Cardano Foundation

Response to U.S. SEC Crypto Task Force Questionnaire

24 April 2025

1 Introduction

As the Cardano Foundation, a central element of our mission is to support the development of regulatory frameworks that are proportionate, technologically neutral, and non-discriminatory towards open, permissionless systems such as the Cardano blockchain protocol. We are convinced that an appropriately targeted, risk-based legal and regulatory framework is beneficial to realizing the potential of blockchain technology in the U.S. and beyond. Regulatory frameworks, built on sensible and suitable principles, help foster innovation while reducing potential risks and unwanted social costs.

The Cardano blockchain is a public, permissionless Layer 1 blockchain protocol based on academic research and built on open-source architecture. Since its launch in 2017, it has maintained ongoing operation and is supported by a globally distributed set of maintainers and participants, such as stake pool operators, developers, and users. Its core design principles—resilience, transparency, decentralization, and adaptability—position Cardano as a form of digital public infrastructure capable of underpinning a wide range of financial and non-financial applications.

The U.S. has long been a global leader in technological innovation and financial market development. With its recalibrated approach towards regulating blockchain technology, the SEC has the opportunity to reinforce the U.S.' leadership by establishing a framework that is open and innovation-friendly while ensuring appropriate investor protection, risk mitigation, and market integrity. The CF appreciates the SEC's constructive engagement with the blockchain industry through the Crypto Task Force (hereinafter "CTF") and we appreciate having this opportunity to contribute our perspective to this discussion.

This submission covers five interrelated thematic areas which represent critical pillars for a coherent and future-proof regulatory approach to blockchain-based systems and respective assets in the U.S. It begins by addressing the need for a **functional and risk-based taxonomy** for blockchain assets and argues **against using decentralization** as a criterion for determining whether a blockchain asset is a security for U.S. federal security law purposes. The submission advocates for **regulatory interoperability**, aligning U.S. frameworks with international standards like MiCAR, and argues for a **technology-neutral approach to tokenization**, emphasizing its potential to enhance market efficiency and transparency. It further discusses **staking as a core network function** (rather than as an investment scheme), outlines the unique features and regulatory challenges of blockchain asset custody, and introduces a **constructive perspective on outsourcing**, proposing a proportionate, function-focused model for public, permissionless infrastructures like Cardano.

2 Regulatory Qualification and Interoperability Considerations

Rightfully, the first critical question from the CTF relates to the "security status"[1] of crypto assets and transactions in crypto assets (hereinafter "blockchain assets"[2]). This matter lies at the heart of many of the regulatory challenges in the U.S.

There are three principles that should guide any regulatory taxonomy for blockchain assets, whether in the U.S. or elsewhere. First, a taxonomy should provide as much **certainty to industry participants** as possible. Second, given the global nature and accessibility of blockchain networks, a taxonomy in the U.S. should **facilitate regulatory interoperability** and try to avoid plain misalignments with non-U.S. approaches of other major Western economies. Third, the taxonomy should use a **functional, risk-based** perspective.

2.1 Lack of Certainty

The lack of certainty has hindered the development of the blockchain industry in the U.S. and—due to the weight of American funding globally—around the world. An increased degree of regulatory certainty will greatly encourage compliant activities in the U.S and elsewhere.

For example, there are many projects building applications that use the Cardano blockchain infrastructure which are based in the U.S. or that would like to provide U.S. persons with access to their applications. Many of them have been forced to take steps to avoid the U.S. or limit their activities due to the regulatory uncertainty. Importantly, these projects seek a reasonable path to compliant activities in the U.S.

We believe that such certainty is best achieved through a combination of a taxonomy that uses **objectively determinable and immutable factors**, and the use of exemptive relief. We think that the taxonomy can make due with three categories of assets, in line with what the CTF sets forth in its request: Intrinsic securities, intentional securities and all other blockchain assets which are not securities.

2.1.1 Intrinsic Securities

This category encompasses all blockchain assets that have the **intrinsic characteristics** of securities. These are blockchain assets that are associated with rights or interests in a legal entity that have the characteristics consistent with one of the items in the definition of "security" under the Securities Act.

With regard to "investment contracts", we recognize that the case law following the *Howey* decision makes clear that assets that do not have the intrinsic characteristics of securities are not in and of themselves securities, even when sold in an investment contract transaction.

[1] "What type of regulatory taxonomy would provide a predictable, legally precise, and economically rational approach to determining the security status of crypto assets and transactions in such assets without undermining settled approaches for evaluating the security status of non-crypto assets and transactions?"

[2] We understand that the SEC uses the term "crypto assets", but given the countervailing tendencies in international taxonomies we prefer to use the term "blockchain assets" to avoid potential confusion.

2.1.2 Intentional Securities

Intentional securities are **tokenized securities**, which are blockchain assets that are representations of traditional securities (please refer to section 3. on tokenization below for more details).

2.1.3 All Other Blockchain Assets Which Are Not Securities

Any other blockchain assets that do not fall into one of the two categories above would not be considered securities. We think establishing further categories of assets based on assessments of criteria outside the SEC's regulatory domain would add to confusion, rather than promote certainty.

For example, categorizing blockchain assets based on whether the blockchain infrastructure to which they relate is decentralized, or not, is in our view a futile endeavour. First, decentralization can apply to many technical (e.g., code architecture, node diversity), organisational (e.g., geographic distribution, change governance etc.) and economic (token distribution, incentive model etc.) aspects of a blockchain infrastructure. The variance of these aspects across projects is also significant, meaning any associated taxonomy would be enormously complex and fact bound. Second, using decentralization as a criterion inevitably promotes regulatory uncertainty as many of these aspects are subject to ongoing change (e.g., token distribution is always in flux, as is geographic node distribution). Whether a blockchain asset meets the applicable decentralization criteria would never be certain for long. In summary, **using decentralization and similar criteria would be more harmful than helpful**.

With respect to this third broad category we do of course recognize that under U.S. securities laws such blockchain assets may be offered or sold in investment contract transactions. We believe the "investment contract" at issue goes beyond the blockchain asset itself and includes all of the aspects of the offer or sale including, for instance, how the blockchain asset is marketed, what promises or representations are made by the seller to the purchaser funding that seller, and whether the purpose of the sale is to raise capital for a common enterprise.

We believe that the SEC should provide clear guidance that when a blockchain asset is sold in an investment contract transaction, it will **not treat the blockchain asset as a security in and of itself**. Instead, we believe the SEC should work to develop a framework that meets the **underlying disclosure policies** foundational to U.S. securities laws by requiring the seller of a blockchain asset to disclose information that would be relevant to purchasers of the investment contract as well as other parties that might acquire the blockchain asset from someone other than the initial seller in a non-investment contract secondary transaction.[3] The obligation to make these disclosures should continue until an objectively determinable point in time to promote certainty. For example, disclosure obligations could continue for a finite period of time (e.g., one year after the conclusion of initial sales of blockchain assets in investment contract transactions) or could continue as long as a sponsor entity is providing essential managerial efforts.

[3] To this end, we commend the work of the CTF in developing the Statement entitled "Offerings and Registrations of Securities in the Crypto Asset Markets" (April 10, 2025).

2.2 Regulatory Interoperability

The blockchain asset sector spans the globe. Similar to the Internet, this is a key aspect and potential of the technology at large. Blockchain infrastructures and their blockchain assets are used and transacted by users in many different jurisdictions and may be subject to different regulatory obligations as a result. To the extent that those regulatory obligations are determined by taxonomies, users will have more certainty and be better positioned to meet regulatory obligations if there is some **level of regulatory interoperability**. While full harmonization may not be achievable, using similar taxonomies already significantly lowers the cost of global operation.

Our proposed categories of blockchain assets above would allow for such regulatory interoperability. They are largely compatible with taxonomies applicable in other jurisdictions.

For example, the EU Markets in Crypto-Assets Regulation ("MiCAR") categorizes blockchain assets into Asset Referenced Tokens, E-Money Tokens, and Other Tokens. Blockchain assets that are themselves, or which represent, financial instruments are not subject to MiCAR. These include assets that are transferable securities under EU law (i.e., MiFID II). This category is similar to the "intentional securities" category set out above. Asset Referenced Tokens under MiCAR are tokens that aim to maintain a stable value by referencing multiple fiat currencies, commodities, or blockchain assets (or a combination thereof). Asset Referenced Tokens could be either intentional securities or non-securities in the U.S., depending on how they are structured (e.g., algorithmically stabilized vs. transfer of yield generated by underlying assets). E-Money Tokens not paying yield would also be non-securities in the U.S, which is consistent with recent guidance released by the Division of Corporation Finance, and treated the same as other dollar-backed (or single asset-backed) stablecoin assets.

Other Tokens that fall within the MiCAR framework (commonly referred to as "Utility Tokens"), i.e., those that provide digital access to a good or service, would also fall into the non-security category in the U.S. Any sale of Utility Tokens for capital raising purposes would require compliance with an SEC exemptive relief scheme as outlined above.

In an effort to achieve harmonization, we suggest that the **SEC should look to the disclosure requirements in place in other jurisdictions** such as Singapore, the United Kingdom, and Switzerland in addition to the European Union. While our example above focused on MiCAR, reference to the requirements across multiple jurisdictions would help to achieve the highest degree of interoperability. Critically, all these examples illustrate that it should be possible to map most categorizations under other regimes to a U.S. disclosure framework, creating global certainty akin to the capital markets.

3 Tokenization

We refer to "tokenization" as the creation of a blockchain-based representation of an asset that already exists in the digital or physical (i.e., non-blockchain-based) world, which, for purposes of consideration

by the SEC, include digital or paper-based securities like stock, debt and other financial instruments. Tokenization, especially when combined with appropriately gated “automated market maker” protocols, can unlock enhanced accessibility and liquidity, combined with transparency and efficiency. These attributes can significantly improve regulatory oversight, risk monitoring, and investor confidence—not only in the blockchain asset space, but also across traditional financial markets. We strongly believe that tokenization offers tremendous opportunities to foster innovation, attract capital, and strengthen market infrastructure.

The current securities laws were enacted long before the advent of the Internet and are not well-suited to address the technological capabilities available today. Applying the current rules rigidly to all tokenized assets risks stifling innovation without meaningfully enhancing investor protection. For instance, current requirements mandating that securities be held in specific centralized depositories may inadvertently obstruct the use of blockchain-based settlement systems and limit the mobility of assets. Modern technologies offer new ways to uphold the core principles of securities regulation while improving efficiency and market access, and reducing capital cost (e.g., by introducing functions like instant and/or atomic settlement, fractionalization, automated reconciliation, programmable assets etc.). To enable this, the **regulatory approach to blockchain-based solutions must ensure equal and principle based treatment on a level playing field**.

As noted above, blockchain assets, by design, are borderless. They can be **created, stored, transferred, and settled globally, near-instantly**, across a wide variety of public, permissionless blockchain infrastructures, including Cardano. This fluidity and openness clashes with the territorial, fragmented nature of securities regulation. In traditional finance, issuers and infrastructure providers operate within national (and sometimes sub-national) legal frameworks. Securities offerings are carefully scoped by geography (e.g., who can invest, how a security is registered or exempt from registration, and where it can be traded). But in the world of public, permissionless infrastructures, those lines blur.

As the SEC and the CTF consider how best to regulate the issuance, custody, and transfer of tokenized securities, we urge it to **adopt an approach that favors a level playing field and global interoperability for securities infrastructures**, while preserving the core principles of U.S. securities regulation based on the following tenets.

3.1 Technological Neutrality

The SEC should continue to apply existing securities laws based on the **economic substance of the instrument**, not the technology used. If a digital token represents a bond, equity, or derivative by conferring rights and obligations similar to traditional securities, it should be regulated accordingly, regardless of whether it exists on a blockchain or in a traditional form. This principle ensures that investor protections remain intact while allowing market infrastructure to evolve. Adopting technology-neutral definitions helps avoid regulatory arbitrage and provides a consistent, predictable framework for market participants. Such an approach also supports innovation by allowing the industry

to develop and deploy new technologies without fear of triggering unintended regulatory consequences solely due to the format of issuance or transaction.

3.2 Equivalence of Automated Compliance

Many public, permissionless infrastructures enable automated, programmatic compliance tools, allowing a more transparent and cost-effective way to fulfil compliance obligations (e.g., smart contract based transfer restrictions, whitelist-based identity controls, on-chain financial disclosure etc.). The SEC should formally **recognize such tools as an option for meeting regulatory requirements and set out clear expectations for their use**.

3.3 Interjurisdictional Coordination and Standard Setters

To support efficient global capital markets and reduce regulatory fragmentation, the SEC should adopt approaches that **permit interoperability across jurisdictions**. In an increasingly digital and borderless financial system, issuers should not be forced to navigate duplicative or conflicting compliance regimes in every jurisdiction where a token might circulate. To facilitate this, the SEC should collaborate with international standard setters (e.g., IOSCO, BIS) and with peer regulators (e.g., the UK's Financial Conduct Authority), the Monetary Authority of Singapore, or the Swiss Financial Market Supervisory Authority) to establish **common definitions, functional categories, and baseline compliance requirements for tokenized assets**. The SEC has an opportunity to take the lead in international coordination to reduce compliance friction and encourage responsible growth in blockchain asset markets.

4 Staking

Staking is a critical component of "proof of stake" blockchain networks, including Cardano. Staking incentivizes participation in so-called consensus, helps to secure the network, and acts as an anti-spam mechanism (see more details below). Each of these help **public, permissionless proof-of-stake infrastructures to function safely and reliably**. Holders of a proof-of-stake network's native blockchain asset that "stake" their assets are rewarded for doing so through automated, programmatic emissions of more of the same assets in accordance with incentive rules in-built into the infrastructure.

Public, permissionless Layer 1 blockchain networks, such as Cardano, rely on a consensus mechanism that allows node operators running the network software to agree on which data is added to the blockchain. This data is recorded in a sequence of linked, batched records known as "blocks". To ensure the majority of operators provide sound data, operators must receive a delegation of native blockchain assets to participate in consensus. Users that hold an amount of the blockchain asset native to the infrastructure—such as ADA for Cardano—can stake that asset with a validator node. In Cardano, the mechanism selects validators to produce new blocks and confirm transactions based on

the amount of ADA they have committed to their own node or received from third parties. Delegations are done by committing the assets to a validator node, with the assets remaining fully available to the delegating user to spend (i.e., no transfer of control of the assets occurs and there is no lock-in or slashing risk). The staking incentives that are distributed are derived from global transaction fees and, in the current phase of the infrastructure, additional ADA created through monetary expansion from an automated, programmatic reserve. In Cardano's case, these and other mechanisms have resulted in an infrastructure that has had no downtime since 2017 and proven its resilience over time.

As illustrated above, staking is a critical component of transaction validation in proof of stake infrastructures. Participation in staking through delegation such as in Cardano amounts to participating and securing the infrastructure for a reward provided by the infrastructure directly with no intermediary. This activity should **not be treated as an investment contract arrangement**. Similarly, validator node operators that receive delegation of assets should **not be treated as investment contract issuers**. Instead, they should be seen as **performing administrative functions** that facilitate participation in the process, similar to recent guidance from the Division of Corporation Finance regarding mining pool operators in proof of work networks.

5 Custody

Traditional financial market custody is dominated by the use of centralized systems where assets are held in digital (or, decreasingly, physical) form by reputable financial institutions or financial market infrastructure providers. These systems use legacy IT infrastructures and benefit from long-established regulatory frameworks that provide clear rules. Security measures for this kind of custody often include a combination of physical security, internal controls, audits, and insurance.

In contrast, blockchain assets, like stablecoins, that are not Intrinsic Securities or Intentional Securities, operate in a different paradigm, where the **assets themselves exist in a mostly decentralized framework on the public, permissionless infrastructure**, generally in the form of tokens. Control over the blockchain assets is tied to **cryptographic private and public keys**. Handling these keys safely requires the integration of software and hardware wallets and multi-signature systems, among other elements. In a nutshell, the security paradigm for blockchain assets is quite different, as lapses in key security can lead to definitive losses due to the generally irreversible nature of blockchain transactions.

The current lack of regulatory clarity in the U.S. applicable to the custody of private keys creates a level of uncertainty that is not typically present in traditional asset management and contributes to an uneven playing field among market participants. Current regulatory requirements are largely designed around traditional financial asset custody. These frameworks assume that custodians have direct, (sometimes physical) oversight over assets or the ledgers on which those assets are maintained and, for instance, can make changes to that ledger if instructed to do so. In contrast, blockchain assets exist on blockchain infrastructures and are controlled through key pairs, rather than through traditional

intermediaries. This difference presents regulatory challenges because many of the **conventional safeguards and oversight mechanisms do not easily translate to an environment where assets are not ultimately accounted for and controlled by one central authority**. The SEC should strive to **review and amend any custody related rules** that are predicated on the intermediated custody paradigm while creating certainty for market participants on the required safeguards that should apply to custodians of blockchain asset keys. Further, for the emerging sector of Intrinsic and Intentional Securities that generally rely on a system of whitelisted addresses permitted to hold the relevant blockchain assets, additional guidance needs to be provided.

6 Outsourcing to a Public, Permissionless Infrastructure

Outsourcing plays a crucial role in enabling financial institutions to manage operational and technological risks effectively by leveraging specialized external infrastructure and expertise. In this context, the ability to rely on diverse infrastructure models—including public, permissionless blockchain infrastructures like Cardano—is essential to enhance resilience, reduce single points of failure, and avoid harmful dependencies on a small number of dominant providers. A regulatory approach that is too narrowly defined risks excluding entire categories of innovative infrastructure. This not only undermines institutions' ability to tailor their risk mitigation strategies but also entrenches systemic vulnerabilities by restricting competition and architectural diversity.

Public, permissionless systems like Cardano are engineered to operate without a single controlling entity. Instead, they distribute infrastructure responsibilities across globally dispersed participants who follow an open protocol. Because these systems lack a single service provider who can enter into a contract or be held liable for network-wide outcomes, they do not fit the mold of traditional outsourcing relationships. We believe that the **current assumptions embedded in traditional outsourcing regulation focus too heavily on centralized, legally identifiable counterparties**, and suggest that the SEC adopts an outsourcing framework for regulated market participants, such as broker-dealers and registered investment advisors, that is **open, technologically neutral, and focused on the functional mitigation of risk**.

Public, permissionless infrastructures provide material benefits, including redundancy, transparency, and reduced single-point-of-failure risks. They can enhance auditability through tamper-proof ledgers and reduce vendor lock-in by virtue of their open-access and open-source design. These systems are maintained collectively by diverse infrastructure operators, such as stake pool operators and open-source contributors, whose distributed roles collectively ensure system reliability and availability. While these benefits are meaningful, public, permissionless infrastructures are also not risk-free. Rather, we propose that their risks differ in nature—and must therefore be addressed through alternative risk mitigation strategies, which we outline in the following.

6.1 Technical Due Diligence Through Infrastructure and Code Review

The first key component is infrastructure design and code base evaluation. In the absence of a central vendor assuming contractual liability, regulated entities must **assess the technological foundations of the system** itself. This includes reviewing the resilience, fault tolerance, and security parameters of the code, and monitoring the system's ongoing performance. Assurance arises not from contractual enforcement, but from verifiable technical characteristics and transparent development processes. Open-source development models allow institutions to independently audit and, if needed, contribute to the infrastructure. Regulators with supervisory authority can periodically evaluate the human and technological capital firms deploy toward making these evaluations and can set minimum standards for these efforts, with disclosures about their efficacy by the regulated firm.

6.2 Collective Assurance and Community Standards

The second component is collective risk assurance. While no single entity operates or controls a public blockchain, key infrastructure participants do exist, including node operators and core developers. These contributors, though not legally liable for the system as a whole, often meet *de facto* operational requirements through the services they provide. Financial institutions may **conduct due diligence on subsets of these contributors—based on reliability, transparency, and adherence to best practices—as a way to manage operational risk**. In practice, infrastructure operators in public systems often run professionalized services subject to reputational constraints and community oversight. Establishing relationships with such contributors, or selecting them based on transparent performance metrics, can create a **collective assurance framework** that approximates traditional vendor risk control without centralization.

6.3 Direct Institutional Participation

The third component is direct institutional participation. **Public, permissionless infrastructures allow and encourage active participation**. Regulated entities can run infrastructure nodes themselves, support network monitoring, or engage in governance, where applicable. This approach offers a high degree of control and visibility, improves operational continuity, and can reduce reliance on third parties altogether. In doing so, institutions not only mitigate risk, but also gain the ability to shape the future trajectory of the infrastructure in line with their regulatory and business objectives. This approach, in fact, mirrors, to some degree, the structure of traditional financial infrastructures, such as SWIFT or clearing facilities like the DTCC or Euroclear, which operate on a member-governed basis. In both cases, **participating institutions collectively contribute to the operation, governance, and oversight of the infrastructure, ensuring its reliability and aligning it with shared standards and requirements**.

Together, these approaches represent a proportionate and effective alternative to traditional third-party outsourcing models. They align risk management practices with the technical realities of distributed

systems and uphold the principles of operational resilience, security, and accountability. Importantly, they do so without requiring systemic compromise or dilution of regulatory objectives.