals affirm their understanding of self-custody risks prior to proceeding. While the enforceability of such acknowledgments presents practical challenges, at a minimum, regulatory authorities should issue public consumer advisories to raise awareness of the unique risks and responsibilities inherent in self-custody arrangements.

A key innovation within the *Finternet* architecture is the application of flow-based compliance mechanisms, which allow certain automated supervisory controls to operate even in self-custody environments. Specifically, transactions originating from self-custodied addresses may be subject to protocol-level compliance triggers based on transaction characteristics, such as value thresholds or behavioral risk indicators. For example, a high-value transfer between self-custodied wallets could prompt automated requests for identity verification

or initiate a temporary transaction hold pending off-chain review if flagged as anomalous. This approach does not undermine the autonomy of self-custody, but ensures that transaction flows (regardless of custody model) are monitored in a proportionate and risk-sensitive manner.

In current practice, blockchain analytics providers already conduct post hoc surveillance of public networks to identify illicit activities. The *Finternet* model envisions integrating such monitoring natively into network protocols, with permissioned oversight nodes capable of verifying compliance *ex ante*. Using this model, proof chain architectures could enable enforcement nodes to detect when transactions lack required compliance data (like identity attestations) particularly for flows above defined regulatory thresholds. This design seeks to strike a balance, where legitimate self-custody users remain unaffected by surveillance of lawful activity, while illicit actors encounter built-in detection and friction mechanisms, even in decentralized transaction environments.

2. Third-Party Custody in the Finternet: *Third-party custody* refers to an intermediary (exchange, bank, custodian firm) holding assets on behalf of users. Within the *Finternet* architecture, custodial intermediaries (like token managers or wallet providers) are envisioned to serve as key *access points* for users who delegate control of their digital assets. These custodians may operate sub-ledgers or smart contract-based structures that aggregate individual customer balances while interfacing with the broader unified ledger on the client's behalf. Custody providers offer significant advantages in terms of user convenience including password recovery, technical support, and simplified user interfaces particularly valuable for non-technical or retail participants. For institutional investors, third-party custody is not merely a convenience but often a regulatory or fiduciary requirement. For example, under U.S. securities law, mutual funds are obligated to entrust assets to qualified custodians; this requirement extends to digital assets, necessitating the use of regulated custodial institutions such as banks or trust companies with explicit authorization to offer crypto custody services. In both retail and institutional contexts, the custodial layer within *Finternet* serves a critical functional and regulatory role, facilitating broader market participation while maintaining compliance with established financial norms.

Key measures outlining safeguards in this relationship structure include:

a. Asset Segregation: Custodians should maintain strict segregation of client assets—both from their own holdings and, ideally, from other clients' assets—to ensure that customer funds remain protected in the event of insolvency. This principle underpins regulatory frameworks in the U.S. (SEC Custody Rule), EU (MiFID safeguarding rules, likely informing MiCA), and Singapore (PSA requirements). In the crypto context, segregation can be achieved through individual on-chain wallets per client or off-chain accounting with regular on-chain reconciliation. The Finternet's unified ledger architecture can enhance transparency and auditability by enabling regulators to verify that the sum of client balances matches the custodian's master account, aligning with proof-of-reserves standards. Over time, the use of cryptographic proofs of reserves and liabilities may become a regulatory norm for digital asset custodians.

b. Qualified Custodian and Standards: Custody of large-scale digital assets should not be entrusted to unregulated entities. Most regulatory frameworks require custodians to be licensed and meet defined standards including capital adequacy, operational expertise, and insurance coverage. However, extending the existing "qualified custodian" designation to crypto has proven inadequate. Traditional custodians are designed for hard custody models, while digital asset custody presents unique, evolving technical risks. Banks and trust companies currently fill this role due to their fiduciary structures and ability to segregate assets and manage default risk. A more appropriate approach would establish a dedicated licensing or chartering regime for digital asset custodians (e.g., crypto trust charters), subject to regular regulatory examinations. These custodians should meet robust operational standards, including multi-layered cybersecurity (e.g., HSMs, MPC), strict internal controls (e.g., dual authorization, role separation), and continuity planning for 24/7 blockchain environments. While these requirements build on traditional custodial norms, they must be continuously updated in response to technological developments best achieved through market-informed rulemaking or self-regulatory organizations (SROs).

c. Disclosure and Client Agreements: A custodian should clearly disclose the terms under which it holds assets. This includes whether it can rehypothecate (lend out) the assets or not. In traditional markets, a custodian for securities generally cannot use the assets except as directed by client; some crypto exchanges have blurred this line (using customer crypto for lending or own trading, leading to trouble). Regulations should prohibit custodians from deploying customer assets for their own gain without consent. If allowed (like a yield program), it essentially becomes a brokerage or lending activity, which should trigger additional regulation. We recommend prohibiting crypto custodians from staking or lending out retail customers' coins to protect them, unless as part of a clearly disclosed program that the user opts into. Capturing consent should be ledger-based to ensure single window validations and disclosures. Additionally, any fees, insurance coverage, or loss-sharing arrangements should be transparent.

d. Situations for Mandatory Custody: Even though *Finternet* allows self-custody, there are scenarios where policy might justifiably require use of third-party custody. One such scenario is institutional participation where regulated funds, pensions, etc., will likely use custodians due to fiduciary duty standards. Regulators should maintain that expectation (indeed it is not just expectation, it is law in many cases). Another is when dealing with regulated token offerings or complex assets. For example, if a company does a security token offering, regulators might require that the tokens initially be issued to investor accounts at a regulated custodian (instead of directly to a personal wallet) to ensure proper KYC and lock-up periods, etc., are enforced by the custodian as an intermediary. Later the investors could withdraw to self-custody if allowed, but the initial distribution via custody can prevent mishaps (akin to how IPO shares go to brokerage accounts, not directly as paper stock certificates to individuals nowadays). Bankruptcy remoteness is so crucial that for certain stablecoins or asset-backed tokens, authorities might insist that a regulated trustee holds the collateral and possibly the minted tokens, rather than a pure code-based control by an operator. This happened in the case of some "stablecoin-like" arrangements: e.g. in some jurisdictions, e-money laws would require customer funds (backing a stablecoin) be held by a licensed institution.

e. Institutional Capital Flows: Large payments between companies or financial institutions, say a multimillion dollar cross-border payment using a wholesale CBDC or tokenized deposit, will likely occur *ledger-to-ledger*, i.e. between custodial accounts at two institutions, rather than between individual self-custodied wallets. The Finternet architecture explicitly envisions big players maintaining their own ledgers that sync to the unified ledger. Regulations might formalize this by saying *systemically important flows* (above X amount or involving critical financial market infrastructures) must occur through supervised institutions. This is similar to how today a $100 million transfer wouldn't be done via a physical cash handoff (self-custody equivalent) but through bank wires.

Both self-custody and third-party custody are foundational to the development of a resilient, inclusive, and user-centric digital asset ecosystem. The *Finternet* architecture is purposefully designed to support both models within a unified and interoperable infrastructure, recognizing that varying user profiles and institutional roles require different custody solutions. A *balanced regulatory approach* is recommended to uphold user choice while implementing safeguards that include: (a) standardized risk disclosures for self-custody users (e.g., "Self-Custody Risk Statements" akin to MiFID II risk profiles) (b) conditional compliance mechanisms (e.g., FATF travel rule thresholds triggering KYC verification) (c) secure key recovery protocols (e.g., opt-in registrars or social recovery services) and (d) robust operational standards for third-party custodians, including asset segregation, proof-of-reserves, and independent audits.

Beyond traditional models, emerging *hybrid custody* solutions offer a promising third path. These include multi-signature (multi-sig) and multi-party computation (MPC) arrangements that enable *shared control* between users and institutions while mitigating key loss and insider risk. Several regulators have adopted such approaches; for instance Wyoming's *Special Purpose Depository Institution (SPDI)* charter that supports digital assets custodial services while preserving legal clarity around bailment structures and asset segregation, thus enabling hybrid custody

under state banking law,[15] the Monetary Authority of Singapore's (MAS) *Guidelines on Risk Management Practices for Digital Token Custody Services*, emphasizing operational resilience and segregation of client assets, including support for technology-enabled controls such as dual approvals and MPC,[16] and EU's *Markets in Crypto-Assets Regulation* (*MiCA*) that includes provisions for CASPs offering custody to require organizational safeguards that could accommodate hybrid architectures, especially where third-party control is shared or delegated with user consent.[17]

Given these developments, policymakers should consider formally recognizing *hybrid custody models within regulatory frameworks* potentially through safe-harbor provisions or tiered compliance obligations based on technological safeguards and operational resilience. This would encourage innovation in custody while maintaining a principles-based supervisory approach aligned with financial stability and consumer protection goals.

F. Embracing Flow-Based Regulation: Regulating Asset Movements and Transactions

Traditional financial regulation has historically focused on categorizing financial instruments (the "containers" of value) and licensing or supervising intermediaries such as banks, brokers, and exchanges. Conventional markets have long enjoyed the stable foundation this entity-product-centric regulatory approach has provided. However, the advent of tokenized assets and decentralized finance (DeFi) challenges these regulatory norms. In tokenized ecosystems, a digital token can represent virtually any asset class (currency, security, commodity, or utility) and peer-to-peer protocols can facilitate trading, lending, or payments without the need for formal

[15] Wyoming Division of Banking. (2020). *Special Purpose Depository Institutions Guidance*. Available at: https://wyomingbankingdivision.wyo.gov

[16] Monetary Authority of Singapore (MAS). (2022). *Guidelines on Risk Management Practices for Digital Token Custody Services*. Available at: https://www.mas.gov.sg

[17] European Union. (2023). *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA)*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114

intermediaries. In this evolving context, a more adaptable paradigm is *flow-based regulation*. Rather than focusing exclusively on the *nature* of the asset or the status of the actor, flow-based regulation targets the movement of assets and transactions themselves as the focus of oversight. This model enables regulators to impose controls based on the *risk characteristics* of a transaction (value thresholds, velocity, counterparties, or jurisdictional exposures) irrespective of whether the transaction involves a regulated intermediary. By shifting regulatory focus from *static classifications to dynamic flows*, this approach offers a promising framework for governing decentralized and tokenized financial systems without stifling innovation.

1. Container-Centric to Flow-Centric: Contemporary securities regulation offers a foundational insight for digital asset governance: regulation is typically triggered by transactional flow, not by mere possession. For example, while individuals may legally hold stock certificates, the trading, clearing, and custody of those securities is heavily regulated through licensed intermediaries, exchanges, and reporting obligations. Thus, the movement or change in ownership activates regulatory oversight, an approach deeply embedded in frameworks such as the U.S. Securities Exchange Act of 1934 and SEC Rule 17a-3 (recordkeeping and trade confirmation requirements).[18] In contrast, the crypto regulatory discourse has often focused on whether a token is a security, commodity, or utility, i.e. a *container-based model*. This approach, exemplified by the SEC's "investment contract" test under *SEC v. Howey Co*. (328 U.S. 293, 1946)[19] and later reinforced in the SEC's *Framework for Investment Contract Analysis of Digital Assets* (2019),[20] tends to focus on the nature of the token at issuance. However, this classification can be ambiguous, evolve over time, and is difficult to enforce uniformly across jurisdictions. On the other hand, a *flow-based regulatory model* emphasizes how a token is used or transacted, aligning regulation with economic substance and behavioral risk. Under this approach, (i) A token functioning like a

[18] U.S. Securities Exchange Act of 1934, 15 U.S.C. § 78a et seq. Available at: https://www.sec.gov/about/laws/sea34.pdf
[19] *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946). Available at: https://supreme.justia.com/cases/federal/us/328/293/
[20] U.S. Securities and Exchange Commission. (2019). *Framework for "Investment Contract" Analysis of Digital Assets*. Available at: https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets

deposit instrument (e.g., stablecoins used for value storage and redemption) may fall under e-money regulation, as reflected in MiCA Title III – E-Money Tokens (Regulation (EU) 2023/1114), which applies prudential and redemption requirements to such instruments (ii) Tokens facilitating investment-like flows, regardless of their label, may be treated as securities or derivatives, consistent with SEC interpretations and recent U.S. Congressional proposals (e.g., the Token Taxonomy Act). Moreover, the Financial Action Task Force (FATF) embraces a form of flow-based oversight in its Travel Rule (Recommendation 16), which requires originator and beneficiary information to accompany virtual asset transfers above thresholds, thus regulating transaction flows rather than static assets.[21]

To operationalize this model, the *Finternet* architecture proposes embedding regulatory metadata directly into digital tokens, assigning designations such as "EU-MiCA-EMT" or "US-144A-Equity" based on their legal classification and use. This would enable smart contracts or compliant nodes to dynamically enforce jurisdictional rules at the point of transaction, reducing the burden on centralized gatekeepers while maintaining regulatory integrity. Rather than attempting to ban or define non-conforming tokens ex ante, this approach accepts token existence but constrains their flow and interaction based on regulatory conditions. Such flow-based enforcement enables a more agile, risk-sensitive, and technologically harmonized model for digital asset regulation, particularly critical in a decentralized, cross-border environment.

2. Permissioned Token as Mechanisms for Flow-Based Regulation: One practical mechanism for implementing flow-based regulation in digital asset markets is the use of *permissioned tokens* defined as crypto-assets embedded with smart contract logic that enforces compliance rules at the point of transfer. These tokens are already operational in the blockchain ecosystem, particularly in regulated asset contexts such as security tokens and tokenized equities. For

[21] Financial Action Task Force (FATF). (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs*. Available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf

example, the ERC-3643 standard on Ethereum (formerly T-REX) provides a protocol framework allowing token issuers to embed transfer restrictions based on predefined compliance criteria.[22] The token contract typically references an off-chain identity registry, against which it checks each transfer request to ensure: (i) the sender and receiver are both authorized, (ii) the transaction complies with jurisdictional or investment limits (iii) off-chain KYC/AML conditions are met and (iv) neither party is subject to blacklisting or sanction. Only if all these conditions are satisfied will the transfer be executed on-chain, effectively embedding regulatory controls directly into the asset's flow logic. This replaces the need for traditional intermediaries (such as brokers or custodians) to enforce compliance manually, creating a self-regulating asset architecture.[23]

In the EU, the MiCA regulations, while technology-neutral, emphasizes obligations around investor protection, fair treatment, and market integrity. A permissioned token architecture could fulfill these obligations automatically, for example by preventing transfers to ineligible or unsophisticated investors.[24] EU regulators may consider providing formal guidance that smart contract-based controls constitute a valid compliance pathway under MiCA Articles 62–68. In the USA, while the SEC and FINRA have not mandated permissioned tokens, they have signaled openness to frameworks that reduce the risk of illicit transfers and improve oversight. For instance, ATS platforms may be eligible for regulatory relief if they exclusively list digital assets that enforce transfer restrictions compatible with securities laws.[25] Permissioned tokens can also support AML/CFT objectives

[22] ERC3643. (2023). *ERC-3643: Compliant Token Standard for Regulated Assets*. Available at: https://github.com/erc3643/standard

[23] OECD. (2022). *Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard*. Organization for Economic Co-operation and Development. https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework.htm

[24] European Union. (2023). *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA)*. Official Journal of the European Union.

[25] SEC & FINRA. (2020). *Joint Statement: Broker-Dealer Custody of Digital Asset Securities*. Available at: https://www.sec.gov/news/public-statement/joint-statement-broker-dealer-custody-digital-asset-securities

outlined in the *FATF Recommendation 15*, which encourages technical solutions for "Travel Rule" compliance.[26]

By embedding such functionality at the protocol level, permissioned tokens enable fine-grained compliance automation, support international regulatory convergence, and reduce the compliance burden on human intermediaries. As flow-based regulation gains traction, such mechanisms offer scalable, programmable tools for real-time enforcement and transaction-specific supervision.

3. Flow Monitoring and Automated Compliance: *Flow-based regulation* can be substantially advanced not only through permissioned token standards but also via network-layer enforcement mechanisms. A key architectural innovation in this space is the *Finternet's* "proof chain" model, wherein each digital asset transaction carries embedded compliance metadata (such as origin, destination, identity attestations, and risk flags) enabling programmable, real-time compliance checks. This architecture reflects a broader shift from entity-based or ex-post compliance to transaction-centric and in-protocol supervision.

   a. Network-Level Monitoring as Embedded Supervision: One of the most promising applications of such architecture is in the enforcement of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) standards. Under conventional AML regimes (such as the U.S. Bank Secrecy Act (BSA) and EU's AMLD5) intermediaries like banks or exchanges must monitor transactions and submit Suspicious Activity Reports (SARs) when anomalous patterns are detected.[27] However, in a decentralized digital asset ecosystem, these responsibilities are harder to assign due to the disintermediation of service layers. The *Finternet* model addresses this gap by enabling *network-wide pattern recognition*, whereby protocol-level monitors operated by regulated nodes or trusted enforcement agents can automatically

[26] FATF. (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Financial Action Task Force. Available at: https://www.fatf-gafi.org/
[27] FinCEN. (2022). *Suspicious Activity Report (SAR) Statistics*. U.S. Department of the Treasury. Available at: https://www.fincen.gov/reports/sar-stats

detect suspicious transaction patterns such as: (i) rapid, high-volume inflows from unrelated sources to a newly created address (ii) layered transactions involving privacy-enhanced tokens or mixing services and (iii) repeated structuring just below reporting thresholds. Such events could trigger automated alerts, route flows to supervisory sandboxes for review, or even delay settlement until further checks are completed, mirroring how traditional banks temporarily freeze atypical wire transfers pending internal investigations.[28] These mechanisms thus support real-time regulatory sandboxing within production systems, balancing innovation with financial integrity.

b. Smart Contracts as Compliance Gatekeepers: Smart contracts and decentralized algorithms can serve as on-chain compliance agents by implementing risk-based transaction screening, KYC-based access controls, and dynamic risk scoring. For instance, Contracts could encode transaction thresholds beyond which identity proofs must be attached, transfers involving jurisdictionally sensitive addresses could require off-chain approval from certified validators, AML flags could trigger "delay-and-report" modes, where settlement is temporarily withheld for human oversight or additional identity attestation. These programmatic actions align with FATF's guidance encouraging the adoption of technological solutions for AML/CFT compliance in virtual asset ecosystems, particularly for Travel Rule enforcement.[29]

c. IVMS 101 and the Travel Rule: Early Implementation Flow Metadata: A prominent early use case of flow-based compliance is the InterVASP Messaging Standard 101 (IVMS 101), which enables the exchange of standardized identity and transaction data for cross-border digital asset transfers. This standard was developed in response to *FATF Recommendation*

[28] Basel Committee on Banking Supervision (BCBS). (2019). *Sound management of risks related to money laundering and financing of terrorism*. Bank for International Settlements. Available at: https://www.bis.org/bcbs/publ/d505.pdf

[29] FATF. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

16, which mandates that virtual asset service providers (VASPs) transmit beneficiary and originator information with covered transactions.[30] In a tokenized ecosystem, IVMS 101–style data could be natively appended to each transfer in the proof chain, ensuring compliance in real time rather than requiring post–hoc forensic investigation. The standard is now referenced in the OECD's CARF regulations as part of its technical implementation guidance.[31]

d. Lessons from Traditional Finance: ISO 20022 and Programmable Messages: Traditional finance is also evolving toward enriched, structured data in payments. The adoption of ISO 20022 by SWIFT for wire messaging allows for the inclusion of detailed transaction metadata (e.g., remittance context, originator IDs, and purpose codes) to support enhanced compliance screening and automation.[32] However, while ISO 20022 relies on financial institutions to implement message–level checks, decentralized networks enable native enforcement at the transaction layer itself, potentially through "compliant routers" or "regulatory firewalls" that only allow tokens to pass through if requisite conditions (e.g., verified identity, geographic permissions, or risk flags) are met.

e. Regulated Wallets and Permissioned Pools: This architectural shift supports the emergence of compliance–aware digital wallets and permissioned DeFi pools, which only allow participation by users who have completed appropriate onboarding or credentialing. For example, a "regulated wallet" could be programmed to route transactions only through FATF–compliant VASPs, prevent transfers to blacklisted or non–whitelisted addresses and trigger compliance modules when threshold conditions are met. This aligns

[30] FATF. (2019). *Interpretive Note to Recommendation 16: Wire Transfers*. Financial Action Task Force. Available at: https://www.fatf-gafi.org/

[31] OECD. (2022). *Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard*. Organization for Economic Co–operation and Development. Available at: https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework.htm

[32] SWIFT. (2022). *ISO 20022 for dummies*. SWIFT & Wiley. Available at: https://www.swift.com/standards/iso-2022.

with MiCA's focus on risk-based oversight and technical neutrality (EU Reg. 2023),[33] and with U.S. proposals for real-time supervision of digital assets using technical means.[34]

4. Cross- Sector Examples:

   a. Securities and Asset Tokenization: A compelling illustration of flow-based regulation arises in the context of tokenized securities issued under legal exemptions. Consider a private company issuing digital shares as security tokens pursuant to Regulation D under the U.S. Securities Act of 1933, which limits initial sales to accredited investors and imposes restricted transfer periods.[35] Under a *flow-based* regulatory approach, the token's smart contract can be programmed to enforce compliance with these rules ex ante. For instance, only wallets associated with verifiable accredited investor credentials (potentially authenticated via an off-chain identity registry or Verifiable Credential framework) would be eligible to receive or hold the token. The smart contract can also implement *Rule 144 resale restrictions*, prohibiting any transfer within the statutory one-year lock-up period. Upon expiration of the holding period, transfer permissions could be dynamically updated to permit peer-to-peer transactions among accredited investors or to enable liquidity via an authorized secondary market platform. Attempts to transfer tokens in violation of these restrictions (e.g., to a non-accredited or non-whitelisted wallet) would result in a failed transaction at the protocol level, thereby embedding compliance into the asset's flow rather than relying on post-facto enforcement or static classification. Such mechanisms are not merely theoretical. Projects such as *Polymath's ST-20* token standard and *Securitize's DS Protocols* have piloted similar architectures, demonstrating the technical viability of automated securities law compliance through smart

[33] European Union. (2023). Regulation (EU) 2023/1114 of the European Parliament and of the Council on Markets in Crypto-Assets (MiCA). Official Journal of the European Union.
[34] FinCEN. (2022). Suspicious Activity Report (SAR) Statistics. U.S. Department of the Treasury. Available at5: https://www.fincen.gov/reports/sar-stats.
[35] U.S. Securities and Exchange Commission. (2023). Regulation D and Rule 144 Overview. Available at: https://www.sec.gov/smallbusiness/exemptofferings.

contract-enforced eligibility and transfer restrictions.[36] [37] These approaches effectively automate key provisions of U.S. securities law, including investor verification and limitations on resale, reducing legal and operational risk. For publicly traded securities, where exchanges enforce compliance through listing standards and broker-dealer rules, smart contract-based control can be lighter. However, tokenized equities could still include logic ensuring that all transfers are routed through designated broker-dealer or exchange addresses, thereby preventing off-market transactions and enhancing market integrity. This approach exemplifies the core principle of *flow-based regulation*: compliance is achieved not by rigidly classifying an asset as a "security" or "commodity," but by programming the conditions under which the asset can legally move. The regulatory status is thus contextually enforced through *dynamic, use-based constraints embedded at the transaction level* – an approach well-suited to tokenized and programmable financial markets.

b. Payment and Stablecoin Flows: Stablecoins are increasingly used in contexts such as retail payments, cross-border remittances, and on-chain financial services, raising regulatory concerns around anti-money laundering (AML), capital controls, and systemic risk. A flow-based regulatory framework offers a pragmatic alternative to rigid classification by focusing on how stablecoins are used, rather than solely on their issuer or intrinsic features. Under such a model, regulators could permit peer-to-peer (P2P) stablecoin transfers below a defined daily transaction threshold, analogous to cash-based exemptions in existing AML regimes, while requiring enhanced verification or routing for larger flows. Technically, this can be implemented by programming the stablecoin's smart contract to check a whitelist of verified addresses, allowing unrestricted transfers for fully KYC-compliant users, while limiting or flagging unverified addresses.[38] A related approach, already under discussion in regulatory circles, is the adoption of tiered wallet systems. For example, the

[36] Polymath. (2018). *ST-20 Security Token Standard*. Available at: https://github.com/PolymathNetwork/polymath-core.
[37] Securitize. (2021). *DS Protocol Overview*. Available at: https://securitize.io/resources.

[38] FATF. (2021). Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers. Available at: https://www.fatf-gafi.org/.

MAS in Singapore has proposed wallet tiers with graduated KYC requirements and transaction limits: (i) Tier 1 wallets may require minimal KYC and allow low transaction volumes (ii) Tier 2 wallets would require full identity verification and permit higher limits.[39] Such systems enable financial inclusion while maintaining oversight of large or risky flows. Rather than banning self-hosted or unhosted wallets, flow-based mechanisms can limit their use for high-value transfers, or require such flows to be routed through regulated intermediaries. Importantly, similar flow-based principles are already being integrated into the design of retail central bank digital currencies (CBDCs). Several central banks, including the European Central Bank and the Bank of Japan, have explored models in which CBDCs impose caps on wallet balances or transaction limits for users without enhanced verification.[40] These caps function as circuit breakers to mitigate systemic risk and ensure proportional compliance burdens. For privately issued stablecoins, such measures can be enforced through licensing conditions or regulatory approval processes. For example, regulators could mandate that any issuer seeking authorization must implement technical safeguards. These mechanisms would make compliance native to the digital infrastructure, reducing the need for post-facto enforcement.

c. Defi and Programmable Logic: DeFi protocols enable complex financial flows without centralized intermediaries. This architecture challenges traditional regulatory approaches as DeFi applications are often deployed by anonymous developers and operate autonomously via smart contracts. However, a *flow-based* regulatory framework offers an alternative model by targeting the behavior and conditions of transactions, rather than the formal status of the entity initiating them. One practical application of flow-based DeFi regulation is the use of programmable compliance checks at the smart contract level. For instance, liquidity pool contracts could be required (through regulatory mandates on deployers, voluntary industry standards, or protocol-level

[39] Monetary Authority of Singapore (MAS). (2021). *Consultation Paper on Proposed Payment Services Regulations*. Available at: https://www.mas.gov.sg/publications/consultations.
[40] Bank for International Settlements (BIS). (2023). *Options for access to and interoperability of CBDCs for cross-border payments*. Available at: https://www.bis.org/publ/othp59.htm.

governance) to accept deposits only from wallets bearing a verifiable "DeFi passport". Such credentials, issued under a unified digital identity framework, would attest to a user's non-sanctioned status and regulatory compliance posture. Projects such as *Polygon ID*, *KILT Protocol*, and *Quadrata* are actively developing credentialing mechanisms for DeFi that preserve user privacy while enabling trust-based interaction.[41] Within the *Finternet* architecture, DeFi credentials would be issued as part of a unified, permissioned identity system, allowing wallet-level attestations to be cryptographically verified before participating in sensitive flows such as liquidity provisioning or high-volume trades. Transactions lacking required credentials could be automatically rejected by the smart contract or routed to *compliance oracles* (independent validators that check on-chain or off-chain regulatory criteria) before authorizing execution. For DeFi protocols that remain non-compliant could adopt containment strategies, such as prohibiting regulated institutions from interacting with those contracts or denying licensing to front-end interfaces connected to non-compliant smart contracts. This "cordoning" approach mirrors established practices in securities markets, where unregistered alternative trading systems (ATSs) or non-transparent dark pools may be excluded from institutional access unless they implement requisite investor protections and reporting mechanisms. Embedding regulatory controls into DeFi workflows through credential-aware contracts, programmable safeguards, and interoperable compliance standards, flow-based regulation can extend supervisory reach into decentralized environments without compromising innovation or decentralization.

5. Advantages of Flow-Based Approach: Flow-based regulation presents a pragmatic and adaptive framework for overseeing digital assets by targeting high-risk activities rather than attempting to control asset issuance or maintain rigid classifications. Traditional regulatory strategies have struggled to keep pace with the proliferation of token types (utility tokens to DeFi governance tokens, NFTs, and newer constructs like NFT-Fi) resulting in a "whack-a-mole" problem

[41] Möser, M., Narayanan, A., & Vazquez, D. (2023). *Decentralized Identity in DeFi: Compliance and Privacy at Scale*. Journal of Financial Technology Regulation, 2(1), 45–67.

where definitional categories rapidly become outdated.[42] By contrast, *flow-based* approaches focus on how digital assets are used in practice. If a particular use case, such as a token facilitating capital raising or acting as a de facto deposit instrument mirrors existing regulated financial activities, regulators can apply analogous rules based on functional equivalence.[43] This method allows for differentiated treatment based on observed transactional behavior rather than static classification, enabling regulators to remain technology-neutral and resilient to innovation. Low-risk or experimental flows can be monitored and left unregulated until sufficient data warrants oversight, while high-risk flows can be constrained through pre-defined protocols. Importantly, this approach does not eliminate the need for institutional regulation. Rather, flow-based regulation functions as a complementary layer, embedding compliance into the infrastructure of the digital asset ecosystem. Within the *Finternet* architecture, regulatory requirements are enforced not only through legal obligations but also smart contracts that check credentials, enforce transfer restrictions, or embed AML rules directly into the asset flow. This "compliance by design" model can lower compliance burdens for regulated actors while increasing consistency and auditability. Technological tools to support this paradigm already exist, such as permissioned token standards (e.g., ERC-1404, ERC-3643) and decentralized identity protocols (e.g., Polygon ID, Verite, KILT Protocol). To enable broader adoption, policymakers should update legal frameworks to recognize technology-enabled compliance mechanisms. For example, a regulation might state that "if a digital asset enforces X condition via smart contract, that shall be deemed sufficient to satisfy Y legal requirement." Legal recognition of such mechanisms would accelerate industry uptake of programmable compliance, aligning regulatory goals with the capabilities of decentralized systems.[44]

---

[42] Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Föhr, L. (2020). *The Markets in Crypto-Assets Regulation (MiCA) and the EU Digital Finance Strategy*. University of Luxembourg Law Working Paper Series.

[43] International Organization of Securities Commissions (IOSCO). (2020). *Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms*. Available: https://www.iosco.org.

[44] Arner, D. W., Barberis, J., & Buckley, R. P. (2017). *Fintech and Regtech: Impact on Regulators and Banks*. Journal of Banking Regulation, 19(4), 1–14. Available at: https://doi.org/10.1057/s41261-017-0038-3.

6. Public Private Partnerships: To operationalize flow-based regulation in decentralized finance and tokenized markets, regulatory authorities must collaborate closely with technologists and industry stakeholders to define interoperable compliance rule-sets and technical standards. One promising model involves the development of *standardized regulatory APIs*, machine-readable interfaces that allow smart contracts to dynamically query real-time compliance conditions. For example, a smart contract might invoke an API provided by a regulatory body to determine whether a wallet address is permitted to receive a specific digital asset at a given moment, based on updated sanction lists, licensing status, or other eligibility criteria. This *modular and federated infrastructure* could centralize compliance logic while preserving decentralized asset custody. Rather than embedding static legal conditions directly into individual smart contracts (requiring manual upgrades with regulation changes) an off-chain compliance oracle or API service could serve as a single source of truth. This would enable regulators to update rules at the source while ensuring consistent application across the ecosystem.[45] Prototypes of such architectures are already being tested. For instance, the BIS Innovation Hub, in collaboration with MAS and financial institutions, has piloted *Project Guardian*, which includes the concept of a "trusted node" responsible for identity verification and access control within DeFi environments.[46] These trusted nodes operate as *compliance gateways*, validating credentials or eligibility before allowing transactions to proceed – akin to an implementation of permissioned flows within a decentralized architecture. Such a federated design could represent a reasonable middle ground between fully decentralized systems and traditional regulatory centralization. It allows compliance updates to be implemented rapidly and uniformly, reduces systemic upgrade burdens, and

[45] Allen, J. G. (2023). *Regulatory APIs and Machine-Readable Law: The Next Frontier in RegTech*. Oxford Journal of Legal Studies, 43(2), 215–240. Available at: https://doi.org/10.1093/ojls/gqad002; Walch, A. (2019). *Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems*. In Chris Brummer (Ed.), *Cryptoassets: Legal, Regulatory, and Monetary Perspectives* (pp. 39–68). Oxford University Press.

[46] Monetary Authority of Singapore (MAS) & Bank for International Settlements (BIS). (2023). *Project Guardian: Asset Tokenization and DeFi Pilots*. Available at: https://www.mas.gov.sg/news/media-releases/2023/project-guardian-expands-to-test-cross-border-foreign-exchange-settlement.

provides regulators with greater assurance of enforceability without sacrificing the core programmability and composability of blockchain systems. Going forward, the formal standardization of regulatory APIs and integration of machine-executable compliance logic may be crucial for scalable, interoperable, and legally sound *flow-based* regulation of digital assets.

Conclusion

Digital assets are reshaping the foundations of modern finance, but without coordinated regulatory and technological responses, the sector risks evolving into a fragmented, inefficient, and potentially unsafe ecosystem. This paper has explored how a unified architectural and policy framework such as that envisioned by the *Finternet* model, can foster an interoperable, inclusive, and compliance-ready financial system.

1. Technological Blueprint: The *Finternet* provides a neutral, interoperable infrastructure built on standards such as the Unified Interledger Protocol (UILP), token-level proof chains, and portable identity credentials. These innovations transcend the limitations of siloed blockchain networks and enable programmable, compliant-by-design asset transfers. Critically, this infrastructure does not privilege specific assets or issuers. Instead, it establishes a shared substrate where fiat currencies, crypto-assets, tokenized securities, and loyalty points can coexist and transact under consistent, programmable rulesets.

2. Regulatory Principles and Comparative Models: Drawing from regulatory regimes in the United States, European Union, and Singapore, we outline a set of emerging best practices for digital asset oversight: (i) *User-centricity* that prioritizes consumer protection and user accessibility, (ii) *Function- and flow-based regulation* shifting from asset-type classifications to regulating activity and transaction patterns, (iii) *Principles-based accountability* mandating outcomes like fairness, integrity, and resilience rather than prescriptive rules alone; and (iv)

Risk-proportional calibration – tailoring regulatory intensity to the scale and systemic risk of an activity or entity.
As stated in prior sections of this paper, two prime examples of this in action can be seen in EU's MiCA regulations that introduces comprehensive obligations for significant stablecoin issuers and Singapore's MAS applies agile, sandbox-driven supervision that allows safe experimentation.

3. Custody Models and Safeguards: Both *self-custody* and *third-party custody* must be supported within a robust regulatory perimeter. *Finternet's* architecture is inherently dual-compatible: users may opt to retain control over their own cryptographic keys or delegate custody to licensed entities. Policymakers should reinforce this flexibility by mandating appropriate safeguards: disclosures and recovery mechanisms for self-custody, and capital, cybersecurity, and segregation standards for custodians (cf. SEC Custody Rule, MiFID safeguarding, MAS custody guidelines).

4. Flow-Based Regulation and Embedded Compliance: A core recommendation of this paper is to move toward *flow-based regulation*, wherein compliance obligations are integrated directly into asset behavior via permissioned token standards (e.g., ERC-3643) and smart contracts. This enables real-time, rules-based enforcement of AML, KYC, and transactional integrity requirements, significantly reducing reliance on ex post reporting or human intermediaries. With the rise of autonomous DeFi protocols and tokenized finance, embedding legal obligations at the protocol level will be essential (Allen, 2023; Brummer & Reis, 2020). Such an approach aligns with global initiatives like FATF's Travel Rule, ISO 20022, and Project Guardian by MAS and BIS Innovation Hub.

5. Policy Harmonization and Legal Reform: While many of these components exist in fragmented form (for instance, tokenized KYC-compliant bond issuances, whitelisted wallet frameworks, or central bank experiments with multi-asset ledgers). However, pivotal to the next steps of integrating such portions into a coherent system requires both *regulatory harmonization* and *legal modernization*. In the U.S., this likely entails removing definitional ambiguity (e.g., around securities vs. commodities), filling legislative gaps, and enabling inter-agency

coordination across the SEC, CFTC, OCC, IRS, and FinCEN. A modular, functionally-aligned framework will support not only domestic clarity but international alignment under evolving standards such as CARF and CRS 2.0.

The task before policymakers extends beyond regulating digital assets to ideating and designing a resilient and inclusive digital financial infrastructure. The *Finternet* initiative represents a vital vision to that end: a programmable and interoperable architecture that embeds public interest regulation by design. Much like the early development of the internet when technologists and governments collaborated to establish open standards and governance frameworks enabling global connectivity and innovation, finance today stands at a comparable inflection point. As articulated by Carstens and Nilekani in 2024, the concept of a *unified ledger* integrating tokenized money and assets with programmability and identity frameworks offers a foundational blueprint for the future of financial infrastructure. The Bank for International Settlements (BIS) has emphasized the potential for such platforms to support high-trust, low-cost, and high-volume transactions across jurisdictions while preserving regulatory sovereignty. Similarly, the International Monetary Fund (IMF) has called for "platform-based finance" that is open, interoperable, and aligned with public policy objectives.[47]

The *Finternet* vision charts a path toward a next-generation financial ecosystem that is user-centric, globally interoperable, and intrinsically accountable. By adopting the recommendations outlined in this paper, regulators and industry participants can ensure digital assets are integrated safely into the economic core just like digital communications were woven into modern life. This transformation, if undertaken thoughtfully, promises not only to unlock new engines of inclusive growth and innovation but also to reinforce the foundational principles of trust, transparency, and systemic resilience.

[47] Adrian, T., & Mancini-Griffoli, T. (2023). *Platform-Based Finance: Building the Future of Financial Infrastructure*. International Monetary Fund. Available at: https://www.imf.org/en/Publications/WP/Issues/2023/03/22/Platform-Based-Finance-531120.