# The Evolving Landscape of Digital Asset Regulation

## The 11th Wharton Reg@Tech Roundtable

**December 15, 2024**
**Blockchain Digital Assets Project | The Wharton School**
**https://bdap.wharton.upenn.edu**

## EXECUTIVE SUMMARY

Conducted since 2017, the Wharton Reg@Tech Roundtable is a high-level global workshop addressing cutting-edge regulatory questions for digital assets. On October 4-5, 2024, a group of carefully selected government officials, academics, legal experts, industry executives, and investors gathered to discuss critical challenges, including:

**Global Regulatory Fragmentation**

The global regulatory landscape for digital assets is fragmented, with various regions adopting different approaches and regulatory priorities. This fragmentation increases compliance costs, creates market entry barriers, and potentially inhibits innovation. Crypto assets' multi-functional nature—serving as payment instruments, investments, or utility tokens—further complicates regulators' ability to determine their legal status with certainty. While regulators have adopted a function-based approach, examining the economic purpose of each asset, inconsistent interpretations and enforcement actions across jurisdictions continue to impede market development.

**Control and Liability in Non-Custodial Systems**

Non-custodial wallets and decentralized finance (DeFi) platforms operate in a regulatory grey area and present complex questions of control and liability. Unlike custodial services that hold user assets, non-custodial wallets provide users with control over their own private keys. Although it may appear that individuals have complete control over their non-custodial wallets, recent enforcement actions by the Department of Justice against platforms like Samourai Wallet and Tornado Cash illustrate that developers and software can be held liable for regulatory violations in certain cases. Consequently, the concept of "control" over digital assets is more complex than it seems, both legally and in terms of enforcement.

**The Stablecoin Landscape**

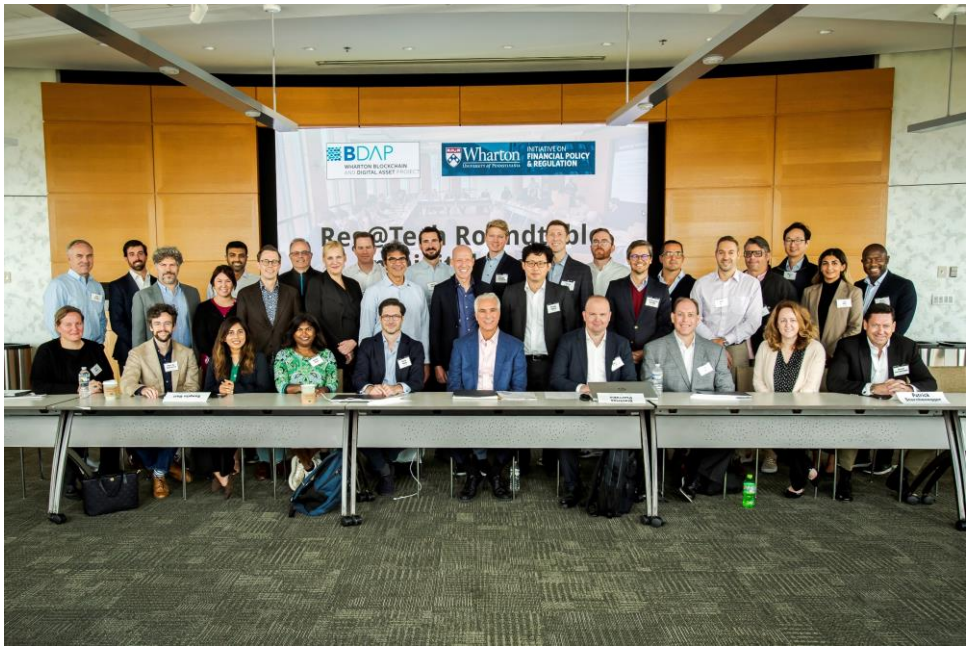
The stablecoin ecosystem presents a fundamental regulatory challenge: despite their promise of stability, there is uncertainty in their classification and oversight. The lack of consensus on stablecoin definitions and stabilization mechanisms creates widespread implications for market adoption, regulatory compliance, risk assessment, consumer protection, and financial stability.

## WORKING GROUP TOPICS

In addition to roundtable discussions, participants were divided into four working groups to consider particular issues relating to:

**Smart Contract Governance** – With the rise of smart contracts in digital finance, the group discussed whether these contracts should be upgradeable to address security flaws and who should bear responsibility in the case of failures. The discussion also considered whether such accountability should be viewed as a product liability or regulatory compliance issue.

**Off-chain Regulatory Considerations—**Typically, a technology or service stack includes both on-chain and off-chain components. The group concentrated on identifying these components using a prediction market ecosystem as an example. They analyzed different scenarios and mapped the associated risks.




**Bridging TradFi and DeFi –** To bridge the gap, the group suggested the development of tools for managing transaction approvals, encouraging innovation by learning from DeFi, ensuring clarity in regulations, and enhancing risk disclosures. Additionally, it is important to support governance standards to make services more accessible while acknowledging that TradFi and DeFi may ultimately operate as separate but complementary systems.

**Beyond KYC and Privacy Concerns** – Traditional Know Your Customer (KYC) requirements are ill-suited to decentralized systems. The group explored decentralized identity (ID) as a solution, leveraging blockchain to enable secure, user-controlled verification. Social graphs and decentralized IDs offer a promising path, though challenges related to privacy and implementation persist. Privacy concerns may vary by region, and KYC systems must incorporate flexible privacy controls.

## List of participants

Karan Aswani (Gnosis); Paul Balzano (House Agriculture Committee); Allison Behuniak (House Financial Services Comm.); Paul Brigner (Coinbase Institute); Austin Campbell (Zero Knowledge Consulting); Joseph Cox (Federal Reserve); Joey Garcia (Xapo); Sangita Gazi (Wharton BDAP); Keisuke Hayashi (Japan FSA); Jorge Herrada (CFTC); Andrei Kirilenko (Cambridge Judge School); Josh Klayman (Linklaters); Christoph Kreiterling (German BaFin); Bill Laufer (Wharton School); Alex Levine (Dapper Labs); Katherine Minarik (Uniswap); Kevin O'Connor (FinCEN); Matthias Obrecht (Swiss FINMA); Michael Oh (FINRA); Dimitrios Psarrakis (Wharton BDAP); Ari Redbord (TRM Labs); Daniel Resas (Wharton BDAP); Carla Reyes (SMU Law School); Luís Roquette Geraldes (Morais Leitão); Nilmini Rubin (Hedera); Giti Said (Arweave); Marco Santori (Kraken); Lee Schneider (Ava Labs); Thomas Scott (Worldcoin); Jesse Spiro (Tether); Patrick Storchenegger (PST Law); Valerie Szczepanik (US SEC); Peter Van Valkenburgh (Coin Center); Kevin Werbach (Wharton School).

## Table of Contents

## I. INTRODUCTION

The digital asset ecosystem stands at a critical regulatory juncture as it enters 2025. The upcoming twelve months will likely bring transformative policy developments, with the 2024 U.S. election results potentially reshaping the regulatory landscape through changes in political leadership and Congressional priorities. In other major jurisdictions, the regulatory efforts are ongoing. In the European Union (EU), the full implementation of the EU's Markets in Crypto-Assets Regulation (MiCAR) in January 2025 will be a watershed moment for the digital asset industry.

Given the rapidly evolving policy environment, the digital asset industry should expect increased compliance burdens, potential restrictions on certain business practices, and a heightened focus on consumer protection and financial stability in the coming months.

Against this backdrop, the Wharton Blockchain and Digital Asset Project (BDAP) convened the 11th Reg@Tech Roundtable that brought together leaders from the digital asset industry, regulatory bodies, and academia to address pressing challenges in digital asset regulation. The collaborative nature of the Roundtable fostered a unique dialogue between practitioners, policymakers, and scholars, resulting in nuanced perspectives on how to balance innovation with regulatory oversight in the digital asset space.

This report synthesizes the key insights and recommendations that emerged from these discussions. Drawing from both plenary sessions and focused working groups, the report is structured in three parts, each examining distinct issues: development in digital asset regulation, the regulatory framework governing non-custodial services, and the legal and regulatory complexities surrounding stablecoins.

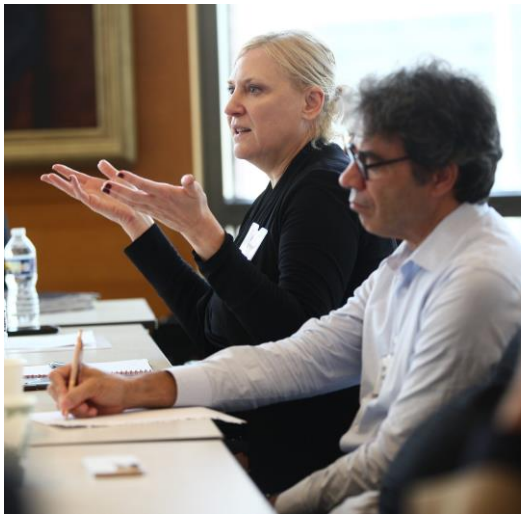
## II. IS CRYPTO A 'FAILED DISCOURSE' BETWEEN REGULATORS AND INNOVATORS?

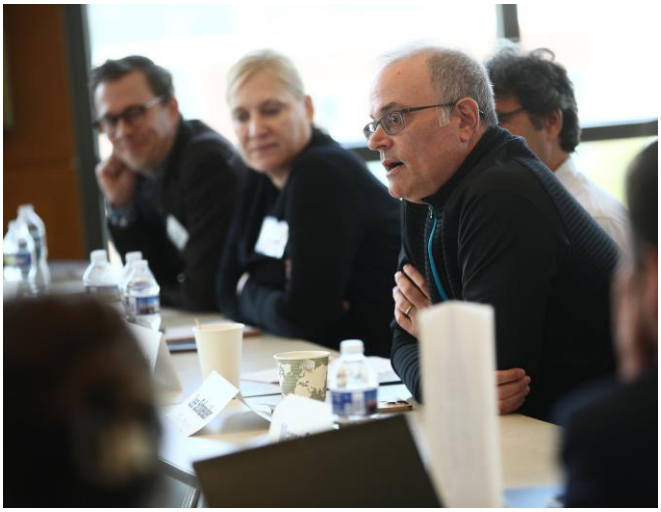
The global regulatory landscape for digital assets has entered a new phase as jurisdictions worldwide adopt diverse digital asset regulation and oversight approaches. The EU has emerged as a pioneer in this space with its MiCAR, which has a comprehensive disclosure-based framework and represents one of the most ambitious attempts at digital asset regulation to date.

The complexity of MiCAR became a key point of discussion during the roundtable, receiving praise for its comprehensive approach while also facing criticism due to its complicated requirements. During the session, the complex and detailed nature of MiCAR was discussed, and it was viewed as a clear example of "regulatory overkill" that would increase compliance costs for cryptoasset service providers.

As the crypto landscape evolves, firms consistently find themselves navigating a maze of regulatory frameworks. This divergence poses major hurdles for market entry, compliance, and smooth business operations. The challenge is not just about following the rules but about staying agile and innovative in a rapidly shifting environment.

Regulatory fragmentation was another key concern. The disparate regulatory frameworks across jurisdictions impede market entry and impose substantial compliance costs on the cryptocurrency industry.





From a regulatory standpoint, the inherent characteristics of cryptocurrency transactions—their instantaneous execution and borderless reach—present unique challenges for regulatory oversight that traditional financial frameworks struggle to address. For instance, a single cryptocurrency transaction might simultaneously trigger regulatory considerations in multiple jurisdictions, each with its own regulatory requirements and enforcement mechanisms.

Also, while cryptoassets represent value, their hybrid nature makes traditional regulatory categorization difficult. A single token might function as a payment method, an investment vehicle, and a utility instrument, sometimes simultaneously. This multifaceted nature has led most regulatory bodies to adopt a function-based approach, where the economic purpose of the cryptoasset determines its regulatory treatment. For example, a stablecoin primarily used for payments might fall under payment services regulations, while a token offering profit-sharing might be subject to securities laws. Moreover, regulators have commitments to protect public interest and national security.

The increasing regulatory uncertainties have emerged as barriers to implementing the regulation. When statutes contain ambiguous language, interpreting cryptocurrency regulations presents a significant challenge, creating a chilling effect on innovation, especially for smaller market participants who lack resources for extensive legal compliance.

### Group A: Smart Contract Governance

*Should smart contracts be upgradeable? If the primary goal of upgradeability is to fix security flaws, does this make developers accountable for outcomes?*

- Factors like decentralization, human involvement, and governance structures influence legal responsibilities and liabilities related to smart contracts. In centralized governance, regulators may hold the central entity responsible for compliance.
- Key questions arise regarding product liability and consumer protection: Who is accountable for code failures? Should developers or auditors be held responsible if a deployed smart contract is breached? Does liability depend on intent, or is negligence enough?
- Smart contracts often interact with each other, creating complex interdependencies that complicate accountability. Users' engagement with these contracts also matters; the principle of *caveat emptor*—buyer beware—applies. Who communicates the associated risks?
- Regarding upgradeability, sometimes only certain features can be enhanced, and specific governance agents often manage these upgrades. Trust has shifted from governance bodies to the code itself. If profit is involved, does that trigger greater accountability?
- Compliance should align with the degree of responsibility, tailored to specific activities. The case of The DAO raises questions about centralized versus decentralized regulation. In the Mango Markets incident, where a user exploited smart contracts that functioned correctly, should developers be held liable?

## III. THE NON-CUSTODIAL WALLETS AND DEFI PROTOCOLS

The oversight of non-custodial products and platforms, including crypto wallets and DeFi protocols, is still inconsistent and lacks comprehensive development. Most jurisdictions focus regulatory attention on custodial services—where an intermediary holds user asset. Non-custodial wallets and protocols give users sole control over their private keys and assets. Since the wallet service providers do not maintain any control, they often fall outside traditional

custodial definitions. Yet, the Department of Justice's (DOJ) prosecution [1] against *Tornado Cash* developers for money laundering conspiracy and violations of sanctions raises important questions about the traditional understanding of liability in non-custodial services and decentralized protocols.

To capture the unique risks of a non-custodial wallet, some regulators are considering the "responsible persons" framework formulated by the International Organization of Securities Commissions (IOSCO), which targets individuals or entities with significant control or influence over the protocol's operation, as a way to hold critical actors accountable without regulating the technology itself.

### A. Custodial vs. Non-custodial Wallets

In the digital asset discourse, a wallet is understood as a hardware or software that holds cryptocurrencies, stablecoins, and NFTs. From a composition perspective, all digital asset wallets are a combination of a public key and a private key. In custodial wallets, the centralized entity, such as a cryptocurrency exchange, retains control of the individual users' private keys. [2] In contrast, non-custodial wallets leave

**UCC Article 12 – a potential solution?**

Article 12 of the Uniform Commercial Code (UCC) was discussed as a possible solution to private law issues concerning digital assets. Article 12 defines the rights of purchasers regarding controllable accounts, payment intangibles, and obligations of account debtors. It introduces "controllable electronic records" (CERs) as electronic information records that can be controlled, clarifying how secured parties can perfect and prioritize security interests in digital assets like cryptocurrency, NFTs, and stablecoins. Control over the ledger becomes a key regulatory tool, especially for addressing AML/CFT concerns, with CER control being akin to possession of a physical asset. To control a CER, a person must: 1) hold substantial benefits of the CER (not necessarily exclusively); 2) have exclusive power to prevent others from accessing those benefits; and 3) possess the exclusive authority to transfer control or enable another person to control the CER.

[1] Press Release, *United States Attorney's Office Southern District of New York, Tornado Cash Founders Charged with Money Laundering and Sanctions Violations* (23 August 2023), https://www.justice.gov/usao-sdny/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations, accessed 22 November 2024.

[2] Jackson Wood, *Custodial Wallets vs. Non-Custodia Crypto Wallets*, CoinDesk (09 March 2022), https://www.coindesk.com/learn/custodial-wallets-vs-non-custodial-crypto-wallets/, accessed 22 November 2024.

private keys entirely in the hands of users, removing any intermediary control over their holdings.[3] Custodial wallets are often subject to clear regulatory obligations. For example, the New York Department of Financial Services (NYDFS) issued guidance on custodial structures, mandating that custodians hold customer assets responsibly and disclose relevant terms.[4] New York's BitLicense requires custodians to adopt measures to protect customer assets and disclose custody arrangements clearly.[5] However, non-custodial wallets complicate compliance due to the lack of third-party oversight.

Recent enforcement actions illustrate the difficulty in categorizing non-custodial wallets within existing frameworks. For instance, in Tornado Cash, the DOJ targeted the non-custodial Samourai Wallet for not complying with AML/CFT requirements under the Bank Secrecy Act (BSA) and KYC rules, arguing that non-custodial services should register with the Financial Crimes Enforcement Network (FinCEN).[6] Similarly, *Tornado Cash*'s developers faced scrutiny on the basis that the protocol facilitated "money transmission," as its code allowed cryptocurrency to move from one address to another upon user command.[7]

### B. Regulatory Debates

From a regulator's perspective, 'control' is the key concept that determines whether a wallet-service provider falls within a regulatory purview. However, the concept of 'control' in the context of digital assets is much more nuanced, both from

**IOSCO's "Responsible Persons" Framework in DeFi arrangements: Four key determinations**

1. **Who is a Responsible Person?** Anyone who has control or influence over a DeFi arrangement or activity. This includes founders, developers, token issuers, DAO participants, and those with smart contract rights.

2. **How to identify Responsible Persons?** Regulators should assess entities to identify Responsible Persons.

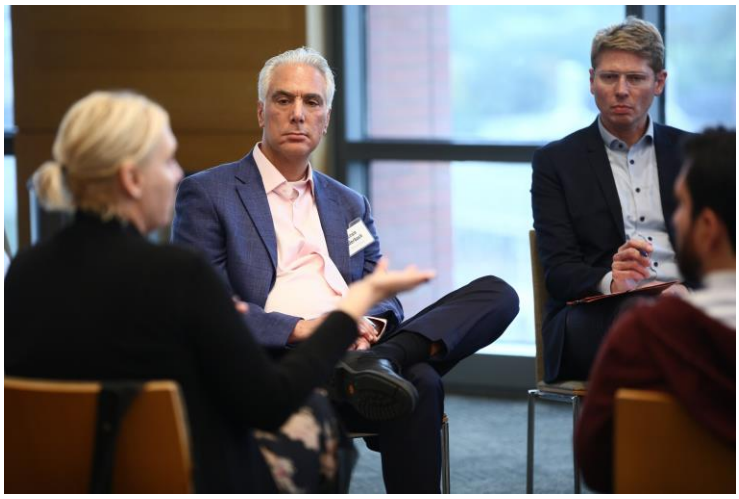
3. **What happens to Responsible Persons?** IOSCO advocates for a regulatory framework that applies to Responsible Persons.

4. **What happens if existing rules don't apply?** IOSCO recommends modifying existing rules to apply to DeFi arrangements.

[3] Id.
[4] Department of Financial Services, *Virtual Currency Guidance* (23 January 2023), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20230123_guidance_custodial_structures, accessed 22 November 2024.
[5] Id.
[6] *U.S. vs. Keonne Rodriguez and William Lonergan Hill* (U.S. District Court, Southern District of New York, 24 April 2024).
[7] *U.S. vs. Roman Strom and Roman Semenov* (U.S. District Court, Southern District of New York, 23 August 2023.

legal and enforcement perspectives. In the 2019 Virtual Currency Guidance, the FinCEN clarified that partial control does not qualify wallet developers as money transmitters, provided they lack "total independent control over the value."[8] The industry lauded this interpretation because it clarifies that only custodial cryptocurrency businesses are eligible for licensing and subject to federal compliance laws and regulations.[9]

However, enforcement actions against Tornado Cash have muddied this distinction, suggesting that the DOJ may consider software facilitating transfers as liable for money transmission. This ambiguous stance raises broader legal questions of whether all cryptocurrency wallets, custodial or non-custodial, might be categorized as money transmitters, potentially including any entity (such as Bitcoin miners, DeFi protocols) involved in transaction facilitation. Regulatory scrutiny over *Tornado Cash* has spared debate about whether enforcement actions accurately capture legal distinctions between unauthorized money transmission and the "specific intent" required to prove money laundering.



The regulatory debates also revolve around the pertinence of the custodial rule in cryptoassets securities. Recent SEC actions against Consensys[10] and Uniswap,[11] among others, demonstrate how securities law may apply to non-custodial platforms, and these services are scrutinized for potential securities violations. Under the U.S. SEC law, 'custody' means when an investment adviser holds 'directly or indirectly, client funds or securities or [has] any authority to obtain

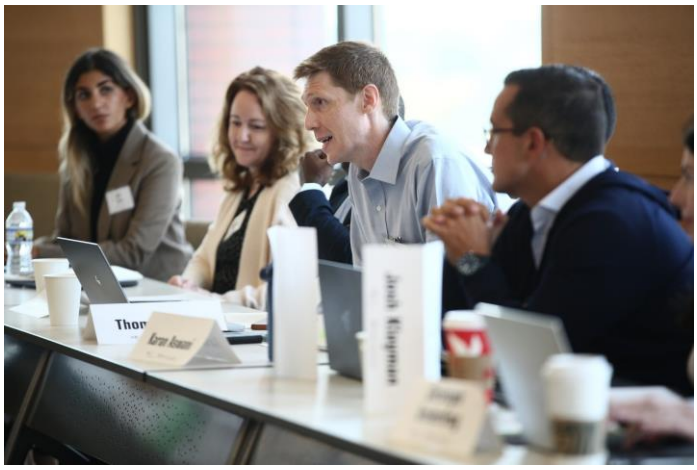
[8] FinCEN, *FinCEN Guidance* (9 May 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf, accessed 22 November 2024.
[9] Peter Van Valkenburgh, *DOJ's New Stance on Crypto Wallets is a Threat to Liberty and the Rule of Law* (Coin Center, 29 April 2024), https://www.coincenter.org/dojs-new-stance-on-crypto-wallets-is-a-threat-to-liberty-and-the-rule-of-law/, accessed 22 November 2024.
[10] SEC, *SEC Charges Consensys Software for Unregistered Offers and Sales of Securities through its MetaMask Staking Service* (Press Release, 28 June 2024), https://www.sec.gov/newsroom/press-releases/2024-79, accessed 22 November 2024.
[11] Dan Primack, *The SEC has questions for VCs about Uniswap* (AXIOS, 12 August 2024), https://www.axios.com/2024/08/12/sec-questions-vcs-uniswap, accessed 05 November 2024.

possession of them.[12] However, the SEC has no requirements for custodial services for crypto-securities. Instead, the SEC's jurisdiction over any custodial question of crypto assets securities hinges on whether the transaction passes the *Howey* test.[13]

### C. Path forward for non-custodial wallet regulation

Following are the areas highlighted during the roundtable:

*Regulatory clarity*: Clear regulations can jump-start innovation through the mass adoption of DeFi services. Ambiguous and generalized regulations may inadvertently discourage potential users and slow industry growth. By establishing a specific 'liability' framework in conjunction with DeFi agreements for wallet service providers, regulators can focus on customer protection while preserving users' autonomy.



*Legal Basis*: The UCC's Articles 8 and 12 provide foundational guidelines on CERs and security interests in digital assets. These articles try to legally base the concept of digital asset 'control' within a decentralized environment.

*Risk-Based Regulation*: The advantages of DeFi, such as transparency and decentralization, should not be regulated; regulatory attention should be paid to mitigating specific risks.

*Case-by-Case Enforcement:* While case-specific rulings provide temporary solutions, they often do not bring the expected clarity, resulting in industry confusion and economic losses.

[12] Amended rule 206(4)-2(c)(1).
[13] *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).

## Group B: Off-Chain Considerations in Prediction Markets

Usually, a technology or a service stack has both on-chain and off-chain components. Group B focused on identifying these components within the prediction market ecosystem, analyzing various scenarios, and mapping the associated risks. These risks were then categorized as high (very high), medium, or low (very low) based on the potential impact of each scenario. The group breaks down the regulator considerations in four scenarios to illustrate these risks:

*Scenario 1*: A Centralized user Interface Company ("UI Co") operates a prediction market with both on-chain and off-chain components. UI Co manages user assets and records some internal transactions while conducting KYC/AML processes.

| **Off-chain elements** | **On-chain elements** | **Risk analysis and risk rating** |
|---|---|---|
| -User interface (UI)<br>-Data for Oracle<br>-Off-chain servers (UI Co. books and records))<br>-Off-chain governance | -Smart contracts<br>-Oracle connection with smart contract | Misconduct risk (*high*)<br>Custody risk (*high*)<br>Infrastructure risk (*medium*)<br>AML risk (*low*)<br>Information asymmetry risk (*high*)<br>Governance risk (*low*)<br>Prudential risks (*high*) |

*Scenario 2*: UI Co sets up the UI and smart contracts and controls the Oracle but does not control the user assets and does not use its own books.

| **Off-chain elements** | **On-chain elements** | **Risk analysis and risk rating** |
|---|---|---|
| -UI<br>-Data for Oracle<br>-Off-chain servers<br>Off-chain governance | -Smart contracts<br>-Connection of Oracle to smart contracts<br>-Assets | -Misconduct risk (*medium*)<br>-Custody risk (*low*)<br>-Infrastructure risk (*high*)<br>-AML risk (*low*)<br>-Information asymmetry risk (*medium*)<br>-Governance risk (*low*)<br>-Prudential risk (*medium*) |

*Scenario 3*: UI Co sets up a platform where users create their own smart contracts and on-chain governance rather than an oracle; UI Co does not control users' assets and does not use UI Co's own books.

| **Off-chain elements** | **On-chain elements** | **Risk analysis and risk rating** |
|---|---|---|

| | | |
|---|---|---|
| -UI | -Smart contracts<br>-Assets<br>-On-chain governance | -Misconduct risk *(low/medium)*<br>-Custody risk (*low*)<br>-Infrastructure risk (*high*)<br>-AML risk (*low*)<br>-Information asymmetry risk (*low*)<br>-Governance risk (*medium*)<br>-Prudential risk (*low*) |

*Scenario 4*: No UI; users connect directly from the proto

| **Off-chain elements** | **On-chain elements** | **Risk analysis and risk rating** |
|---|---|---|
| **-None** | -Smart contract<br>-Assets<br>-On-chain governance<br>-Direct access via an API | -Misconduct risk *(very low)*<br>-Custody risk (*low*)<br>-Infrastructure risk (very *high*)<br>-AML risk (*high*)<br>-Information asymmetry risk (*very low*)<br>-Governance risk (*medium/ high*)<br>Prudential risk (*very low*) |

## IV. THE ONGOING REGULATORY DEVELOPMENTS OF STABLECOINS AND TOKENIZATION

The role of stablecoins and tokenized assets in the digital financial landscape is rapidly evolving beyond their original purpose as trading pairs for cryptocurrencies. They are increasingly becoming integral to payment systems that offer faster and more cost-effective cross-border transactions while enabling round-the-clock settlement capabilities. This transformation is particularly significant in regions with volatile currencies, where stablecoins can provide a more reliable store of value and increase access to global financial services.

### A. Back to basic – What is a stablecoin?

The stablecoin ecosystem currently faces a fundamental challenge that affects its development and market adoption: the lack of a universally accepted definition and uniform understanding of its categorization and the technical terms, such as stabilization mechanisms.

The Canadian Blockchain Consortium defines stablecoins as ‘value-referenced cryptoassets’, which maintain their stable value by pegging to a stable fiat currency, cryptocurrency or

commodity held in reserve or by an algorithmic mechanism or combination of these two.[14] Financial Stability Board (FSB) defines stablecoins as a form of cryptoassets "intended to maintain a stable value relative to a specified asset or basket of assets." [15] It further includes 'global stablecoins' (GSC) as another category, based on its potential to be adopted and used across multiple jurisdictions and its ability to be used as a store of value or means of payment.[16]

*"Not everything under the sun is a stablecoin."*

However, in practice, stablecoins' definitions vary depending on the stakeholder perspective. Regulators primarily focus on the promise of stable value and potential systemic risks to the financial system, while developers emphasize technical mechanisms and smart contract implementation. Users, meanwhile, are most concerned with practical aspects, such as price stability, its redeemability at par, and transactional capability. The fragmentation in understanding and categorizing stablecoins has significant implications for regulation, adoption, and market developments. Additionally, there is no uniform consensus on what precisely constitutes 'stable' in the context of stablecoins.

Another crucial element of stablecoin issuance is the stabilization mechanism, which represents the 'core' claim of stablecoins of reducing the volatility of the crypto market and underpins the users' expectations that stablecoins are redeemed at par, on-demand, anywhere in the world."[17] Traditional classification methods have typically categorized stablecoins based on the collateral types used as their basis for the stabilization mechanisms (such as fiat-backed, crypto-backed, commodity-backed, and algorithmic). [18] Decisions regarding stablecoin arrangement are usually made by governing bodies, which can affect the composition of the stablecoins' nature, the collateral used, and the characteristics of their stabilization mechanisms.[19]

The lack of uniformity in stablecoin taxonomy and stabilization mechanisms brings regulatory challenges, given that stablecoin arrangements may function like liquidity providers, payment

[14] Canadian Blockchain Consortium, *Conceptual Framework for Value-Referenced Cryptoassets (Stablecoins)* (01 November 2023), https://www.canadablockchain.ca/wp-content/uploads/2024/09/Canadian-Blockchain-Consortium-Conceptual-Stablecoin-Framework-v2.-11.01.23.pdf, accessed 22 November 2024.
[15] FSB, Regulation, *Supervision and Oversight of "Global Stablecoin" Arrangements: Final Report and High-Level Recommendations* (13 October 2020), https://www.fsb.org/uploads/P131020-3.pdf#page=12.55, accessed 22 November 2024.
[16] Id.
[17] Parma Bains, *Regulating the Crypto Ecosystem: The Case of Stablecoins and Arrangements* (2022) IMF Fintech Notes 008, https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Stablecoins-and-Arrangements-523724, accessed 22 November 2024.
[18] FSB classifies any algorithmic stablecoin as 'unbacked.'
[19] IMF, *supra* note 17.

instruments, bank deposits, or money market funds. As a result, in the U.S., multiple regulatory bodies maintain overlapping oversight over stablecoins.

## Group C: Bridging TradFi and DeFi

**Understanding TradFi and DeFi**

TradFi encompasses financial institutions such as banks and credit institutions operating within heavily regulated environments. These institutions offer financial services with strict regulatory oversight, using client funds within a framework designed to maintain stability and investor confidence. DeFi, on the other hand, represents a paradigm shift. Built on blockchain technology, DeFi enables financial transactions without intermediaries, empowering users to engage directly in activities such as yield farming and staking. However, the decentralized nature of DeFi brings both opportunity and risk, as it sidesteps the rigid compliance structures of TradFi. Platforms like Coinbase, which provide access to cryptocurrency, have emerged as potential bridges between these two worlds, though the extent to which they can facilitate a seamless connection remains uncertain.

**Identifying bridges and managing risks**

For TradFi and DeFi to interact effectively, several potential bridges, such as regulated exchanges and banks, are being considered. Virtual Asset Service Providers (VASPs) may also serve as conduits for interaction, provided they operate with the necessary compliance layers. A fully licensed approach within TradFi could provide a foundational structure for engaging with DeFi, potentially reducing risks by ensuring adherence to financial service regulations. Conversely, unlicensed DeFi activities, such as staking or yielding, operate in a largely self-regulated space where traditional compliance protocols may not apply.

However, bridging TradFi and DeFi introduces significant risks. TradFi operates on established compliance frameworks that prioritize consumer protection and transparency. DeFi, without such frameworks, presents new challenges, especially concerning security, liability, and liquidity risks. Security issues in DeFi—such as vulnerabilities in smart contracts or liquidity pools—raise questions about where liability should lie. Without adequate disclosure and consumer protection measures, users in DeFi are exposed to risks unfamiliar to the average TradFi user. Thus, any bridge must consider the liability and risk distribution between these systems.

**Recommendations**

- Developing tools to manage transaction approvals, fostering innovation by learning from DeFi, ensuring regulatory clarity, and improving risk disclosures.
- Governance standards be supported to make services widely available while recognizing that TradFi and DeFi may ultimately function as separate but complementary systems.

The regulatory inconsistency also exists in the MiCAR framework. For example, MiCAR classifies stablecoins as *asset-referenced cryptoassets* and *e-money tokens*. However, it is unclear if the e-money tokens will also be regulated by the EU E-Money Directive 2009,[20] provided that stablecoins may well be built on a decentralized, open network.

The session moderator raised four key questions regarding stablecoins:

- *Value Generation*: How do stablecoins create value?
- *Market Dynamics*: What market conditions allow stablecoins to be profitable?
- *Stabilization Mechanisms*: What ensures the stability of stablecoins?
- *Stability-Profitability Relationship*: What models ensure stable value creation and market stability?

The legal definition of 'cryptoassets' is context-specific and dependent on the relevant EU legislation. For example, under the EU's Transfer of Funds Regulation, e-money tokens are treated purely as cryptoassets, while under the EU's recently updated sanctions regime, they are to be classified as 'funds'.[21] The dual classification of e-money tokens as crypto assets and funds under MiCAR can make it cumbersome for service providers to carry out stablecoin operations across the EU. The EU's position of stablecoins as a store of value (for example, remittance payments in stablecoins/ cryptocurrency) also triggers compliance requirements.

Questions persist about whether tokens requiring modification or additional utility features necessitate new white papers, highlighting the difficulties in creating static regulations for dynamic digital assets.

## Group D: Beyond KYC

**The limits of traditional KYC**

KYC processes are fundamental in financial systems, designed to verify customers' identities, prevent fraud, and comply with anti-money laundering regulations. However, traditional KYC has limitations. One proposal to address these limits suggests "deputizing" SWIFT or requiring all banks to use a public blockchain for deposits, thus increasing transparency and accessibility. Yet, these ideas introduce new questions about feasibility, data security, and user privacy.

**Potential solutions: Decentralized ID**

*Decentralized ID* leverages digital credentials on a blockchain, allowing users to control access to their information. One viable model is using social graphs, which map users' relationships and provide multiple dimensions of identification. The W3C standard for

[20] Directive 2009/110/EC.

[21] Chainalysis, *MiCA's Stablecoin Regime and Its Remaining Challenges: Part 3* (Chainalysis, 03 July 2024), https://www.chainalysis.com/blog/mica-stablecoin-regime-challenges-part-3/, accessed 22 November 2024.

verifiable credentials supports this approach, enabling identification based on various markers of authenticity. This structure could be token-based, meaning users become a "hash value" instead of holding a traditional account, providing a more private and decentralized verification system.

While promising, decentralized ID faces several challenges. Early efforts, such as those initiated by the Obama administration through NIST and Project Liberty's DNSP protocol, highlight the importance of collective action. Building a decentralized ID system requires a substantial network effect and an effective entry point, as the technology alone cannot solve all practical challenges. Third-party attestations, where trust levels are verified by external entities, could play a role in bridging trust gaps within decentralized ID.

**The privacy debates**

The group's discussion emphasized that privacy expectations differ based on geographical location, cultural norms, and government policies. Some users are comfortable trading privacy for ease, while others demand higher levels of control over their data. This variability highlights the need for KYC systems to offer flexible privacy settings, respecting different user preferences and regulatory requirements.

### B. Do stablecoins make the payment system fairer?

Banks and other traditional financial institutions currently dominate the payment system. The real issue at hand isn't whether stablecoins are a blessing or a curse; it's about how fair our current payment system truly is and what stablecoins do to improve its fairness.

Stablecoins offer several benefits to the modern payment system. They provide a bridge between traditional financial and the digital asset ecosystem, leveraging the advantage of blockchain technology while maintaining a stable value pegged to established currencies or assets. In cross-border transactions, stablecoins significantly reduce the friction and costs associated with international money transfers. Traditional remittance systems often involve multiple intermediaries, high fees, and processing delays that can stretch for days. Stablecoins enable 'atomic' settlements at any time, reducing costs for merchants and individuals.

For emerging markets, stablecoins serve as a powerful tool for financial inclusion. In countries experiencing high inflation or currency instability, stablecoins provide citizens access to a stable store of value without requiring traditional banking relationships. In many Latin American countries, stablecoins are used as a means of payment and a store of value and play a significant role in enabling the unbanked to access banking. According to a Google search, the highest interest in stablecoins among internet users is recorded in Brazil, Colombia, the Dominican Republic, Ecuador, Mexico, Peru, and El Salvador.

Stablecoins also present risks that require careful consideration from regulators, users, and market participants. The 2022 collapse of Terra/UST and Silicon Valley Bank, which resulted in a de-peg event for Circle's USDC, highlighted how stablecoin failures can trigger widespread

**Project Guardian: Singapore's Public-Private Partnership for DeFi Regulation**

The Monetary Authority of Singapore (MAS), in collaboration with the BIS and high-profile global banks, such as HSBC and JPMorgan, among others, launched Project Guardian, which aims to establish open and interoperable private networks for tokenizing assets on DeFi protocols.

The project intends to explore the regulatory framework of DeFi activities that is compliant with international standards, such as IOSCO's Objectives and Principles of Securities Regulation, Policy Recommendations for Crypto and Digital Asset Market, the Basel Committee on Banking Supervision Standards, and the use of the Financial Action Task Force's recommendation, including Recommendation No. 15 applicable to virtual asset service providers.

market instability and investor losses. Operational risks stem from the technological infrastructure underlying stablecoins. Smart contract vulnerabilities and cybersecurity breaches can compromise the stability and functionality of these tokens.

Regulatory uncertainty creates additional risk as jurisdictions adopt varying approaches to stablecoin oversight. Additionally, various regulators have unique viewpoints on the risks associated with stablecoins, each bringing their own perspective to the table. MiCAR stresses stablecoins' 'systemic' or 'bank run' risk and requires a high proportion of reserves to be held at banks,[22] while the SEC This affects profitability and exposes the stablecoin to credit risk.[23]

The obscurity in the stablecoin market may contribute to uneven competition between stablecoin issuers and incumbent financial institutions. Big commercial banks could leverage a stablecoin issuer's business model. Legacy financial institutions are adopting projects to issue tokens against bank deposits on a private or public blockchain (known as tokenized deposits). For example, JPMorgan issued 'JPM Coin' against their corporate clients' U.S. dollar deposit accounts on a permissioned blockchain. They are used to settle transactions between JPMorgan's clients. Germany is looking into issuing commercial bank money tokens on a non-blockchain platform.

[22] Art. 54, MiCAR.
[23] Ledger Insight, Report Highlights Pros & Cons of Stablecoin MiCA Regulations, https://www.ledgerinsights.com/report-highlights-pros-cons-of-stablecoin-mica-regulations/, accessed 4 July 2024.

## V. CONCLUSION

This report underscores the complexities and evolving nature of the digital asset regulatory landscape. As the industry grows, so does the need for comprehensive, adaptable regulatory frameworks that balance consumer protection, market stability, and innovation. The roundtable discussions and working groups highlighted critical issues, such as smart contract governance, the challenges posed by non-custodial wallets and DeFi protocols, and the role of stablecoins in transforming payment systems. Moving forward, a collaborative approach between industry participants, policymakers, and regulators will be essential to establish clear, risk-sensitive, and innovation-friendly regulations. This alignment can foster a more secure, inclusive, and resilient digital asset ecosystem.

The Blockchain and Digital Asset Project, part of the Wharton Initiative on Financial Policy and Regulation, explores the implications of distributed ledger technology for organizations, governments, and individuals. Working with policy-makers and a global network of experts, BDAP develops insights on cryptocurrencies, blockchain networks, decentralized applications, and Web3.

For more information, please contact us at https://bdap.wharton.upenn.edu/contact-us/.