Teresa Goody Guillén, *Esq.*, MBA

BY ELECTRONIC SUBMISSION

January 26, 2026

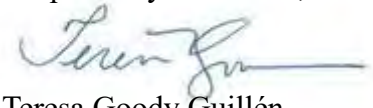
SEC Crypto Task Force
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549-0213

Dear Members of the Task Force,

I am writing in response to the letter from Ripple dated January 9, 2026 ("Ripple Letter")[1] to clarify references to one of my publications on digital asset market structure. I sincerely appreciate Ripple's thoughtful engagement with my work and commend their commitment to constructive dialogue. I agree with Ripple's assertion that "[f]rameworks suggesting that a 'passive economic interest' alone could trigger securities laws mistakenly conflate speculation with investment rights,"[2] and I clarify that the citation to my paper after that proposition is not as an example of a framework making such a conflation. Rather, when discussing economic abstraction factors, my paper specifically states: "These factors should be considered on a sliding scale in which no single factor is determinative."[3]

For further context, I have annexed to this letter the proposed market structure legislation, a speech delivered at Carnegie Mellon explaining the underlying rationale of my approach, a summary of the evolving methodology, the essential revisions to current legislative proposals cited by Ripple, and the initial paper outlining the general approach to creating regulatory frameworks based on historical practice.[4]

Respectfully submitted,



Teresa Goody Guillén

---

[11] Ripple letter to U.S. Securities and Exchange Commission Crypto Task Force (Jan. 9, 2026), available at https://www.sec.gov/files/ripple-letter-crypto-task-force-010926.pdf.

[2] *Id.* at 3.

[3] *See* Goody Guillén, Teresa, "Essential Revisions to Strengthen Digital Asset Market Structure Proposals, Prevent Market Failure, and Ensure Securities Law Consistency" (Sept. 7, 2025), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5458774.

[4] *Id.*; Goody Guillen, Teresa, Measure Twice: Designing Trust for the Algorithmic Age (October 08, 2025). Available at SSRN: https://ssrn.com/abstract=5621370 or http://dx.doi.org/10.2139/ssrn.5621370; Goody Guillen, Teresa, A Framework for Regulating Programmable Digital Asset Markets (October 08, 2025). Available at SSRN: https://ssrn.com/abstract=5621450 or http://dx.doi.org/10.2139/ssrn.5621450; Goody Guillen, Teresa and Corbett Sterling, Isabelle, Paving the Path for Crypto Clarity: A Framework for Digital Asset Regulatory Structure: Discussion Draft (February 17, 2025). Available at SSRN: https://ssrn.com/abstract=5156725 or http://dx.doi.org/10.2139/ssrn.5156725.

ATTACHMENTS

1. Digital Markets Restructure Act of 2026
   Discussion Draft

2. Measure Twice: Designing Trust for the Algorithmic Age
   (October 08, 2025)

3. A Framework for Regulating Programmable Digital Asset Markets (October 08, 2025)

4. Essential Revisions to Strengthen Digital Asset Market Structure Proposals, Prevent Market Failure, and Ensure Securities Law Consistency (Sept. 7, 2025)

5. Paving the Path for Crypto Clarity
   A Framework for Digital Asset Regulatory Structure
   Discussion Draft (February 17, 2025)

ATTACHMENT 1

Teresa Goody Guillén

Discussion Draft

Digital Markets Restructure Act of 2026

119TH CONGRESS
1ST SESSION

S. ____

To establish a uniform Federal framework for the issuance, trading, custody, and supervision of digital assets and Digital Value Instruments; and for other purposes.

IN THE SENATE OF THE UNITED STATES

_____ introduced the following bill; which was read twice

and referred to the Committee on _____.

A BILL

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS

(a) This Act may be cited as the "Digital Markets Restructure Act of 2026."
(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SECTION I. SHORT TITLE; TABLE OF CONTENTS
TITLE I. FINDINGS; PURPOSE; DEFINITIONS
TITLE II. RISK-BASED CLASSIFICATION AND JURISDICTION
TITLE III. UNIFIED REGISTRATION AND FEDERAL PREEMPTION
TITLE IV. LEAD SUPERVISOR AND ROTATION MODEL
TITLE V. DISCLOSURE AND MARKET INFRASTRUCTURE
TITLE VI. INNOVATION EXEMPTION
TITLE VII. AMENDMENTS TO THE SECURITIES ACT OF 1933 AND THE SECURITIES EXCHANGE ACT OF 1934
TITLE VIII. AMENDMENTS TO THE COMMODITY EXCHANGE ACT
TITLE IX. RESIDUAL-RISK ASSESSMENT MODEL
TITLE X. TECHNOLOGICAL EQUIVALENCE AND DIGITAL IDENTITY
TITLE XI. ENFORCEMENT, ANTI-OBSTRUCTION, AND JUDICIAL REVIEW
TITLE XII. IMPLEMENTATION AND REPORTING
TITLE XIII. EFFECTIVE DATE AND TRANSITION

This draft was prepared primarily by Teresa Goody Guillén, with input and editorial contributions from generous others. It seeks to synthesize concepts articulated in public statements by SEC Chairman Atkins, CFTC Chairman Selig, and SEC Commissioner Peirce, as understood by the author. None of these individuals has approved this document, nor confirmed that the views expressed herein accurately reflect their positions. The approach is a principles-based legislative framework, reserving more granular—though still principles-based—regulatory requirements to the Securities and Exchange Commission and the Commodity Futures Trading Commission. This goal is adaptability over time, enabling regulatory evolution in response to market and technological developments without requiring repeated statutory amendment or stifling future innovation pending statutory amendment, which facilitates a future-proof regulatory regime.

TITLE I — FINDINGS; PURPOSE; DEFINITIONS

SEC. 101. FINDINGS.

Congress finds the following:

1. Digital assets, financial instruments, commodities, and other economic interests existing or transferable in electronic form are predominantly interstate in character and affect interstate commerce.
2. Federal and State statutes governing securities, derivatives, and commodities were enacted prior to the widespread use of electronic and distributed systems for the issuance, trading, custody, and settlement of such instruments.
3. The technological development of digital assets has enabled financial instruments to comprise a combination of characteristics of securities, commodities, and/or derivatives. As a consequence, some digital assets cannot be defined as solely a security, commodity, or derivative, rendering regulation by this classification inaccurate and ineffective.
4. Digital assets that combine characteristics of securities, commodities, and/or derivatives possess a risk profile that is not addressed by the regulation for these classifications, and doing so would impede fair and efficient markets. Instead, these instruments that separate economic exposure from meaningful control or enforceable recourse modularize the rights capable of being combined into a single asset and require similar flexible modular regulatory treatment to be fit-for-purpose.
5. Fragmented and overlapping jurisdiction among Federal and State regulators has resulted in impractical and inefficient regulatory requirements that prevent use of the technology, as well as duplicative registration, inconsistent supervision, regulatory arbitrage, and uncertainty that undermines investor protection and market integrity.
6. Advances in electronic and cryptographic systems permit verification of ownership, integrity of records, and compliance with regulatory objectives through functionally equivalent means that do not depend on physical instruments and current regulatory intermediation requirements.
7. A uniform Federal framework grounded in economic substance and residual risk will promote responsible innovation, protect market participants, and strengthen the competitiveness of United States financial markets.
8. Prior statutory classifications were framed for instruments whose economic characteristics, control rights, and settlement mechanics were ordinarily bundled in a single form; digital and programmable instruments may unbundle such attributes, and effective market correction and supervision therefore requires modular regulation keyed to residual enterprise, exposure, and market risks rather than to labels or technological form.

SEC. 102. PURPOSES.

The purposes of this Act are—

1. to establish a uniform Federal framework for the registration, supervision, and trading of certain digital assets and Digital Value Instruments;[1]
2. to allocate regulatory authority between the Securities and Exchange Commission and the Commodity Futures Trading Commission based on the predominant economic risks presented by such instruments and activities;
3. to preempt inconsistent State or territorial laws that would otherwise regulate the issuance, trading, custody, or transfer of Digital Value Instruments by federally regulated persons, including registered and some exempted persons;
4. to modernize the application of the Federal securities and commodities laws to electronic and digital market infrastructure, including spot markets, trading facilities, and clearing arrangements; and
5. to recognize functionally equivalent technological and privacy-preserving methods of compliance consistent with Federal law.
6. to require that regulation under this Act be applied according to the predominant residual enterprise, exposure, or market risks presented, and not solely by reference to the form, label, or method of recordation of an instrument or transaction.

SEC. 103. DEFINITIONS.[2]

For purposes of this Act:

1. Securities and Exchange Commission.—The term "Securities and Exchange Commission" means the Securities and Exchange Commission.
2. Commodity Futures Trading Commission. — The term "Commodity Futures Trading Commission" means the Commodity Futures Trading Commission.
3. Commissions.—The term "Commissions" means the Securities and Exchange Commission and the Commodity Futures Trading Commission acting jointly under this Act.
4. Prudential Regulator.—The term "Prudential Regulator" means the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, or a State banking or trust-company regulator participating pursuant to a memorandum of understanding authorized under this Act.
5. Digital Asset.— The term "digital asset" means any unit of account, value, or right that exists or is transferable solely in electronic form, whether issued natively or represented electronically, and is not embodied in a physical instrument as such instrument.[3]

[1] NTD. This Act seeks to create definitions that are to be used uniformly across legislation. In later legislation, Congress should update and unify the definition across all federal laws but must rely on the expertise of the agencies, which should be involved early to opine on the accuracy of competing definitions.
[2] NTD. All cross-reference must be checked and confirmed after editing. To solicit input on what portions of this draft should be moved from legislation to interagency and intra-agency rules (which can thereafter be codified if determined legislation of them is needed to protect their integrity and is future-proof.
[3] NTD. Cannot use definition from GENIUS Act: "any digital representation of value that is recorded on a cryptographically secured distributed ledger." It defines a technical storage method rather than a legal form of property, the "cryptographically secured distributed ledger" definition both excludes tokenized and future electronic instruments and locks the statute to a specific technology that courts and markets will inevitably outgrow. The use of "property" and "property law" herein is based on the recognition of intangible rights by their enforceability and

6. Digital Value Instrument.—
   The term "Digital Value Instrument" or "DVI" means any digital asset or electronically embodied unit of value or right that confers or represents a financial, economic, or proprietary interest or exposure and is not limited to immediate consumptive use.[4]
7. Economic Abstraction.—The term "economic abstraction" means the separation of economic exposure from meaningful control or enforceable recourse by the holder. Economic Abstraction is deemed to exist when residual risk exists based on enterprise risk, exposure risk, and/or market risk (as these terms are defined below).[5]
8. Residual Risk.—The term "residual risk" means investment, leverage, or market-integrity risk that remains after technological, contractual, or structural mitigation.[6]
9. Enterprise Risk.—The term "enterprise risk" means residual risk arising from agency problems, information asymmetry, or managerial discretion tied to an identifiable enterprise, network, or managerial group.[7]
10. Exposure Risk.—The term "exposure risk" means residual risk arising from synthetic or leveraged exposure to reference assets, rates, or indices.
11. Market risk.—The term "market risk" means residual risk arising from custody, integrity, manipulation, settlement, or operational failure of a trading or settlement facility.[8]
12. Unified Registration Certificate.—The term "Unified Registration Certificate" or "URC" means the Federal registration issued jointly by the Commissions under section 301 authorizing covered activities under this Act.
13. Unified Digital Market Registry.—The term "Unified Digital Market Registry" or "UDMR" means the electronic filing and disclosure system established under section 501.[9]
14. RegNode.—The term "RegNode" means the permissioned audit and supervisory ledger maintained jointly by the Commissions under section 502.[10]

---

transferability rather than physical form, such that electronically embodied units of value or right are property in the same sense as uncertificated securities, book-entry accounts, and choses in action long treated as property. Need to amend GENIUS Act to correct definition.

[4] NTD. Solicit specific input on this proposed language.

[5] NTD. The purpose of this structure is to modularize risk. Because digital assets enable assets to separate functions (and the risks associated with those functions) that were previously inextricably linked, the regulation must now likewise be modularized. Failure to modularize regulation necessarily means that the regulation does not address risks that actually exist, but address some risks that do not exist, and likely do not address risks that exist in a fit-for-purpose/least intrusive means/most effective manner (to correct market failures/misaligned incentives)

[6] NTD. The residual risk requirement is intended to identify the actual risk and whether any regulation is required in the first place, and if so, to identify the type of regulation that is needed. Cybersecurity risk as it is viewed today was not in existence at the time the securities and commodities laws were created. Therefore, that is a risk that will need to be addressed by inclusion of an appropriate federal agency with cybersecurity expertise (potentially by requiring a certification or private/public audit optionality to ensure cybersecurity, or other proposals to be solicited).

[7] NTD. Enterprise risk is intended to capture the securities law risks, not only investment contracts and equity, but also evidence of indebtedness (regulates repayment risk), and voting trusts (regulate control risk), which also are securities as they separate economic interest from either repayment certainty or governance authority.

[8] NTD. These risks are intended to capture the different categories of risks that the Securities and Exchange Commission and Commodity Futures Trading Commission and their regulations are intended to address (to provide guardrails and align incentives).

[9] NTD. This is intended to create a shared registry across Securities and Exchange Commission and Commodity Futures Trading Commission to facilitate trading platforms that list assets regulated by the Securities and Exchange Commission and/or Commodity Futures Trading Commission.

[10] NTD. RegNodes are being considered on an international basis and is a means to enable a more efficient global regulatory approach. RegNodes would enable more reciprocity among regulators, the ability for regulators to access

15. Lead Supervisor.—The term "Lead Supervisor" means the Commission designated as the primary supervisory authority for a registrant pursuant to section 401.
16. Integrated Trading System.—The term "Integrated Trading System" or "ITS" means a multi-asset platform licensed under section 503 that provides retail or institutional users access, through a unified compliance interface, to DVIs regulated under this Act and/or are otherwise digital assets classified as securities, derivatives, and/or digital commodities.[11]
17. Integrated Trading Facility.—The term "Integrated Trading Facility" or "ITF" means a registered facility authorized under section 503 to provide access to trading, execution, custody, and/or settlement of securities, Digital Value Instruments, or digital commodities through a unified compliance framework.[12]
18. Qualified Transaction.—The term "qualified transaction" means any issuance, sale, or transfer of a Digital Value Instrument effected through a URC-registered exchange, alternative trading system, Integrated Trading Facility, or other registered intermediary.
19. Digital Identity Credential.—The term "Digital Identity Credential" means an optional, privacy-preserving credential meeting standards established under section 1003 that may be used to satisfy lawful identification or verification requirements without disclosure of transaction-level data beyond what is necessary for such purpose.[13]
20. Market Structure Coordination System.—The term "Market Structure Coordination System" or "MSCS" means the inter-agency coordination framework established under section 701.
21. Person.—The term "person" means any natural person, corporation, partnership, association, trust, or other legal entity.

TITLE II — RISK-BASED CLASSIFICATION AND JURISDICTION

SEC. 201. RISK-BASED APPLICABILITY.

(a) General Rule.— Any digital asset evaluated under this section that satisfies the criteria herein shall, for all purposes of this Act, be treated as a Digital Value Instrument and subject to the applicable provisions of this Act. A digital asset shall be deemed a Digital Value Instrument (DVI) and subject to regulation under this Act if, in a capital-raising, investment, or secondary-market trading context, it exhibits three or more of the following characteristics:[14]

---

information related to heightened risks for that jurisdiction or a jurisdiction's particular market. There must be limitations on the data that can be accessed and this should not infringe on the privacy rights. Privacy rights must be addressed to ensure that governments are not able to use this mechanism to collect privacy infringing data, or data that impacts national security. This is easily achievable, but must be considered and addressed.

[11] NTD. This is intended to codify Chairman Atkins' Super-App concept.

[12] NTD. This distinguishes between an Integrated Trading System (which is intended to refer to integration horizontally only, with different types of assets on the same platform), and an Integrated Trading Facility for an Integrated Trading System that is also vertically integrated (similar to how most crypto exchanges operate today).

[13] NTD. Solicit specific input on this requirement and how it can be best achieved. This is critical to enable a workable system that is internationally competitive and protects privacy. This is a key to solving regulatory issues related to bearer instruments and decentralized finance.

[14] NTD. Solicit input on the most appropriate combination of factors and meaningfulness required to warrant regulation under this Act (that is, by the Commodity Futures Trading Commission and/or Securities and Exchange Commission). Assets not triggering this test would not be regulated by the Securities and Exchange Commission

1. Transferability.—The instrument is freely transferable or assignable on secondary markets, including on trading systems or trading facilities.
2. Passive Economic Interest.—The holder bears enterprise-level, network-level, or system-level risk without possessing meaningful operational control or managerial control.
3. Limited Individual Enforcement.—The holder lacks individualized contractual rights to compel performance or obtain recourse, other than through shared code-based, protocol-based, or governance mechanisms.
4. Systemic Dependency.—The instrument's value depends materially on managerial, coordinated, or technical execution by an identifiable enterprise, protocol sponsor, foundation, or managerial group.
5. Limited Collective Action.— lack practical ability, individually or collectively, to oversee, replace, or discipline the persons or systems materially affecting the instrument's value or operation.

(b) Presumption.—An instrument that satisfies the conditions of subsection (a) shall be presumed to present residual risk requiring regulation under this Act, unless the issuer or operator demonstrates by clear and convincing evidence that the instrument is used solely for immediate consumptive purposes.

(c) Ongoing Application.—Applicability under this section shall be determined on a continuing basis. Changes in risk characteristics shall be reflected in classification and jurisdiction as provided in this title and recorded in the RegNode.

SEC. 202. CLASSIFICATION BY RESIDUAL RISK.

(a) Risk categories.[15]—Regulatory oversight shall correspond to the predominant residual risk presented by a DVI or related activity as follows:

1. Enterprise Risk.—Residual risk arising from agency problems, information asymmetry, governance discretion, or managerial control associated with an identifiable enterprise, network, or coordinating group shall fall within the jurisdiction of the Securities and Exchange Commission.

---

and/or the Commodity Futures Trading Commission. These factors are intended to identify the risks that underlie the creation of the securities and commodities/derivatives laws (i.e., the reasons the laws exist and their intended purpose/market correction). This Act is based on the reality that a derivative is a umbrella concept that includes futures and other specific derivative structures, and considered a financial contract regulated because it references a commodity (the commodity being the underlying good/statutory category.

[15] NTD. These concepts build on the frameworks and approaches developed by Adolf Berle. *See* Goody Guillén, Teresa, Measure Twice: Designing Trust for the Algorithmic Age (October 08, 2025), available at SSRN: https://ssrn.com/abstract=5621370 or http://dx.doi.org/10.2139/ssrn.5621370; *see also* Goody Guillén, Teresa, A Framework for Regulating Programmable Digital Asset Markets (October 08, 2025). Available at SSRN: https://ssrn.com/abstract=5621450 or http://dx.doi.org/10.2139/ssrn.5621450; Goody Guillén, Teresa, Essential Revisions to Strengthen Digital Asset Market Structure Proposals, Prevent Market Failure, and Ensure Securities Law Consistency (September 07, 2025). Available at SSRN: https://ssrn.com/abstract=5458774 or http://dx.doi.org/10.2139/ssrn.5458774; *see generally* Goody Guillén, Teresa and Corbett Sterling, Isabelle, Paving the Path for Crypto Clarity: A Framework for Digital Asset Regulatory Structure: Discussion Draft (February 17, 2025). Available at SSRN: https://ssrn.com/abstract=5156725 or http://dx.doi.org/10.2139/ssrn.5156725.

2. Exposure Risk.—Residual risk arising from synthetic, leveraged, or derivative exposure to reference assets, rates, indices, or economic variables shall fall within the jurisdiction of the Commodity Futures Trading Commission.
3. Market Risk.—Residual risk arising from custody, settlement, integrity, manipulation, surveillance gaps, or operational failure of a trading or settlement facility shall be subject to joint oversight by the Commissions.

(b) Hybrid Classification.[16]—Where measurable residual risks are materially present across more than one category, the instrument shall be treated as a hybrid instrument and subject to coordinated supervision as provided by rule.

(c) Predominant Risk Standard.—In the event of ambiguity, the category carrying the highest measurable residual-risk score shall determine jurisdiction subject to election or rotation as provided in this Act.[17]

(d) Prudential carve-out.—When a Digital Value Instrument is issued by, or fully backed by, a prudentially supervised depository institution, solvency and safety-and-soundness oversight shall remain with the appropriate Prudential Regulator, while market conduct and disclosure obligations shall be governed by this Act only to the extent the Commissions jointly conclude that prudential regulation is inadequate for the residual risk profile of the assets.[18]

SEC. 203. ADJUSTMENT OF JURISDICTION AND SUPERVISORY DESIGNATION.

(a) Adjustment.—When the predominant residual-risk profile of an instrument or registrant changes, supervisory designation shall adjust accordingly as provided under this Act.

(b) Record and notice.—Any adjustment shall be time-stamped and recorded in the RegNode set forth in Section 502, with notice provided promptly to the affected registrant.

(c) Continuity.—Upon adjustment, existing registrations, exemptions, and approvals shall remain effective unless expressly modified or revoked.

[16] NTD. Recommended that the legislation is more broad strokes with minimal prescriptive rules (otherwise it will not be nimble to be future-proof) and the agencies enter a Memorandum of Understanding (MOU)/MSCS. Congress can codify parts of the MOU if appropriate. The hybrid definition for the MOU would solicit input on a proposal, such as: A DVI exhibiting residual-risk scores within ± 0.10 parity across two or more categories shall be deemed a hybrid DVI and subject to joint supervision unless and until one residual-risk score exceeds the others by 0.15." As a reminder, a minimum of three factors must be triggered for any regulation under this Act.

[17] NTD. This provides options for the regulated to choose their regulator/competition among regulators among federal agencies/federal vs state/ among states. If a regulator goes rogue, then the market can correct by choosing a different regulator. This can borrow from the banking regulatory model with a lead supervisory regulator.

[18] NTD. To solicit input, specifically by crypto industry participants who would be impacted by this requirement, which must be tailored appropriately. The banking rules are not applicable as is to this technology, and must be modified to be fit-for-purpose. Regulations that are not modified for technology do not address the true risks, and may be arbitrary and capricious as they address risks that do not exist/are not applicable due to the technology.

SEC. 204. CONSUMPTIVE-USE EXCLUSION.

(a) In general.—A digital asset used solely for immediate consumptive use and not priced or marketed by reference to enterprise value or performance shall not be treated as a Digital Value Instrument under this Act, regardless of whether it operates in an open or closed system or a secondary market exists for the digital asset.

(b) Hybrid Assets.—The exclusion does not a apply to hybrid digital assets that possess a consumptive use as well as residual enterprise, exposure, and/or market risk.

SEC. 205. YIELD NEUTRALITY FOR STABLE VALUE INSTRUMENTS

(a) Non-Exclusivity of Yield.
Notwithstanding any other provision of Federal or State law, the payment, distribution, or attribution of yield, interest, rewards, or other economic return on a stablecoin, payment stablecoin, or digital asset designed to maintain a stable value relative to a fiat currency shall not be limited to, conditioned upon, or reserved for issuance by an insured depository institution or affiliate thereof.

(b) Permissible Yield by Registered Non-Bank Entities.
Any person holding a valid Unified Registration Certificate under this Act may offer, distribute, or facilitate yield on a stablecoin, provided that—

1. the stablecoin and any associated yield mechanism are fully disclosed through the Unified Digital Market Registry;
2. the source of such yield is clearly identified as arising from reserve management, permitted asset backing, market activity, protocol operation, or other disclosed mechanism;
3. the stablecoin and yield mechanism are subject to classification and supervision under the Residual-Risk Assessment Model established by this Act; and
4. no representation is made that such yield is insured, guaranteed, or backed by the United States or any insured deposit guarantee scheme, unless such insurance scheme exists.

(c) No Deposit Classification by Yield Alone.
The offering of yield, interest, rewards, or other economic return on a stablecoin shall not, by itself, cause such stablecoin to be deemed a deposit, bank account, or banking product under the Federal Deposit Insurance Act, the National Bank Act, or any other Federal or State banking law.

(d) Functional Regulation.
Stablecoins and associated yield mechanisms shall be regulated exclusively according to their predominant residual-risk profile under this Act, including enterprise risk, exposure risk, and market risk, and not according to the charter status of the issuer.

(e) Preemption and Supersession.
This section supersedes and preempts any provision of Federal law enacted before the date of

enactment of this Act—including the GENIUS Act or any successor legislation—to the extent such provision would—

1. restrict the payment of yield on stablecoins to insured depository institutions;
2. condition stablecoin yield on bank charter status; or
3. impose bank-exclusive privileges with respect to stablecoin issuance, reserve management, or economic return.

(f) Rule of Construction.
Nothing in this section shall be construed to—

1. require the payment of yield on any stablecoin;
2. prohibit prudential regulation of insured depository institutions; or
3. limit the authority of the Commissions to restrict, condition, or prohibit specific yield mechanisms that materially increase residual risk under this Act.

SEC. 206. INTEGRITY AND SECURITY OF DIGITAL ASSETS AND DIGITAL VALUE INSTRUMENTS.

A Digital Value Instrument subject to this Act shall be created, recorded, or transferred through an electronic system providing integrity and authenticity sufficient to prevent unauthorized creation, alteration, or duplication in the ordinary course of operation.

The use of cryptographic or functionally equivalent mechanisms shall satisfy this requirement so long as such mechanisms provide reasonable assurance in light of prevailing technological capabilities.

TITLE III — UNIFIED REGISTRATION AND FEDERAL PREEMPTION

SEC. 301. MARKET STRUCTURE COORDINATION SYSTEM.

(a) Establishment.—There is established a Market Structure Coordination System (MSCS) to ensure interoperability of supervision among the Securities and Exchange Commission, the Commodity Futures Trading Commission, prudential regulators, and State financial regulators overseeing trust or money-transmission entities.

(b) Functions.—The MSCS shall—

(1) maintain a Joint Data Registry (Registry) and audit trail accessible to participating regulators;

(2) coordinate examinations to prevent duplication;

(3) harmonize data standards for continuous measurement of enterprise risk, exposure risk, or market risk, as applicable to the DVI and the facilitation of its issuance, offer, listing, matching, executing, clearing, settling, or custody; and

(4) publish technical specifications for machine-readable supervisory reporting.

(c) Integration.—RegNode and the Registry shall be components of the Market Structure Coordination System.

(d) Data sharing.—The Market Structure Coordination System may provide for synchronization of nonconfidential data among the Commissions and participating Prudential Regulators pursuant to written agreements, subject to other provisions of this Act.

(e) Joint Rulemaking.—Within 120 days, the Commissions shall establish a shared registration pathway for entities that list, execute, or clear instruments across multiple regulatory categories.

(f) Access controls.—The Commissions shall, by joint rule, establish access levels for public, supervisory, and confidential information maintained under this title.

(g) Mutual Recognition.—Compliance with joint standards shall be deemed compliance with the Securities Act of 1933, the Securities Exchange Act of 1934, and the Commodity Exchange Act for substantially identical activities.

(h) No Duplicative Registration.—Entities operating under joint registration shall not be required to maintain duplicative licenses or filings with multiple federal agencies for substantially identical activities.

SEC. 302. UNIFIED REGISTRATION CERTIFICATE.

(a) Establishment.—The Securities and Exchange Commission and the Commodity Futures Trading Commission (in this Act referred to collectively as the "Commissions") shall provide for a single Federal registration to be known as the Unified Registration Certificate (in this Act referred to as the "URC").

(b) Who must register.—The Commissions shall, by joint rule, issue a URC to any person that, as a business—

(1) issues, offers, lists, matches, executes, clears, settles, or custodies a Digital Value Instrument; or

(2) otherwise effects, or holds itself out as effecting, transactions in Digital Value Instruments for the account of others.

(c) Effect of URC.—A person holding a URC—

(1) shall be deemed registered under the Federal securities laws and the Commodity Exchange Act to the extent the person engages in the same or substantially identical activities; and

(2) shall not be required to obtain any other Federal or State license, charter, permit, or registration for the activities authorized by the URC, except as the Commissions jointly

determine by rule for prudential safety-and-soundness supervision of insured depository institutions.

(d) Joint rules.—Not later than 180 days after the date of enactment of this Act, the Commissions shall prescribe jointly such rules, forms, and procedures as are necessary to carry out this section.

(e) Transition.—A person registered under Federal law on the date of enactment of this Act and engaged in activities covered by this section shall be deemed to hold a provisional URC for 1 year, subject to conversion or renewal under joint rules.[19]

SEC. 303. LEAD SUPERVISOR; ELECTION IN PARITY; LIMITATION ON DESIGNATION.

(a) General rule.—Each URC registrant shall have one Commission designated as Lead Supervisor under this Act, based on the predominant residual risk category assigned under this Act, with the assessment methodology to be established by joint rule.

(b) Election.—If the registrant's residual risk assessment, as determined by the Commissions, are within the parity threshold established by joint rule, the registrant may elect either the Securities and Exchange Commission or the Commodity Futures Trading Commission to serve as Lead Supervisor for a term established by joint rule.

(c) Procedure.—An election under subsection (b) shall be made by filing such notice as the Commissions prescribe, and shall take effect upon recordation in RegNode.

(d) Secondary authority preserved.—The non-lead Commission shall retain authority to enforce Federal antifraud, anti-manipulation, and market-integrity provisions within its jurisdiction, and shall have reciprocal access to supervisory information subject to sections 505 and 506.

(e) Limitation on designation.—Neither Commission may designate itself as Lead Supervisor contrary to the residual-risk classification recorded under this Act, except—

(1) pursuant to a registrant election under subsection (b); or

(2) pursuant to a joint order of the Commissions issued under section 403(c).[20]

SEC. 304. FEDERAL PREEMPTION OF STATE LAW; SAVINGS CLAUSE.

(a) In general.—This Act and the regulations issued hereunder supersede and preempt any State law, regulation, order, or requirement that, as applied to a URC registrant or to a qualified instrument or transaction—

[19] NTD. To include a time-limited coverage for persons who have been unable to register under any Securities and Exchange Commission/Commodity Futures Trading Commission provision (e.g., exchanges).
[20] NTD. Coordinate this provision with 203(a).

(1) requires licensing, registration, bonding, net worth, examinations, reports, approvals, or operational conditions with respect to the issuance, offer, sale, exchange, custody, settlement, transfer, or administration of a Digital Value Instrument;

(2) treats any such activity as money transmission, virtual-currency business, trust-company activity, or other financial licensing category; or

(3) imposes a securities or commodities qualification, merit review, or filing requirement upon an instrument or transaction governed by this Act.[21]

(b) Money Transmission Preemption.—A qualified transaction conducted by, through, or with a URC registrant shall not be deemed money transmission under the law of any State solely because value is received, held, transmitted, or made transferable in connection with such transaction.

(c) Covered instruments and transactions.—No State may apply its securities or commodities laws to a qualified transaction occurring on a facility or intermediary registered under this Act.

(d) Savings clause.— Nothing in this section shall be construed to impair the authority of any State to enforce generally applicable antifraud or consumer-protection statutes that—

(1) do not impose licensing, registration, money transmitter, ancillary asset, capital, custody, margin, financial responsibility, recordkeeping, bonding, financial operational reporting, any other regulatory requirement or substantive supervisory obligations inconsistent with this Act or subject to this Act or the federal securities, commodity, derivatives, or banking laws; and

(2) are applied in a manner that does not discriminate against Digital Value Instruments or URC registrants.

(e) State participation by agreement.—A State regulator may participate in information sharing or coordination with the Commissions pursuant to a written agreement, but such participation shall not create, expand, or preserve any State licensing authority over URC registrants or qualified transactions.

(f) Privacy construction.—No State may require a URC registrant to collect or report transaction-level identity or spending information in a manner inconsistent with this Act.

(g) Rule of construction.—For the avoidance of doubt, Congress intends by this section to occupy the field of registration, licensure, and substantive supervision of Digital Value Instruments, issuers, exchanges, custodians, and intermediaries thereof. Any State or territorial law inconsistent with this Act is hereby preempted and of no force or effect.

[21] NTD. The state money-transmission licenses will remain an alternative regime. State regulatory regimes are not preempted to the extent that the federal government has not opined (exercised jurisdiction or taken the position that it does not have jurisdiction (i.e., a state government cannot deem an instrument a DVI if the federal government has already taken the position that it is not a DVI).

SEC. 305. NO DUAL-REGISTRATION REQUIREMENT.

(a) Prohibition.—No person registered under this Act shall be required to obtain or maintain separate registration under the Securities Act of 1933, the Securities Exchange Act of 1934, or the Commodity Exchange Act for the same or substantially identical activity.

(b) Conforming interpretation.—Any provision of Federal or State law inconsistent with subsection (a) is hereby superseded to the extent of such inconsistency.

(c) Construction**.**—Nothing in this section limits the authority of the Securities and Exchange Commission or the Commodity Futures Trading Commission to require additional registration for materially different activities outside the scope of the URC, as determined by joint rule.

SEC. 306. RULES OF CONSTRUCTION.

(a) Preservation of enforcement authority.—Nothing in this title shall limit or otherwise affect the ability of the Securities and Exchange Commission, the Commodity Futures Trading Commission, or any other Federal agency to bring enforcement actions under existing antifraud, anti-manipulation, or anti-money-laundering statutes subject to the precondition that the Lead Supervisor has not initiated an investigation or enforcement action based on the same conduct or nucleus of operative facts.[22]

(b) No implied State authority.—The absence of express Federal regulation of a particular DVI activity under this Act shall not be construed to permit State regulation of such activity.

(c) Continuity of prior rights.—All rights, obligations, and contracts valid under prior law shall remain valid and enforceable except to the extent inconsistent with the express preemption of this title.

(d) Technological Form.—Nothing in this Act shall be construed to classify a digital asset or Digital Value Instrument as a security, derivative, or commodity solely by reason of its electronic form or method of recordation or transfer.

(e) Privacy.—Nothing in this title authorizes general collection, retention, or disclosure of transaction-level identity or spending data beyond what is permitted under section 509.

TITLE IV — LEAD SUPERVISOR AND ROTATION MODEL

SEC. 401. LEAD SUPERVISOR FRAMEWORK.

(a) In general.—The Securities and Exchange Commission and the Commodity Futures Trading Commission shall coordinate supervision of persons and facilities registered under this Act through a Lead Supervisor framework.

[22] NTD. Solicit specific input on this proposed language.

(b) Designation.—The Lead Supervisor for each URC registrant shall be determined by the registrant's predominant residual-risk category as recorded under this Act and shall be recorded in RegNode.

(c) Duties.—The Lead Supervisor shall—

(1) conduct examinations and supervise compliance under this Act;

(2) serve as the principal supervisory contact for the registrant;

(3) act on applications, interpretations, and approvals as provided by this Act and joint rules; and

(4) coordinate with the non-lead Commission on enforcement and systemic-risk monitoring.

(d) Reciprocal access.—Each Commission shall have timely access to supervisory information necessary to administer this Act, subject to Confidential Supervisory Information protections and the privacy limitations of section 506.

(e) Coordination with prudential regulators.—For a registrant that is also subject to prudential supervision, the Lead Supervisor shall coordinate, as appropriate, to avoid duplicative examinations, provided that nothing in this subsection expands prudential regulator jurisdiction over activities governed by this Act.

SEC. 402. ROTATION; NOTICE EFFECT.

(a) Rotation.—If a residual-risk assessment changes so that a different category becomes predominant, the Lead Supervisor shall change accordingly, as prescribed jointly by the Commissions.

(b) Record and notice**.**—A change under subsection (a) shall be recorded in RegNode and notice shall be provided to the registrant and to both Commissions within the time prescribed jointly by the Commissions.

(c) Continuity.—A change in Lead Supervisor shall not impair the continuing effect of any order, exemption, approval, or interpretation previously issued under this Act, except as modified in accordance with this Act.

(d) Election preserved.—Where parity exists, the registrant may elect a Lead Supervisor under section 302(b) and as prescribed jointly by the Commissions.

SEC. 403. JOINT SUPERVISION; DISPUTE RESOLUTION; REGULATOR CONSTRAINT.

(a) Joint Supervision.—For registrants classified as hybrid under this Act, the Commissions shall conduct coordinated supervision and examinations under joint procedures.

(b) Lead Supervisor designation.—The Commissions shall designate one agency as Lead Supervisor for each joint supervision based on the predominant risk factor for that registrant.

(c) Dispute resolution.—Any jurisdictional dispute between the Commissions concerning classification or Lead Supervisor assignment shall be resolved by joint order within 30 days, and in compliance with the election provisions of this Act. Pending resolution, the existing designation shall remain in effect.

(d) No unilateral override.—Neither Commission may override a residual-risk classification or block a rotation required by this Act except by joint order under subsection (c) or pursuant to judicial review.

SEC. 404. EFFECT OF LEAD SUPERVISOR DESIGNATION.

(a) Primary authority.—The Lead Supervisor shall exercise primary supervisory and enforcement authority with respect to the registrant's activities subject to this Act.

(b) Preservation of secondary authority.—Nothing in this title shall limit the authority of the non-lead Commission to—

(1) bring actions to enforce antifraud, anti-manipulation, and customer-protection provisions of Federal law; or

(2) participate in rulemaking or joint guidance applicable to registrants under this Act.

(c) Privacy.—Supervisory demands for information shall be subject to section 506 and shall be reasonably tailored to the administration of this Act.

SEC. 405. REVIEW AND REPORTING.

(a) Judicial review.—A person aggrieved by a final designation, rotation, or denial of election under this title may petition for review in the United States Court of Appeals for the District of Columbia Circuit within 30 days. Review shall be de novo as to classification and jurisdiction.

(b) Reporting.—Each Lead Supervisor shall report annually to Congress, in such form as the Commissions jointly prescribe, on the operation of the rotation framework, including aggregate statistics on rotations and supervisory actions, consistent with the confidentiality protections of section 505 and the privacy limitations of section 506.

TITLE V — DISCLOSURE AND MARKET INFRASTRUCTURE

SEC. 501. UNIFIED DIGITAL MARKET REGISTRY.

(a) Establishment.—The Commissions shall establish and maintain a public electronic system to be known as the Unified Digital Market Registry (in this Act referred to as the "Registry").

(b) Purpose.—The Registry shall serve as the single Federal system for filings, disclosures, and public access to nonconfidential information required under this Act.

(c) Operation.—The Commissions shall operate the Registry jointly, or through a service provider acting under joint supervision pursuant to a written agreement.

(d) Form of filings.—The Registry shall accept submissions in machine-readable form as the Commissions prescribe by joint rule, and shall make nonconfidential filings available to the public in a reasonable and searchable manner.

(e) Registrant profile.—Each registrant shall maintain a current profile in the Registry containing, at a minimum—

(1) organizational and control information;

(2) material governance and conflict disclosures;

(3) such financial condition, reserve, or solvency attestations as the Commissions prescribe by rule; and

(4) identification of Digital Value Instruments issued, listed, custodied, or otherwise supported by the registrant.

(f) Legal effect.—A filing made through the Registry shall be deemed filed with each Commission for purposes of this Act and for any substantially identical filing obligation under the Federal securities or commodities laws. This does not limit the Commissions abilities to otherwise accept furnished materials, either on an individual basis or the Commissions jointly.

SEC. 502. REGNODE; SUPERVISORY AUDIT LEDGER.

(a) Establishment.—The Commissions shall establish and maintain a permissioned supervisory ledger to be known as RegNode.

(b) Functions.—RegNode shall—

(1) record, in time-stamped form, supervisory actions under this Act, including registrations, examinations, material orders, residual-risk classifications, and changes in Lead Supervisor;

(2) maintain tamper-evident integrity proofs for records and filings made through the Registry; and

(3) provide verifiable audit trails for the Commissions and for auditors designated under this Act, subject to the protections of section 505.

(c) Standards.—The Commissions shall, by joint rule, prescribe technical and operational standards for RegNode sufficient to provide integrity, authenticity, access control, and continuity of operation, taking account of prevailing technological capabilities and known classes of attack.

(d) Official record.—Entries recorded in RegNode, and certified extracts therefrom, shall constitute official records of the United States for purposes of this Act.

SEC. 503. INTEGRATED TRADING SYSTEM LICENSE; INTEGRATED TRADING FACILITY LICENSE.

(a) Establishment.— The Commissions shall jointly establish a license for registered multi-asset trading systems to be known as an Integrated Trading System. The Commissions shall jointly establish a license for registered multi-asset trading systems and custody facilities to be known as an Integrated Trading Facility.

(b) Integrated Trading System.—Scope and Requirements.

(1) An Integrated Trading System may provide, as authorized by its license—

(i) access to the trading of securities, Digital Value Instruments, digital commodities, and digital derivates; and

(ii) clearing, settlement, or transfer services incident to such trading, as the Commissions jointly permit by rule.

(2) Core Requirements.—Each Integrated Trading System shall—

(i) maintain operational resilience, incident-response capability, and reconciliation standards as the Commissions prescribe by joint rule, including attestations where appropriate;

(iii) maintain surveillance and controls reasonably designed to detect manipulation, wash trading, conflicts of interest, and abusive practices; and

(iv) comply with applicable Federal anti-money-laundering and sanctions obligations, as determined under Federal law, and as administered consistent with this Act.

(c) Integrated Trading Facility.—Scope and Requirements.

(1) An Integrated Trading Facility may provide, as authorized by its license—

(i) access to the trading of securities, Digital Value Instruments, and digital commodities;

(ii) custody, clearing, settlement, or transfer services incident to such trading; and

(iii) such payment or transfer functionality as the Commissions jointly permit by rule.

(2) Core requirements.—Each Integrated Trading Facility shall—

(i) segregate customer assets from proprietary assets;

(ii) maintain such reserve, control, and reconciliation standards as the Commissions prescribe by joint rule, including proof-of-reserves or functionally equivalent attestations where appropriate;

(iii) maintain operational resilience and incident-response capability consistent with joint standards adopted under this Act;

(iv) maintain surveillance and controls reasonably designed to detect manipulation, wash trading, conflicts of interest, and abusive practices; and

(v) comply with applicable Federal anti-money-laundering and sanctions obligations, as determined under Federal law, and as administered consistent with section 509.

(d) Preemption.—A person operating an Integrated Trading System or an Integrated Trading Facility in compliance with this Act shall not be required to obtain any State license or authorization as a money transmitter, virtual-currency business, trust company, or similar status solely by reason of activities authorized under this section.

SEC. 504. DISCLOSURE OBLIGATIONS OF REGISTRANTS.

(a) Periodic reports.— Each registrant shall file with the Registry—

(1) an annual statement of financial condition in such form as the Commissions prescribe;

(2) quarterly reports of material changes in risk profile, control, custody arrangements, or conflicts of interest, as specified jointly by the Commissions;[23] and

(3) prompt notice of any material incident affecting custody integrity, operational continuity, or market functioning, not later than such time as specified jointly by the Commissions.

(b) Continuous disclosure.—The Commissions may, by joint action, require more frequent reporting for registrants or facilities that are widely used, systemically significant, or present elevated residual risk.

(c) Safe harbor—Good-faith reliance on the Registry, and on standards adopted under this Act recognizing functional technological equivalence, shall satisfy any substantially identical filing or disclosure requirement under the Federal securities or commodities laws to the extent provided jointly by the Commissions.

[23] NTD. Determine appropriate timing and whether bi-quarterly is more appropriate and consistent with recent Securities and Exchange Commission statements.

SEC. 505. CONFIDENTIAL SUPERVISORY INFORMATION.

(a) Definition.—The term "Confidential Supervisory Information" means examination materials, risk reports, incident reports, and other nonpublic records created or obtained by a Commission in the course of supervision under this Act.

(b) Confidentiality.—Confidential Supervisory Information shall be exempt from disclosure under section 552(b)(8)[24] of title 5, United States Code, and shall not be disclosed except—

(1) to another Federal agency, where necessary to the performance of official duties and subject to equivalent confidentiality protections;

(2) pursuant to lawful process in a particular matter; or

(3) with the written consent of the registrant to whom the information pertains.

(c) Privileges preserved.—Confidential Supervisory Information shall not lose its privileged character by sharing among the Commissions or with a Prudential Regulator pursuant to regulation under this Act.

(d) Improper Use or Disclosure.—The use or disclosure of Confidential Supervisory Information in any manner not authorized by this Act or jointly by the Commissions is prohibited. Confidential Supervisory Information is not subject to disclosure or used in speech or debate, or otherwise protected under any judicial and legislative grant of immunity.

(d) Penalty.—A person who knowingly and willfully discloses Confidential Supervisory Information in violation of this section shall be subject to discipline and, upon conviction, to a fine under title 18, United States Code.[25] No civil or criminal immunity is available for any person who discloses Confidential Supervisory Information under this Act.

SEC. 506. PRIVACY; LIMITATION ON TRANSACTION SURVEILLANCE.

(a) Data minimization.—The Commissions, and any operator of the Registry or RegNode, shall collect, retain, and disclose only such information as is reasonably necessary to administer this Act.

(b) No general transaction-history reporting.—Nothing in this Act shall be construed to require any registrant, facility, or protocol to report to any Government authority the transaction-level history of lawful transfers between noncustodial accounts, except pursuant to lawful process in a particular matter.

[24] NTD. Consider rendering it exempt under (b)(4) or another provision.
[25] NTD. Solicit specific input on this proposed language and whether government employees who act in bad faith would be subject to criminal prosecution.

(c) No centralized identity or spending database.—Nothing in this Act shall be construed to authorize the establishment or maintenance by the Federal Government of a centralized database of individual identity information, wallet identifiers, or transaction histories for persons not subject to an individualized investigation.

(d) Privacy-preserving compliance.—The Commissions shall jointly establish, with the advice of the Secretary of the Treasury shall, permissible compliance methods that demonstrate eligibility, screening, or authorization while minimizing disclosure of personally identifiable information and transaction-level data beyond what is necessary for the compliance purpose.

(e) Construction.—Nothing in this section limits the authority of the United States to obtain information by subpoena, warrant, or other lawful process in a particular investigation.

SEC. 507. INTEROPERABILITY AND TECHNICAL STANDARDS.

(a) In general.—The Commissions shall, in consultation with the Department of the Treasury and relevant Federal agencies, adopt joint standards to promote interoperability of the Registry and RegNode with Federal reporting systems.

(b) Contents.—Such standards may address data formats, taxonomies, interfaces, integrity proofs, version control, and other matters necessary for secure and efficient administration of this Act.

(c) Private standards.—Nothing in this section shall be construed to prevent the use or development of compatible private standards, provided the registrant demonstrates conformance to the joint standards adopted under this Act.[26]

SEC. 508. LEGAL PROTECTIONS FOR REGNODE AND REGISTRY DATA.

(a) Official records.—All entries in the RegNode and all filings in the Registry shall be considered official records of the United States within the meaning of sections 2071 and 2076 of title 18, United States Code.

(b) Tampering.—Whoever knowingly alters, falsifies, or deletes a RegNode entry, a Registry filing, or an integrity proof with intent to impede, obstruct, or influence the administration of this Act shall be punished under section 1519 of title 18, United States Code.

(c) Evidentiary status.—Certified extracts from RegNode or the Registry shall be admissible as prima facie evidence of the matters stated therein.

(d) Limited protection for operators.—A Federal employee or contractor operating RegNode or the Registry in good-faith compliance with this Act and applicable rules shall not be liable in

[26] NTD. These are minimum standards, not maximum standards. To reduce barriers to entry, to the extent feasible, the government should provide options to provide certifications and approval that meet auditing requirements, but also enable market participants to alternatively use certified/registered private third parties to demonstrate compliance with the requisite minimum standards.

damages for acts within the scope of such operation, except for knowing and willful misconduct or recklessness.

TITLE VI — INNOVATION EXEMPTION

SEC. 601. SHORT TITLE; PURPOSE

(a) Short Title.—This title may be cited as may be cited as the "Digital Asset Innovation Exemption Act of 2026."

(b) Purpose.—To permit innovative digital asset projects to raise capital and operate in U.S. markets under a limited exemption, without requiring full securities registration, provided that risk-based disclosures, smart contract constraints, and oversight mechanisms are satisfied.

SEC. 602. INNOVATION EXEMPTION. [27]

(a) In general.—An issuer may rely on the Innovation Exemption if the issuer meets the conditions prescribed in this title and in joint rules adopted by the Commissions.

(b) Eligibility.—To qualify, the instrument and offering shall meet such criteria as the Commissions jointly prescribe, which shall include, at a minimum, criteria addressing—

(1) the capital-raising context and the intended use of proceeds;

(2) disclosure of ongoing financial obligations, to include debt claims or fixed repayment obligations;

(3) disclosure regarding allocation, governance, and treasury or reserve management;

(4) limitations on leverage, synthetic exposure, or materially misleading representations or omissions;

(5) compliance with applicable Federal anti-money-laundering and sanctions obligations, administered consistent with this Act; and

(6) such offering size limits and investor protection conditions as the Commissions jointly determine appropriate.

[27] NTD. Consider any changes needed, such as Securities and Exchange Commission as supervisor given the exemption applies to only securities related risks in capital raising efforts only, at least until the asset launches. Proposed disclosure items are set forth in the Appendix of Goody Guillen, Teresa, Essential Revisions to Strengthen Digital Asset Market Structure Proposals, Prevent Market Failure, and Ensure Securities Law Consistency (September 07, 2025), available at https://ssrn.com/abstract=5458774 or http://dx.doi.org/10.2139/ssrn.5458774.

SEC. 603. DURATION; TERMINATION.

(a) Duration.—An Innovation Exemption shall be time-limited as prescribed by the Commissions and shall not exceed a period specified by the Commissions without renewal.

(b) Early termination.—The Commissions shall prescribe conditions under which the exemption terminates early, including conditions tied to market scale, trading activity, or changes in residual risk.

SEC. 604. INVESTOR PROTECTIONS; COMPLIANCE MECHANISMS.

The Commissions shall jointly prescribe investor protection conditions reasonably designed to address information asymmetry, custody integrity, conflicts of interest, exposure risk, market risk, enterprise risk, and material changes in governance or control. Such conditions may be satisfied through technological or contractual mechanisms, or both, as recognized under this Act.

SEC. 605. DISCLOSURE; TECHNOLOGICAL EQUIVALENCE.

(a) Disclosure.—An issuer relying on this title shall satisfy disclosure obligations through filings in the Registry, in such form and manner as the Commissions prescribe.

(b) Equivalence.—Where a technological mechanism provides functionally equivalent transparency, auditability, or enforcement of conditions required under this title, the Commissions shall recognize such mechanism as satisfying the applicable requirement, as provided by joint rule.

SEC. 606. SUPERVISION; ENFORCEMENT.

(a) Lead Supervisor.—The Lead Supervisor for an issuer relying on this title shall be determined under this Act based on residual risk.

(b) Revocation.—The Commissions may suspend or revoke reliance on this title for fraud, material misstatement, manipulation, or failure to comply with conditions prescribed jointly by the Commissions.

SEC. 607. RELATION TO OTHER LAW.

Nothing in this title limits enforcement under the Federal securities laws, the Commodity Exchange Act, or other applicable Federal law. State law is preempted to the extent provided in this Act.

TITLE VII — AMENDMENTS TO THE SECURITIES ACT OF 1933 AND THE SECURITIES EXCHANGE ACT OF 1934

SEC. 701. AMENDMENTS TO THE SECURITIES ACT OF 1933.

(a) Short Title Reference.

This title may be cited as the "Reclassification Securities Amendments of 2026."

(b) Amendment to Section 2(a)(1). — Definition of "Security."

Section 2(a)(1) of the Securities Act of 1933 (15 U.S.C. 77b(a)(1)) is amended to read as follows (shown in boldface):

"(1) The term 'security' means any note, stock, treasury stock, security future, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a 'security', or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase any of the foregoing**.**

A nonexclusive standard for classifying whether an asset is "in general, any interest or instrument commonly known as a 'security'" is whether the asset constitutes an economic property interest that represents a contribution of capital or enterprise risk to a common enterprise, network, or system, and that confers residual economic exposure to the performance of that enterprise while separating such exposure from meaningful managerial control, governance authority, or individualized contractual enforcement rights sufficient to internalize that risk, as reflected in one or more structural characteristics of economic abstraction, including pro rata participation, passive dependence on the operation or functioning of the enterprise or system, limited individualized enforceability, systemic rather than bilateral dependency, and constrained collective action.[28]

An investment contract[29] is an agreement representing the exchange of:

[28] NTD. This formulation classifies a type of economic property interest based on structural allocation of enterprise-level risk and control, rather than evaluating a transaction or scheme based on purchaser intent, expectations of profit, or reliance on the efforts of others, it operates independently of—and does not define—an investment contract.

[29] The investment contract definition should be revised and codified to make clear that a *quid pro quo* exchange is required. First, there must be the provision of capital or other assets—this constitutes the investment ("*quid*"). Second, there must be a legally recognized right or contractual claim to both another party's future efforts to manage a venture on behalf of the investor, and the proceeds of those obligated efforts (e.g., income, revenue, profit)—this represents legal entitlement ("*quo*"). Third,, there must be (i) information asymmetry between the purchaser and the

(1) capital or other assets by a purchaser, for
(2) a legally cognizable property right or contractual claim to both (a) another party's future efforts to manage a venture on behalf of the investor, and (b) the proceeds of those obligated efforts—whether in monetary profit or other asset(s) or instrument(s), and
(3) when there is (i) information asymmetry between the purchaser on the one hand, and the issuer or promoting party on the other hand, such that the purchaser requires information disclosures to monitor the issuer's and/or promoter's efforts in managing an enterprise or (ii) the investors are unable to meaningfully participate in collective action to exercise meaningful supervisory control over the management of the investment.

(c) Amendment to Section 2(a)(15). This section is replaced in its entirety.

Section 2(a)(15) is amended to read as follows:

"(15) The term 'accredited investor' shall mean—
(A) any natural person who—
(i) attests to an intent to invest in private, exempt securities offering(s);
(ii) completes an investor acknowledgment form comprised of:
(I) an understanding that the investment may be illiquid, risky, and without guaranteed returns; and
(II) a waiver of reliance on wealth as a proxy for sophistication;
(iii) completes a self-certification process or completes a comprehension module provided by the issuer or regulated intermediary;[30]
(B) any person currently defined as an accredited investor under Rule 501(a) of Regulation D;
(C) any person or entity meeting criteria established by the Commission under future rulemaking."

---

issuer/promoter such that the purchaser requires information disclosures to monitor the issuer's/promoter's efforts in managing an enterprise or (ii) collective action problems existing because multiple investors struggle to coordinate their oversight efforts, making it difficult to exercise meaningful supervisory control over the management of the investment. Fourth, there must be an identifiable issuer/promoter who is capable of providing meaningful periodic disclosures (without conflicting with the lawful purpose of the digital asset and associated technology). To solicit input whether this should be in legislation or left to the Securities and Exchange Commission to provide guidance. For purposes of the second part of the third element (also referred to as the fourth element), the characteristic of not being "identifiable" does not include the purposeful obfuscation of control or reckless disregard for legal duties (such as those under tort law, common law, implied warranties, etc.)A digital asset may be a security, categorized as an investment contract; however, a digital asset representing the investment contract is not the subject of the investment contract (e.g., an asset, a venture), nor is it an asset the investor receives as proceeds from the investment opportunity (e.g., an asset, profit). Although the subject of an investment contract or the proceeds of an investment contract may itself be a security (including a digital asset that is a security, whether an investment contract or other type of security).

[30] NTD. The unfair exclusion of persons from financial markets based on wealth must be changed. Alternative, unobservable financial markets will inevitably be created in response to unfairness. This is intended to allow investors to request brief educational materials on securities investment. This may be best provided by the Securities and Exchange Commission through its investor education resources.

The Securities and Exchange Commission shall revise applicable rules under Regulation D within 180 days of enactment to conform with the amended definition of 'accredited investor."

(d) Amendment to Section 3(b)(2).

Section 3(b)(2) (15 U.S.C. 77c(b)(2)) is amended —

1. by striking "$75,000,000" and inserting "$150,000,000 in the case of a Digital Value Instrument offering qualified through the Unified Digital Market Registry,"; and
2. by inserting after "offering statement filed with the Commission" the following: ", or filed jointly with the Commissions through the Unified Digital Market Registry under the Digital Markets Restructure Act of 2026,".

(e) Amendment to Section 4.

The SEC may exempt any person or group thereof, any transaction or group thereof, from any condition or requirement under this Section 4 to facilitate crowdfunding as technology, instruments, and markets change.

(f) Technical and Conforming Amendments.

Wherever appearing in the Securities Act of 1933, the phrase "this Act" shall be deemed to include reference to the Digital Markets Restructure Act of 2026 with respect to Digital Value Instruments.

SEC. 702. AMENDMENTS TO THE SECURITIES EXCHANGE ACT OF 1934.

(a) Amendment to Section 3(a)(10) — Definition of "Security."

Section 3(a)(10) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(10)) is amended to read as follows (with insertions in boldface and deletions in strike-through):

"(10) The term 'security' means any note, stock, treasury stock, security future, bond, debenture, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, or, in general, any instrument commonly known as a 'security'; or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing.

For the avoidance of doubt, the determination of whether an instrument constitutes a security shall be based on its economic substance and trading venue and not on its technological medium of recordation."

(b) Amendment to Section 3(a)(77). — Definition of "Alternative Trading System."

Section 3(a)(77) (15 U.S.C. 78c(a)(77)) is amended by adding at the end the following:

"The term includes any trading facility that lists or matches orders in Digital Value Instruments registered under the Digital Market Restructure Act of 2026, whether or not such facility is otherwise subject to Regulation ATS as in effect on the date of enactment of such Act."

(c) Amendment to Section 5.

(1) Section 5 (15 U.S.C. § 78e) is amended by adding the following new subsection:

> (f) Notwithstanding subsections (a) through (d), a digital asset that qualifies for exemption under Section 4(a)(6), 4(a)(7), or Regulation A of the Securities Act of 1933, and is issued in compliance with applicable obligations for disclosure, and smart contract or other mechanism deemed acceptable by the Commissions,[31] may be traded on a registered Digital Crowdfunding Portal (DCP), any trading facility that lists or matches orders in Digital Value Instruments registered under the Digital Markets Restructure Act of 2026, or any trading system, as defined jointly by the SEC and CFTC, without being listed on a national securities exchange.

(2) The Securities and Exchange Commission shall issue implementing regulations to define bearer digital instruments that, if meeting registered or exempt criteria, may trade on DCPs or any trading systems, as specified by the Securities and Exchange Commission or jointly by the Securities and Exchange Commission and Commodity Futures Trading Commission with verifiable provenance, integrity, and investor protection features.

(d) Amendment to Section 12. — Digital Asset Functional Exemption.

Section 12(g)(9) is added — Digital Asset Functional Exemption

> (A) Exemption. The registration requirements of this subsection shall not apply to an issuer, network, or protocol whose instruments or digital assets—
> (1) are recorded on a distributed ledger or comparable technology that provides continuous, public, and auditable disclosure of transactional and governance information; and
> (2) meet the criteria of technological equivalence under Section 1001.
>
> (B) Functional Measurement. For purposes of this subsection—
> (1) a "holder of record" means any person who maintains right, title, or ownership of any digital asset except it shall not include digital wallet addresses or intermediaries acting solely as network validators, custodians, or liquidity providers; and
> (2) the term "assets" shall exclude reserves, smart-contract collateral, or other technical balances maintained for protocol functionality rather than investment return.

[31] NTD. Identify whether any other mechanism be included here. Global note to all mentions of "smart contract" as a requirement.

(C) Residual-Risk Override. The Commission may, by rule, withdraw the exemption where the network's residual agency risk materially increases, as measured under the Residual-Risk Assessment Model established under the Digital Markets Restructure Act of 2026.[32]

(D) Safe Harbor Transition. An entity or network relying on this exemption shall have not less than 12 months after the effective date of any revocation or material change in residual-risk classification to achieve compliance with Section 12(g) registration requirements.

(e) Digital Asset Spot-Market Authority.

1. Section 15 of the Securities Exchange Act of 1934 (15 U.S.C. 78o) is amended by adding at the end the following new subsection:

"(r) Digital Asset Spot Markets.—[33]
(1) The Commission is authorized to adopt rules governing the operation, registration, and oversight of digital-asset spot markets and trading facilities that make Digital Value Instruments available for trading to the public.
(2) Such rules shall be issued jointly with the Commodity Futures Trading Commission where appropriate to ensure consistent standards across securities and commodity markets.
(3) An entity registered under a Unified Registration Certificate under the Digital Markets Restructure Act of 2026 shall be deemed to satisfy the registration requirements of this section for substantially identical activities."

(f) Amendment to Section 15(a). — Broker-Dealer Registration.

Section 15(a) (15 U.S.C. 78o(a)) is amended by inserting after the second sentence the following:

"A person holding a Unified Registration Certificate under Digital Markets Restructure Act of 2026 and engaged solely in activities covered by such certificate shall not be required to obtain separate registration as a broker or dealer under this section for those activities."

(g) Amendment to Section 17A — Clearing Agencies.

Section 17A (15 U.S.C. 78q-1) is amended by adding at the end the following new subsection:

"(f) Digital Clearing Agencies. — The Commission, in consultation with the Commodity Futures Trading Commission, shall establish standards for registration and operation of digital asset clearing agencies handling Digital Value Instruments. Such standards shall ensure finality of settlement, cybersecurity, and transparency consistent with the requirements of the Digital Markets Restructure Act of 2026."

[32] NTD. Confirm consistent language is used throughout.
[33] NTD. Solicit input, particularly on this section.

(h) Joint Enforcement and Information Sharing.

Section 24 (15 U.S.C. 78x) is amended by adding at the end the following new subsection:

"(d) Joint Information Sharing for Digital Value Instruments. — The Commission may share supervisory and enforcement information with the Commodity Futures Trading Commission and Prudential Regulators to the extent necessary to administer the Digital Markets Restructure Act of 2026, and such information shall retain its privileged and confidential status after disclosure."

(i) Conforming Amendments.

1. Wherever the term "security" appears in sections 3, 12, 13, 15, 17A, and 19 of the Securities Exchange Act of 1934, it shall be deemed to include Digital Value Instruments to the extent those instruments are traded on registered securities venues.
2. References to "registered broker or dealer" shall be deemed to include persons holding Unified Registration Certificates for equivalent activities.
3. References to "national securities exchange" shall include registered digital asset trading systems and registered digital asset trading facilities operating pursuant to this Act.

TITLE VIII — AMENDMENTS TO THE COMMODITY EXCHANGE ACT

SEC. 801. DEFINITION OF DIGITAL VALUE INSTRUMENT.

Section 1a of the Commodity Exchange Act (7 U.S.C. 1a) is amended—

1. in paragraph (9), by striking "and" at the end;
2. in paragraph (10), by striking the period at the end and inserting "; and"; and
3. by adding at the end the following new paragraph:

"(11) Digital Value Instrument.—The term 'Digital Value Instrument' or 'DVI' means any digital asset or electronically embodied unit of value or right that confers or represents a financial, economic, or proprietary interest or exposure and is not limited to immediate consumptive use, as defined in section 103 of the Digital Markets Restructure Act of 2026. A DVI may represent, in whole or in part, a security, derivative, or commodity interest and shall be supervised in accordance with that Act."[34]

SEC. 802. JOINT AUTHORITY OVER DIGITAL VALUE INSTRUMENTS.

(a) In general.— Section 2(a)(1)(A) of the Commodity Exchange Act (7 U.S.C. 2(a)(1)(A)) is amended by adding ", Digital Markets Restructure Act of 2026,":

after "The Commission shall have exclusive jurisdiction, except to the extent otherwise provided in the Wall Street Transparency and Accountability Act of 2010 (including an amendment made by that Act)"[35]

[34] NTD. Solicit input, specifically on this proposal.
[35] NTD. Solicit input, specifically on this proposal.

(b) Section 2(c)(2) of the Commodity Exchange Act is amended by adding the following new paragraph:

"(H) Notwithstanding any other provision of this Act, the Commission may recognize trading system authorized by the CFTC and jointly by the CFTC and SEC as a lawful venue for the offer, sale, or trading of Digital Value Instruments."

(c) Conforming amendment.— Section 2(c)(2)(D)(i)(II)(bb) is amended by inserting after "(V) an identified banking product, as defined in section 27(b) of this title"—

"; and (VI) any Digital Value Instrument and any digital asset on a trading system, as authorized by the SEC and/or CFTC".

SEC. 803. NEW CATEGORY OF FUTURES COMMISSION MERCHANT—'FCM-DA.'

(a) In general.— Section 4d of the Commodity Exchange Act (7 U.S.C. 6d) is amended by adding at the end the following new subsection:

"(k) Digital Asset Custodians and FCM-DA Registration.— [36]
(1) The Commission shall establish a registration category to be known as 'FCM-DA' for persons engaged solely in the custody or fully-collateralized settlement of Digital Value Instruments.
(2) An FCM-DA registrant shall be subject to capital, segregation, and recordkeeping standards appropriate to its limited risk profile, as determined by rule.
(3) An FCM-DA registrant shall not be required to register separately as a futures commission merchant under this section for the same activities.
(4) The Commission may recognize a Unified Registration Certificate issued under the Digital Markets Restructure Act of 2026 as satisfying the registration requirements of this subsection."

(b) Rules.— Within 180 days after the date of enactment of this Act, the Commodity Futures Trading Commission shall promulgate rules to implement subsection (k).

SEC. 804. CONSUMER PROTECTION AND DISCLOSURE FOR DIGITAL ASSET COMMODITY SPOT MARKETS.

(a) New section.— The Commodity Exchange Act (7 U.S.C. 1 et seq.) is amended by inserting after section 4s the following new section:

"SEC. 4t. DIGITAL ASSET COMMODITY SPOT MARKETS.[37]
(a) Registration required.— No person may operate a digital asset spot market unless registered with the Commission or holding a Unified Registration Certificate under the Digital Asset Market Structure and Coordination Act of 2026.

[36] NTD. Solicit input, specifically on this proposal.
[37] NTD. Ensure Digital Asset Commodity Spot Markets is used consistently as appropriate, as opposed to Digital Asset Spot Markets. Also solicit input, specifically on this proposed section.

(b) Customer protections.— The Commission shall by rule establish requirements for digital-asset spot markets with respect to—
(1) disclosure of material information concerning trading rules, fees, and conflicts of interest;
(2) prevention of market manipulation and fraud; and
(3) maintenance of books and records sufficient to demonstrate compliance.
(c) Coordination with the Securities and Exchange Commission.— The Commission shall consult with the Securities and Exchange Commission to ensure that rules issued under this section are consistent with rules for Digital Value Instruments classified as securities.
(d) Preemption of State law.— Operation of a digital asset spot market in compliance with this section and with the Digital Asset Market Structure and Coordination Act of 2026 shall preempt any State or territorial law that would require separate licensure or registration of such market or its operators."

SEC. 805. DIGITAL ASSET SPOT MARKETS.[38]

(a) Section 5 of the Commodity Exchange Act is amended by inserting after subsection (d) the following: [39]

"(e) Digital Asset Spot Markets.—[40]

(1) The Commission is authorized to adopt rules governing the operation, registration, and oversight of digital-asset spot markets and trading facilities that make Digital Value Instruments available for trading to the public.
(2) Such rules shall be issued jointly with the Securities and Exchange Commission where appropriate to ensure consistent standards across securities and commodity markets.
(3) An entity registered under a Unified Registration Certificate under the Digital Markets Restructure Act of 2026 shall be deemed to satisfy the registration requirements of this section for substantially identical activities."

SEC. 806. JOINT RULEMAKING AND ENFORCEMENT.

(a) Joint authority.—The Commodity Futures Trading Commission and the Securities and Exchange Commission shall jointly issue rules to harmonize margin, custody, recordkeeping, and reporting requirements for Digital Value Instruments to the extent such requirements overlap under their respective statutes.

(b) Cross-agency enforcement.—Each Commission may bring enforcement actions for violations of the Digital Markets Restructure Act of 2026 within its jurisdictional scope, and may share investigatory information consistent with this Act.

[38] NTD. Consider whether it is preferable to have a separate section for bearer form instruments, which can address DeFi. Consider section 5 versus centralized exchanges in section 4 above, or whether to merge these.
[39] NTD. Solicit input, specifically on this proposal.
[40] NTD. Solicit input, particularly on this section.

(c) Judicial review.—Final rules issued jointly under this section shall be subject to review in the United States Court of Appeals for the District of Columbia Circuit under chapter 7 of title 5, United States Code.

SEC. 807. CONFORMING AMENDMENTS.

(a) References to 'commodity'.—Wherever the term 'commodity' appears in sections 1a, 2, 4d, and 4t of the Commodity Exchange Act, it shall be deemed to include Digital Value Instruments to the extent it is subject to CFTC jurisdiction under the Digital Markets Restructure Act of 2026.[41]

(b) References to 'registered entity'.—Such term shall be deemed to include any entity holding a Unified Registration Certificate pursuant to the Digital Markes Restructure Act of 2026 for activities subject to this title.

TITLE IX — RESIDUAL-RISK ASSESSMENT MODEL

SEC. 901. ESTABLISHMENT OF MODEL.

(a) In general.—There is hereby established within the joint authority of the Commissions a quantitative framework, to be known as the Residual-Risk Assessment Model (hereinafter in this Act referred to as the "Model"), for the purpose of—

(1) classifying Digital Value Instruments according to their predominant residual-risk profile;

(2) assigning supervisory responsibility among the Commissions; and

(3) triggering rotation of Lead Supervisor designations pursuant to section 402.

(b) Governance.—The Model shall be maintained by a Joint Risk Committee composed of equal representation from the Securities and Exchange Commission and the Commodity Futures Trading Commission, with participation by a technology and cybersecurity expert. The participation by the National Institute of Standards and Technology or similar agency is sufficient but not required to meet the expert participant requirement. The Joint Risk Committee shall—

(1) publish model parameters and calibration schedules annually in the Unified Digital Market Registry;

(2) review empirical data concerning enforcement outcomes and market events; and

[41] NTD. Consideration whether to insert the risk classifications into legislation amendments or leave outside the legislation to be more future-proof and to enable the Commissions to be nimble.

(3) certify the integrity of model updates by recordation in the RegNode using a mechanism that meets verification standards, as set by the Commissions.[42]

SEC. 902. VARIABLES AND INDICES.[43]

(a) The Commissions shall jointly determine standardized methods to assess the core variables of each DVI, based on residual risk categories (enterprise risk, exposure risk, and market risk), and/or any other relevant factors, as determined and agreed jointly by the Commissions.

(b) Classification rule.—The Commissions shall jointly determine the supervisory classification and registrant election of its Lead Supervisor pursuant to section 303.[44]

SEC. 903. THRESHOLDS AND ROTATION TRIGGERS.

(a) Thresholds.—The Commissions shall jointly establish thresholds for changes to risk profiles that warrant a rotation of Lead Supervisor.

(b) Rotation protocol.—The Commissions shall jointly establish a rotation protocol for a rotation event.[45]

(c) Public summary.—The Unified Digital Market Registry shall publish, on a regular schedule to be determined jointly by the Commissions, anonymized summary data on rotation events and average residual-risk scores by category, excluding Confidential Supervisory Information.

SEC. 904. MODEL CALIBRATION AND AUDIT.

---

[42] NTD. A cryptographic hash would meet the present day standard. But caution not to include specific technology into the legislation.

[43] NTD. The exact methodology would be determined through interagency collaboration. A proposed approach for an approach to be considered in an Securities and Exchange Commission-Commodity Futures Trading Commission MOU for example, is:

(a) Core variables. Each DVI shall be assigned standardized index values as follows:

Symbol	Range	Description	Associated Abstraction
A	0.00 – 0.50	Agency / Information Asymmetry Index	Enterprise
L	0.00 – 0.50	Leverage / Synthetic Exposure Index	Exposure
C	0.00 – 0.30	Custody / Integrity Index	Market
T	–0.30 – 0.00	Transparency / Enforceability Offset	Mitigating
K	0.00 – 0.20	Collective-Action / Dispersion Index	Amplifier

(b) Computation of scores. For each DVI, the following composite scores shall be calculated:

(1) Enterprise Score (ES) = A + 0.5 × K – T.

(2) Exposure Score (XS) = L – T.

(3) Market Score (MS) = C – T.

(c) Classification rule. The residual-risk category corresponding to the highest composite score shall govern supervisory classification, unless otherwise authorized by the Commissions. Where two or more scores are within ± 0.10 parity, the registrant may elect its Lead Supervisor unless otherwise authorized by the Commissions.

[44] NTD. The exact methodology would be determined through interagency collaboration. One proposal is that where two or more scores are within ± 0.10 parity, the registrant may elect its Lead Supervisor pursuant to section 402.

[45] NTD. To address whether the RegNode does this automatically.

(a) Bi-annual calibration.—The Joint Risk Committee shall assess and recalibrate the model if necessary at least every two years.

(b) Audit and validation.—The Joint Risk Committee shall obtain an independent validation of the Model at least every third year to verify reproducibility and to ensure that model drift remains within parameters set by joint rule.

(c) Record keeping.— All model versions, calibration data, and validation reports shall be recorded and preserved on the RegNode for not less than ten years and shall be deemed official records of the United States.

SEC. 905. LEGAL EFFECT AND TRANSPARENCY.

(a) Transparency.—Except for Confidential Supervisory Information and other materials as specified by the Commissions, all model documentation, parameters, and historical performance data shall be publicly available through the Unified Digital Market Registry.

TITLE X — TECHNOLOGICAL EQUIVALENCE AND DIGITAL IDENTITY

SEC. 1001. RECOGNITION OF TECHNOLOGICAL EQUIVALENCE.

(a) Equivalence Principle.— Whenever a mechanism or technology exists—including but not limited to, cryptographic process, distributed-ledger protocol, automated compliance mechanism, or smart-contract architecture—that provides protection or verification equal to or greater than that required by an existing rule, such mechanism or technology shall be deemed to constitute compliance with that rule.

(b) Joint Standards.—Not later than 180 days after the date of enactment of this Act, the Commissions shall, in consultation with the Department of the Treasury and other regulatory bodies as the Commissions deem appropriate, jointly establish criteria for determining technological equivalence, including—

(1) cryptographic strength, immutability, and auditability of records;

(2) automatic enforcement of contractual obligations; and

(3) mechanisms for real-time reporting and regulatory visibility.

(c) Certification.—A technology standard approved under this section shall be certified as established jointly by the Commissions and recorded in the RegNode, and reliance thereon shall create a rebuttable presumption of compliance with the requirement for which the technology was substituted.

(d) Revocation or Modification.—The Commissions may jointly revoke or modify a certification for cause upon public notice and comment and recordation of findings on the RegNode.

(e) No preclusion of innovation.—Not later than 180 days after the enactment of this Act, the Commissions shall, in collaboration, develop a process by which registrants may submit technologies for technological equivalence certification. This process shall allow for approval by either Commission and provide an appellate mechanism to a federal court established under Article III of the United States Constitution.

SEC. 1002. FLEXIBLE RULEMAKING AUTHORITY.

(a) General authority.—The Commissions may by joint rule add or remove requirements applicable to registrants under this Act to the extent that—

(1) technological equivalence has rendered a requirement unnecessary or redundant; or

(2) recent technologies or market practices introduce risks not addressed by existing rules.

(b) Procedures.— Any rule adopted pursuant to this section shall be issued jointly under section 553 of title 5, United States Code, and subject to de novo review under section 1102 of this Act.

(c) Periodic review.—At least once every five years, the Commissions shall review all rules issued under this Act to determine whether advances in technology warrant their modification or repeal.

SEC. 1003. DIGITAL IDENTITY CREDENTIAL FRAMEWORK.

(a) Establishment.—The Department of the Treasury, in consultation with the Department of Commerce and the Commissions, shall establish a program for certifying privacy-preserving digital identity credentials for use in customer identification, verification, and anti-money-laundering compliance.

(b) Optional use.—Use of a certified digital identity credential shall be voluntary and may be provided by Federal, State, or private issuers meeting standards to be established by the Department of Treasury, in consultation with the Department of Commerce and the Commissions.

(c) Legal effect.—Presentation of a certified digital identity credential shall constitute prima facie evidence of compliance with the know-your-customer and customer-identification program requirements of the Bank Secrecy Act and any comparable Federal rule. Any state or territory of the United States law that prevents the universal acceptance of a certified digital credential under this Act is preempted by this section 1003 and rules and regulations established hereunder.

(d) Standards and privacy.—The Department of Treasury, in consultation with the Department of Commerce and the Commissions shall establish standards for digital identity credentials, which shall be reviewed every three years and updated based on technological advancements. The standards for digital identify credentials shall include—

(1) us of privacy-enhancing technologies to minimize disclosure of personally identifiable information;[46]

(2) multi-factor authentication and tamper-resistant hardware modules; and

(3) interoperability with the Unified Digital Market Registry and RegNode systems.

(e) Non-discrimination.—A registrant shall not deny service to a customer solely because the customer chooses not to use a digital identity credential if the customer otherwise complies with lawful identification requirements.

(f) Rule of construction.—Nothing in this section shall authorize the Federal Government to maintain a centralized database of individual identity information; certification shall be limited to the credential framework and standards thereof.

SEC. 1004. TECHNOLOGY ADOPTION AND PUBLIC INNOVATION PILOT[47] PROGRAMS.

(a) Pilot program.—The Commissions may jointly establish a pilot program to test emerging technologies that demonstrate potential for enhanced market integrity; investor protection; enhanced mitigation of enterprise risk, exposure risk, or market risk; operational efficiency; or for other purposes approved by the Commissions.

(b) Duration and extension.— Pilot authorizations shall not exceed two years but may be extended for cause by joint approval of the Commissions.

(c) Evaluation and reporting.— At the conclusion of each pilot, the Commissions shall publish a report evaluating the technology's efficacy and recommending whether permanent rulemaking is warranted.

SEC. 1005. RULE OF CONSTRUCTION.

(a) No limitation on innovation.—Nothing in this title shall be construed to limit the ability of any person to develop or deploy innovative technologies consistent with Federal law.

(b) No mandatory technology.—The Commissions may recognize multiple technological solutions as equivalent under this Act and shall not mandate exclusive use of any particular technology or vendor.

[46] NTD. Consider whether use of zero-knowledge proofs would be sufficient to meet this requirement for purposes of agency development of the framework.
[47] NTD. Confirm the currently preferred noun for "pilot," "sandbox," and similar programs.

(c) Preemption of inconsistent State standards.—Any State or territorial law purporting to impose inconsistent technological or identity-credential requirements on registrants covered by this Act is hereby preempted.

TITLE XI — ENFORCEMENT, ANTI-OBSTRUCTION, AND JUDICIAL REVIEW

SEC. 1101. CONSISTENT ENFORCEMENT STANDARDS.

(a) Policy.— Congress declares that enforcement of this Act shall be based on objective residual-risk metrics and classifications recorded under Title IX, and not on the technological form or descriptive terminology of any Digital Value Instrument (DVI).

(b) Uniform procedures.— The Commissions shall jointly establish mechanisms for the consistent application of—

(1) investigation initiation standards;

(2) criteria for determining material violations; and

(3) civil-monetary-penalty guidelines.

(c) Cross-designation of staff.— Employees of either Commission may be cross-designated to conduct joint examinations and investigations under this Act. Evidence collected by one Commission shall be admissible in any administrative or judicial proceeding brought by the other.

SEC. 1102. JUDICIAL REVIEW.

(a) Right of review.—Any person aggrieved by a final action of either Commission under this Act may obtain review by filing a petition in the United States Court of Appeals for the District of Columbia Circuit within 60 days after such action.

(b) Standard of review.—Review shall be de novo with respect to questions of classification, jurisdiction, and residual-risk assessment, and under section 706 of title 5, United States Code, with respect to all other questions.

(c) Record on review.—The complete RegNode record relating to the challenged action shall constitute the administrative record for judicial review. The Commissions shall certify such record within 45 days after service of the petition.

(d) Relief.—The court may affirm, reverse, or modify the challenged action and may remand with instructions to the Commissions. Pending review, the court may issue a stay of the challenged action upon a showing of good cause.

SEC. 1103. ANTI-OBSTRUCTION AND INDEPENDENCE OF CLASSIFICATION.

(a) Prohibition.—No Commission official or employee, or Member of Congress shall, by threat, influence, or coercion, attempt to obstruct or delay—

(1) the application of the Residual-Risk Assessment Model;

(2) the publication of results or rotations recorded in the RegNode; or

(3) the issuance of a URC or Lead-Supervisor rotation required by this Act.

(b) Void actions.—Any classification suspension, rotation freeze, or similar action taken in violation of subsection (a) shall be void ab initio.

(c) Civil penalty and private right of action.—Any person who knowingly and willfully violates this section shall be subject to a civil penalty of not more than $10,000 for each violation. The SEC, CFTC, Department of Justice, or Department of Treasury shall initiate an administrative or judicial process to determine violations and assess penalties. Any penalty imposed under this section shall be collected by the prosecuting agency and deposited into a fund to be used for the enforcement of this law. Any person who is injured by a knowing violation of this section may recover three times the actual damages suffered by the person, or $10,000, whichever is greater, and the costs of the action, including reasonable attorney's fees. No civil action may be brought under this section if an agency has already initiated an administrative or judicial action to enforce the same provision. Nothing in this section shall be construed to limit any other remedy that may be available under any other provision of law, including criminal penalties. This statute specifically authorizes tort liability for actions of federal employees within the scope of their employment, and waives immunity of federal employees to the maximum extent permitted by law.

SEC. 1104. WHISTLEBLOWER PROTECTIONS.

(a) Protection from retaliation.—No registrant or government official may discharge, demote, threaten, or otherwise discriminate against an employee or contractor because of any lawful act in providing information relating to a potential violation of this Act to the Commissions or law-enforcement agencies.

(b) Remedies.—An individual subjected to retaliation may file an action in the United States district court for the district in which the violation occurred. Remedies shall include reinstatement, double back pay with interest, and reasonable attorney's fees.

(c) Confidentiality.—The identity of a whistleblower shall be protected to the fullest extent permitted by law.

SEC. 1105. COOPERATION AND COOPERATION WITH OTHER AGENCIES.

(a) Inter-agency coordination.—The Commissions may share information, coordinate examinations, and enter into memoranda of understanding with the Department of the Treasury, the Department of Justice, the Financial Crimes Enforcement Network, any Prudential Regulator, and any federal office, department, or agency to carry out this Act.

(b) International cooperation.—The Commissions may, consistent with section 24 of the Securities Exchange Act of 1934 and section 8 of the Commodity Exchange Act, share information with foreign regulatory authorities under reciprocal confidentiality agreements to prevent fraud and promote market integrity.

TITLE XII — IMPLEMENTATION AND REPORTING

SEC. 1201. IMPLEMENTATION TIMELINES.

(a) Rulemaking deadlines.—Unless otherwise provided herein,

(1) Within 90 days after the date of enactment of this Act, the Commissions shall jointly publish in the Federal Register a schedule of rulemakings required under this Act.

(2) Within 180 days after the date of enactment of this Act, the Commissions shall issue initial rules establishing the Unified Registration Certificate, the Unified Digital Market Registry, and the Residual-Risk Assessment Model.

(3) All remaining rules required by this Act shall be issued within one year after the date of enactment.

(b) Operational readiness.—

(1) The Unified Digital Market Registry and RegNode shall become fully operational within 12 months after the date of enactment.

(2) If either Commission fails to meet an implementation deadline, the other Commission may issue interim joint standards that shall remain in effect until superseded by final rules jointly established by the Commissions.

SEC. 1202. OVERSIGHT AND REPORTING REQUIREMENTS.

(a) GAO evaluation.—The Comptroller General of the United States shall—

(1) evaluate the effectiveness of this Act and its implementation within 24 months after enactment and every three years thereafter; and

(2) submit a report to the Senate Committee on Banking, Housing, and Urban Affairs, Senate Committee on Agriculture, Nutrition & Forestry, the House on Committee on Financial Services, and House Committee on Agriculture containing findings and recommendations.

(b) Annual Commission reports.— Each Commission shall submit annually to Congress—

(1) a summary of supervisory activities, rotations, and enforcement actions under this Act;

(2) aggregate data on residual-risk scores and market integrity; and

(3) recommendations for legislative or regulatory improvements.

(c) Treasury market-impact report.—The Secretary of the Treasury shall, within two years after enactment, evaluate the effects of this Act on capital formation, liquidity, and systemic risk in the United States financial markets and transmit the report to Congress.

SEC. 1203. PUBLIC DISCLOSURE AND TRANSPARENCY.

(a) Public access.—The Unified Digital Market Registry shall make available to the public—

(1) all non-confidential filings and notices required under this Act; and

(2) aggregate market and supervisory statistics updated at least quarterly.

(b) Plain-language summaries.—The Commissions shall mandate that registrants submit plain-language summaries of each initial and annual filing, limited to 10,000 words, to enhance public comprehension.

(c) Protection of confidential information.—Nothing in this section shall be construed to require disclosure of Confidential Supervisory Information as defined in section 505.

SEC. 1204. BUDGET AND APPROPRIATIONS.

(a) Authorization of appropriations.—There are authorized to be appropriated such sums as may be necessary to carry out this Act for each fiscal year.

(b) Use of fees.—The Commissions may collect and retain reasonable registration and filing fees to defray the costs of operating the Unified Digital Market Registry and RegNode, subject to annual review by the Comptroller General.

(c) User fees for technology certification.—The Department of the Treasury may collect certification fees from issuers of digital identity credentials to recover administrative costs.

SEC. 1205. INTERIM PROVISIONS.

(a) Temporary rules.—Until permanent joint rules are issued, the Commissions may adopt temporary rules and procedures necessary to implement this Act.

(b) Continuation of enforcement.—All enforcement actions, investigations, and proceedings pending on the date of enactment shall continue unaffected except that jurisdiction and supervisory responsibility shall transfer to the Commissions as provided in this Act.

(c) Savings clause.—All valid orders, permits, and licenses issued before the effective date shall remain in effect until amended or revoked pursuant to this Act.

TITLE XIII — EFFECTIVE DATE AND TRANSITION

SEC. 1301. EFFECTIVE DATE.

(a) Immediate effect.— Except as otherwise provided in this Act, this Act shall take effect on the date of its enactment.

(b) Rulemaking and operational transition.—

(1) The Commissions may exercise all rulemaking and administrative authorities conferred by this Act immediately upon enactment.

(2) Rules issued under this Act may take effect on an interim basis without prior notice and comment if the Commissions jointly determine that such immediate effectiveness is necessary for the orderly transition to the new regulatory framework.

(c) Conforming of existing regulations.—All existing Federal regulations inconsistent with this Act shall be conformed or repealed by the issuing agency within 12 months after the date of enactment.

(d) State coordination.—The Commissions shall notify all State and territorial financial regulators of the effective date and preemptive effect of this Act not later than 30 days after enactment.

SEC. 1302. SAVINGS AND SEVERABILITY.

(a) Savings clause.— Nothing in this Act shall be construed—

(1) to impair or affect the authority of any Federal agency under statutes not amended by this Act, except to the extent of direct conflict;

(2) to invalidate any lawful regulation, order, or license issued under such other statutes unless specifically superseded; or

(3) to alter the jurisdiction of any court except as expressly provided herein.

(b) Severability.—If any provision of this Act or the application thereof to any person or circumstance is held invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected.

SEC. 1303. REPEAL OF INCONSISTENT PROVISIONS.

(a) General repeal.— All laws and parts of laws in conflict with the provisions of this Act are hereby repealed to the extent of such conflict.

(b) Specific repeals.— The following are repealed:

(1) Any State or territorial statute requiring licensure or registration of digital-asset businesses or money transmitters insofar as such statute applies to persons or activities subject to this Act.

(2) Any inconsistent rule or interpretive guidance issued by the Securities and Exchange Commission or the Commodity Futures Trading Commission prior to the date of enactment.

ATTACHMENT 2

Teresa Goody Guillén

Measure Twice: Designing Trust for the Algorithmic Age

(October 08, 2025)

Available at SSRN: https://ssrn.com/abstract=5621370 or http://dx.doi.org/10.2139/ssrn.5621370

Measure Twice: Designing Trust for the Algorithmic Age
By Teresa Goody Guillén

Keynote Speech[1]
Conference on Advances in Financial Technologies
Carnegie Mellon University
October 8, 2025

I. Introduction

Good morning, and thank you, Carnegie Mellon for the invitation—a university that does not wait for the future but helps design it. It is a privilege to be here among the technologists, economists, professors, and students who build this future and bring it to life.

It is also a privilege to be back in Pittsburgh. My Dad grew up in Jeannette—a small town not too far from here—a tough town, with good people who are full of heart. To my Dad, Pittsburgh was proof that hard work builds something bigger than circumstance. So, when as a little girl I told my Dad that I wanted to be a running back for the Pittsburgh Steelers—just like the "Bus"—he smiled and said, "Sweetheart, you can do anything you put your mind to, but considering your stature and gender, why don't you consider being a lawyer and the first female President instead." And for those of you familiar with the Bus (Jerome Bettis), you are my kind of people.

While I'm not a little girl anymore; at 5-feet-tall, my stature is still a small one. My Dad was teaching me that, even with my small stature, I can still catch stars if I reach for them; but to be strategic and use good judgment in deciding which star to aim for. He was teaching me to find my purpose before breaking barriers to achieve it because when talent, timing, and conviction line up, effort becomes impact. And while I'm not a running back, football and financial markets actually have a lot in common. Really, they do! A healthy market, like a good game, requires committed players, fair score keeping, and rules so everyone knows how to play fairly and safely. There will always be winners and losers, but when the play goes out of bounds, someone has to blow the whistle—not to stop the game, but to save it.

It means a lot to me to be talking with you all about market structure and design, and particularly at the invitation of Dr. Chester Spatt—who once tried to teach me statistics and, against all odds, succeeded. He along with Chairman Harvey Pitt shaped how I see markets, as behaving according to the incentives and constraints embedded in their design. The architecture sets the incentives, and the incentives shape behavior. Fairness and efficiency are not accidents; they are outcomes of structure. The law protects trust; it does not to replace it.

This perspective of architecture, trust, and measured intervention, brings us to why we are here today.

---

[1] Portions of this text were delivered as the keynote address for the 2025 Conference on Advances in Financial Technology at Carnegie Mellon.

Today's question is deceptively simple: How do we design markets that deserve our trust?

Before we jump in, I want to introduce the first "Sophia Guillén Methodology"—she has many. And you may be familiar with this methodology, especially if you are a parent. Sophia is my four-year-old who knows no limits and has an insatiable appetite for seeking knowledge, truth, and understanding. She is always asking questions. She does not feel the need to wait for me to finish a sentence before asking her questions. And her questions do not necessarily relate to whatever it is I was talking about. I encourage you to adopt her methodology to asking questions while I'm speaking today.

The Moment We Are In

This year, after President Trump's win, Congress seemed like the dog that caught the car; chasing the opportunity to write practical digital-asset legislation and then haphazardly grabbing the steering wheel and speeding off in the wrong direction while simultaneously holding hearings about who gets to drive. Meanwhile, the rest of the world is already directing traffic and implementing rules of the road to keep the public safe.

It's the Fourth Industrial Revolution—favoring decentralized and distributed ecosystems over centralized operations and trust by design as opposed to individual mandate. Some say decentralization and programmability remove human bias; but they are mistaken because humans wrote the code.

II. The Fourth Industrial Revolution—How to Design Trust Architecture

Let's look briefly at the first three revolutions—fundamentally, they outsourced labor.

- The first mechanized muscle with steam. Labor of muscle to mechanism.
- The second scaled production with electricity. Labor if skill to systems.
- The third digitized knowledge with the computer. Labor of thought to computation.

Each revolution handed more human effort to machines. This one is different. Now, we're outsourcing something far deeper: ***trust—trust to code***. This is not belief in a feeling, but confidence in rules, records, and results. We're teaching our systems to do what some courts, accountants, and gatekeepers once did.

We are, in a very real sense, ***making trust programmable***. Contracts which once needed a courthouse now live as self-executing code. Atomic settlement reconciles ledgers (in seconds) obviating much of the auditor's role. Markets that once depended on middlemen now rely on cryptography and distributed code. This is a change in governance. And governance—which is how we align incentives and settle disputes—is the deep plumbing of capitalism. We are ***replacing an institutional trust with an architectural one***.

When I say architecture, I mean design decisions that become behavior:

- Who sees what, when?
- Who can change what, how?
- What happens by default, even when no one's watching?

Adam Smith might have called it the invisible hand—coordination without command. Others would call it error correction or efficiency. The logic is the same: if the signals are clear, the system self-corrects. But signals are never perfect. There's noise. There's power. There's human nature.

In the twentieth century, we answered that with institutions—exchanges, auditors, regulators. In the twenty-first, we're answering with architecture—transparency by default, rules that run while we sleep, settlement that doesn't forget. This shift is equal parts possibility and peril. This is a reminder that innovation doesn't erase risk; it just rewrites where it lives.

- ***Possibility***, because when we design incentives well, systems self-correct faster and include more people.
- ***Peril***, because design is never neutral. Code is an opinion. Every rule creates incentives and consequences, the latter of which are all the more dangerous when unintended and unforeseen. Contracts—including "smart" ones—function to allocate risks among parties.

So this is why the real question is "How do we design systems that deserve our trust?"

Because once enforcement itself becomes programmable, the old playbook is incomplete.

- How do we govern a world where rules are software and referees are algorithms?
- How do we preserve flexibility and fairness when more and more of our lives are governed by code?

This isn't just a technical question—it's also a civilizational one. This is where the law comes in. Law has a job here—it's an ancient job: ***The purpose of law is not to suppress change; it is to civilize it.*** Law has never existed to freeze society in place. It exists to translate disruption into order—to give new technologies and new relationships a moral vocabulary.

You'll see a recurring theme in my approach—I think about when "we" (humanity) have done this before.

- When commerce outgrew barter, contract law evolved.
- When industrialization created new risks, labor and securities law evolved.
- When networks collapsed distance and identity, privacy and data law evolved.

In every case, law didn't crush the new; it civilized it—gave it rights, boundaries, and responsibility. ***This moment is no different—and it demands the same.*** Because information symmetry, enforceability, and collective action—the classic constraints of markets—are now design choices we can engineer.

The Principles of Design

The principles to design markets with trust require basic principles of discipline:

- Design for clarity, so information reveals, and doesn't obscure.
- Design for accountability, so power meets consequence.
- Design for incentives, so incentives encourage self-correcting conduct.
- Design for resilience, so failure is contained, not contagious.

Do that well, and markets self-correct. Do that well, and oversight stays measured—government intervention becomes the exception, not the rule. Do that well, and trust becomes something we can verify, not just hope for because hope, as every regulator and entrepreneur eventually learns, is not a strategy. **But, *design* is a strategy.**

That's why I talk about architecture. Architecture asks what works. It measures incentives. It tunes for behavior. It understands that a small change in a rule—a fee, a disclosure, an order type, an order prioritization—can reshape the whole game. And it's why I talk about measured intervention rather than permanent policing.

Systems should run on their own—until they can't. Markets are self-correcting—until they're not. When residual risk builds beyond what contract, competition, or code can absorb, governance must activate—not to take over, but to restore the conditions under which freedom works. That's the hinge of our time: building systems that rarely need rescuing—and rescuing lightly when they do.

So, our task is not to stop innovation at the water's edge. It's to understand why this revolution is happening—to measure its contours with care—and only then decide where the lines must be drawn. We are here to civilize code:

- To make programmable trust not only efficient, but just.
- To make markets not only faster, but fairer.
- To make opportunity not only open, but credible.

And to do that, we don't need a thousand new commandments. ***We need craft.*** What do I mean by craft—

- Craft is knowing that better rules come from better design, not just more of them.
- The craft to choose the right mechanism.

- The craft to align the right incentive.
- The craft to intervene only when the system can't heal itself.

Or, as my Father would say—mainly because he couldn't afford to waste the lumber—to ***measure twice, cut once.*** That's how we build systems that earn trust—through design that is honest, proportionate, and nimble enough to last. Freedom is not self-sustaining; it depends on how well we care for it. And to care for it, we have to get the measurements right.

III. The Long Arc of Economic Abstraction—Why Risk, Control, and Trust Keep Falling Out of Alignment

To understand where we are, we have to understand the pattern we keep repeating. Every financial revolution, from Amsterdam to Wall Street to Web3, has been a revolution in abstraction—in how we separate economic value from its physical or institutional source. ***Abstraction is the genius of finance***. It's what allows value to move freely—to be divided, combined, and traded.

But it is also what creates fragility, because every layer of abstraction widens the distance between risk and control—between those who bear the losses and those who make the decisions. That tension—between freedom to innovate and the responsibility to govern risk—is the recurring drama of financial history. This again, is the theme of my approach—when have we seen this before, and let's learn from it rather than making the same mistakes.

For that reason, let's take a stroll down memory lane to walk through some lessons of the past. Like my Dad always said, if you don't learn the lesson the first time, life will give you the same lesson again—and again, and again . . .

1. The Invention of Scalable Ownership

Let's look at scalable ownership. In the seventeenth century, the Dutch East India Company introduced the world to the joint-stock company. For the first time, an ordinary investor could buy a share of a voyage to the East Indies without leaving home. That innovation unlocked scale—hundreds of investors could now fund a single enterprise.

But it also created an agency problem. The investors owned the voyage's profits, but not its decisions. They carried the risk, but the captains and company officers held the control. The result was a new kind of conflict—what we now call the separation of ownership and control. Abstraction had allowed enterprise to scale—but it also required governance to keep power accountable.

2. Later Came The Abstraction of the Commodity

Another leap came in the nineteenth century with the invention of futures and commodities exchanges—most famously, in Chicago. A wheat farmer could lock in a price for his harvest months before it was grown. That was a revolution in stability. It turned nature's uncertainty into a tradable risk. But as the markets evolved, the contracts themselves became the product.

Futures contracts were bought and sold purely for speculation, detached from any actual wheat. And so the first derivatives were born—contracts about contracts, value stacked on value.

Used carefully, derivatives spread and price risk. Used recklessly, they conceal it. They allow leverage and exposure to multiply invisibly across the system. That's the double-edged sword of abstraction: it democratizes participation—but also hides where the real risk lives.

3. Modern Corporation and the Regulation of Trust

By the early twentieth century, abstraction moved from grain to governance itself. Corporations had become vast, anonymous machines. Shareholders technically owned them, but a dispersed public couldn't exercise control. Professional managers and intermediaries—banks, brokers, exchanges—now sat between capital and decision-making.

In 1932, Adolf Berle and Gardiner Means diagnosed this new condition in a book I highly recommend, *The Modern Corporation and Private Property*. They warned that capitalism had entered a new phase: ownership and control were no longer the same thing. That separation, they argued, was not a moral failure but a structural fact—and it demanded a structural response.

A year later, Congress gave that response with the Securities Act of 1933 and the Securities Exchange Act of 1934. ***Congress didn't outlaw abstraction—it civilized it.*** It accepted that separation was inevitable in a complex economy, and instead, built systems of disclosure and accountability to manage it. Transparency became a public substitute for direct control. From then on, markets operated on a social contract: ***if you separate ownership from power, you must compensate with visibility and truth***.

4. Derivatives, Leverage, and the Return of Hidden Risk

Every generation seems to forget its own lessons. By the late twentieth century, a new wave of financial engineering promised to make markets safer through sophistication—swaps, options, synthetic collateral, mortgage derivatives. Each was a tool for managing risk. Together, they created a fog of complexity.

The 2008 financial crisis was not caused by a single factor but it was in part caused by abstraction outpacing comprehension. Risk had been repackaged, tranched, and reinsured until it was difficult to see who ultimately bore it. Once again, exposure and control had drifted apart. The instruments that were supposed to hedge risk had become vehicles for hiding it. When the tide went out, no one knew what the paper represented anymore. The connection between symbol and substance had snapped—and with it, public trust.

5. Commodities and the Disconnection from the Physical

Around the same time, commodities markets underwent a quiet transformation. Commodities ceased to be physical goods and became financial exposures—tradable risk units detached from barrels of wheat and bushels of corn. Derivatives on oil and metals became so detached from the physical goods that prices could swing violently without any change in supply. We turned

tangible resources into speculative abstractions. And when volatility hit, it wasn't farmers or miners who failed first—it was the financial market participants.

Each episode repeated the same mistake: We stopped measuring the distance between risk and control. ***And a spoiler alert here: decentralization is not the answer***. I discuss this at length later, but here, I want to point out that decentralization does not measure risk or its abstraction from control. The loss in vertical trust has resulted in the shift to democratization —a shifting of power to the masses for shared control and shared access. ***It seeks to replace vertical trust with horizontal dependencies***. It doesn't create independence—it multiplies reliance. I'm expressing no ideology here, just that it is not a useful variable for measuring risk or its abstraction from control. That does not mean that it's not effective for measuring something else.

6. The Digital Continuation

Now, we've entered a new phase. Digital assets take the logic of abstraction to its limit. They make economic property ***modular/or disaggregated***, and programmable. We can separate not only ownership and control, but every right within property itself—such as, economic benefit, voting, access, and governance—each as its own tradable unit. These modularized economic interests, and their associated risks, are tradable. When technology allows risk to move faster than accountability, we recreate the same vulnerabilities we've seen before, just in a different form and different combinations of vulnerabilities.

This time, the danger may be ***false clarity***. Everything is ***visible*** on-chain, but not everything is ***understandable***. We can see the ***data***, but not the ***risk***. We've built ***transparency*** but often without ***intelligibility***. And it's by thinking through these risks from abstraction that we can design purposeful market structure that realign incentives when self-correction fails.

IV. The Intervention Threshold

Markets, left alone, are extraordinary at self-correction. ***Competition, contract, and reputation (called "private ordering") do most of the work.*** But when the gap between risk and control widens too far, those mechanisms stop working. That's when ***residual risk—risk no one sees or owns—begins to accumulate***. At that moment, governance must step in—not to replace the market, but to restore the feedback loop that makes it work. That is the ***threshold for intervention***. Below that threshold, the market governs itself. Above it, governance activates to bring accountability back into view. And once equilibrium returns, regulation should recede again. That's how you preserve both innovation and integrity: regulation as a circuit breaker, not a constant current.

There are indicia that tend to trigger a need for guardrails and the potential threshold for intervention. These triggers can apply in both securities and non-securities contexts:

i. ***Retail Market Access***: Assets available for trading by retail investors through centralized or decentralized exchanges trigger disclosure requirements if

information asymmetry exists and market surveillance to ensure fair and efficient markets.

ii. ***Market Depth and Volume***: Significant trading volume, market capitalization, or liquidity metrics above specified thresholds could require more comprehensive market structure oversight and manipulation prevention measures. While large volumes and deep liquidity indicate healthy trading environments, they also increase market susceptibility to manipulation and fraud if left unchecked.

iii. ***Ecosystem Interdependence and Significance***: Assets integral to broader digital asset ecosystems or serving as infrastructure for other tokenized instruments may warrant systemic risk assessment and potentially regulatory requirements narrowly tailored and proportionate to the specific risks.

Then you get to the harder question of how do we make markets that are self-correcting by architecture, not by accident? Or stated differently, how do you build this ***Architecture of Trust***. I see that it starts with three basic principles:

i. ***Transparency as Default:*** information symmetry with frequency relative to market pace and content based on traditional notions of "materiality," or what a reasonable investor would deem important in making an investment decision.

ii. ***Accountability by Design:*** power must always meet consequence.

iii. ***Proportionate Intervention:*** oversight must expand and contract with residual risk, not ideology.

And feedback—that is visible, verifiable, and self-correcting—transforms the complexity into order.

1. Lessons from the Early 20th Century—How We First Civilized Abstraction

Before getting to my proposed approach, I want to walk through a few more lessons-learned that we need not repeat. The 1920s weren't reckless by accident; they were reckless by design—or more specifically, ***design flaw***. Finance had evolved faster than measurement. But the deeper failure was not moral—it was informational. People did not lose faith in enterprise; they lost faith in what enterprise meant. The markets didn't run out of capital; they ran out of comprehension. Investors no longer knew what their holdings represented—who controlled them, what risks they carried, or how far removed they were from real assets. Abstraction had outrun measurement. And when measurement collapses, trust collapses with it.

The ingredients were familiar:

- Leverage without transparency.
- Ownership without control.

- Control without accountability.

There were fundamental missteps in the development of corporate law in the early 1900s. There was a failure to identify and appreciate the misaligned incentives and risks resulting from the abstraction of ownership from control of economic interests. It was the 1929 crash that forced this reckoning.

2. The Pre-1929 System—Innovation Without Insight

Before 1929, new vehicles of finance were celebrated as progress. Investment trusts promised ordinary Americans a stake in industrial growth. Margin lending let them participate with borrowed money. Banks and trusts packaged assets into nested structures that multiplied profits—and risk. Each layer was an innovation. But together, they produced opacity. ***You could own a share of something without ever knowing what it contained.***

Abstraction had outpaced comprehension. The system worked beautifully—until confidence faltered. Then the whole system collapsed, not because capitalism failed, but because trust was broken.

3. What 1929 Taught Us—When Measurement Replaced Morality

The crash of 1929 was a ***crisis of information before it was a crisis of liquidity.*** Investors didn't lose faith in markets—they lost faith in ***what those markets represented.*** Congress responded with a radical but elegant idea: ***disclosure as design.*** The Acts of 1933 and 1934 did not outlaw abstraction; they civilized it. They accepted complexity as inevitable but demanded clarity as its price. ***The principle was simple: If you separate ownership from control, you must provide visibility in return. It regulated by function, not by form.*** Congress responded with a two-track system: securities law (1933/1934) to curb agency and disclosure failures, and futures regulation (strengthened in 1936) to contain excessive speculation, manipulation, and contagion.

4. Adolf Berle's Contribution—The Economic Lens

Adolf Berle and Gardiner Means gave that principle its economic foundation. They advocated that modern corporations were no longer personal enterprises—they were private engines running on public trust. When ownership and control diverge, they said that markets need a new mechanism of alignment. That mechanism was governance—as the connective tissue between power and consequence. And they saw law not to punish innovation, but rather, to ensure that freedom didn't collapse under its own complexity.

Whether you agree with Berle or not, his underlying principles of balance and purpose are sound. We have drifted from those principles and logic. The New Deal regulated ***functions***—it asked what an instrument ***did***. Our system today regulates ***forms***—it asks what an instrument is ***called***. We have turned disclosure into documentation, classification into comfort, and labels into law.

But markets don't care what something is called. They care how it behaves and what risks it creates. And technology is changing that behavior faster than the law can track. Code can reduce certain risks—automating enforcement, removing middlemen, making fraud impossible by design. But it can also create new ones—hidden leverage, oracle failures, algorithmic cascades. Risk doesn't disappear; it migrates. Technology can shift risk invisibly and completely. And yet our rulebooks still treat assets as if they were static categories, not dynamic systems. That's the heart of our current problem: Regulation frozen in time, applied to risks that have already changed shape.

V. When Regulation Breaks Markets—Why Our Legislation Proposals Will Lead to Market Failure

1. The Legislative Proposals Measure the Wrong Variable

When law stops measuring the right variables, regulation itself becomes a source of market failure. That's what is happening now. The House CLARITY Act, the Senate market-structure drafts, and much of our digital-asset debate are all driven by flawed logic—and fail the basic principle: ***they measure the wrong variable***. Instead of mapping risk, they define form. They ask whether something is a "security," a "commodity," or the ***fictional*** "ancillary asset"—as if classification were comprehension. But digital assets don't live in those silos. A single instrument can behave like a security, when holders depend passively on others' governance; a derivative, when it embeds leverage or mirrored exposure; and a commodity, when it functions as network fuel. These are not competing labels—they are coexisting risk behaviors. Treating them as separate categories is not clarity; it is confusion.

Consequently, function shifts, but our statutes, written for discrete categories, cannot keep up with dynamic instruments. What, therefore, is the impact of such rules? They over-reach where technology already solves the problem and under-reach where it creates new ones. ***It's not bad faith—but it is bad measurement.***

i. Measurement Is Civilization—A Societal Requirement

Measurement is not just a technical act. It is how societies turn complexity into accountability. ***Market failures generally share one trait: a failure to measure where risk truly lived.*** When systems stop measuring risk accurately, they drift toward fragility. ***When regulation chases form instead of function, it institutionalizes that fragility.*** To measure something is to admit it might fail—and to build feedback strong enough to learn before it does.

2. The Legislation Ignores Derivative-Like Nature of Many Crypto Assets

One of the most critical "misses" in the current legislation is the failure to grapple with the derivative-like nature of many crypto tokens. This goes beyond nomenclature—it is about the economic behavior and risk profile of tokens, and it ties directly into why these markets could develop to experience systemic failures reminiscent of 1929. Let's break down this issue:

A derivative is a financial instrument whose value is based on (derived from) some underlying asset, index, or event. Importantly, owning a derivative does not mean owning the underlying—you just have exposure to some metric (like a price). Key risks include hidden leverage, opacity, misaligned incentives, and weak investor protections, all of which haunted the 1920s markets and could resurface under the proposed legislation.

In the 1920s, unregulated investment trusts and bucket shops allowed rampant hidden leverage and speculation, companies disclosed little information, insiders' incentives diverged from public investors', and ordinary shareholders were largely unprotected. These conditions culminated in the 1929 crash. Today's crypto markets can involve similar risks—complex leverage in decentralized finance (DeFi), opaque token structures, issuer incentives to hype without accountability, and retail buyers with little recourse. The House and Senate bills, as written, risk locking in these vulnerabilities. They emphasize whether a token's network is "decentralized" or create new terminology like "ancillary asset," but do not fully address the fundamental concerns of information asymmetry, investor coordination failures, opaque leverage, speculative volatility, and so forth. These are risks that can be addressed, and do not require thousands of pages of prescriptive rules or forced intermediation.

Why does this matter? If these issues remain unmitigated, the crypto market—and with the dawn of tokenized securities already upon us, our traditional capital markets—could experience a destabilizing crash, which could lead to a rapid loss of confidence, runaway sell-offs, and contagion across the financial system. After 1929, Congress responded with securities regulation to curb agency and disclosure failures, and futures regulation to contain excessive speculation, manipulation, and contagion. The current bills miss those lessons, potentially leaving crypto markets on a similarly precarious footing.

Programmability adds potential for additional leverage, rehypothecation (reusing/repledging collateral being held for a third party to secure its own loans), recursive exposure looks like diversification but exposed to same risk indirectly repeatedly, such as DeFi loops, where crypto borrowed, re-deposited, and borrowed against across multiple DeFi protocols. For example, you can deposit/stake ETH in lending protocol, and receive the synthetic token stETH, then you use that collateral to buy a stablecoin, and swap that stablecoin for more ETH in the lending protocol, earning more stETH—this creates risk for instability in the market. The extreme interconnectedness means a single token's crash can cascade (e.g., if Token A is collateral for loans of Token B, a drop in A forces liquidations of B, etc.). This is analogous to how in 1929, the collapse of one highly leveraged trust could force sales and margin calls in others—a chain reaction.

The bills' blind spots are basically the structural issues that led to prior financial crises—excessive leverage, lack of transparency, misaligned incentives, and inadequate investor safeguards. All have analogies in the crypto markets, although some are, or can be mitigated by the technology, but the current bills risk codifying a regulatory framework that fails to address those issues, or even exacerbates them. ***It's a design flaw that codifies market failure into law***.

When legislation locks in outdated categories, three predictable things happen:

i. ***Regulatory arbitrage.*** Risk migrates to the gaps between agencies. That is where the next crisis always begins.

ii. ***Innovation flight.*** Builders leave jurisdictions that regulate uncertainty faster than risk.

iii. ***False security.*** Lawmakers believe the system is governed, but the most dangerous risks—hidden leverage, recursive derivatives, structural opacity—remain unseen.

That is not overregulation or under-regulation. It's mis-regulation. And it is exactly where we have been and where we could be headed—and what we need to try to prevent.

3. The Dangers of the Legislation's Over-Relying on Howey and Decentralization

The current legislative proposals reduce the security test to a single variable: decentralization. This factor, which may influence one element of the *Howey* test for one type of security (investment contract), is being elevated to the overarching test for all 30+ securities named by statute. This produces an incoherent and contradictory framework that engenders market instability.[2]

Over-reliance on the *Howey* test and decentralization leads to two primary problems:

i. ***False Negatives****:* Instruments that function as securities escape regulation, leaving investors unprotected.

ii. ***False Positives****:* Tokens with genuine utility or functionality are incorrectly classified as securities due to superficial factors like centralization.

This myopic approach will lead to critical failures, including stifled innovation, as projects contort themselves to an amorphous decentralization standard, and increased investor harm

---

[2] The Securities Act defines as a security as follows:

> [U]nless the context otherwise requires—(1) [t]he term "security" means any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a "security," or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing.

15 U.S.C. § 77b(a)(1). While the foregoing definition from the Securities Act is slightly different in the Securities Exchange Act of 1934 (15 U.S.C. § 78c(a)(10)), these definitions are typically interpreted consistently. *United Housing Foundation, Inc. v. Forman*, 421 U.S. 837, 847 n.12 (1975).

from premature project abandonment. The proposals create inconsistency and ambiguity across the securities law regime, including the scope and applicability of certain anti-fraud provisions and whether a private right of action exists for people to sue one another for violating the rules. It is also unclear whether, and to what extent, Congress intends to attempt to preempt state statutory and common law (*e.g.*, tort and contract law), and other legal regimes, such as the Uniform Commercial Code.[3]

4. Why the "Ancillary Asset" Concept is Doctrinally Misguided

The Senate Discussion Draft II introduces the notion of an "ancillary asset" by defining it as "an intangible asset, including a digital commodity, that is offered, sold, or otherwise distributed to a person pursuant to the purchase and sale of a security through . . . an investment contract[,]" which may or may not itself a security. This concept inverts longstanding doctrine. An investment contract is the mechanism for an investment opportunity; the token is the subject of that opportunity and/or proceeds.[4] Labeling the token as "ancillary" is a confusing mischaracterization (present only for subjects of investment contracts that are digital assets, as opposed to other types of assets); misstates both economic reality and legal substance; consequently, producing bizarre results in practice. Its definition arbitrarily distinguishes between tangible and intangible assets and creates inconsistent treatment across federal securities laws. To the extent the goal is to reach digital assets on a DLT network, there are more precise distinctions than intangibility, which extends to intellectual property, business-related property (e.g., goodwill), and many financial and contractual claims. It also ignores the other securities instruments and transactions that are capable of involving a digital asset beyond investment contracts and profit-sharing agreements. While the safe harbor provisions for ancillary assets offer a thoughtful framework, anchoring the analysis in economic abstraction—not decentralization—provides a more functional comprehensive approach.

5. The Myth of Decentralization—and the Need for Measurable Reality

There is one word that has dominated every conversation about digital assets: decentralization. It has become our generation's regulatory shorthand—a proxy for virtue, a stand-in for safety, and sometimes, an excuse for inaction. But decentralization is not really a single concept.

- It's a dozen different ones that don't always move together.
- You can decentralize nodes and still centralize control.
- You can decentralize geography and still concentrate decision-making.

---

[3] Goody Guillen, Teresa, *Essential Revisions to Strengthen Digital Asset Market Structure Proposals, Prevent Market Failure, and Ensure Securities Law Consistency* ("*Essential Revisions to Strengthen Digital Asset Market Structure*"), at 16 n.17 (Sept. 15, 2025) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5458774.

[4] Goody Guillen, Teresa and Corbett Sterling, Isabelle, *Paving the Path for Crypto Clarity: A Framework for Digital Asset Regulatory Structure* ("*Paving the Path for Crypto Clarity*"), at 15, 29-30 (Feb. 17, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5156725.

- You can decentralize voting while code updates remain in the hands of a few developers.
- You can decentralize ownership and still have information asymmetry such that no one can see where the real power lives.
- It may reduce some types of risk—like operational dependence or single-point failure—but it often amplifies others, like hidden influence and coordination failure.
- It might mean freedom for a network, but it can also mean anonymity without accountability.
- It can remove human bias, but it can also remove human judgment.
- It can mitigate some risks, but it cannot erase all of them.
- Decentralization doesn't eliminate reliance—it redistributes it.

There's a common ***myth in digital markets that decentralization means independence***—that if no one's in charge, no one's responsible. But that's not how networks, or economies, actually work. Even in a decentralized system, you still rely on others:

- Validators or miners to maintain consensus.
- Developers to maintain and upgrade code.
- Oracle providers to deliver real-world data.
- Custodians and exchanges to provide access.
- And millions of other participants to keep the network functional and secure.

In consequence, decentralization doesn't erase reliance; it multiplies it. It replaces a vertical chain of trust with a horizontal web of dependencies. That web can be stronger—but it can also hide new weak points. And that's not new. In the early 1900s, the corporate form did the same thing. Investors no longer relied on a single entrepreneur; they relied on an entire managerial class. Ownership became distributed; control became concentrated.

That's what Berle and Means diagnosed—a system where enterprise scaled faster than accountability. Today's distributed networks are reminiscent of that story. They democratize participation but diffuse responsibility. ***A market is not safe because it's decentralized; it is safe because its dependencies are disciplined; incentives are aligned to encourage fair and efficient markets and self-correction.*** Decentralization, by itself, tells us nothing about risk. Only measurement does.

VI. From Decentralization to Measurement

Markets fail when risks hide, incentives are misaligned, reporting is outdated, oversight is fragmented—not when code centralizes. That's why the question is not whether a network is decentralized. The question is whether the residual risk it creates—agency risk, derivative-like exposure, market-integrity vulnerability—has truly been reduced by its design. To the extent technology has reduced risk, then regulation can recede.

But to the extent technology has simply changed the shape of the risk or created new risks, then the system still needs a framework of accountability. Accordingly, the path forward is not to pick sides in a debate about decentralization versus control. It is to ask a more fundamental question: When does technology truly reunite risk and control—and when does it just disguise the distance? That's the purpose of the Economic Abstraction Framework I'm about to describe. It is not a political compromise between regulators and innovators. It is a diagnostic tool—a way to see, measure, and respond to risk in real time, across any system.

VII. The Economic Abstraction Framework—Measuring What Matters

Let me start with what this framework is not. It is not the ***Howey*** test. *Howey* looked for human behavior—promises, solicitations, expectations. That made sense in 1946, when most enterprise was centralized, promises were personal, and "trust" meant believing in a promoter. But the world we regulate now doesn't run on promises; it runs on systems. Code executes autonomously. Governance happens through distributed mechanisms. Value creation is collective and ongoing.

There's no single "other" whose effort you depend on—there's a network you participate in.

Thus, the right question is not who's making the effort; it is how the risk behaves. The Economic Abstraction Framework looks for structural imbalances—separations between risk, control, and enforceability. It's dynamic, not static. It asks:

- Where does risk live?
- Who can control it?
- Who can correct it?
- And how much risk remains after technology has done its best to manage it?

It doesn't measure expectation; it measures exposure. It doesn't assume reliance; it maps residual risk. It fits a programmable economy. We don't need to reinvent the law. We just need to measure what's left when technology does its job. The way forward is not thousands of pages of new rules. It's a single principle, revived from 1933 and updated for 2033: ***Regulate residual risk, not form.***

1. The Five Diagnostic Factors of Abstracted Economic Interests

The framework measures abstraction along five dimensions—five ways to think about risk being separate from control. Each factor is observable, measurable, and scalable.

i. Transferability—How Fast Can Risk Move?

The more easily an instrument can be transferred, the faster risk can spread. Transferability creates liquidity—and liquidity is good—but it also amplifies contagion. A freely tradable token moves information and emotion faster than any regulator can respond. So high transferability demands continuous visibility. If you open the gates of liquidity, you must keep the windows of transparency open too.

ii. Passive Economic Property Right/Interest—Who Creates the Value?

The second lens is passive economic interest: ***Is the holder depending on others for value creation?*** In traditional finance, that meant the investor relied on a company's managers.

In digital systems, it might mean reliance on developers, validators, or governance participants. The point is not whether that reliance exists—it always does. The question is whether it is matched by control, and if not, are the agency costs and collective action difficulties mitigated? When people bear risk without the means to influence outcomes, accountability weakens—regardless of whether it's a corporation, DAO, or network.

iii. Limited Enforceability—Can Participants Protect Themselves?

The third lens is limited enforceability. If the system fails, can a participant obtain redress?

In traditional markets, rights are enforceable through courts or contracts. In code-based systems, remedies may exist or being meaningful only if the code itself allows them—or not at all. When enforcement depends solely on software, and that software fails, what is the fallback? Limited enforceability doesn't mean fraud. It means fragility—a gap where trust must re-enter because code alone cannot heal the breach. When economic rights/interests are insufficiently enforceable—either lacking contractual or common law protections, or just not practically feasible—regulation can compensate for the lack of ex ante bargaining power, ex post remedies, and so forth.

iv. Systemic Dependency—What Keeps the System Running?

The fourth lens is systemic dependency. How many actors must continue acting in good faith for the system to survive? Every network, even a decentralized one, depends on something—the developers who patch vulnerabilities, the validators who maintain consensus, the oracles that feed it truth. The narrower that dependency, the higher the systemic risk. So systemic dependency tells us when "distributed" is another word for "fragile."

v. Limited Collective Action—Can the Participants Coordinate?

The final lens is limited collective action. Even if ownership is broad, can participants act collectively to correct a problem? If governance requires unanimous coordination among thousands of token holders, it is not governance—it is paralysis. That is how self-regulation fails. When private ordering cannot self-correct, public oversight must step in—temporarily, proportionately, and with clear exit criteria.

2. How the Framework Works

Each of these five factors tells us something about how far risk has drifted from control.

When they cluster—high transferability, passive exposure, limited enforceability, narrow dependency, weak collective action—abstraction has extended to needing a guardrail. That is the intervention threshold: the point where governance must activate to restore balance. But when technology mitigates these risks—when rights are enforceable, transparency is real-time, and participants can meaningfully coordinate—then the system earns back autonomy. Regulation can step back. ***That is the goal: a self-correcting market architecture that requires less oversight because it deserves less oversight.***

3. Residual Risk—The New Measure of Trust

Residual risk is what is left after technology, competition, and contract have done their work.

That's what law should measure. Because in a programmable economy, the question is not whether code replaces law—it is how much law the code already performs. When technology unites risk and control, regulation should recede. When it separates them, oversight must return. It is about returning to equilibrium.

In truth, this is not new. It is the same philosophy that underpinned the reforms of the 1930s.

Then, we built disclosure regimes to make financial abstraction legible. Now, we can use technology to make abstraction measurable in real time. The principles are unchanged

- Align risk with control.
- Make visibility the price of access.
- Intervene only when self-correction fails.

So how do we make this real? We return to the craft of law and we apply the ethic of measurement—measure twice, cut once. In carpentry, it means don't waste the lumber. In governance, it means don't waste the trust. First, measure abstraction—how far risk has drifted from control. Then, measure residual risk—what technology has not yet fixed. Only then, act—with proportion, precision, and purpose. That's the process to build systems that can bear their own weight.

- ***Identify the type of risk.***
    - Agency risk: hidden control, insider advantage, asymmetric power, collective action difficulties.
    - Derivative risk: embedded leverage, recursive payoff loops, contagion potential.
    - Market-integrity risk: manipulation, custody failures, thin liquidity.
- ***Measure the residual risk.***
    - What risk remains after transparency, automation, and verification are built in?
    - If technology already neutralizes the risk, oversight can recede.
    - If the risk persists or migrates elsewhere, targeted regulation activates.
- ***Scale proportionally.***
    - Regulation expands only where residual risk grows, and contracts where technology proves itself.

That's law behaving more like a thermostat: responsive, not reactive. If we regulate too soon, we freeze innovation. If we regulate too late, we repeat 1929—just faster, and on-chain. But if we measure twice and cut once, we preserve what matters most: a market free enough to innovate and fair enough to endure. Because the goal of law has never been to suppress change. It's to civilize it—to translate disruption into order, and to build systems worthy of the trust we place in them. That's how we keep freedom durable in a world written in code.

And that is what "measure twice, cut once" means in the digital age: ***Measure the abstraction, measure the residual risk, and cut only where the system still needs a human hand.***

4. Disclosure as the First Technology of Trust

The brilliance of the 1933 and 1934 securities laws was not in the paperwork—it was in the philosophy. Congress did not outlaw abstraction; it civilized it. It treated disclosure as a technology of trust—a way to make complexity legible and accountability visible. The topic for another day is how that disclosure regime has devolved into a bloated, self-defeating exercise distorted by politics. But just because we've lost sight of the purpose—clear, usable, information to provide transparency for everyday people—does not change that the purpose and principle is still sound: ***If you separate ownership from control, the public must be able to see what it owns. If you disperse risk, you must concentrate truth. That was the first great act of market architecture: turning transparency into infrastructure, law into a system of measurement.***

VIII. A Simpler Way Forward—The Modern Market Structure Compact

We can fix this with a framework as compact as it is powerful. We can restore function over form without rewriting a century of law. The legislative fix is to establish the structure in a matter of pages by articulating clear principles, jurisdictional boundaries, and accountability mechanisms, while delegating technical rulemaking to the agencies with subject-matter expertise. The goals in not to script every detail from Capitol Hill, but to design a durable framework that empowers those on the front lines—the SEC, CFTC, and others—to implement proportionate, data-driven rules as markets evolve. Brevity guided by clarity achieves more than volume guided by uncertainty.

1. Oversight based on function, not form.

Define regulation by residual risk, not label. These risks are measured directly, not inferred from form.

First, we assess the diagnostic factors that reveal economic abstraction.

- ***Transferability:*** it trades freely.
- ***Passive economic risk:*** you bear risk or reward without real control.
- ***Limited enforceability:*** you cannot compel performance or obtain meaningful remedies for operational failures.
- ***Systemic dependency***: your outcome depends on the whole enterprise functioning, not just your own use.
- ***Weak collective action:*** investors cannot coordinate to oversee the enterprise.

Then we assess the modular abstracted economic property along the three universal axes for financial instruments:

- ***Agency and collective action risk:*** hidden control, insider dominance, asymmetric information, and collective action impracticalities.
- ***Derivative risk:*** leverage, recursive exposure, or systemic contagion.
- ***Market-integrity risk:*** manipulation, custody failure, or data opacity.

2. Coordinated supervision with a designated lead supervisor.

Assign oversight dynamically. Jurisdiction follows risk, not political turf.

- The SEC governs when passive exposure, informational asymmetry, or collective action problems dominate.
- The CFTC governs when derivative contagion or leverage is systemic.

- Joint oversight applies when market integrity or other risks overlap.

It is also important to get the input of other relevant experts. That includes technical participation by the National Institute of Standards and Technology (NIST), and coordination with the Federal Reserve Board for overlapping banking products. The rulebook should not be created in a vacuum from the Department of Treasury and the Department of Commerce.

3. Recognize technological mitigation.

If a system's design—its code, consensus mechanism, or audit trail—demonstrably neutralizes a risk, that risk is deemed technologically mitigated. Regulation scales down automatically. Code that proves compliance enables lighter law.

Regulatory intervention should be implemented ***through the least intrusive means necessary to achieve these objectives***. For example, core purposes of securities regulation to promote capital formation, protect investors, and facilitate fair and orderly markets were to be implemented ***through the least intrusive means necessary to achieve these objectives***.[5] This pillar has been forgotten and has demonstrated the need for its inclusion in legislation.

4. Single touch—creates a shared registration pathway.

A shared registration and disclosure infrastructure. A cryptographically assured audit ledger—a Regulatory Node—which would provide continuous, verifiable transparency and non-duplicative oversight.

A single venue can list securities, derivatives, and commodities (and stablecoins) under one rulebook.

5. Interoperability—shares oversight through data.

A unified registry coordinates transparency across agencies. The SEC and CFTC supervise jointly via a shared audit trail—not duplicative exams.

6. Why It Works

We already do this in banking. The OCC, Fed, and FDIC share supervision through a lead examiner model—one agency leads, others observe through common data. No chaos. No duplication. Just coordination. We can do the same here. It's law behaving like an ecosystem—differentiated but interoperable.

---

[5] Federal Securities Act, Hearings Before the House Interstate and Foreign Commerce Committee, 1st Session, on H.R. 4314 (Mar. 31, 1933) (Hon. Huston Thompson, former member of the FTC who helped develop the federal securities legislation, stated: "The purpose and policy here is to protect . . . with as little interference with business as possible. This is the main theme upon which we played in building up this bill."); *see* 77 Cong. Rec. 937 (1933) (President Franklin D. Roosevelt observed that federal securities legislative proposals did not pursue investor protection at all costs and were designed to impose "the least possible interference to honest business.").

IX. Conclusion

Anther Sophia Guillén Methodology

As I close, I return to the question of mindset. Sophia is lending us another one of her methodologies. As I mentioned, conversations with Sophia are often nonlinear and she interrupts constantly. She questions everything, and refuses to wait for the end of a debate before starting a new one. Sophia demands clarity—not necessarily to challenge—but to understand. And she reminds me that in a world that's changing this quickly, questioning is not disruption; it's discipline.

This is another Sophia Guillén Methodology I encourage everyone to adopt, especially policymakers: ***stay curious, stay interruptible, and keep asking why—challenge assumptions.*** We do not need perfect answers; but we do need an honest process. We need humility in the face of complexity, and confidence in collaboration.

My Call To You—To Collaborate

At this moment in time, we are being called to collaborate—to get this architecture and design right. We need the economists who understand incentives and equilibrium. We need the engineers who know where code can sustain—or silently subvert—the law. We need the lawyers who can translate complexity into structure. We need the data scientists who can ground every debate in evidence rather than ideology. None of us can solve this alone.

But together, through research, dialogue, and design, we can help Congress and the regulators get this right—not by demanding perfection, but by offering perspective, precision, and purpose.

So my invitation to you—the thinkers, builders, and teachers in this room—is simple: lend your insight, your data, your ideas. Help move this from theory to structure. Our goal is to build the next system of trust—one designed, tested, and improved by all of us.

Thank you.

ATTACHMENT 3

Teresa Goody Guillen

A Framework for Regulating Programmable Digital Asset Markets

(October 08, 2025)

Available at SSRN: https://ssrn.com/abstract=5621450 or http://dx.doi.org/10.2139/ssrn.5621450

Measure Twice: Designing Trust for the Algorithmic Age

A Framework for Regulating Programmable Digital Asset Markets

By Teresa Goody Guillén

I. Executive Summary

The Fourth Industrial Revolution is characterized by efforts to make trust programmable, distributed, and decentralized. Yet, while decentralization aims to remove bias, human-coded systems are inherently imbued with human influence. The progression of prior industrial revolutions was outsourcing labor—first mechanizing muscle with steam; second, scaling production with electricity; and third, digitizing knowledge with computers. Now, we are outsourcing trust to code. This shift replaces institutional trust with architectural trust, which includes design decisions that are embedded in systems and govern behavior and incentives. Key questions arise about governing a world where rules are dictated by software and decisions are refereed by algorithms, including how to preserve fairness and flexibility in code-governed lives. The law's ancient purpose is to civilize society by translating disruption into order, as it has done throughout history as commerce, industrialization, markets, and networks have evolved.

The Fourth Industrial Revolution is shifting the foundation of capitalism from human institutions to algorithmic architecture. While trust has been enforced by courts, regulators, and intermediaries, it is now increasingly ensured by code. This transformation promises efficiency, but also redefines where risk lives—and who bears it.

Current U.S. digital asset legislation measures form instead of function — defining assets by name ("security," "commodity," and a proposed "ancillary asset") rather than by the economic behaviors and risk exposures they generate. This proposal presents a Market Architecture of Trust, a structural framework for regulating digital asset markets through measurement, design, and proportionate intervention, rather than categorical overreach. The approach revives the principles of the 1903's securities and derivatives laws—function over form, visibility as accountability—while updating them for programmable economies.

Regulatory intervention has been necessary when there is abstraction of ownership and control of economic interests/rights, which is more exacting in its analysis since those interests/rights are modularized or disaggregated from the previously inextricably combined bundles of rights. The central concept is to regulate residual risk, not form. Technology can internalize many governance functions once performed by law; regulation should scale only where residual risk—risk not neutralized by architecture—remains.

II. Current Market Structure Legislative Proposals

Below are key features of the market structure proposals. The fundamental flaw in both is that decentralization is not required for an asset to be a non-security.

Feature	House CLARITY Act (H.R. 3633)	Senate Draft II (Sept 2025)
Key Difference	It is binary: decentralization decides everything.	Creates a temporary period to become decentralized after launch; non-decentralized tokens can avoid being treated like full securities if they follow the ancillary asset disclosure regime, with the goal of becoming decentralized.
Regulatory Categories	**Two:** either a **Security** or a **Digital Commodity**. Classification hinges on network decentralization. Introduces term "investment contract asset" for tokens in investment contracts, but this is only a label (tokens are still either securities or commodities).	**Three: Security**, **Commodity**, or **Ancillary Asset**. Fully decentralized tokens = **commodities**; tokens with traditional security characteristics = **securities**; others can be designated **ancillary assets** (a new category with temporary securities-lite treatment).
Decentralization Test	**Determinative:** a bright-line **"decentralization = commodity"** rule. A **"mature, decentralized"** blockchain (no controlling persons, widespread use) means its token is not a security. If a network is not mature/decentralized, its token is a security. Self-certification of mature blockchain status is deemed mature after 60 days unless the SEC objects.	**Determinative:** tokens on **fully decentralized** networks are treated as commodities. **Lack of Decentralization** = security or **ancillary asset** if it lacks traditional security rights. It sets an expectation that ancillary asset networks will decentralize over time (within 4 years).

Token Characteristics & Definitions	**"Digital Commodity":** a token intrinsically linked to a functioning blockchain and not controlled by an issuer. The Act **excludes** any token that represents a security, any **derivative contract**, or stablecoin from being a digital commodity. Tokens on centralized networks are simply **"digital asset securities"** (investment contracts). The Act's "investment contract asset" terminology refers to the same token but does not alter its treatment.	**"Ancillary Asset":** defined as an **intangible digital asset** offered pursuant to an investment contract, **so long as it carries no debt/equity interest or entitlement to profits, dividends, or other financial rights**. Ancillary assets are part of the **securities offerings** at the time of sale, but the token itself is not called a security. Tokens that do embed traditional security interests or represent an investment fund share are carved out of this category. Self-certification of ancillary asset status becomes effective unless SEC rebuts within 60 days.

III. Market Fundamentals of Self-Correction and Triggers for Regulatory Intervention

Markets are best structured and designed to be self-correcting. Markets behave according to the incentives and constraints embedded in their design. The architecture sets the incentives, and the incentives shape behavior. Markets can be further structured to discipline themselves through contract, competition, and reputation (called "private ordering"). When information is visible and incentives are aligned, the invisible hand operates as self-correcting mechanism. Prices transmit knowledge, reputation reinforces honesty, and competition rewards efficiency.

When "abstraction" enters—that is, when risk becomes detached from control, which can result from complexity outpacing comprehension, or information becoming asymmetric or hidden (including inside code)—the self-correction mechanisms of the market fails and the feedback loop breaks. That's when residual risk begins to accumulate and cannot be priced, contracted away, or revealed by competition alone. When hidden exposures build up, private discipline loses traction. The market stops being a self-governing ecosystem.

When markets cannot self-correct, this is where regulation intervenes to restore the balance between private responsibility and public trust. Regulation is an error correction mechanism to re-establish the feedback loop that allows the invisible hand to work. Generally, it makes visible again the relationship between those who create risk and those who bear it.

IV. The Problem: Measurement Failure as Market Failure

Markets are systems of measurement; they turn complexity into prices, incentives, and accountability. When law stops measuring the right variables, it becomes part of the problem. Contemporary legislative drafts (House CLARITY Act and Senate Digital Asset Market Structure bills) measure the wrong variables. They fixate on classification—security vs. commodity vs. proposed (misguided) "ancillary asset"—instead of economic behavior and their residual risk. This produces three predictable failures:

1. **Regulatory Arbitrage:** Risk migrates between agencies and across jurisdictions. Hidden leverage and manipulation thrive in the gaps.
2. **Innovation Flight:** Builders move offshore to avoid ambiguous frameworks that regulate uncertainty faster than risk.
3. **False Security:** Lawmakers and investors believe markets are governed when the most dangerous risks—recursive derivatives, opaque leverage, and fragile interdependencies—remain invisible.

The historical parallel to this is the 1920s investment trusts and the 2008 derivatives markets; both failed due to the widening separation of risk from control (abstraction) without measurement. Today's digital asset markets risk repeating those failures unless measurement catches up with abstraction. This is not overregulation or under-regulation—it is mis-regulation.

V. How Current Legislative Proposals Codify Market Failure

A. Mis-Measuring the Variable of Risk

Digital assets are multi-behavioral instruments: they can simultaneously behave as securities (e.g., when there is agency), as derivatives (e.g., when there is synthetic exposure), and as commodities (e.g., when they serve as network fuel). The proposed bills attempt to force these hybrid instruments into static silos. This mis-measurement creates blind spots identical to those that preceded 1929 and 2008: hidden leverage, information asymmetry, and a false sense of control. Classification replaces comprehension.

It is important to identify which of the risks are present, if any that the regulations are designed to address (the purpose for regulation in the first place). We do not create regulations for the sake of regulating; they must exist to achieve a legitimate purposes and be not more restrictive than needed to achieve their aim. Depending on the type and level of potential risk, regulations serve as guardrails to address or contain those specific types of risks when markets do not self-correct. But market rules can be created to align

incentives to address risks and self-correct. Below is a summary of the reasons the various law regimes exist and the risks the rules are designed to address.

1. **Securities law:** agency (information asymmetry) and coordination (protect dispersed investors from those with control / supervision over their economic property interest).

2. **Derivatives law:** systemic stability and integrity of references (protect counterparties and markets from hidden leverage, contagion, manipulation).

3. **Commodities law:** market integrity and delivery assurance (protect commercial participants and consumers from manipulation, fraud, and distortions in price discovery, ensuring fair competition and functional spot and futures markets).

The existence of the risks from these categories are not mutually exclusive for digital assets. This is because digital assets enable modularization, such that rights previously inextricably combined in one asset can now be unbundled into separate assets, and that digital assets can possess any number of combinations of these rights, and layer them.

B. Ignoring the Derivative-Like Nature of Tokens

Many tokens function economically similar to derivatives—representing synthetic, leveraged, or recursive exposure to underlying assets or networks. The programmability of digital assets adds leverage, rehypothecation (reusing/repledging collateral holding for a third party to secure its own loans), and recursive exposure looks like diversification but is exposed to same risk indirectly and repeatedly (DeFi loops, where crypto borrowed, re-deposited, and borrowed against across multiple DeFi protocols)—all of which can create instability in the market. An illustration of a DeFi loop is if ETH is lent to a protocol in exchange for synthetic tokens ("stTokens") that are used as collateral to buy stablecoins, which in turn are swapped for more ETH from the original protocol to earn yield in the form of additional stTokens. Participants are able to stack synthetic claims that can unwind in cascades. Agency is in contract design.

These are functionally similar to 1920s investment trusts: leveraged claims nested within each other, appearing diversified but systemically intertwined. When the first fails, contagion cascades. The proposed legislation fails to recognize this behavior, ensuring that the next crash—like 1929—will stem not from fraud, but from measurement failure. While many market participants proactively manage risk, legislation that requires them to address risks mischaracterized by inaccurate labels—rather than actual residual risks—may result in critical risks remaining unmitigated, potentially decreasing overall market stability.

C. The "Ancillary Asset" Concept: A Category Error

The Senate draft introduces the "ancillary asset"—an "intangible" associated with an investment contract. This is doctrinally incoherent.

- In traditional jurisprudence, the investment contract is the mechanism of investment; the token is the subject and/or the proceeds.
- By labeling the subject as "ancillary," Congress risks inverting the logic of property itself—treating the medium of value as legally secondary.

This definitional confusion hardwires inconsistency into law, producing arbitrary and bizarre results, particularly when applied across the securities law overall regime.

D. Over-Reliance on "Decentralization" as a Proxy for Safety

Current bills hinge regulation on decentralization metrics—a political aesthetic, not a risk variable. Decentralization is multifaceted and, in some cases, borders on illusory; it is often conflated with distributed; and it does not guarantee reduced risk or accountability. Nodes can be decentralized but control centralized; ownership can be decentralized while information asymmetry endures. Decentralization does not eliminate reliance—it multiplies it, or at the very least transfers and may obscure it. It replaces vertical trust chains with horizontal dependencies, which can hide new vulnerabilities. The key question should not be "is it decentralized" but whether residual risk is reduced by design, and if not, how to address it. Measurement of risk, not decentralization status, should guide regulation.

The legislative proposals are further misguided in reducing the test for a security to a single variable: decentralization. This factor, which may influence one element of the multi-factor *Howey* test for one type of security (investment contract), is being elevated to the overarching test for all 30+ securities named by statute. This produces an incoherent and contradictory framework that engenders market instability.

E. The Result: Structural Fragility by Design

If enacted, the current legislative framework would have the resulting design flaws and consequences.

Design Flaw	Consequence
Categorical classification of assets	Jurisdictional confusion and regulatory arbitrage; false positives and negatives leading to application of wrong regulations and addressing wrong risks
Derivative-like behaviors ignored	Hidden leverage and systemic contagion
Overemphasis on decentralization	False positive and false negatives; false confidence; limiting competition and innovation inconsistent with decentralization
Favors decentralized token networks	Ignores tokens' risk even if otherwise the same
Mis-definition of "ancillary asset"	Legal incoherence and inconsistent enforcement

Static statutory categories	Market ossification and innovation flight

This is not a question of intent, but of using an incorrect measurement. The bills institutionalize opacity under the guise of clarity. They legislate the same design flaws that 1933 sought to correct.

VI. The Policy Principle: Law as Architecture, Not Reaction

Law's purpose is not to freeze innovation, but to civilize it. It must act as an adaptive architecture that restores alignment between risk, control, and accountability. Like the disclosure-based reforms of 1933 and 1934, regulation must make abstraction legible, measurable, and self-correcting. When markets self-correct, oversight should recede. When they cannot, regulation must re-enter proportionately. The craft of law lies in precision, not proliferation.

A. Principles of Design

Markets with trust require principles of discipline including clarity (information revealing, not obscuring), accountability (power meeting consequence), incentives (encouraging honest behavior), and resilience (containing failure). Proper design leads to self-correcting markets and measured government intervention, making trust verifiable rather than illusory. Design is a strategy that tunes incentives and behavior, emphasizing measured intervention only when systems fail to self-correct. When adequate design elements are present such that markets self-govern, then intervention can recede.

B. Intervention Threshold

Markets self-correct by competition, contract, and reputation until residual risk—unseen or unowned risk—accumulates. At this threshold, governance must restore feedback loops to maintain market function, intervening proportionally and retreating once equilibrium is restored. The architecture of trust relies on transparency, accountability, and proportionate intervention, transforming complexity into order.

VII. The Economic Abstraction Framework

The Economic Abstraction Framework is not *Howey* or any other human behavioral lens, rather, it is an architectural one. It identifies when regulation is needed by measuring the distance between risk and control—measuring exposure not expectation.

A. Historical Lessons in Abstraction and Governance

Scalable Ownership: The seventeenth-century joint-stock company allowed ordinary investors to share profits without control, creating the separation of ownership and control and necessitating governance to ensure accountability .

Commodity Abstraction: The nineteenth century introduced futures markets, turning natural uncertainty into tradable risk and eventually derivatives detached from physical goods, spreading but also hiding risk.

Modern Corporation: By the early twentieth century, dispersed ownership and professional management required legal responses like the 1933 and 1934 Acts to provide transparency as a substitute for direct control, establishing a social contract linking abstracted ownership (separated from control) with disclosure and accountability.

Derivatives and Hidden Risk: Late twentieth-century financial engineering increased complexity and opacity, contributing to the 2008 crisis through repackaged risks that obscured true exposure and broke public trust.

Commodity Detachment: Financialization of commodities in the early 2000s such that commodity prices (e.g., wheat, corn) were no longer primarily determined by physical market forces of supply and demand, led to speculative price swings disconnected from physical supply, affecting entire economies.

Decentralization is not a panacea, as it redistributes reliance horizontally rather than eliminating it, potentially multiplying dependencies and vulnerabilities.

B. Five Diagnostic Factors of Abstraction

1. **Transferability.** How freely does the asset trade? How fast can risk move? High transferability amplifies contagion; it requires real-time visibility.

2. **Passive Economic Exposure.** Who creates the value? When holders bear risk without influence over value creation, accountability gaps emerge.

3. **Limited Enforceability.** Can participants protect themselves? Code-based systems may lack legal or feasible remedies; this is fragility, not necessarily fraud.

4. **Systemic Dependency.** What keeps the system running? Dependency on narrow actor sets (developers, oracles, validators) increases and obfuscates systemic risk. What systems are built on this system such that system failure cascades to other systems failing?

5. **Limited Collective Action.** Can participants coordinate? When governance requires mass unanimity, markets lose self-correcting capacity.

When these factors cluster, regulation should activate—not to replace markets, but to restore equilibrium between risk and control. When technology mitigates them, oversight should recede automatically. Law becomes dynamic—a thermostat, not a shackles.

C. Residual Risk as the New Measure of Trust

Residual risk is the risk remaining after technology, competition, and contracts act. Law should regulate this residual risk, not form or labels, adapting oversight proportionally to technological mitigation. This approach echoes the 1930s philosophy of aligning risk with control, making transparency mandatory, and intervening only when necessary.

VIII. The Modern Market Structure Compact

A. Simpler Way Forward—Modern Market Structure Compact

The proposed compact framework to restore function over form by:

- Regulating residual risk across three axes: agency risk, derivative risk, and market-integrity risk.
- Creating a shared registration pathway and joint oversight between SEC and CFTC.
- Assigning lead supervisors dynamically based on risk dominance.
- Recognizing technological mitigation to scale regulation accordingly. This model parallels banking supervision, emphasizing coordinated, interoperable regulation rather than duplication.

B. The Ethic of Measurement—Measure Twice, Cut Once

Borrowing from carpentry, governance should avoid wasting trust by measuring abstraction and residual risk carefully before acting, balancing innovation and protection to build lasting markets that deserve trust.

C. Oversight Based on Function, Not Form—with Lead Supervisor

Oversight shall correspond to predominant residual risk rather than statutory label:

- Investment risk (enterprise abstraction) — subject to SEC oversight;
- Leverage or synthetic exposure (exposure abstraction) — subject to CFTC oversight;
- Custody and market-integrity risk (market abstraction)—jointly, but deftly, supervised.

A lead supervisor will be designated based on predominant residual risk. Oversight authority shall rotate as risk shifts, with data shared through a joint regulatory node accessible to both agencies.

D. Joint Registration and Oversight

- Agencies develop and maintain digital compliance portals responsive to the technology they regulate, including establishing a regulatory node—a shared, cryptographically assured audit ledger.

- Agencies access a unified data registry to avoid duplication and enhance visibility.
- Modeled after banking supervision: one lead examiner, shared data, no overlap.
- Create a shared registration and disclosure infrastructure across SEC/CFTC.
- Enable one-rulebook for venues where securities, commodities, derivatives (and stablecoins) can coexist.

E. Recognition of Technological Mitigation

- When verifiable code neutralizes a risk (e.g., automated transparency, tamper-proof audits), the law scales down.
- Code that achieves compliance obtains regulatory relief.
- Industry solutions and safeguards shall be recognized, avoiding duplicitous and burdensome oversight.

F. Proportionate Intervention

- Regulation should expand and contract with measured residual risk, not ideology.
- Law behaves as a circuit breaker: active when markets cannot self-correct; dormant when they can.
- In so doing, laws and regulations shall avoid incentivizing one design architecture (e.g., decentralization) over another (centralization) to foster competition and a free market.

These principles allow law to evolve with innovation while protecting the public trust.

IX. Conclusion: Building Systems That Deserve Trust

Trust is shifting from being institutional to architectural. The goal of law is not to stop innovation, but to civilize it—to translate code into confidence and markets into mechanisms of fair opportunity. The 1930's securities reforms civilized financial abstraction by requiring transparency, aligning incentives, curbing excessive speculation and leverage, and controlling contagion. Today, we must civilize financial abstraction through measurement. By regulating residual risk of abstracted economic interests instead of form, Congress can preserve both innovation and integrity—ensuring markets that are free enough to innovate and fair enough to endure. Freedom is not self-sustaining—it must be maintained by design. Measure twice. Cut once. Build systems that deserve our trust.

ATTACHMENT 4

Teresa Goody Guillén

Essential Revisions to Strengthen Digital Asset Market Structure Proposals, Prevent Market Failure, and Ensure Securities Law Consistency

(Sept. 7, 2025)

Available at SSRN: https://ssrn.com/abstract=5458774 or

http://dx.doi.org/10.2139/ssrn.5458774

Essential Revisions to Strengthen Digital Asset Market Structure Proposals, Prevent Market Failure, and Ensure Securities Law Consistency

By: Teresa Goody Guillén

Introduction[1]

The rapid development of Distributed Ledger Technology ("DLT") and associated digital assets demands a timely and precise regulatory approach. Delay stifles innovation and weakens U.S. competitiveness, while overreach or missteps could trigger market failure. The legislative goal is not to construct a sprawling regime, but to chart a correct course and empower executive agencies with flexible tools to respond as markets evolve. We do not need perfection, but we must avoid steering in the wrong direction.

Current legislative proposals—the House Clarity Act[2] and the Senate Discussion Draft II[3]— would benefit from being scaled back to simple, smart guardrails and nimble agency oversight. A rulebook that takes years to write will be outpaced by the market it seeks to govern. These proposals are myopic in their reliance on decentralization as the key factor in classifying an asset. Further, the Senate draft's re-labeling of the "subject" of an investment contract as an "ancillary asset" is doctrinally incorrect and confusing. The resulting classification based on intangibility is arbitrary, lacks grounding in economic reality, and will result in inconsistent application of securities laws. Procedural requirements, such as agency auto-approvals resulting from resource constraints, are impractical and create misaligned incentives, improperly transferring accountability from private market participants to the government. Additional unintended consequences that will negatively impact the digital asset market and/or create inconsistent or absurd results in the securities law regime are also discussed.

This proposal revises and synthesizes these competing frameworks. It advances an alternative approach to asset classification and proportionate regulation based on: (i) economic property rights (or interests) and the abstraction thereof—the separation of ownership and control over the economic property; (ii) the modularized economic property made possible by DLT—the unbundling of rights and obligations that previously were inextricably combined; and (iii) the

---

[1] This paper builds on the prior paper co-authored by the same author. Goody Guillen, Teresa and Corbett Sterling, Isabelle, *Paving the Path for Crypto Clarity: A Framework for Digital Asset Regulatory Structure* (Discussion Draft) (February 17, 2025), https://ssrn.com/abstract=5156725.

[2] The Clarity Act seeks to provide a regulatory system for the offer and sale of digital asset commodities. Digital Asset Market Clarity Act of 2025 or Clarity Act of 2025 ("Clarity Act"), H.R. 3633, https://www.congress.gov/bill/119th-congress/house-bill/3633/text.

[3] The Senate Discussion Draft II seeks to differentiate digital asset securities and commodities, and create a disclosure regime for newly-created "ancillary assets." Chairman Tim Scott (R-SC), Senators Cynthia Lummis (R-WY), Bill Hagerty (R-TN), and Bernie Moreno (R-OH), Discussion Draft of the Responsible Financial Innovation Act of 2025 (Senate Discussion Draft II") (Sept. 5 2025), https://cdn.sanity.io/files/ifn0l6bs/production/c0fd5849c0fa5f8f591d3825a17a4eaa44db8c9b.pdf. A prior version of the discussion draft ("Senate Discussion Draft I") is available at https://www.banking.senate.gov/imo/media/doc/senate_banking_committee_digital_asset_market_structure_legislation_discussion_draft.pdf.

various risks created by economic abstraction factors (discussed below) and particular modular stacking—risks of ownership of the specific economic property rights without effective control thereof. The approach builds on both longstanding regulatory principles and the thoughtful work of the House and Senate proposals.

Executive Summary

To delineate between a security and non-security, or to more precisely identify what constitutes "any interest or instrument commonly known as a 'security,'"[4] it is necessary to identify the *sine qua non* of a security—or the essential element necessary for a security to exist. The more than 30 types of securities enumerated by federal statute all involve economic property interests and the separation of ownership from control (e.g., voting trust certificates, passive partnership interests). Accordingly, this proposal advocates for a framework centered on two core concepts: ***Economic Abstraction*** and ***Modular Ownership***.

Economic Abstraction exists when an economic interest's value depends on an enterprise's[5] success, but the holder lacks meaningful control and direct, enforceable rights. This concept is assessed through five "Economic Abstraction Factors":

1. **Transferability**: The instrument can be freely traded in secondary markets.
2. **Passive Economic Interest**: The holder bears the enterprise's risk or reward without meaningful operational control.
3. **Limited Enforceability**: The holder lacks direct contractual rights to compel performance or obtain meaningful redress for operational failures.
4. **Systemic Dependency**: The instrument's value depends on enterprise-wide performance or managerial execution by an identifiable group rather than external market forces or individual use.
5. **Limited Collective Action**: Holders cannot meaningfully coordinate to exercise collective supervision over the enterprise.

Modular ownership recognizes that DLT allows the unbundling of traditional ownership rights—such as voting, economic interest, and enforceability—into distinct components. This modular approach clarifies the classification of tokens and distinguishes securities from commodities based on structural economic realities.

A central premise of this proposal is that ***capital raising marks the critical trigger for securities market regulation***. It is at this moment—when an enterprise sells financial claims to outsiders to fund its operations or growth—that investor protection and disclosure obligations attach. Outside investors become exposed to financial risk without direct managerial control or internal enterprise information, heightening the risk of information asymmetry and agency conflicts.

[4] The definition of a security includes this as one of its components. 15 U.S.C. § 77b(a)(1).
[5] An "enterprise" is broadly construed generally refers to a venture or undertaking. It is purposeful in its existence in that there is some sort of organized activity with the intent to achieve certain objectives (economic, operational, strategic, etc.), but it does not require any specific structure or scale.

Where these factors do not warrant the application of securities laws, the same risk-based principles can determine the appropriate non-securities regulatory intervention, if any. By leveraging DLT's inherent capabilities—such as transparency and programmability—regulation can be made proportionate to the specific risks an asset presents. For example, digital assets functioning as bearer instruments can be treated as such with modifications. DLT enhances transparency, reduces theft risk, and enables programmable legal compliance, mitigating the concerns associated with traditional bearer bonds. This framework proposes safe harbors for digital bearer instruments that meet specified transparency, antifraud, and AML standards.

A proposed **18-Month Legislative Timeline** would include statutory amendments to direct the U.S. Securities and Exchange Commission ("SEC") to define a "digital asset security" using the Economic Abstraction Factors, broaden the Commodity Futures Trading Commission's ("CFTC") exemptive authority, and grant the CFTC commodity spot market regulatory authority.

I. Foundational Principles and Theoretical Framework

A. Core Regulatory Philosophy

This proposed structure builds on the House and Senate bills, offering modifications to avert the critical market failures their current forms might precipitate. While cognizant of the apparent appeal for behavioral tests like decentralization,[6] this proposal advocates for an additional functional approach, based on economic property interests and market structure analysis.[7] This philosophy applies to both securities and non-securities. Central to the securities approach is the recognition that capital raising establishes the basis for regulatory intervention. At this point, the core purposes of securities regulation—capital formation, investor protection, and market efficiency—are most implicated and should be implemented ***through the least intrusive means necessary to achieve these objectives***. This fourth pillar to "protect . . . with as little interference with business as possible" was a main theme of Securities Act of 1933 ("Securities Act"),[8] but it has since been forgotten. The "least intrusive means" is a required and integral element to the development and implementation of the regulatory regime.

This approach is anchored in foundational economic and legal theories, designed to avoid over-regulating markets while instituting safeguards when information asymmetry and moral hazard

[6] While I do not believe that decentralization is an appropriate approach for legislation defining a digital asset security, I am cognizant that this is one method that legislators wish to apply. Accordingly, rather than eliminate the decentralization approach and return to other doctrinal approaches altogether, I propose modifications and alternatives to avoid critical market failure that would ensue if decentralization is a requirement for a digital asset to be a non-security.

[7] *See* Posner, Richard A., *Economic Analysis of Law*, Boston: Little, Brown and Company (1973).

[8] Federal Securities Act, Hearings Before the House Interstate and Foreign Commerce Committee, 1st Session, on H.R. 4314 (Mar. 31, 1933) (Hon. Huston Thompson, former member of the FTC who helped develop the federal securities legislation, stated: "The purpose and policy here is to protect . . . with as little interference with business as possible. This is the main theme upon which we played in building up this bill."); *see* 77 Cong. Rec. 937 (1933) (President Franklin D. Roosevelt observed that federal securities legislative proposals did not pursue investor protection at all costs and were designed to impose "the least possible interference to honest business."); 77 Cong. Rec. 3801- 2 (May 20, 1933) (On H.R. 5480, Fletcher stated: "The country justly demands that the public have some protection . . . and honest business a legitimate chance.").

exist.[9] The framework is rooted in rights/interests, obligations, and risks rather than subjective factors such as profit motive or decentralization.[10] The framework's philosophical foundation rests on four principles:

1. **Economic Abstraction as the Defining Characteristic**: Regulation should apply when economic exposure to enterprise value is separated from meaningful control, creating information asymmetries, agency costs, and collective action difficulties.
2. **Modularized Ownership Recognition**: Regulation must acknowledge that DLT enables the disaggregation of traditional ownership bundles into distinct, transferable modules, each requiring tailored treatment.
3. **Functional Market Structure Analysis**: Regulatory treatment should be determined by the actual economic relationships not formulaic categorizations.
4. **Proportionate Regulation to Specific Risks**: Regulation must be proportionate to the actual risks posed, leveraging an asset's technological capabilities to reduce the regulatory burdens where appropriate.

B. Inadequacies of Current Proposed Models

The Dangers of Over-Relying on Howey and Decentralization

The current legislative proposals reduce the security test to a single variable: decentralization. This factor, which may influence one element of the *Howey* test for one type of security (investment contract), is being elevated to the overarching test for all 30+ securities named by statute. This produces an incoherent and contradictory framework that engenders market instability.[11]

---

[9] *See* Smith, Adam, *The Wealth of Nations*, Oxford, England: Bibliomania.com Ltd. (2002). The framework also incorporates Adolf Berle's insight that securities holders possess rights or interests that are economic in nature, divorced from control, and held by individuals who require protection from those who do exercise control. *See* Adolf A. Berle, Gardiner C. Means, *The Modern Corporation and Private Property*, New York: The Macmillan Company (1933, revised ed. 1970).

[10] There are numerous decentralization metrics and indicators, generally falling into the categories of political, economic, and administrative decentralization. If a comprehensive framework is universally adopted, this would reduce subjectivity and enable decentralization to be meaningfully compared across DLT networks. *See* Ovezik, C., Karakostas, D., Milad, M., Woods, D.W., Kiayias, A. (2025). SoK: Measuring Blockchain Decentralization. In: Fischlin, M., Moonsamy, V. (eds) Applied Cryptography and Network Security. ACNS 2025. Lecture Notes in Computer Science, vol 15825. Springer, Cham. https://doi.org/10.1007/978-3-031-95761-1_7.

[11] The Securities Act defines as a security as follows:

> [U]nless the context otherwise requires—(1) [t]he term "security" means any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a "security," or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing.

Over-reliance on the *Howey* test and decentralization leads to two primary problems:

1. **False Negatives**: Instruments that function as securities escape regulation, leaving investors unprotected.
2. **False Positives**: Tokens with genuine utility or functionality are incorrectly classified as securities due to superficial factors like initial fundraising. Examples of non-securities in centralized systems:
   - Prepaid Functional/Utility Token: Redeemable only for services, not transferable
   - Enforceable Royalty NFT: Embedded contract rights tied to IP
   - Cooperative Governance Token: Voting and usage without economic abstraction

This myopic approach will lead to critical failures, including stifled innovation, as projects contort themselves to an amorphous decentralization standard, and increased investor harm from premature project abandonment. Consequently, the proposals fail to address the actual risks, which prevents effective investor/consumer protection (including technological integrity), transparency, and market fairness. Additionally, the proposals create ambiguity regarding the application of specific securities laws, including various anti-fraud provisions and private rights of action. It is also unclear whether, and to what extent, Congress intends to attempt to preempt state statutory and common law (*e.g.*, tort and contract law), and other legal regimes, such as the Uniform Commercial Code.

Why the "Ancillary Asset" Concept is Doctrinally Misguided

The Senate Discussion Draft II introduces the notion of an "ancillary asset"—"an intangible asset, including a digital commodity, that is offered, sold, or otherwise distributed to a person pursuant to the purchase and sale of a security through . . . an investment contract[,]" which may or may not itself a security. This concept inverts longstanding doctrine. An investment contract is the mechanism for an investment opportunity; the token is the subject of that opportunity.[12] Labeling the token "ancillary" misstates both economic reality and legal substance, producing absurd results. Its definition arbitrarily distinguishes between tangible and intangible assets and creates inconsistent treatment across federal securities laws. To the extent the goal is to reach digital assets on a DLT network, there are more precise distinctions than intangibility, which extends to intellectual property, business-related property (e.g., goodwill), and many financial and contractual claims. It also ignores the other securities instruments and transactions that are capable of involving a digital asset beyond investment contracts and profit-sharing agreements. While the safe harbor provisions for ancillary assets offer a thoughtful framework, anchoring the analysis in economic abstraction—not decentralization—provides a more functional comprehensive approach.

15 U.S.C. § 77b(a)(1). While the foregoing definition from the Securities Act is slightly different in the Securities Exchange Act of 1934 (15 U.S.C. § 78c(a)(10)), these definitions are typically interpreted consistently. *United Housing Foundation, Inc. v. Forman*, 421 U.S. 837, 847 n.12 (1975).

[12] *Paving the Path for Crypto Clarity* at 15, 29-30.

C. The Core Concepts: Economic Abstraction and Modularized Ownership

Under § 2(a)(1) of the Securities Act, a "security" encompasses a range of instruments including stocks, bonds, notes, debentures, voting trust certificates, evidence of indebtedness, profit-sharing agreements, and more. These instruments share structural DNA: they are transferable, passive, and represent abstracted economic interests in an enterprise. Enterprise generally refers to a venture or undertaking (regardless of its structure or scale). The fundamental element of a security is essentially economic abstraction in a capital raising context—the condition when an individual bears economic exposure (i.e., risk or reward) to the outcome of an enterprise without having enforceable rights to control or secure that outcome. This condition, where control and risk are separated, is a hallmark of many securities and one reason why regulatory oversight is often needed to mitigate information asymmetry and agency problems. Risk/control separation is not determinative on its own, but its presence across traditional instruments (e.g., voting trust certificates, passive partnership interests, debt notes) suggests it may serve as a foundational diagnostic feature in a functional taxonomy of securities.[13]

Digital assets magnify these issues. ***Economic Abstraction*** manifests as detached exposure to value generation by others, with potentially limited participation but lacking meaningful control, and for which direct enforceable rights are insufficient or structurally limited. [14] ***Modularized Ownership*** allows for the unbundling of rights traditionally bundled in a single asset. By splitting these rights apart, each can be tokenized and sold independently, creating securities-like instruments. DLT enables this unbundling in unprecedented ways, which is why certain digital assets are more akin to securities than others. Digital assets, as modular rights to abstracted economic property, can be analyzed based on the elements that warrant regulation, considering the technological advancements that may mitigate the need for it.

II. Agency Problems and Collective Action Challenges

Federal securities laws were designed to address two foundational market failures: (1) agency problems (and resulting information asymmetry), and (2) collective action and bargaining failures. These failures provided the structural rationale for mandatory disclosure regimes, fiduciary duties, and antifraud provisions.

---

[13] This approach bears some similarity to the *Howey* test, as the investment contract category has been used to capture nontraditional securities transactions that are ***not enumerated by statute***. However, this proposed regulatory approach differs in significant ways, as it identifies the fundamental requirement(s) of a security—meaning securities enumerated by statute (e.g., voting-trust certificate) and nontraditional investment arrangements that may be an investment contract. This approach identifies what is meant by the term in the definition of a security: "***any interest or instrument commonly known as a 'security,'***" 15 U.S.C. § 77b(a)(1), and is consistent with significant developments of the meaning of a security in federal securities jurisprudence, including: (i) applying a family resemblance test to determine the characterization of an instrument, *Reves v. Ernst & Young*, 494 U.S. 56, 64-65 (1990); (ii) whether the securities laws are necessary as a key factor in determining whether they should apply, *Marine Bank v. Weaver*, 455 U.S. 551 (1982); and (iii) whether the purpose of obtaining the asset is fundamentally consumptive or for speculative investment, only the latter of which requires the extra protection of the securities laws, *United Housing Foundation, Inc. v. Forman*, 421 U.S. 837 (1975).

[14] Notably, decentralized nature and pseudo-anonymity can make enforcement more difficult and people may incorrectly assume these features mean they have no liability under common law tort, contract, etc.

A. Agency Problems

Agency costs arise from the separation of ownership and control, particularly when agents (issuers, developers) possess more information than principals (tokenholders). DLT can modify this relationship by aligning incentives and increasing transparency, but it also introduces new risks related to software integrity and cybersecurity.

B. Collective Action Problems

Securities regulation addresses the difficulty dispersed securities holders face in coordinating oversight, such as to demand information, negotiate principal terms, or monitor management. DLT can either exacerbate this problem through pseudonymity or mitigate it through mechanisms like DAOs. In designing a risk-based approach, the more automated a system, the more critical the integrity of its underlying technology becomes.

C. DLT as a Disclosure Substitute

DLT's inherent transparency can serve as a substitute for traditional disclosure. On-chain data on token supply, governance, and transactions is often immutable and immediately visible. Smart contracts can embed operational information directly into the asset, providing automated updates. This real-time access can significantly reduce information asymmetry. Consequently, where DLT achieves the core objectives of disclosure, mandatory requirements can be scaled back.

A ***DLT-Based Disclosure Exemption for Securities*** could be warranted when:

1. On-chain data is complete, reliable, and publicly accessible (on a venue and in a format easily accessible by the general public).
2. Tokenholder rights are programmatically enforced via smart contracts.
3. Information accessibility and symmetry exist by virtue of the protocol.
4. Active governance systems allow for effective, coordinated oversight.

This approach prioritizes regulation that is justified by persistent market failures, not rigid adherence to legacy frameworks. It operationalizes the principle that securities regulation must be justified by the persistence of agency costs or collective action problems. Where DLT remedies these market failures, regulatory intervention can step back, resulting in a flexible, cost-effective framework that leverages the benefits of DLT systems. As discussed above, regulatory safeguards may be warranted for technological integrity and cybersecurity to ensure proper functioning of the DLT-based tools.

III. Digital Assets as Bearer Instruments and DLT Advantages

Many digital assets function as bearer instruments, where control depends on possessing a private key. While traditional bearer bonds were phased out due to risks of money laundering and tax evasion, DLT addresses these concerns through:

1. ***Transparency***: Unlike physical bearer bonds, digital assets on public ledgers provide an immutable transaction history.
2. ***Reduced Theft Risk***: While digital assets face cybersecurity risks, cryptography and multi-signature mechanisms provide security generally superior to physical instruments.
3. ***Audit Trail***: DLT creates comprehensive, tamper-evident audit trails that facilitate regulatory oversight.
4. ***Programmable Compliance***: Smart contracts can embed regulatory requirements directly into digital assets.
5. ***Real-Time Settlement***: DLT enables near-instantaneous settlement and clearing, and reduces counterparty risk and operational inefficiencies.

Given these advantages, the prohibitions on traditional bearer securities can be re-evaluated for DLT-based "smart" bearer instruments.

A. Safe Harbor Provisions for Digital Bearer Instruments

A safe harbor could deem a digital bearer instrument lawful if it meets certain requirements, such as immutable public recording of transfers, built-in anti-fraud measures, and AML compliance at trading venues. This would provide legal certainty for issuers and developers without precluding necessary disclosures or liability for misconduct.

B. Modernization of Section 12(g) for DLT Assets

Securities and Exchange Act of 1934 ("Exchange Act") §12(g) requires issuers with widely held equity securities to register their securities and become subject to periodic reporting and disclosure requirements. The triggers for an issuer to register its equity securities are:

1. The issuer has total assets greater than $10 million; and
2. The issuer exceeds 2000 "holders of record,"[15] or if there are 500 or more non-accredited investors among the holders of record (employee compensation-related holders are excluded, and collective investment vehicles and securities held in street name are counted as one holder).

This trigger applies to any class of equity security,[16] which recognizes that equity holders often have a long-term stake in the issuer and bear the issuer's ultimate risk. Debt holders, on the other

[15] A holder of record is "each person who is identified as the owner of such securities on records of security holders maintained by or on behalf of the issuer, subject to" several provisions, two of which are more notable here: (1) when the records of security holders are not properly maintained then holder of record includes any person who would be counted if records were kept in a generally accepted practice; (2) outstanding unregistered or bearer certificates are each counted as being held of record by a separate person unless the issuer can establish that, if registered, the securities would be held by less people. 17 CFR § 240.12g5-1.

[16] For purposes of this section, the term "equity security" is defined as follows:

> to include any stock or similar security, certificate of interest or participation in any profit sharing agreement, preorganization certificate or subscription, transferable share, voting trust certificate or certificate of deposit for an equity security, limited partnership interest, interest in a joint venture, or certificate of interest in a business trust; any security future on any such security; or any security convertible, with or without consideration into such a security, or carrying any warrant or right to

hand, are often more concerned with creditworthiness and repayment, as opposed to governance, or a claim on profits or capital appreciation.

Applying this to decentralized networks requires modification. Potential amendments to § 12(g) include:

- Redefine "holders of record" to count unique beneficial owners with freely transferable, economically exposed tokens, omitting custodial or protocol-controlled accounts.
- Registration and disclosure duties could be triggered based not on raw headcounts but market conditions: free transferability, thresholds for retail trading, liquidity, and depth.
- A safe harbor could also exempt issuers from duplicative SEC reporting when all material information is public, reliable, and verifiable on-chain, and is on a venue and in a format making it generally available to the public.

IV. The Economic Abstraction Framework

A. Framework Development

The Economic Abstraction Factors provide an analytic framework for determining when an asset should be subject to securities regulation, and are additionally informative to develop regulatory frameworks for non-security digital assets. These factors focus on the risks arising from the separation of economic exposure from meaningful control. Crucially, this framework recognizes that DLT's transparent, programmable infrastructure can mitigate the need for traditional mandatory disclosure. Where DLT provides equivalent or greater market transparency and enforceability, duplicative disclosure requirements are unnecessary.

B. The Economic Abstraction Factors

An instrument may constitute a security if it exhibits a sufficient clustering of the following characteristics ***in a capital-raising context***. These factors should be considered on a sliding scale in which no single factor is determinative:

1. ***Transferability***: The instrument is capable of being transferred, assigned, or traded in secondary markets without operational involvement in the underlying enterprise.
2. ***Passive Economic Property Right/Interest***: The holder possesses an economic property right or interest such that the holder bears risk or reward of the enterprise (project or venture) without meaningfully participating in operational control. The inability to exercise meaningful control serves as a key indicator that some level of protection may be needed, and may exist due to the: (a) lack of legal control due to agreement or technological restrictions; (b) absence of capacity to control due to requisite expertise; or (c) lack of

---

subscribe to or purchase such a security; or any such warrant or right; or any put, call, straddle, or other option or privilege of buying such a security from or selling such a security to another without being bound to do so.

17 CFR § 240.3a11-1.

practical control due to over-reliance on an identifiable group with unique abilities, including expertise or access.

3. ***Limited Enforceability***: The holder lacks direct, enforceable contractual rights to compel enterprise performance or obtain meaningful redress for operational failures. When economic rights/interests are insufficiently enforceable by private contract, regulation can compensate for the lack of ex ante bargaining power, ex post remedies, etc. This requires someone to be accountable for operational failures, which could include an insurance-like feature, or certain assumptions of risk.[17]
4. ***Systemic Dependency***: The value of the instrument depends on enterprise-wide performance or managerial execution by an identifiable group,[18] rather than individual usage, consumption activities, traditional market forces, and similar factors external to the enterprise.
5. ***Limited Collective Action***: The holders lack the meaningful ability to coordinate with one another to exercise collective responsibility and supervision over the enterprise.

C. Interplay Between Economic and Governance Rights

An instrument granting both economic exposure and effective governance control may not be a security in the conventional sense. However, nominal governance rights do not equate to meaningful control. If voting rights are practically ineffective due to holder dispersion, information asymmetry, or insider dominance, the holder remains in a state of economic abstraction, and the Economic Abstraction Factors should be considered.

D. Liability Nuances

Liability for fraud remains, with criminal statutes and common law rights of action fully applicable. Federal securities laws provide enhanced protection, such as relaxed reliance requirements for plaintiffs in certain fraud cases.[19] The regulatory framework must distinguish between ***exempt securities*** and ***exempt transactions***, as they carry different liability standards. The

[17] Notably, digital assets that are goods are subject to express and implied warranties (such as merchantability and fitness for a particular purpose), and certain public policy limitations on the enforceability of disclaimers for strict liability in tort, unconscionability, and fraud/misrepresentation. And those assets or activities that are classified as services are also subject to common law, including contract and tort law, such as principles of implied covenants of good faith and fair dealing, workmanlike performance, professional duty standards, negligence, etc. In most U.S. jurisdictions, one cannot waive liability for gross negligence or willful misconduct as it is against public policy to protect conduct approaching bad faith. The doctrine of unconscionability also serves as a non-waivable backstop: procedurally, it protects from unequal bargaining power and unfair surprise, and substantively it invalidates contract terms that are unreasonably harsh or one-sided. It is worth noting that a smart contract (computer program that automatically executes predefined actions when coded conditions are met) is not the same as a contract (a legally binding agreement between parties formed through offer, acceptance, and consideration), but a smart contract may be used as the performance mechanism. The enforceable contract obligations are rooted in law, not code.

[18] This paper applies a common sense, reasonable interpretation of words. For example, a "an identifiable group" intends to mean an articulable group of persons who coordinate in some manner and are capable of being identified even if they evade or make it difficult to identify them.

[19] Generally, common law fraud requires the plaintiff to prove the elements: (1) material misrepresentation (false statement or omission), (2) defendant know the statement was false or acted with reckless disregard for the truth, (3) defendant made the statement with the purpose of causing the plaintiff to act/not act, (4) plaintiff justifiably relied on the misrepresentation, and (5) plaintiff suffered actual harm as a result of the reliance.

SEC may also exercise its broad exemptive authority under Securities Act § 28 and Exchange Act § 36, which offer flexibility to exempt—conditionally or unconditionally—any person, transaction, or instrument from all provisions of the respective Act.

E. The Decentralization Puzzle

A sophisticated framework must also account for varying network control structures.

1. ***No Identifiable Control Group, But Economic Rights/Interests Exist.*** When tokenholders have economic exposure, such as price appreciation aligned with increased network usage, but there is no centralized managerial group, the traditional securities law rationale is weaker because there is no identifiable "other" managing the enterprise. Nonetheless, the absence of a control group does not render regulation unnecessary. Systemic risks, including fraud, manipulation, and persistent collective action problems, may still be present, particularly as market-based triggers such as broad retail accessibility and deep liquidity emerge. Thus, regulatory intervention (not necessarily within the securities regime) may still be warranted based on these market characteristics, recognizing that governance failures and regulatory gaps can arise even in the absence of a centralized agent. In addition, technological integrity (e.g., bugs) and cyber risks (e.g., hacking) may warrant different types of regulatory considerations.
2. ***No Identifiable Control Group, and Only Consumptive Use Rights*.** If the instrument confers purely consumptive utility—such as a non-transferable subway card—without any exposure to the enterprise's economic value, it falls outside the scope of securities regulation. The functional token operates solely as a voucher or payment method. A fluctuation in value based on demand for the functional token does not change its non-security characteristics, and does not create the information or agency asymmetries that justify securities law intervention. However, other consumer protections are warranted.
3. ***Diffuse or Fragmented Control*.** When control is so widely dispersed that, while governance rights exist in theory, practical collective action is infeasible. The separation between formal governance entitlements and actual decision-making power results in a persistent economic abstraction: the token holder cannot meaningfully participate in management due to coordination challenges, expertise gaps, or information asymmetry. Regulatory intervention may be warranted to ensure the effectiveness, not simply the formal existence, of governance mechanisms.

This framework encourages regulation that tailors oversight to genuine risks arising from abstraction and control dynamics in digital asset markets.

V. Market Structure Triggers

Regulatory oversight should be calibrated to market structure characteristics that indicate heightened risk of manipulation, fraud, information asymmetry, or collective action difficulties. These triggers can apply in both securities and non-securities contexts:

1. ***Retail Market Access***: Assets available for trading by retail investors through centralized or decentralized exchanges trigger disclosure requirements if information asymmetry exists and market surveillance to ensure fair and efficient markets.
2. ***Market Depth and Volume***: Significant trading volume, market capitalization, or liquidity metrics above specified thresholds could require more comprehensive market structure oversight and manipulation prevention measures. While large volumes and deep liquidity indicate healthy trading environments, they also increase market susceptibility to manipulation and fraud if left unchecked.
3. ***Ecosystem Interdependence and Significance***: Assets integral to broader digital asset ecosystems or serving as infrastructure for other tokenized instruments may warrant systemic risk assessment and potentially regulatory requirements narrowly tailored and proportionate to the specific risks.

VI. Registration and Disclosure Framework

Proportionate Registration: The regulatory requirements should be scaled to market capitalization, with streamlined procedures for smaller offerings and exemptions for instruments meeting specified criteria related to reduced agency costs and collective action difficulties.

Proportionate and Flexible Disclosure: Ongoing disclosure requirements should be calibrated to the degree of information asymmetry, with a focus on materiality. Lighter-touch disclosures, such as something inspired by Form D or Form CF, may be more appropriate.

Technical Implementation: Regulatory reporting should leverage DLT technology and standardized data formats to minimize compliance costs while enhancing regulatory visibility and market transparency.

VII. Legislative Language and Implementation

A. Proposed Statutory Amendments

Definition of Digital Asset Security: One option is to create a new term, "digital asset security," meaning any digital representation of rights or interests in economic property that, in the context of a capital-raising activity, exhibits economic abstraction, as determined by the Economic Abstraction Test, to be established by Commission rule. An alternative is to request that the Commission undergo rulemaking to formalize that "any interest or instrument commonly known as a 'security'" includes any representation of rights or interests in economic property that, in the context of a capital-raising activity, exhibits economic abstraction, as determined by the Economic Abstraction Test, to be established by Commission rule. Under either approach, the Commission would be required to develop an objective test that creates a rebuttable presumption of a security.

Broad Exemptive Authority for the CFTC: Extend broad authority to the CFTC to exempt any transaction or instrument from the CEA, similar to the SEC's authority.

Broad Spot Market Regulatory Authority for the CFTC: Provide the CFTC with regulatory authority (not only enforcement authority) over the commodity spot markets.

B. Implementation Timeline

Phase I (Months 1-6): Establish a digital asset regulatory coordination council and develop initial guidance on the Economic Abstraction Test.

Phase II (Months 7-12): Promulgate rules implementing the proportionate regulation framework and streamlined registration procedures.

Phase III (Months 13-18): Implement market infrastructure requirements for trading platforms and custody providers.

Phase IV (Ongoing): Continuously monitor and refine the framework based on market developments and technological evolution.

VIII. Specific Comments to Senate Discussion Draft II

The following non-exhaustive list highlights issues, in addition to those discussed elsewhere in this proposal, that require particular attention.

1. **Over-reliance on Investment Contract Analysis**: The proposals' focus on investment contracts is doctrinally incorrect. The SEC's historical analysis of analogous assets, such as trading stamps in 1958, is instructive. The Commission correctly refrained from exercising jurisdiction over items like trading stamps, meal tickets, and gift certificates, that may be evidence of indebtedness securities, recognizing they were not what Congress intended to regulate as securities.[20] There are other securities and transactions that are capable of involving digital assets.
2. **Definition of Digital Asset**: The definition requires cryptographic security, but not all DLT assets are cryptographically secured. Permissioned or enterprise DLT systems may use other control mechanisms.
3. **Gratuitous Distributions**: The draft's position that a gratuitous distribution is not an offer or sale must be consistent across the securities laws such as Rule 144 and mindful of long-established securities law precedent that a "gift" intended to create a public market constitutes a sale for "value."[21]

---

[20] SEC Interpretative Rel., The Commission's Statement Regarding Trading Stamps, 17 C.F.R. § 231.3890 (Jan. 24, 1958), https://www.govinfo.gov/content/pkg/FR-1958-01-25/pdf/FR-1958-01-25.pdf ("SEC Stamps Rel."). The SEC concluded that trading stamps were not securities in 1958, which was 12 years after the *Howey* decision and 25 years after the Securities Act was enacted. Trading stamps were small, colorful coupons with adhesive backings provided to customers as a reward mechanism and were a widely used marketing tool used by merchants. 43 Individually, each stamp held minimal monetary value— typically just a few pennies. In 1956, over 168 billion trading stamps were distributed, and there was a significant trading stamps market, including a secondary market. Merchants purchased these stamps from issuers and distributed them to customers, who could collect and redeem them for cash or valuable items such as furniture or toys. In the stamp ecosystem, merchants controlled the distribution, which they significantly altered by offering promotions like "double" or "triple" stamp days, and stamp issuers determined the value of the merchandise for which stamps could be redeemed. Notably, the SEC did not even consider the investment contract analysis potentially applicable here, and only considered whether the stamps were evidence of indebtedness.

[21] The Commission has repeatedly taken the position for over 50 years that the lack of monetary consideration does not mean that there was not an offer or sale for purpose of Section 5; for example, a gift of stock is a sale when the

4. **Consistent Definitions Across Existing Securities Laws**: The concept of ***common control*** must be applied consistently with existing statutes, rules, and precedents. The proposals' new standards and definitions of common control need to be clarified to the extent they are inconsistent with already-existing definitions and thresholds. The use of ***equity interest***, versus ***equity stock***, versus ***share***, need to be adequately defined and in a manner consistent with the already-existing definitions of these terms.
5. **Self-Certification Impracticality**: The Commission lacks the resources to review all self-certifications. This system would transfer liability to the government and create perverse incentives and free-riding, likely leading to a flood of automatic approvals or denials without substantive review due to resource limitations.
6. **Voluntary Disclosure and Liability**: The provisions for opting into securities laws must clarify which liability provisions apply, and how long they apply, if not indefinite, to provide predictability for issuers and purchasers.
7. **Furnished vs. Filed**: The distinction between filed certifications (with heightened liability) and furnished materials should be consistent with the disclosure requirements across the federal securities laws.
8. **Investment Contract Rulemaking**: The proposed rulemaking does not correct existing problems with judicially created tests and introduces new issues. The definition should be revised to require a clear quid pro quo exchange. First, there must be the provision of capital or other assets—this constitutes the investment ("quid"). Second, there must be a legally recognized right or contractual claim to both another party's future efforts to manage a venture on behalf of the investor, and the proceeds of those obligated efforts (e.g., income, revenue, profit)—this represents legal entitlement ("quo").[22]
9. **Conflation of Instruments**: Profit-sharing agreements and investment contracts are distinct instruments and should not be collapsed. Similarly, passive interests in partnerships, limited liability companies, or trusts should not be automatically construed as investment contracts.
10. **Bank Custody and Basel III**: Legislative carve-outs are needed for banks engaging in digital asset services to avoid the prohibitively high capital requirements under Basel III for Group 2 crypto-assets.[23]
11. **Regulatory Sandbox Prohibition**: A permanent prohibition from the sandbox for a fraud conviction, without a time limit, appears improperly targeted.

---

purpose of the "gift" is to advance the donor's economic objectives rather than to make a gift for simple reasons of generosity. *See, e.g.*, Capital General Corporation, 54 SEC Docket 1714, 1728-29 (July 23, 1993) (Capital General's "gifting" of securities constituted a sale because it was a disposition for value, the "value" arising "by virtue of the creation of a public market for the issuer's securities."); *see also SEC v. Harwyn Industries Corp.*, 326 F. Supp. 943 (S.D.N.Y. 1971). SEC, *SEC Brings First Actions to Halt Unregistered Online Offerings of So-Called 'Free Stock*,' SEC Rel. 99-88 (July 22, 1999) (By gifting stock and in some cases receiving additional shares for linking to the issuer's website or soliciting additional investors, the issuers "received value by spawning a fledgling public market for their shares, increasing their business, creating publicity, increasing traffic to their websites.").

[22] Further discussion of proposed changes to the test of an investment contract are discussed in our prior paper. *Paving the Path for Crypto Clarity* at 15, 29-30.

[23] Basel III requires banks to classify crypto assets into two groups, with much different capital requirements, and most crypto exposures are capital-inefficient. Group 2 covers all unbacked crypto (e.g., bitcoin) and requires prohibitively high risk weights (upwards of 1,250%).

12. **Tokenized Real-World Assets**: These assets should continue to be regulated similarly to their underlying counterparts, with the underlying asset's regulator involved in marketplace rulemaking.
13. **DeFi Protocol Regulation**: The draft places too much weight on decentralization and fails to address the actual risks, including information accessibility, cybersecurity, and the enforcement of common law rights and duties, as discussed in footnote 17 *supra*.
14. **Undefined Terms**: Key terms, such as what constitutes a "mass-minted" NFT series, require clear definition.
15. **Failure to Address Accredited Investor Definition**: The antiquated and paternalistic wealth thresholds to access investment opportunities results in arbitrary exclusion from our markets. Intermediation and exclusion from financial markets are significant drivers of DLT and decentralized finance, as well as the creation of alternative economic property structures that fall outside securities regulations. To democratize our financial markets and enable fair access to digital asset securities, the accredited investor definition must be changed contemporaneously, to require no more than basic financial literacy or access to expert advice.[24]

IX. Conclusion

This proposal's alternative approach—focused on economic abstraction, modularized ownership, and proportionate regulation—addresses the fundamental inadequacies of current legislative proposals. By focusing on the purposes underlying regulatory intervention and leveraging DLT's inherent capabilities, this principle-based approach can better facilitate capital formation, ensure fair and efficient markets, and protect investors without imposing undue burdens on legitimate business activities.

[24] Discission of potential changes to the accredited investor definition are discussed in our prior paper. *See Paving the Path for Crypto Clarity* at 35-36.

Appendix: DA-K Lite – Disclosure Checklist

To operationalize this framework, the "DA-K Lite" offers a principles-based disclosure standard tailored to DLT-based enterprises. It is a practical, cost-effective alternative to legacy reporting, focused on materiality and feasibility. Many projects already make this information publicly available.

Core Protocol Information

1. **Protocol Description:** Plain-English explanation of the protocol's function and key technical dependencies.
2. **Tokenomics & Supply Schedule:** Disclosure of total supply, issuance/burn schedule, vesting arrangements, and token distribution.

Governance & Control

3. **Governance Structure:** Description of voting mechanisms, quorum thresholds, and proposal procedures.
4. **Material Participants:** Identification of core developers, holders with ≥10% governance rights or token supply, and operators of critical infrastructure.

Financial & Risk Profile

5. **Treasury & Financials:** DAO treasury balance, major holdings, and spending policies.
6. **Conflicts of Interest:** Disclosure of related-party transactions and governance capture risks.
7. **Known Risks & Dependencies:** Smart contract audit status, legal/regulatory risks, and critical operational dependencies.

Market Activity

8. **Trading & Liquidity:** Platforms where the token trades, approximate volume, and any transferability restrictions.

Ongoing Updates (Event-Driven)

9. **Material Code Changes**: Major protocol upgrades or forks with economic impact.
10. **Material Governance Events**: Significant votes on treasury allocations or token supply.

Key Features of the DA-K Lite

- **Lean**: A principles-based checklist focused on materiality.
- **Machine-Readable**: Encourages reporting in machine-readable formats.
- **Event-Driven**: Emphasizes timely updates rather than rigid quarterly filings.
- **Enforced Access**: Disclosures may be required by trading platforms as a condition for listing.

ATTACHMENT 5

Teresa Goody Guillén and Isabelle Corbett Sterling

Paving the Path for Crypto Clarity: A Framework for Digital Asset Regulatory Structure

Discussion Draft (February 17, 2025)

Available at SSRN: https://ssrn.com/abstract=5156725 or

http://dx.doi.org/10.2139/ssrn.5156725

Paving the Path for Crypto Clarity: A Framework for Digital Asset Regulatory Structure

Discussion Draft

By Teresa Goody Guillén and Isabelle Corbett Sterling

February 17, 2025

Discussion Draft: February 17, 2025
Do not cite in academic work without authors' consent.

Paving the Path for Crypto Clarity: A Framework for Digital Asset Regulatory Structure

Teresa Goody Guillén
Isabelle Corbett Sterling

Abstract

The rapid growth of digital assets presents both unprecedented opportunities and significant regulatory challenges, necessitating a thoughtful and comprehensive legal framework. Paving the Path for Crypto Clarity: A Framework for Digital Asset Regulatory Structure proposes a structured approach to creating a regulatory regime that encourages innovation while ensuring reasonable consumer protection and accountability. Our approach is structured as a thorough assessment of the market, its components, participants, design, and infrastructure, as well as the roles, interconnectedness, risks, and other significant factors related to each.

In creating the framework we first considered existing classes for traditional assets, and identified how those classes are defined and how their respective assets are grouped. We then applied a similar grouping logic to develop a methodology to define and group digital assets into classes. Specifically, we identified many of the most common types of digital assets, as well as their defining characteristics, remaining mindful that innovation is ongoing. For each digital asset type, we evaluated its particular qualities and the risk/return profile to determine, as a preliminary matter, whether it should be subject to regulatory oversight and, if so, what issues regulations would likely address. We also identified significant categories of market participants and their respective roles, and considered potential risks and concerns related to these roles, particularly in the context of the current market structure.

The framework ultimately recognizes twelve broad digital asset classes and identifies which digital assets fit within each class. The digital asset classes are compared to existing asset classes, entities, and activities to identify potential suitable regulatory authorities. Such classification and assessment provides an overall system to analyze and determine the appropriate legal and regulatory regimes to apply to the market as a whole and to its components.

Throughout this paper, we emphasize the need for clarity in the classification of assets in order to ensure fair market practice and mitigate systemic risk. We also identify and integrate foundational regulatory principles—including transparency, protection, adaptability, due process, and proportionality to guide the crafting or amending of regulation. The framework also integrates lessons from traditional corporate governance while acknowledging the distinct decentralized, transparent, and peer-to-peer nature of Digital Ledger Technology ("DLT") networks. We analyze DLT networks as an emerging business structure contrasting it with traditional corporate structure and identifying characteristics and incentives that shape its governance.

Inspired by Justice Louis Brandeis's advocacy for transparency and accountability, the framework highlights disclosure as a powerful regulatory tool. As Brandeis famously observed, "Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman."[i] However, in the digital era, excessive disclosure can be counterproductive. As former SEC Commissioner Troy Paredes cautions, "Sunlight can also be blinding."[ii] While transparency is essential, an overload of unstructured or excessive information can obscure meaningful insights, hindering consumer protection and regulatory effectiveness. The framework seeks to strike a balance, ensuring transparency while preventing information saturation that could undermine oversight and informed decision-making.

The framework advocates for adaptive, forward-thinking regulation that balances innovation and responsibility. By encouraging collaboration among regulators, industry participants, and policymakers, the framework seeks to foster market stability, consumer protection, and the growth of a dynamic digital asset ecosystem.

The paper invites feedback and collaboration to further refine this evolving blueprint into a functioning regulatory landscape for digital assets that is effective, practical, and adaptable to the fast-paced evolution of technology.

[i] *Louis D. Brandeis, Other People's Money and How the Bankers Use It, New York: Frederick A. Stokes Company, at 92 (1914).*
[ii] *Troy A. Paredes, Blinded by the Light: Information Overload and Its Consequences for Securities Regulation, Washington University Law Quarterly, Vol. 81, No. 2, at 417-85 (2003).*

Table of Contents

I. Introduction 1

II. DLT Networks As A New Business Form 2

A. DLT Networks As Economic And Governance Structures 3

B. Parallels Between DLT Networks And The Evolution Of Corporate Structures 3

C. The Transformation Of Property, Ownership, And Control 4

D. DLT Networks, Profit Models, And Ecosystem Participants 6

E. Regulatory Considerations For Future DLT Governance 6

III. Methodology For A National Regulatory Approach 6

IV. Principles Driving Regulation 9

V. Foundational Concepts For Digital Asset Analysis 10

A. Digital Asset Description 10

B. Digital Asset Characteristics 10

C. Digital Asset Risk/Return Profile 11

D. Potential Concerns 11

E. Digital Asset Market Structure And Market Participants 11

VI. Digital Asset Classes 12

A. Digital Payment Units 12

B. Primary Digital Currencies 13

C. Functional Digital Assets 13

D. Digital Commodities 13

E. Digital Asset Securities 14

F. Asset-Backed Stablecoins 17

G. Tokenized Real World Assets 17

H. Non-Fungible Digital Assets 17

I. Tribal And Social Digital Assets 17

J. Non-Functional Inert Digital Assets 17

K. Hybrid Digital Assets 18
L. Other Digital Assets 18
VII. Classification Analysis Of Specified Digital Assets 18
VIII. Securities Law Principles And Modifications Applied In The Framework 29
A. Revised Definition Of "Investment Contract" 29
B. The Application Of The Principle Of Control 32
C. Revised Approach To "Accredited Investor" Definition 35
IX. Classification Of Specific Digital Assets 37
X. Identifying Appropriate Legal And Regulatory Regimes 37
A. Securities And Exchange Commission 38
B. Commodity Futures Trading Commission 38
C. Federal Trade Commission 39
D. U.S. Department of the Treasury 40
E. Banking Regulators 40
F. Department of Justice 41
XI. Considerations For Coordinated Comprehensive Regulation 41
A. Coordinated Agency And Legislative Action 41
B. Considerations For Regulatory Oversight Of Digital Asset Centralized Exchanges 42
C. Considerations For Regulatory Oversight Of Spot Digital Assets Markets 44
XII. Conclusion And Next Steps 46

Exhibit 1: Proposed Digital Asset Classification Chart

Exhibit 2: Proposed Market Participant Chart

Discussion Draft: February 17, 2025
Do not cite in academic work without authors' consent.

Paving the Path for Crypto Clarity: A Framework for Digital Asset Regulatory Structure

Teresa Goody Guillén*
Isabelle Corbett Sterling**

I. Introduction[1]

The rapid evolution of Distributed Ledger Technology ("DLT") and associated digital assets presents both an unprecedented opportunity and a profound challenge for policymakers worldwide. Cryptocurrencies, stablecoins, decentralized finance ("DeFi"), and other types of digital assets are fundamentally reshaping financial systems, commerce, and the global economy. Regulating this dynamic industry is inherently multidisciplinary, requiring seamless coordination across regulatory agencies and the executive and legislative branches. This burgeoning industry intersects with and is shaped by numerous areas of law, requiring a unified and coordinated regulatory framework capable of fostering innovation while providing pragmatic safeguards to protect consumers.

In President Trump's Administration, the regulatory approach is no longer confined to patchwork solutions and artificial boundaries. This Framework for Digital Asset Regulatory Structure provides a structured approach to create a regulatory regime for digital assets and a methodology to determine how digital assets should be categorized and treated from a legal and regulatory perspective. This framework is designed to be forward-thinking and anticipate the future of technology, considering not-yet-emerged products and assets, rather than merely trying to catch up with current developments.

---

* Teresa Goody Guillén leads an AmLaw100 firm's Digital and Innovative Markets team and co-leads its Web3 and Digital Assets team. She has a broad practice spanning litigation and investigations, as well as corporate matters, and is nationally-regarded for her securities law expertise. A seasoned advocate, Teresa represents clients in high-stakes litigation and before the SEC, DOJ, and other government entities, and formerly worked for the SEC's Office of the General Counsel. She has extensive experience in both financial and digital asset markets, and their intersection. Teresa also advises clients on capital raises under Regs S, D, A+ and CF and on navigating the evolving regulatory landscape surrounding digital assets and DLT (including blockchain), particularly regarding securities laws, commodities laws, and anti-money laundering regulations. A veteran of the industry, she is heavily engaged in the discussions around an appropriate framework and market structure for digital assets.
** Isabelle Corbett Sterling is a commodities and derivatives lawyer with significant experience in digital assets and Web3 technologies. She advises clients on a broad range of matters in those areas, including regulatory, enforcement, investigations, transactional and legislative. A seasoned lawyer with significant advocacy experience, Isabelle advises clients on the implementation of new technologies and the development of innovative products, such as virtual currencies and DLT-based assets, and guides them through registrations, compliance issues, and regulatory investigations and enforcement actions. Her policy experience includes seven years as global head of government relations at a blockchain company as well as several years in Washington, D.C.
[1] This framework was shaped through extensive discussions and collaboration with industry participants, thought leaders, legal experts in various areas of law, and technology visionaries. "Crypto" as used herein is a noun that is synonymous with the digital assets associated with DLT.

This blueprint is useful for a U.S. framework, as well as frameworks globally. While the terminology may differ among countries, we encourage countries and international organizations to apply consistent principles, to the extent possible, to these borderless assets and markets.

We welcome insights and feedback as we continue to refine and enhance this framework, and we look forward to continued collaboration on its further development.

II. DLT Networks As A New Business Form

When considering appropriate regulatory frameworks, the overall context of what is being regulated is important. In this case, digital assets are not stand-alone instruments but are integral to DLT networks—they operate together.[2] The differing rights and obligations represented by these assets are inherently tied to their respective DLT networks and associated ecosystems. As DLT evolves, its applications and governance structures continue to expand, reshaping economic activity, governance, and value exchange.

This transformation extends beyond a structural shift; DLT networks redefine how trust, ownership, and economic coordination function. They challenge traditional business models, financial systems, and governance structures, necessitating a reexamination of regulatory approaches. DLT and Web3 technologies are working to solve longstanding challenges related to trust, privacy, efficiency, centralization, financial inclusion, and more by enabling decentralized and secure solutions across various industries. These technologies are reshaping the way individuals and organizations interact with data, assets, and services. These solutions should be understood within the broader context of our current era—the Fourth Industrial Revolution—a period of rapid technological advancements encompassing artificial intelligence ("AI"), blockchain and other DLT networks, quantum computing, and biotechnology.[3] Just as previous industrial revolutions reshaped industries through mechanization, electrification, and digital computing, today's technological innovations are transforming financial markets, corporate governance, and societal structures at an unprecedented pace. Accordingly, DLT networks and digital assets should be analyzed within this broader technological shift, recognizing that they will continue to evolve and redefine economic paradigms.

---

[2] DLT is an overarching term that encompasses various technologies, including blockchain, Directed Acyclic Graph ("DAG"), Hashgraph, and Holochain. *See Distributed Ledger Technology (DLT),* Legal Information Institute, Cornell Law School (explaining and distinguishing various DLTs), https://www.law.cornell.edu/wex/distributed_ledger_technology_%28dlt%29; *see also* RSM US LLP, *Blockchain and the Island of Yap*, https://rsmus.com/insights/industries/financial-services/blockchain-and-the-island-of-yap.html (describing the first distributed ledger system).

[3] *See* Klaus Schwab, *The Fourth Industrial Revolution: What It Means, How to Respond*, World Econ. F. (Jan. 14, 2016), https://www.weforum.org/stories/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/; *see also* United Arab Emirates Gov't, *The UAE Strategy for the Fourth Industrial Revolution*, UAE, https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/the-uae-strategy-for-the-fourth-industrial-revolution.

A. DLT Networks As Economic And Governance Structures

As DLT networks facilitate economic activity and commercial transactions, they are increasingly integrating with—or in some cases, replacing—traditional business models. In some respects, they resemble corporate entities by performing similar roles in resource allocation, value creation, and governance. Many DLT networks implement formalized governance mechanisms, such as token-holder voting and delegated decision-making, akin to corporate board structures. However, DLT-based ecosystems differ significantly from traditional corporate structures in several ways:

- **Decentralization:** DLT networks operate on a spectrum of decentralization, often dispersing control among a distributed network rather than centralizing it within a corporate hierarchy.
- **Permissionless versus Permissioned Access:** While some DLT networks are open and permissionless, allowing anyone to participate, others impose access restrictions akin to corporate or financial gatekeeping.
- **Transparency and Pseudonymity:** Transactions on DLT networks are typically transparent and auditable, yet participants often remain pseudonymous.
- **Distributed Consensus:** Governance in DLT networks is executed through decentralized consensus mechanisms rather than hierarchical corporate oversight.
- **Automation and Smart Contracts:** Smart contracts enable automated enforcement of agreements, shifting governance functions from individuals to code.

There are a variety of DLT networks and governance structures, including direct token-holder participation and delegated authority models. This decentralization of control echoes historical shifts in corporate governance and legal theory.

B. Parallels Between DLT Networks And The Evolution Of Corporate Structures

It may be that DLT enables separating rights that previously were bundled and granting new rights. This would not be the first time that previously bundled rights have been separated in a way that challenged traditional theories. The evolution of the corporate structure likewise challenged conventional logic, particularly with regard to ownership, control, and property. Originally, a natural person and their business were not separate, which is significant when the liability of the person owning and managing the business cannot be detached from the business itself. The incentives of the owner, controller, and accountable person were fully aligned (in the same person or group). As businesses evolved into separate entities from their owners and managers, the dynamics and incentive structure changed. The fundamental theory of corporate law is "the establishment of a *form* of doing business; i.e., the creation of an artificial entity, the conferring upon it of such powers as are necessary to give it proper business efficiency, while placing upon it such restrictions as will properly safeguard the interests of those peculiarly concerned in the

corporation, as well as the public."[4] Juxtaposing this structure to DLT, the entities that create DLT networks are similar artificial entities in that they are legal constructs, state-registered entities, and/or state-licensed businesses, but the networks themselves often operate autonomously without formal incorporation. A DLT network's governance structure may be a separate entity (e.g., a decentralized autonomous organization ("DAO")), which may be a recognized legal entity or a type of association, depending on the developing applicable law.

DLT's democratization and distribution of control over enterprises may be viewed as separating rights and obligations that have historically been united. The corporate form has undergone significant transformations, particularly regarding the separation of ownership and control.[5] Corporations first developed as "groups of investors pooling their individual contributions of risk capital to organize and carry on an enterprise"—the same individuals both owned and controlled the enterprise.[6] When ownership of the corporation (represented by stock) was separated from control (management of the enterprise), "the two attributes of ownership-risking collective wealth in profit-seeking enterprise and ultimate management of responsibility for that enterprise[. . .]had become divorced."[7] These changes to incentives, rights, and obligations called for a "new form of economic organization of society."[8] New questions had to be answered, such as whether an owner who relinquishes control of their wealth should still retain all the benefits derived from it, or if their interest in the wealth changes as a result of the relinquishment.[9]

Similar to the evolution of the business structures and the corporate form, DLT networks enable new forms of economic organization that challenge aspects of conventional notions of ownership, control, and property.

C. The Transformation Of Property, Ownership, And Control

The evolution of the corporate structure led to changes in property relationships, distinguishing between:

1. **Passive Property:** "a set of relationships between an individual and an enterprise, involving rights of the individual toward the enterprise but almost no effective powers over it"; and

---

[4] U.S. House of Representatives. *Report of the Commissioner of Corporations*, 58th Congress, 3d Session, Document No. 165, at 38 (Dec. 1904) Government Printing Office, 1937 ("Comm. Corp. Rep."), www.sechistorical.org/collection/papers/1900/1904_1221_ReportCorporations.pdf.
[5] Adolf A. Berle, Gardiner C. Means, *The Modern Corporation and Private Property*, at xx (revised ed. 1970) ("Berle").
[6] *Id.* at xxvi.
[7] *Id*.
[8] *Id*.
[9] *Id.*

2. **Active Property:** "a set of relationships under which an individual or set of individuals hold powers over an enterprise but have almost no duties in respect to it which can be effectively enforced."[10]

DLT networks introduce a novel consideration: whether the possession of active property is itself private property that can "belong to and be disposed of by its possessor."[11] For example, governance tokens that are owned or controlled by their holder, transferable, grant control over network decisions, and do not confer traditional equity ownership seemingly create a property right in the active property (i.e., a property right in the digital asset, which represents active property). This warrants further consideration about this new type of property, as well as the rights, responsibilities, and relationships associated with it. Specific factors include use, transferability, limitations or conditions on use or transferability, its relation to other types of property and their respective owners, and its relation to other property rights in the same active property and their respective owners.

Historically, corporate law evolved to address similar concerns. About 125 years ago, corporate law was characterized as "relatively new and untried—an experiment only just begun."[12] From the outset, certain structural issues of the corporate form caused unintended consequences that were mitigated by regulatory intervention.[13] Notably problematic were the divisibility of interests (in terms of ownership and control and the creation of special classes of stock); reduced accountability of managers due to their limited liability; and the disconnect of laborers, owners, and creditors from direct involvement with, and authority over, the means of production.[14] To mitigate the resulting negative impact on commercial dealings, misaligned incentives, and outsized corporate power relative to the government, regulatory interventions sought to address risks stemming from:

- Disparities in information and control between shareholders and managers;
- The influence of corporate entities over labor, creditors, and consumers;
- Unchecked economic power without accountability and its impact on public interests; and
- Corporate influence on government policymaking for private gain.[15]

These same considerations evaluating disparities in information and control, influence over enterprise and market participants, economic power, accountability, and impacts on all stakeholders are relevant when evaluating any new business form, including DLT networks. The structural differences of DLT networks and their ecosystems, including decentralization of governance and automation of decision-making, may require a reassessment of property,

[10] *Id.* at 304-05.
[11] *Id*. (discussing this concept in the 1930's as a potential future property right and illustrating a hypothetical circumstance in which "if by custom the position of director became hereditary and this custom were given legal sanction").
[12] Comm. Corp. Rep. at 37.
[13] *Id*. at 37.
[14] *Id*. at 38-39.
[15] *Id*.

ownership, and control, as well as their relationships to each other. In addition, changes to the bundling (or de-bundling) of various rights and obligations may also necessitate an assessment of incentive alignment, accountability, transparency, and fairness.

D. DLT Networks, Profit Models, And Ecosystem Participants

DLT networks may also be redefining the concept of profit. Traditionally, corporations derive profits from a combination of internal operations and external market factors. Some economic theories argue that because corporations rely on broader societal contributions, such as infrastructure, workforce development, and consumer engagement, profit distribution should account for these external contributions.[16]

Consumers, and others, have always been a functioning part of an enterprise,[17] but DLT networks enable participants to engage more actively within ecosystems. The ecosystems enable new forms of value creation that challenge traditional corporate profit models. Instead of value in the form of profits accruing solely to shareholders, value can be distributed among network participants based on governance contributions, staking mechanisms, or other incentive structures. In addition, this may challenge conventional notions of what constitutes value.

E. Regulatory Considerations For Future DLT Governance

To develop forward-looking regulations, policymakers must recognize the evolving nature of DLT networks and both the opportunities and risks associated with new economic structures. Lessons from corporate governance provide useful frameworks, including:

- Transparency and disclosure standards;
- Incentive alignment between stakeholders and governance participants;
- Accountability mechanisms for decentralized decision-making; and
- Balancing innovation with consumer protections and market integrity.

III. Methodology For A National Regulatory Approach

With the foregoing context in mind, we developed a methodology to approach creating a comprehensive framework for a digital asset regulatory approach in a structured and methodical manner, allowing for flexibility and iterative refinement. The framework is designed to create a regulatory regime that encourages innovation while ensuring reasonable consumer protection and accountability.

First, we considered the existing classifications of assets, and reviewed the logic applied to their groupings, which is based on similar characteristics and similar market behaviors. The

[16] Berle at xviii.
[17] *Id*. at 306.

distinguishing features and behaviors inform purchasers and market participants as to various risks, returns, or benefits.

Non-Exhaustive List of Existing Asset Classes

- **Equities** (Stocks): Ownership in a company, offering dividends and capital appreciation potential. Example: Shares of stock in companies.

- **Bonds** (Fixed-Income): Debt instruments that provide regular interest payments and principal repayment. Examples: U.S. Treasury bonds, corporate bonds, municipal bonds.

- **Cash and Cash Equivalents**: Highly liquid, low-risk short-term investments. Examples: Money market funds, Treasury bills, certificates of deposit ("CDs").

- **Real Estate**: Ownership in physical property or real estate funds. Examples: Residential and commercial properties, real estate investment trusts ("REITs").

- **Commodities**: Raw materials or agricultural products. Examples: Gold, oil, agricultural products.

- **Private Equity**: Investments in private companies or buyouts of public companies. Traditional private equity focuses on more mature companies or buyouts. Venture capital is a subset of private equity that focuses on investments in early-stage companies.

- **Hedge Funds**: Pooled investment funds that typically invest in public markets. Examples: Long/short equity funds, global macro funds.

- **Collectibles**: Assets bought for potential appreciation. Examples: Art, rare coins, vintage cars.

Second, applying the same logic to distinguish existing asset classifications, we identified many of the most common digital assets and considered the following:

- **Common Characteristics**: The assets' attributes, including their functionality and use; their traits, including risk (volatility, credit or default risk, liquidity risk), return potential (income generation, capital appreciation), liquidity (high or low), time horizon (short- term versus long-term goals/purposes), income versus growth (income-oriented or focus on capital gains/long-term growth), and correlation with other asset classes (positive/high or negative/low, the latter increases diversification); and associated risks and concerns, such as consumer protection. For example, stocks and bonds differ in volatility and risk, while their liquidity impacts how easily they can be traded without price disturbances.

- **Similar Behavior in Response to Economic Factors**: The expected responses of the assets' function or performance to economic trends. For instance, equities perform well in strong economies, while commodities often perform well in inflationary environments.

- **Common Market Participants and Instruments**: Who purchases or uses the assets or are otherwise market participants for the assets. Also, what types of instruments the assets are associated with, the purpose of the assets, and the markets in which the assets are traded. For example, mutual funds and exchange-traded funds that invest in stocks are both equity-related products with common retail investor and institutional investor participation.

- **Historical Precedent and Classification Systems**: The general financial theories and widely accepted market conventions, such as the Global Industry Classification Standard ("GICS"), also guide asset categorization.

Third, for each type of digital asset, we identified the concerns (e.g., consumer protection, market integrity) that a legal or regulatory regime may aim to address.

Fourth, we also identified many of the most significant categories of market participants and their respective roles, and considered various potential risks and concerns related to these roles, particularly in the context of the current market structure. This is set forth in the attached Exhibit 2.

Fifth, after considering these various aspects of the types of digital assets, we identified twelve broad digital asset classes, which are listed below and explained in Section VI.

Sixth, we analyzed numerous types of digital assets and identified which digital asset class or classes each type of digital asset would fit into. The asset classes are not mutually exclusive. The types of digital assets are discussed below in Section VII and the classifications are set forth in Exhibit 1.

Seventh, we compared these digital asset classes to existing asset classes, entities, activities, and trends already addressed by existing federal regulators, and suggested potential suitable regulatory authorities. These are identified in the respective parentheticals of the list of twelve digital asset classes below.

1. Digital Payment Units (securities and banking)
2. Primary Digital Currencies (commodities)
3. Functional Digital Assets (commodities and regulators of associated goods, services, or rights)
4. Digital Commodities (commodities)
5. Digital Securities (securities)
6. Asset-Backed Stablecoins (banking, commodities, and regulators of collateral)
7. Tokenized Real World Assets (commodities and regulators of underlying asset)
8. Non-Fungible Digital Assets (commodities, intellectual property, and regulators of associated asset)
9. Tribal And Social Digital Assets (commodities and intellectual property regulators)
10. Non-Functional Inert Digital Assets (commodities and intellectual property regulators)
11. Hybrid Digital Assets (regulators of the various above categories that are implicated by the asset's characteristics)
12. Other Digital Assets

Once these proposed asset classifications, applicable regulators, and potential risks and concerns are finalized, the next phase is to analyze the legal and regulatory regimes that apply to each class and market participant, and identify any regulatory changes that are necessary. To inform this next step, we include a set of goals and guiding principles that should be considered in establishing and amending regulations to fit digital assets in a future-proof way. These overarching principles guide the analysis for class-specific regulatory frameworks, fostering a comprehensive and collaborative approach.

In addition, we discuss some obstacles that are hindering regulatory clarity for the digital asset industry and outline guiding principles designed to address these challenges. We also discuss various considerations specific to digital assets that should be taken into account when creating and evaluating regulatory approaches.

IV. Principles Driving Regulation

Regulation serves diverse purposes depending on the perspective, but there is a universal principle we should all align with: regulation should seek to "do no harm."[18] Regulation is not an objective in and of itself; rather, it is a tool that, when overused, can harm innovation, restrict markets and individual freedoms, and create inefficiencies. Thoughtful regulation should, however, play a critical role in maintaining social order, fostering market stability, and ensuring fairness in competition. Before implementing regulation, it is essential to evaluate its necessity and clearly define its objectives, with careful consideration of potential unintended consequences.

Regulation should target specific concerns, managing risks, and promoting transparency without stifling innovation. Underlying this approach is the acknowledgment that our laws prohibiting lying, cheating, and stealing already provide a baseline for consumer protection. Regulatory regimes are generally created when enforcement alone is insufficient to protect the public or public goods, necessitating a proactive, structured approach to manage complex systems and mitigate significant harm. Heightened regulatory measures, which require the government to exercise additional oversight and monitoring, are generally established when the potential harm or the nature of what needs protection justifies intervention. For example, when harm reaches a certain magnitude of potential risk (such as in the case of securities regulation), heightened regulation is often implemented. Given that the health of our securities markets is vital to a strong national economy, this relationship is a core rationale for heightened regulatory oversight.

In some instances, such as with digital assets, the lack of clear rules and a practical regulatory regime is destructive to an industry. "Where a statute allows wide range for policy choice the agency's failure to define policy may give rise to evil consequences and bring administrative

[18] Greek physician Hippocrates, who created a code of ethics known as the "Hippocratic Oath" that included principles to abstain from deleterious, mischievous, and corrupt conduct, and whose writings included that a physician should, among other things, "do no harm." Hippocrates. *Hippocrates: Collected Works I*, pp. 165, 299-30. Edited and translated by W. H. S. Jones, William Heinemann Ltd., and G. P. Putnam's Sons (1923), https://archive.org/details/hippocrates0000hipp/page/n1/mode/2up?q=oath.

delegation into disrepute. A broad delegation of power is not only a power, it is a summon to create order."[19] In this instance, there is a call to create order, but doing so while mindful of the foregoing principles to guide its development.

Furthermore, to foster the growth of a robust market, we intend to identify structural barriers that hinder expansion and recommend implementing targeted incentives to address them. Strengthening key market participants and enhancing competition, for example, may play a significant role in developing the necessary market structure.

V. Foundational Concepts For Digital Asset Analysis

The framework addresses what we refer to as "digital assets." Other countries and international frameworks use different terminologies, often reflecting the terms used in other jurisdictions' legal regimes. While it would be ideal if all countries used the same terminology, in some circumstances it would require countries to amend the nomenclature of numerous bodies of law.

A. Digital Asset Description

A digital asset broadly refers to any item of value that exists in a digital format. The digital assets discussed in this framework are a subset of the broad category and are generally those that are intangible, digitally represented units of value, right, or ownership that are created, issued, or transferred using DLT[20] or comparable technology. These digital assets may be programmable, enabling automated functions through smart contracts or embedded logic. They can serve various uses, and their characteristics may evolve over time. Digital assets typically have a tribal component—fostering community or network effects—but the strength of this aspect varies by asset and ecosystem. Transactions involving digital assets are recorded in a secure, tamper-resistant distributed ledger, often using cryptographic techniques and various consensus mechanisms to ensure integrity, transparency, and security. Validation methods can be centralized or decentralized, depending on the system's design.

B. Digital Asset Characteristics

Digital assets are intangible and composed of digital information that can be owned, controlled, or otherwise used to represent or produce positive economic value, and they can represent other types of assets (e.g., tangible, intangible, financial).

---

[19] SEC Chairman William Casey, keynote for *The SEC Speaks*, at 9 (Feb. 18, 1972) (quoting Professor Louis L. Jaffe, *Judicial Control of Administrative Action 49* (1965)), https://www.sec.gov/news/speech/1972/021872casey.pdf.
[20] Digital assets associated with a DLT network may more precisely be termed "DLT Digital Assets."

C. Digital Asset Risk/Return Profile

The risk/return profile of an asset varies by asset type. There may be high risk/high return for speculative assets or low risk for more stable and predictable assets. It is important to consider both technology risk and the risk of the asset itself.

D. Potential Concerns

Certain digital assets may present particular risks and vulnerabilities, some of which are unique, that may require legal or regulatory intervention. This section attempts to identify the most pressing concerns with the intention of later assessing whether legal or regulatory interventions are necessary and, if so, ascertaining the least restrictive means of accomplishing the regulatory goal. Regulatory goals should be pursued while minimizing interference with honest business activities.[21]

It is important to recognize the general prohibition against dishonesty, including lying, cheating, and stealing, which is enforced through the civil and criminal authorities of various government entities. When these protections prove insufficient, regulatory regimes are established to impose additional duties and government oversight. While an imperfect analogy, it may be helpful to think of regulatory regimes as mechanisms for setting requirements, such as safe speed limits, and oversight such that speeding can be caught and stopped before there is a catastrophic accident.

In identifying concerns and potential regulation to address those concerns, there are two fundamental questions:

1. What is needed more than the basic prohibition against lying, cheating, and stealing to reasonably protect against consumer and market harms?
2. Are there monitoring mechanisms and enforcement authorities that need to be bolstered, and/or is there a regulatory/registration regime that is required?

E. Digital Asset Market Structure And Market Participants

Market participants generally are the various individuals, institutions, and entities that engage in market activities. These can include developers, retail customers, institutional investors,

---

[21] *See* 77 Cong. Rec. 937 (1933) (President Franklin D. Roosevelt observed that federal securities legislative proposals did not pursue investor protection at all costs and were designed to impose "the least possible interference to honest business."); Federal Securities Act, *Hearings Before the House Interstate and Foreign Commerce Committee,* 1st Session, on H.R. 4314 (Mar. 31, 1933) (Hon. Huston Thompson, former member of the FTC who helped develop the federal securities legislation, stated: "The purpose and policy here is to protect . . . with as little interference with business as possible. This is the main theme upon which we played in building up this bill."); S. Rep. No. 47, at 1 (1933) (Rep. Thomas Brooks Fletcher from the Committee on Banking and Currency stated: "The purpose of this bill is to protect the investing public and honest business . . . to protect honest enterprise, seeking capital by honest presentation . . . to aid in providing employment and restoring buying and consuming power."); 77 Cong. Rec. 3801-2 (May 20, 1933) (On H.R. 5480, Fletcher stated: "The country justly demands that the public have some protection . . . and honest business a legitimate chance.").

exchanges, custodians, and so forth. Each type of participant plays a distinct role and influences market dynamics, which may impact liquidity, price discovery, stability, market efficiency, and other significant factors. A summary of certain market participants and potential risks and considerations related to each are set forth in the annexed Exhibit 2.

Market structure generally refers to the overall organization of a market, including the design and infrastructure. Identifying the classifications of the digital assets that trade in the markets and their distinguishing characteristics, and the categories of market participants and their respective roles, is required to understand the current market structure. Evaluating the current functioning of the market—how assets move within it, the technological, infrastructural, and legal constraints in place, the risks involved and their sources, as well as the consequences of the market's existing structure—provides insights for designing an effective regulatory framework to govern both the market's operations and the behavior of its participants.

VI. Digital Asset Classes

With the foundational concepts for digital assets established, we turn to the twelve classes of digital assets into which we classify the identified types of digital assets. The following classes are not mutually exclusive. The asset class names and descriptions are intended to encompass not only existing digital assets, but also future digital assets. One goal of new regulatory frameworks is to be forward-looking and as future-proof as possible. In the Classification Chart, annexed as Exhibit 1, each digital asset is categorized as included (marked with an "✅"), excluded (left blank), or potentially subject to inclusion (marked with an "➖") within the classification.

A. Digital Payment Units

Digital Payment Units refers to digital assets serving primarily as a medium of exchange (payments and transfers). These are used similarly to traditional currencies but are not legal tender.

The proposed definition does not include a unit of account or store of value. Consideration should be given to whether those should be included. Generally, these terms are understood to have the following meanings:

- Medium of exchange: Can be used to directly purchase goods and services from merchants who accept them.
- Unit of account: A standard to measure the value of different goods and services relative to each other.
- Store of value: Can be held and exchanged later for goods and services, potentially retaining purchasing power over time.[22]

[22] *See generally*, IRS Notice 2014-21 (Mar. 25, 2014); 6 FIN-2013-G001, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, (Mar. 18, 2013).

B. Primary Digital Currencies

Primary Digital Currencies refers to assets that are inherently associated with, and integral (native) to, a base layer DLT network (also referred to as a layer 1 blockchain or DLT). The asset (often referred to as a token or coin) and protocol do not function without each other; the asset is needed to transact on the platform. These DLT networks provide the core infrastructure, consensus mechanisms, and security protocols that enable decentralized transactions.

Primary Digital Currencies function as the primary (also referred to as principal) currency of a protocol but may have additional functionalities. This digital asset also qualifies as a Functional Digital Asset (described below), but it is distinct from other types of functional digital assets in that it is required for operation of base DLT networks, as well as technology built on top of it (e.g., layer 2 blockchain or DLT), and thus has unique characteristics that should be considered in analyzing appropriate legal and regulatory regimes.

C. Functional Digital Assets

Functional Digital Assets are assets that have a function or purpose within a network, platform, or ecosystem, such as to provide access to a specific application, product, or service within a DLT ecosystem or similar platform. These are not designed to raise capital but rather to facilitate transactions involving DLT-based goods or services, or to enable special features.

These include assets that are inherently associated with, and integral to, a layer 2 distributed ledger, and any distributed ledgers built on top of another distributed ledger. Layer 2 may provide solutions for scaling, efficiency, interoperability, various applications, off-chain, side-chain, and other purposes. Functional Digital Assets also include Primary Digital Currencies.

D. Digital Commodities

Digital Commodities are digital representations of goods, services, rights, and interests in which contracts for "future delivery are currently or will be traded in the future."[23] The underlined phrase has been interpreted in various ways, with the middle-of-the-road approach being that the existence of a futures market for one asset renders all assets within that same class "commodities" under the Commodity Exchange Act ("CEA").[24] This approach requires defining the "class" of items. If this interpretation is followed, then it could be interpreted to mean that all cryptocurrencies (if

[23] Commodity Exchange Act § 2(a).

[24] *Commodity Futures Trading Comm'n v. My Big Coin Pay, Inc.*, Civ. No. 18-CV-10077 (D. Mass. Oct. 29, 2020) ("The CEA defines 'commodity' generally and categorically, 'not by type, grade, quality, brand, producer, manufacturer, or form.'"). The narrow reading is that only assets that are explicitly structured for futures trading or have a demonstrated history of being traded in a futures-like manner qualify as a commodity. The broad reading is that any asset that could potentially have a futures contract on it would be a commodity, regardless of market demand, history, structure, or any other factors.

considered a class) are commodities since there are futures on some cryptocurrencies. This would require defining the class "cryptocurrency."

An important feature of commodities is their interchangeability or fungibility.

General Commodities Context

For context, traditional commodities are basic goods and materials that are widely used, not meaningfully differentiated from one another, and interchangeable with other goods and materials of the same type. They are generally classified into:

- Hard commodities, which are natural resources that are mined or extracted (e.g., energy products like oil and natural gas, and metals like gold and copper); and
- Soft commodities, which are agricultural or livestock products that are grown or harvested (e.g., wheat, coffee, and cattle).

In addition to physical commodities, traditional commodities include financial commodities, such as interest rates and stock indices, and other specialized commodities, such as weather.

Generally, commodity prices rise when inflation accelerates, and commodities are used to protect against inflation. Since the commodities themselves are rising in price, owning them preserves value compared to holding cash, which loses purchasing power. As inflation expectations grow, investors purchase more commodities. This higher demand causes prices to increase. For this reason, commodities can potentially be used to hedge against a currency's decreased buying power when inflation rates increase. There are other risks, such as supply problems, policy changes, and global demand fluctuations that can influence the value of commodities.

E. Digital Asset Securities

A Digital Asset Security is a digital asset (computer code) that represents rights and obligations that render it a security per the definition in the Securities Act of 1933 ("Securities Act") and the Securities Exchange Act of 1934 ("Exchange Act"), similar to a physical stock certificate (paper) that represents ownership interest in a company and is considered a security. A Digital Asset Security may represent an investment contract; however, a Digital Asset Security is not the subject of the investment contract (e.g., an asset, a venture), nor is it an asset the investor receives as proceeds from the investment opportunity (e.g., a commodity, profit). We propose a revised Investment Contract definition, which is more fully explained in Section VIII.A.

Digital Asset Securities include (but are not limited to) transactions in which digital assets are offered or sold for capital raising and investment purposes by contracts that represent an ownership stake, a debt obligation, or the right to receive proceeds from the issuer's or promoter's successful operation of a venture on behalf of the investor. This requires (1) a *quid pro quo*, and (2) information asymmetry between the purchaser and the issuer/promoter such that the purchaser requires information disclosures to monitor the issuer's/promoter's efforts in managing an enterprise, and an identifiable issuer/promoter who is capable of providing meaningful periodic

disclosures (without conflicting with the lawful purpose of the digital asset and associated technology).

In the context of an agreement for future tokens, there are several alternative structures that may change the classification of an asset and transaction. Often, the agreement represents the investment contract and describes the investment opportunity, and the future tokens are the "proceeds." The investment opportunity involves a capital raising activity, as discussed in the immediately preceding paragraph and in Section VIII.A. The transaction concludes upon the investor receiving the assets (tokens) in return for their investment pursuant to the agreement. While not typical, it is possible that the tokens ultimately received are digital asset securities; that is, the investor receives securities as proceeds. Both of these structures are distinguished from an agreement to buy and sell a non-security asset at a specific price on a specific date (forward and futures contracts).

General Securities Context

In determining whether the securities laws apply, it's important to consider the purposes of the securities laws and whether those purposes are served in the circumstances. Securities laws fundamentally address the risks associated with investors entrusting their capital to another party's management, particularly when the investors face challenges in overseeing that management effectively. This dynamic gives rise to two central economic concerns: agency costs and collective action problems.

- **Agency costs** arise from the separation of ownership and control, where the agent (such as the issuer or promoter) has more information than the principal (the investor or owner), which can lead to conflicting incentives. These costs manifest in the efforts needed to gather information, negotiate restrictions, and monitor or supervise those in control of the investment.
- **Collective action problems** emerge when multiple investors struggle to coordinate their oversight efforts, often making it difficult to exercise meaningful supervisory control over the management of the investment.

To determine whether something qualifies as a security under the Securities and Exchange Commission's ("SEC") jurisdiction, it must fall within the statutory definition of a security:

> [U]nless the context otherwise requires—(1) [t]he term "security" means any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any

> interest or instrument commonly known as a "security", or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing.[25]

Two aspects of this definition are particularly noteworthy. First, the general caveat allows flexibility in that the definition applies unless the context dictates otherwise. This has been applied to exclude instruments from the definition of a security if they are adequately regulated by another regulatory regime.[26] Second, digital assets that implicate the securities laws may fall under various classifications—not only an investment contract—such as a note, evidence of indebtedness, or a certificate of interest or participation in any profit-sharing agreement.

There are two exemptions that merit mentioning. While applying the exemptions is nuanced and implicates other provisions, generally, the Securities Act exempts from registration a seller who is not an issuer, underwriter, or dealer. This exemption generally allows retail purchasers to sell securities in the secondary market without registering the transaction, so long as they are not acting in one of the prohibited roles. The second exemption involves short-term notes. A note that arises out of a current transaction and matures within nine months is exempt from registration.[27] However, the timing of maturity is not the sole determinant. Instead, the Supreme Court applies a "family resemblance" test, creating a rebuttable presumption that a note is a security unless it fits into an exempt category.[28] The factors considered in this test are:

- The motivations of the buyer and seller (e.g., if the note is for commercial or consumer goods purposes, it is less likely to be a security);
- The method of distribution (e.g., if the note is widely offered and sold, it is more likely to be a security);
- The reasonable expectations of the investing public (e.g., if there is an expectation of profits from the efforts of others, it is more likely to be a security); and
- Other considerations (e.g., if the note is not collateralized, is not traded on a secondary market, or is not regulated under a non-securities framework, it is more likely to be a security).[29]

---

[25] 15 U.S.C. § 77b(a)(1) (emphasis added to highlight particular elements of the definition to consider when analyzing digital assets and associated transactions). While this definition is from the Securities Act and the definition is slightly different in the Exchange Act (15 U.S.C. § 78c(a)(10)), these definitions are typically interpreted consistently. *United Housing Foundation, Inc. v. Forman*, 421 U.S. 837, 847 n.12 (1975).

[26] *Marine Bank v. Weaver*, 455 U.S. 551 (1982) (holding that, notwithstanding that a bank CD has many attributes of long term debt, that an applicable alternative regulatory regime rendered securities regulation unnecessary). Separately, and notably, the *Marine Bank* court also determined that a profit-sharing agreement was not a security as it was privately negotiated and gave the purchasers significant control over the operation. *Id*.

[27] Securities Act § 2(a)(1), 15 U.S.C. § 77b(a)(1); Securities Exchange Act § 3(a)(10), 15 U.S.C. § 77c(a)(3).

[28] *Reves v. Ernst & Young*, 494 U.S. 56, 64-65 (1990).

[29] *See generally, id*.

We recommend considering a return to more closely following the statutory language, exempting notes with a clear maturity requirement, potentially with conditional safe harbors.

F. Asset-Backed Stablecoins

Asset-Backed Stablecoins are digital assets typically used as a medium of exchange or store of value that is pegged to and backed by the value of a stable asset, such as fiat currency or commodities, to maintain price stability.

G. Tokenized Real World Assets

Tokenized Real World Assets ("RWAs") refer to digital assets that represent RWAs (such as commodities, real estate, or other physical assets) and can be traded or transferred in whole or in fractions, using DLT or a similar platform or technology.

These intangible representations of tangible assets are regulated according to the nature of the underlying asset. In addition, as with all assets, regulations are also triggered based on the manner in which they are transacted. For example, just as nondigital fractionalized interests in tangible assets may implicate the securities laws, so too may fractionalized Tokenized RWAs.

H. Non-Fungible Digital Assets

Non-Fungible Digital Assets are digital assets that represent unique, indivisible digital assets that are typically used for digital art, collectibles, or other distinct items. These are valued for being unique, rare, non-replicable, bespoke, and non-interchangeable on a one-to-one basis.

This includes a series of the same non-fungible token ("NFT"), provided they are numbered. The precise number of series that renders the asset fungible depends on the facts and circumstances. We propose a presumption that a series not in excess of a certain number (e.g., 50,000) is non-fungible. At a certain point, the abundance of the same NFT diminishes its value based on uniqueness, effectively making it fungible.

I. Tribal And Social Digital Assets

Tribal And Social Digital Assets are digital assets that are used for social proof, cultural identity, community involvement, community membership, a shared identity, or similar purpose. They are used for things like supporting a creator, showing allegiance to a community, or being part of a tribal ecosystem. Unless it is a hybrid digital asset, it has no function (e.g., governance, access to services) and is not for capital raising purposes.

J. Non-Functional Inert Digital Assets

Non-Functional Inert Digital Assets refer to digital assets that lack a clear function or practical use. This includes airdrops with no immediate function and may be intended for marketing purposes or to create initial interest in a project, but they do not necessarily have any functionality at the time of distribution.

K. Hybrid Digital Assets

Hybrid Digital Assets are digital assets that have a combination of various types of characteristics and are classified in more than one of the classifications above.

L. Other Digital Assets

Digital assets categorized in the "Other" class do not fit into any of the above categories and/or have attributes of a traditional asset class not fully represented by the digital asset-specific classes.

VII. Classification Analysis Of Specified Digital Assets

In this section, we include a non-exhaustive list of common digital assets, and their associated description, characteristics, risk and return considerations, and consumer protection or market integrity concerns that may drive the focus of regulation. Each of these assets fall within one or more of the twelve classes discussed in the preceding section. To the extent a particular type of transaction or its participants implicate a different concern, such as national security, those considerations would need to be considered.

Digital Asset	**Description, Characteristics, Risk/Return, and Potential Concerns**
Cryptocurrencies (e.g., bitcoin, ether, and altcoins)	**Description**: Digital assets secured by cryptography and operating on decentralized networks using DLT, are fungible/interchangeable, and are peer-to-peer (can be exchanged directly between users without intermediaries such as banks or payment processors). **Characteristics**: Differing levels of liquidity, subject to more volatility, traded 24/7, speculative; some serve as a medium of exchange or store of value, or for decentralized apps ("dApps"). They are designed to function autonomously from centralized institutions. Many—but not all—of these assets have frequently been the subject of an investment contract or the proceeds of the investment contract. **Risk/Return**: Potential for high returns, especially during growth. Often subject to higher volatility. Depending on additional functionality, one may have lower return potential compared to purely speculative tokens. More stability often related to liquidity and strength/popularity of functional use (e.g., integrated and necessary for many other DLT networks). **Consumer/Market Concerns**: Fraud, market manipulation, information asymmetry if there is a controlling entity or group, illicit use (e.g., money laundering).

Fiat-Backed Stablecoins	**Description**: Digital assets whose value is pegged to and backed by fiat currency, often used for payment in commercial transactions.
	Characteristics: Designed to minimize volatility by being backed by and pegged to fiat currency. Volatility is linked to volatility of underlying currency. Used for trading, remittances, or as a store of value.
	Risk/Return: Lower risk than traditional cryptocurrencies; risk mirrors that of the underlying fiat currency. Still exposed to counterparty risk. Lower returns than other digital assets.
	Consumer/Market Concerns: Inadequate asset backing, inadequate disclosure, and redemption risks. Risk of de-pegging and loss of value.
Asset-Backed Stablecoins	**Description**: Stablecoins backed by a basket of assets, such as commodities or real estate.
	Characteristics: Similar to fiat-backed stablecoins except volatility linked to volatility of underlying assets. May be more diversified than fiat-backed stablecoins.
	Risk/Return: Risk mirrors that of the underlying asset(s). Moderate risk depending on transparency of reserves. Lower returns than other digital assets.
	Consumer/Market Concerns: Inadequate asset backing, inadequate disclosure, and redemption risks. Risk of de-pegging and loss of value.
Algorithmic Stablecoins	**Description**: Stablecoins using algorithms for price stabilization.
	Characteristics: Algorithmic mechanisms to maintain price stability.
	Risk/Return: High risk due to potential algorithm failures and lower returns than other digital assets.
	Consumer/Market Concerns: Lack of algorithm transparency, risk disclosures, and stability guarantees.
Non-Fungible Tokens	**Description**: Unique, non-fungible digital assets representing ownership or proof of authenticity of items, typically art or collectibles.
	Characteristics: Indivisible, stored on DLT, used for digital ownership, cannot be exchanged on a one-to-one basis.
	Risk/Return: Low to moderate risk due to speculative nature, potential low liquidity, and potential fraud.

	Consumer/Market Concerns: Fraud, market manipulation, and intellectual property theft.
Meme/Community Tokens	**Description**: Tokens without functionality, generally driven by online communities, social media, or pop culture.
	Characteristics: Speculative, community-driven.
	Risk/Return: Moderate to high risk due to the prevalence of fraudulent schemes (rug pulls, pump-and-dump schemes).
	Consumer/Market Concerns: Fraud, market manipulation, and information asymmetry.
Fundraising Token	**Description**: Issued to raise capital, often through Initial Coin Offerings ("ICOs") or similar methods. These transactions may involve the pre-sale of tokens before the digital asset is fully developed whereby the fundraising token is a placeholder token (also referred to as an IOU token), or the sale of an existing digital asset. In exchange for their capital or assets (investment), purchasers entrust the issuer/promoter with managing their investment and undertaking the venture on their behalf (e.g., developing the protocol or dApp and associated network) with the purchaser's right to receive the proceeds from those efforts.
	Characteristics: Can be risky with high reward potential. These transactions are not agreements to purchase digital assets for a predetermined price in the future (forward or futures contracts), but are a capital raising vehicles in which proceeds are used for similar purposes as capital raises for traditional equity and debt instruments.
	Risk/Return: High risk with potential for fraud and loss of funds.
	Consumer/Market Concerns: Fraud, market manipulation, and information asymmetry.
Tokenized Security Tokens	**Description**: Digital tokens representing ownership of financial instruments such as equity or debt.
	Characteristics: Subject to securities regulations, due to underlying asset.
	Risk/Return: Risk mirrors that of the underlying asset, which reflects the entity in which (or against which) the asset is issued.
	Consumer/Market Concerns: Same investor protection and market integrity concerns as all securities.

Tokenized Real-World Assets	**Description**: Digital representations on a DLT of physical or tangible assets (such as real estate, gold, or art). These assets are backed by real-world value, meaning the DLT token represents actual ownership or rights to the underlying asset. **Characteristics**: Enables fractional ownership, reduced barriers to entry, enhanced liquidity. Used to fractionalize ownership of RWAs, enabling easier trade and access. **Risk/Return**: Risk mirrors that of the underlying asset and the structure of fractionalization. **Consumer/Market Concerns**: Transparency in ownership rights, disclosures, and asset backing verification.
Decentralized Finance ("DeFi") Tokens	**Description**: Digital assets used within decentralized financial platforms and applications to facilitate lending, borrowing, trading, staking, and liquidity provision. Typically used in DeFi protocols to provide governance, participate in yield farming, or earn interest. DeFi tokens have specific utilities within their respective platforms. **Characteristics**: Facilitates decentralized financial services without intermediaries. **Risk/Return**: Potential for high risk due to smart contract vulnerabilities, information asymmetry until there is no controlling entity or group of holders. **Consumer/Market Concerns**: Unfair lending practices, inadequate consumer disclosures, smart contract security risks, illicit finance (money laundering), and use of platform to facilitate unlawful activities.
Access Tokens	**Description**: Digital assets used to access a product or service. These have been referred to as utility tokens, non-security tokens, and a variety of other names. **Characteristics**: Typically for platform usage, access, or service provision. **Risk/Return**: Potential for high returns, especially during growth and higher risk periods. Often subject to higher volatility. Depending on the function, they may have lower return potential compared to purely speculative tokens. More stability depending on strength/popularity of functional use (e.g., integrated and necessary for many other DLT networks).

	Consumer/Market Concerns: Fraud, misleading claims, and lack of clarity regarding duties and rights based on governance structures.
Privacy Coins	**Description**: Digital assets that focus on providing enhanced privacy and anonymity for users. These digital assets use advanced cryptographic techniques to obscure transaction details, ensuring that users' transaction histories and balances remain confidential. **Characteristics**: Aim to offer higher levels of privacy than traditional cryptocurrencies, and use technologies such as ring signatures, zero-knowledge proofs, and stealth addresses to protect users' identities and transaction information. **Risk/Return**: Moderate risk depending on verification standards. **Consumer/Market Concerns**: Data privacy, identity verification standards, identity theft, and illicit use; balancing compliance with global identity protection laws while maintaining decentralized principles.
Carbon Credits and Environmental Assets	**Description**: Digital representations of carbon credits or other environmental assets, often issued as tokens on a DLT. They allow individuals or organizations to buy, sell, or trade carbon offsets to help mitigate their environmental impact, such as reducing greenhouse gas emissions. **Characteristics**: Carbon credit tokens are used to incentivize environmentally-friendly behavior and can be traded on decentralized platforms. They help track emissions reductions and ensure transparent, verifiable environmental contributions. DLT is used for transparency and traceability in carbon offset trading. **Risk/Return**: Moderate risk depending on verification standards. **Consumer/Market Concerns**: Legitimacy, greenwashing, and lack of verifiable tracking systems.
Identity/ Reputation Tokens	**Description**: Represent digital identities or reputational scores for individuals, organizations, or services. These tokens are used to establish trust and credibility in decentralized networks (e.g., DeFi platforms or DAOs). **Characteristics**: Help verify an individual's identity or reputation in digital ecosystems, ensuring that users are accountable and trustworthy

within the network. They can be used to prove user identity for services, financial transactions, or voting rights.

Risk/Return: Moderate risk—while these tokens enhance trust, they are vulnerable to misuse, identity fraud, and data privacy concerns.

Consumer/Market Concerns: Data privacy, identity verification standards, and identity theft; balancing compliance with global identity protection laws while maintaining decentralized principles.

Governance Tokens

Description: Provide holders with voting rights on protocol upgrades, project decisions, and the overall direction of a DLT network or decentralized application ("dApp"). These tokens allow for decentralized decision-making, enabling users to participate directly in the governance process.

Characteristics: Usually issued by DAOs or DeFi projects. Holders can vote on various proposals that influence the future development of the project, such as tokenomics changes, platform upgrades, or community initiatives.

Risk/Return: Generally lower risk but potential lack of transparency may increase risk.

Consumer/Market Concerns: Unfair voting processes, governance takeovers, and potential for manipulation particularly related to controlling ownership of tokens and associated information asymmetry.

Central Bank Digital Currencies ("CBDCs")

Description: Digital currencies issued and backed by central banks.

Characteristics: Government-controlled, combining cryptocurrency benefits with fiat stability. They aim to enhance payment systems, reduce transaction costs, and provide an alternative to private cryptocurrencies. They can be issued in both retail and wholesale forms.

Risk/Return: Low risk, but raises concerns over surveillance and impact on financial stability.

Consumer/Market Concerns: Privacy, monetary policy implications, and consumer protections.

Synthetic Assets ("Synths")

Description: Digital assets that represent the price movements of another asset (e.g., stocks, commodities, or currencies) without owning or representing the underlying asset itself. Instead, a synth derives its value from the price of the underlying asset through a contract or algorithm and is a type of derivative product.

	Characteristics: Decentralized, collateral-backed, offering exposure to underlying asset price movements. Used for speculation, hedging, or exposure to the price movements of assets without needing to own them directly.
	Risk/Return: Generally similar risk as the underlying asset except potential heightened risk if low liquidity in the synth itself.
	Consumer/Market Concerns: Information asymmetry, derivatives risks, smart contract risks (inherently subject to vulnerabilities), and oracle risks (oracle is the source of data so it must be reliable/not susceptible to manipulation or hacking).
Virtual or Metaverse Assets	**Description**: Digital goods, land, or properties that exist within virtual worlds or metaverse platforms. These assets may be represented by NFTs, and their value is derived from the demand for virtual spaces, digital real estate, or in-game assets in these online ecosystems.
	Characteristics: Can be traded, used, or monetized within virtual worlds. They allow users to own digital property, interact with other users in virtual spaces, or create and sell digital goods (e.g., accessories for avatars).
	Risk/Return: Potential for low liquidity on-platform and no liquidity if traded outside the platform; speculative and return is dependent on platform success.
	Consumer/Market Concerns: Fraud prevention, consumer protection, and potential for digital property disputes.
Gaming Assets/ Play-to-Earn ("P2E") Tokens	**Description**: Digital assets that exist within video games, virtual worlds, or gamified environments. These assets can include in-game items, characters, skins, or other assets that have real-world value or can be traded across platforms.
	Characteristics: Often represent ownership of digital items within a game or platform and can be bought, sold, or traded on secondary markets. P2E games allow players to earn rewards or tokens that can be exchanged for other digital assets or fiat money. DLT integration allows for ownership of the gaming assets and more transparent gameplay economies.
	Risk/Return: Potential for low liquidity on-platform and potential no liquidity if traded outside of platform. Risk/return is speculative and is dependent on platform success.

Consumer/Market Concerns: Fraud prevention, consumer protection (including in-game mechanics), and potential for ownership disputes.

Layer 2 Tokens

Description: These digital assets are inherent to Layer 2 blockchains or DLT, which are built on top of primary DLT (Base Layer or Layer 1), and may enable functionality such as faster transactions, enhanced security, lower fees, or interoperability between different DLT networks.

Characteristics: Enhance or enable functionality of a DLT network while maintaining the characteristics of the protocol. These tokens are essential for scaling dApps and DLT networks, making them more usable in real-world applications.

Risk/Return: Potential for high returns, especially during growth. Often subject to higher volatility. Depending on additional functionality, may have lower return potential compared to purely speculative tokens. More stability depending on strength/popularity of functional use (e.g., integrated and necessary for many other DLT networks).

Consumer/Market Concerns: Fraud, market manipulation, information asymmetry if there is a controlling entity or group, illicit use (e.g., money laundering); security standards for interoperability with Base Layer and other DLT networks.

Yield-Bearing Tokens

Description: Represent assets that generate rewards (often other digital assets) through interest, staking, or other forms of yield generation. They are often issued by DeFi platforms or staking protocols, where they represent participation in a particular income-generating activity.

Characteristics: Can be used in DeFi protocols to earn interest, rewards, or staking yields. They may be locked or staked for a specific period and can appreciate in value or provide periodic payouts based on the underlying platform's performance.

Risk/Return: Potentially high risk due to potential platform insolvency and hacking risks, and risk of loss and low to no liquidity. Potential for high returns.

Consumer/Market Concerns: Inadequate disclosures on risks and returns, inadequate collateralization, fraud, market manipulation, information asymmetry if there is a controlling entity or group, illicit use (e.g., money-laundering concerns).

Staking Rewards

Description: Staking involves locking up digital assets (yield-bearing tokens) on a DLT network to help secure the network and validate transactions in exchange for staking rewards. The more tokens a user stakes, the higher their chances of being selected to validate and earn rewards. Users can delegate their assets to a service provider, who selects validators and manages the logistics of staking on their behalf.

Characteristics: Depending on its structure, it is often akin to a service agreement (as opposed to a security transaction). The rewards may be earned through network participation in its functional operation, as opposed to a customer generating profits based on the service provider's management of those funds. The staking service enables a technical process and may select a validator, but it does not make investment decisions. These transactions may be structured in a way as to implicate other regulatory regimes, such as the securities laws.

Risk/Reward: Low to moderate risk of slashing penalties (losing staked assets due to network rule violations), lock-up periods, and exposure to the underlying asset's volatility.

Consumer/Market Concerns: Fraud and information asymmetry if the staking is concentrated in a few large validators. Liquidity issues due to long unbonding periods (time between user deciding to unstake and assets becoming accessible). Risk of loss, fraud, and transparency concerns related to custody.

Liquidity Provider ("LP") Tokens

Description: LP tokens represent a liquidity provider's share in a liquidity pool. Liquidity pools are smart contracts that hold assets to facilitate decentralized trading, lending, or financial activities. Providers deposit assets into the pool to ensure liquidity for transactions. In return, they receive LP tokens, which often serve as proof of ownership and can be used to claim their share of the pool's assets and rewards at any time.

Characteristics: Created and managed by decentralized smart contracts on DeFi platforms, which facilitate transactions by ensuring liquidity. They do not typically represent ownership in a company or entitle holders to profits from a third party's efforts; instead, they often reflect shared ownership and an operational role in the platform's governance and function. Depending on the structure and assets involved, LP tokens may be functional digital assets (e.g., enabling platform operations), commodity pools, securities (e.g., profit-sharing agreements), or other asset types.

	Risk/Reward: Higher risk related to impermanent loss (when the value of deposited assets changes relative to holding them), smart contract vulnerabilities, and potential pool insolvency.
	Consumer/Market Concerns: Complexity and users' understanding of the structure from a financial and technological perspective; liquidity provision, such as liquidity concentrated among only a few providers, which may result in their disproportionate influence over the price and operations of the automated market maker ("AMM");[30] and risk of liquidity withdrawal leading to pool collapse, especially in volatile markets.
Tokenized Intellectual Property ("IP")	**Description**: This refers to digital representations of IP, such as patents, trademarks, copyrights, and other intangible assets, on a DLT. Tokenizing IP allows for fractional ownership, transparent licensing, and more efficient transfer of rights.
	Characteristics: Allows creators and owners to issue tokens representing ownership stakes or rights to a piece of IP. This can make the licensing process more transparent and accessible and open new monetization models for creators. The structure may implicate different asset classifications.
	Risk/Return: Low risk based on IP enforcement and legal frameworks.
	Consumer/Market Concerns: Definition of ownership rights and clarity around dispute resolution mechanisms.
Tokenized Fund Shares/Investment Tokens	**Description**: Tokenized fund shares represent fractional ownership in investment funds, such as mutual funds or hedge funds, via DLT-based tokens. These tokens give investors exposure to a diversified portfolio without the need for traditional financial intermediaries.
	Characteristics: Can be traded on DLT platforms, providing liquidity and fractional ownership of traditionally illiquid assets like private equity or hedge funds. This may facilitate more accessible investment in high-value or institutional-grade assets.

[30] AMMs use liquidity pools and mathematical formulas to facilitate decentralized trading. Prices adjust automatically based on the ratio of assets in the pool, with trades directly executed by the AMM, removing the need for an order book or third-party market maker.

Risk/Return: Risk mirrors that of the underlying assets, but the tokens may have limited secondary market liquidity, making it difficult to exit their holdings quickly.

Consumer/Market Concerns: Custodial risk if the token is backed by assets held in custodial accounts and transparency into the underlying assets, management strategies, and real-time performance of the fund.

Social Media and Content Creation Tokens

Description: Digital assets designed to be used within platforms focused on social media or content creation. These tokens enable creators, users, and viewers to interact, reward, or monetize content in various ways. They generally serve as a medium of exchange, incentive, or governance within these ecosystems.

Characteristics: Represent a shift from traditional ad-driven business models to user-driven economies, creating new ways for users and creators to exchange value directly. They enable monetization via tipping, exclusive content, or paid memberships and provide governance rights, allowing token holders to vote on platform decisions. These tokens can also represent ownership stakes, access to services, or digital assets, enhancing community involvement and incentivizing active participation without relying on intermediaries.

Risk/Reward: There may be more volatility due to market sentiment or platform changes, risk of reduced user engagement or platform failure, and token value loss. There is the potential for high returns if the platform grows and the token value appreciates. Creators and users can also monetize content or engagement and gain access to content, rewards, and other benefits.

Consumer/Market Concerns: Information asymmetry, fraud, and manipulation.

Cross-Chain Assets

Description: Digital assets that exist on multiple DLT networks or allow for interaction between different DLT ecosystems, thus creating interoperability between various DLT networks.

Characteristics: Allow for greater flexibility and liquidity by enabling seamless movement of digital assets between different DLT ecosystems, reducing the siloed nature of some DLT networks.

Risk/Return: Moderate risk due to security vulnerabilities in cross-chain bridges and volatility of the underlying assets enhanced by market fluctuations across different chains. Increase potential for diversification with access to a broader range of assets and liquidity

across chains, and reduce reliance on a single DLT network's performance.

Consumer/Market Concerns: Security standards for cross-chain interoperability, information asymmetry, fraud, and manipulation regarding multiple assets, DLT networks, and liquidity pools.

VIII. Securities Law Principles And Modifications Applied In The Framework

We identified existing regulatory barriers that hinder the establishment of clear and practical classifications and negatively impact market structure. The current definition of an investment contract is a prominent impediment that has led to significant confusion, inconsistent and unpredictable application, and unintended consequences, including the improper classification of assets as securities. The proposed modification aims to resolve these issues. Similarly, the term decentralization as a predominant defining characteristic has led to confusion and inconsistent application, which has diverted attention from when and to what extent it is relevant or required. We propose framing decentralization within the well-established concept of control, providing a clearer and more consistent regulatory approach, particularly in terms of potential consumer protection and market integrity risks. Additionally, the definition of an accredited investor imposes unnecessary restrictions on market access—both for those seeking capital and those wishing to invest—resulting in unfairness and inefficiencies that distort market incentives. To mitigate these constraints on market structure, we propose a revised approach to the accredited investor definition. Furthermore, fundamental principles underlying securities laws—such as the concepts of an investment contract, accredited investor, and control—offer valuable insights into market structure challenges and potential regulatory solutions.

A. Revised Definition Of "Investment Contract"

The definition of an investment contract and the application of the *Howey* test have long been problematic, and the test's application to digital assets has lacked practical and predictable boundaries for determining what qualifies as a security. Under *SEC v. W.J. Howey Co.*,[31] an arrangement must include each of the following to qualify as an investment contract: (1) an investment of money; (2) in a common enterprise; (3) with a reasonable expectation of profits based on the managerial efforts of others.

The investment contract definition should be revised to make clear that a *quid pro quo* exchange is required. First, there must be the provision of capital or other assets—this constitutes the investment ("*quid*"). Second, there must be a legally recognized right or contractual claim to both another party's future efforts to manage a venture on behalf of the investor, and the proceeds of those obligated efforts (e.g., income, revenue, profit)—this represents legal entitlement ("*quo*").

[31] 328 U.S. 293 (1946).

Securities Principles and Historical Context[32]

In rethinking the standard for an investment contract, we began with first principles. By considering the context and purposes of the federal securities law, we can more clearly define the fundamental nature of an investment contract.[33] These laws were established in response to a disastrous stock market crash that devastated the Nation's economy, causing widespread bank closures, the loss of deposits and savings, restricted access to credit, soaring unemployment, increased bankruptcies, and poverty spread across the Nation. To put this into perspective, the market value of stocks listed on the New York Stock Exchange peaked at over $89.6 billion on September 1, 1929. By November 1, 1929, it had plummeted by approximately $18 billion, and by July 1, 1932, it had dropped to around $15.6 billion—representing a loss of $74 billion from the peak.[34]

The federal securities laws were designed to address the primary causes of that financial collapse, namely, lack of transparency for investors that resulted in information asymmetry between buyers and promoters and misuse of confidential, nonpublic information by insiders and major stockholders.[35] Consequently, the securities regime became heavily focused on disclosure requirements, with enforcement mechanisms in place to address fraud.

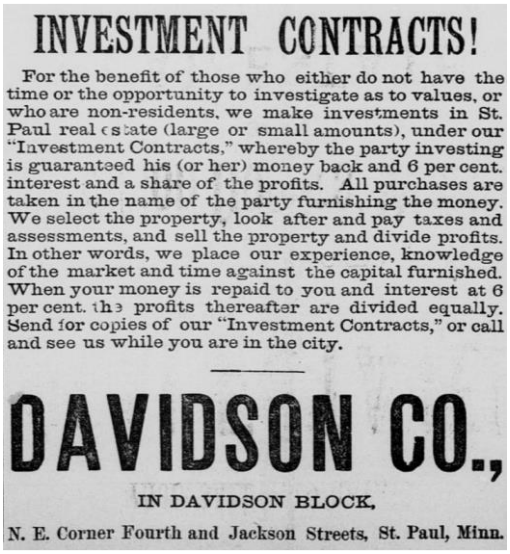
The investment contract category has been used to encompass unconventional investments where investors face practical challenges in evaluating and overseeing the actions of those entrusted with managing their capital or assets. It was not intended to regulate an entire industry or technology, and it is ill-suited to do so. Even though Congress crafted the definition of "security" broadly to include "virtually any instrument that might be sold as an investment," it did not intend the federal securities laws to serve as a sweeping remedy for all forms of fraud.[36]

While the definition of an investment contract is now amorphous, in the 1930s, when the Securities Act and Exchange Act were drafted, it was commonly understood to refer to the sale of an investment opportunity through the purchase of a contract.[37] Common investment opportunities included real estate, bonds, insurance, diamonds, and mining ventures, which were all advertised to the public with rights to guaranteed returns, such as profit shares or fixed weekly earnings.

---

[32] More fulsome historical context can be found at Amicus Curiae Br. of The Digital Chamber In Support of Pls.' Mot. for Summ. J. *Lejilex v. SEC*, Case No. 4:24-cv-00168 (N.D. Tex. Jul. 10, 2024) ("TDC Amicus Br.").
[33] *See generally*, Guillén, Teresa Goody, "10 Commandments for Federal Securities Laws." *CoinDesk*, (Feb.3 2025), https://sg.finance.yahoo.com/news/10-commandments-federal-securities-laws-220211311.html.
[34] *Stock Exchange Practices Report of the Committee on Banking and Currency*, S. Res. 84, 72d Cong., 76 Cong. Rec. 5241 (1932); S. Rep. 73-1455, at 7 (1934) ("Stock Exchange Report").
[35] James M. Landis, *Legislative History of the Securities Act of 1933*, 28 Geo. Wash. L. Rev. 29, 30 (1959); 78 Cong. Rec. 7693 (1934) (statement of Rep. John J. Cochran); 78 Cong. Rec. 7863 (1934) (statement of Rep. Charles A. Wolverton); Stock Exchange Report, at 68.
[36] *Reves v. Ernst & Young*, 494 U.S. 56, 61 (1990) (citations omitted).
[37] Edward Lee, *The Original Public Meaning of Investment Contract*, 58 U.C. Davis L. Rev. 667 (2024) ("Lee"); *see also* Jonathan R. Macey and Geoffrey P. Miller, *Origin of the Blue Sky Laws*, 70 Tex. L. Rev. 347, 352 (1991), and Montreville J. Brown, *A Review of the Cases on "Blue Sky" Legislation*, 7 Minn. L. Rev. 431, 431 (1923).

Illustrative advertisements from 1887 and 1901 provide examples of the types of investment contracts in common use at the time.[38]



INVESTMENT CONTRACTS!

For the benefit of those who either do not have the time or the opportunity to investigate as to values, or who are non-residents, we make investments in St. Paul real estate (large or small amounts), under our "Investment Contracts," whereby the party investing is guaranteed his (or her) money back and 6 per cent. interest and a share of the profits. All purchases are taken in the name of the party furnishing the money. We select the property, look after and pay taxes and assessments, and sell the property and divide profits. In other words, we place our experience, knowledge of the market and time against the capital furnished. When your money is repaid to you and interest at 6 per cent. the profits thereafter are divided equally. Send for copies of our "Investment Contracts," or call and see us while you are in the city.

DAVIDSON CO.,

IN DAVIDSON BLOCK,

N. E. Corner Fourth and Jackson Streets, St. Paul, Minn.

C. E. SMITH, Pres. F. E. BAIRD, Sec. and Treas.
S. M. WARE, General Manager.

THE JEFFERSON GUARANTY & SURETY CO.,

(Incorporated.)

Offers you the best INVESTMENT CONTRACT On the Market.

The BEST because it will make you the Most Money.

It is BEST because there is no high ratio 3 for 1 business on our Books.

It requires LESS money to complete an Investment in "The Jefferson" than in any other Company.

"The Jefferson" is NOW under its WEEKLY Contract, can sell you virtually "Ground Floor" Business every 18th week.
A trial will prove the wisdom of an Investment in "The Jefferson."

HOME OFFICE
No. 22 N. Upper St. LEXINGTON, KY.

Another source of guidance for redefining an investment contract comes from the 1933 dictionary definitions, which reinforce the essential *quid pro quo* nature of an investment contract:

- **Investment** (Oxford Dictionary): "[c]onversion of money or circulating capital into some species of property from which an income or profit is expected to be derived in the ordinary course of trade or business."[39] This is consistent with the legal definition of "invest" (Black's Law Dictionary): "loan[ing] of money upon securities of a more or less permanent nature, or to place it in business ventures or real estate, so that it may produce a revenue or outcome."[40]
- **Contract** (Oxford Dictionary): "a mutual agreement between two or more parties that something shall be done or forborne by one or both; a compact, covenant, [or] bargain"; "[a]n agreement enforceable by law, [or] an accepted promise to do or forbear."[41] This is similar to the legal definition (Black's Law Dictionary): "[a] promissory agreement between two or more persons that creates, modifies, or destroys a legal relation."[42]

Central to these definitions are two fundamental features: the provision of money or assets, representing the initial investment or contribution of resources, and the establishment of a legal right or promise to income, revenue, or profit that arises from that contribution.

---

[38] *Id.* at 32 and 38 (cited in TDC Amicus Br.).
[39] 5 OXFORD ENGLISH DICTIONARY, at 458 (1st ed. 1933).
[40] BLACK'S LAW DICTIONARY, at 1006 (3d ed. 1933). This version of Black's Law Dictionary is also the version in effect in 1946, the year that the *Howey* decision was rendered.
[41] OXFORD ENGLISH DICTIONARY, at 458.
[42] BLACK'S LAW DICTIONARY at 421.

It is also helpful to review historical occasions when the SEC analyzed an analogous asset or applied the investment contract framework. A particularly insightful instance is its analysis concluding that trading stamps were not securities in 1958, which was 12 years after the *Howey* decision and 25 years after the Securities Act was enacted. Trading stamps were small, colorful coupons with adhesive backings provided to customers as a reward mechanism and were a widely used marketing tool used by merchants.[43] Individually, each stamp held minimal monetary value—typically just a few pennies. In 1956, over 168 billion trading stamps were distributed, and there was a significant trading stamps market, including a secondary market.[44]

Merchants purchased these stamps from issuers and distributed them to customers, who could collect and redeem them for cash or valuable items such as furniture or toys.[45] In the stamp ecosystem, merchants controlled the distribution, which they significantly altered by offering promotions like "double" or "triple" stamp days,[46] and stamp issuers determined the value of the merchandise for which stamps could be redeemed.[47] Under recent applications of the *Howey* test and the SEC Staff's 2019 digital asset framework,[48] these stamp transactions would be classified as investment contracts, requiring that offers and sales of stamps be registered or conducted pursuant to an exemption. Because it is impossible to register and trade stamps on a national securities exchange, nonaccredited investors would have been excluded—for their own protection—from purchasing these gummy-backed stickers and participating in the stamp ecosystem. It is instructive that the SEC did not even consider the investment contract analysis potentially applicable here, and only considered whether the stamps were evidence of indebtedness. Also significant is the SEC's prudent determination to refrain from exercising jurisdiction, recognizing that similar arguments could apply to items like streetcar tokens, meal tickets, and gift certificates—which the legislative history shows Congress did not intend to regulate as securities.[49]

B. The Application Of The Principle Of Control

Because DLT allows data to be recorded, stored, and shared across a distributed network, it removes the need for central authorities for managing and verifying data. The elimination of

---

[43] *See* Alan Morrell, *Whatever Happened to . . . Trading Stamps?*, Rochester Democrat and Chronicle (Jul. 31, 2015), https://www.democratandchronicle.com/story/news/local/rocroots/2015/07/31/whatever-happened-trading-stamps/30963275.

[44] Arthur C. Canady, *Trading Stamps–The Great American "Pastetime,"* 12 Fla. L. Rev. 213, 215 (1959) ("Canady"); *see, e.g.*, Jeff Lonto, *The Trading Stamp Story*, Studio Z-7, http://www.studioz7.com/stamps.html.

[45] SEC Interpretative Rel., *The Commission's Statement Regarding Trading Stamps*, 17 C.F.R. § 231.3890 (Jan. 24, 1958), https://www.govinfo.gov/content/pkg/FR-1958-01-25/pdf/FR-1958-01-25.pdf ("SEC Stamps Rel.").

[46] Canady, at. 215.

[47] *Id*.

[48] SEC staff, *Framework for "Investment Contract" Analysis of Digital Assets, Strategic Hub for Innovation and Financial Technology of the SEC* (2019), https://www.sec.gov/about/divisions-offices/division-corporation-finance/framework-investment-contract-analysis-digital-assets.

[49] *Id.* The commission noted that, if trading stamps were used for capital raising activities, its position might be different.

centralization is often referred to as decentralization. Decentralization has been used to refer to the distribution of control, decision-making, token issuance, token allocation, and/or data storage across a network of participants rather than being concentrated in a single entity or authority, among other things. Control is the foundational principle that underpins all these aspects, as it is essentially deconcentrating or distributing control. The concept of control is well-established within legal frameworks and offers a clearer, more concrete meaning compared to the more abstract and evolving notion of decentralization. Control is an important part of the analysis of distributed ledgers as a new business model, discussed in Section II.

There are various applications of control we glean from existing legal principles, whether it is controlling the computer code, the network, or the overall ecosystem. For example, the determination of whether the ownership interests in a typical organization are securities is guided by the legal form but ultimately depends on the economic realities of the parties' relationship. A nominal general partner may be able to assert a security interest by demonstrating the inability to exercise meaningful control over the partnership. This could be evidenced by: (1) the lack of legal control, where the partnership agreement distributes power in a way that significantly limits the investor's influence; (2) the absence of capacity to control, where the investor is too inexperienced or lacks the necessary business acumen to effectively exercise their partnership powers; and (3) the lack of practical control, where the partner is overly reliant on the unique managerial abilities of the promoter and is incapable of replacing the manager or exercising meaningful partnership authority.[50]

The lack of purchasers' meaningful control leads to concerns of transparency and information asymmetry between the purchaser and issuer/promoter. The already-existing concepts of "control," "majority-owned subsidiary," "affiliate," and "associate" in federal securities laws are valuable for understanding governance and ownership structures.[51] These are also helpful concepts for crafting and evaluating legal frameworks and tests applicable to digital assets and decentralization. "Control" refers to the ability to directly or indirectly direct an entity's management and policies through voting securities, contracts, or other means. A "majority-owned subsidiary" is an entity where a parent or related subsidiary holds over 50% of voting rights. An "affiliate" denotes shared control, in that a person "controls or is controlled by, or is under common control with" a specified party. Significant relationships are captured by the term "associate," including the relationship between an entity and its officer or partner of the entity, the beneficial ownership of 10% of certain stock, or familial ties with officers and directors, all of which may impact governance and decision-making. While these definitions do not lend themselves to many digital assets, the authority, influence, and control concepts are transferable to various systems.

In contexts when it is determined that disparities in control create risks, those risks often relate to information asymmetry, and potential fraud and manipulation. In those circumstances, when

[50] *See Willaimson v. Tucker*, 645 F.2d 404 (5th Cir. 1981).
[51] 17 CFR § 230.405 (defining terms, including "control," "majority-owned subsidiary," "affiliate," and "associate," that are described in this paper).

additional regulatory oversight and safeguards are required, the focus is often on disclosure and transparency to mitigate those risks. This includes identifying the controlling and managing persons or entities and providing purchasers with significant information regarding business or venture plans, risk, use of capital and proceeds, and the beneficial ownership of controlling and managing persons as well as large asset holders. For example, the SEC imposes rigorous disclosure requirements to ensure transparency and provide investors with the information needed to assess their investments, such as ownership in a company. Stockholders who, individually or as a group, acquire more than 5% of a registered class of equity securities must promptly disclose their background and investment intentions. This enables investors and companies to monitor potential influences on management and corporate policies. Additionally, officers, directors, and shareholders owning 10% or more of an SEC-reporting company's equity securities must promptly report transactions involving those securities, facilitating transparency, accountability, and oversight.[52]

Control in DLT networks is a multifaceted issue that impacts not only the structure and functionality of these networks but also consumer trust, market adoption, and effective and practical regulatory requirements. It is important to evaluate how control is distributed or concentrated across different aspects to appropriately balance innovation, freedom, competition, consumer protection, and market integrity. The issues where control may play a significant role include:

- **Consensus Mechanisms:** Control over transaction validation and network operations is governed by consensus algorithms, such as proof of work ("PoW"), proof of stake ("PoS"), Gossip protocol, and distributed hash table ("DHT"). These mechanisms ensure that no single entity can unilaterally control the network. However, if a small group of participants or mining pools dominate the consensus process, they may have the ability to disproportionately influence decisions, leading to centralization and undermining the decentralized nature of the system.

- **Permissionless versus Permissioned Control:** Permissionless DLT networks (e.g., Bitcoin, Ethereum) allow anyone to participate in validation and decision-making, increasing decentralization. But if too many resources are required to participate (e.g., costly mining equipment or high staking requirements), this can concentrate control among a smaller group, which limits decentralization. Permissioned DLT networks (e.g., Hyperledger Fabric, Corda) restrict access to specific entities, often for regulatory, operational, or privacy reasons. This inherent control structure can prevent true decentralization, as a select group of entities can control decisions and data, reducing the distribution of power and consensus.

[52] The SEC disclosure and reporting requirements discussed are located in the Securities Act, the Exchange Act, and the rules and regulations promulgated thereunder, including Exchange Act Sections 13(d), 13(g), and 16 and Regulation S-K.

- **Smart Contract Automation:** Decentralized control is enhanced by smart contracts, which automatically execute transactions based on predefined conditions without intermediaries, reducing reliance on centralized control. However, the creators of the smart contracts or the platforms that deploy them may retain influence in the form of the ability to modify or override the contracts after deployment, leading to centralized control over processes meant to be autonomous.
- **Node Distribution and Governance Influence:** A greater number of independent nodes with more widely distributed information throughout the network strengthens decentralization, preventing any single entity from gaining excessive control. If too many nodes are controlled by a few entities, this could give those entities disproportionate influence over the network's operations. Some networks implement delegated governance models where certain participants (e.g., validators, stakers) have greater control over protocol upgrades or decision-making. While this can improve efficiency, it also concentrates control among a limited group of participants, undermining the egalitarian nature of full decentralization.
- **Censorship Resistance:** No central authority can unilaterally censor transactions, making decentralized control of DLT networks resistant to external control. However, if a small group of miners, validators, or stakers controls the majority of the network's resources, they could potentially block or change transactions, which compromises the fundamental principle of censorship resistance.
- **Forking as a Form of Control:** If users disagree with network changes or governance decisions, they can initiate a hard fork or soft fork on some DLT networks (e.g., blockchain) to create a separate version of the blockchain, effectively shifting control to a new community. While forking can be a tool for decentralization, it can also serve as a mechanism for a group to seize control of the network and create a split, leading to potential fragmentation and less coherence across the blockchain ecosystem.

Understanding these dimensions of control is critical for navigating the challenges and opportunities in DLT ecosystems. And it can also provide guidance and well-established terminology to DLT concepts, such as decentralization and centralization.

C. Revised Approach To "Accredited Investor" Definition

To foster greater inclusivity within financial markets, the criteria for accredited investor status should be updated to include alternative pathways to qualification. Market participation should be permitted by basic financial literacy or access to expert advice. The test alternative would be simple and accessible, akin to a driver's license test, assessing basic knowledge of financial markets, investment products, and associated risks. It would ensure investors are able to make informed decisions without approaching the rigor of professional licensing exams.

Alternatively, individuals could qualify by working with certified financial professionals, such as investment advisers or financial planners, who have a responsibility to act in their clients' best

interests. This enables participation through relying on the expertise and ethical commitment of their adviser.

The evolution of financial markets calls for increased inclusivity, both for those seeking to raise capital and for those who wish to invest. Historically, access to key economic rights and opportunities was often tied to property ownership or the accumulation of wealth. Over time, these criteria served as the gatekeepers to participation in various financial activities. However, in today's complex and interconnected economy, such measures are increasingly becoming antiquated.

Wealth thresholds are not a proxy for sophistication in investing. Many individuals possess extensive financial acumen gained through education or experience, yet because they do not meet income or net worth requirements, they are barred from accessing certain investment opportunities. For some academics, nonprofit workers, and public service employees, wealth accumulation may not align with their knowledge and capacity to invest responsibly. Indeed, if it were not for the locality pay adjustment for the Washington, D.C. area, SEC Commissioners would not meet the salary thresholds to be accredited investors.[53] It is nonsensical that many of the government employees who develop and regulate our financial markets, pursuant to the accredited investor definition, would be deemed incapable of protecting themselves in the markets. This perverse disconnect excludes talented and informed individuals from participating in wealth-building opportunities that could benefit not only them but also the broader economy.

At its core, an enduring American principle is that individuals should retain the freedom to make choices about how to manage their own money. The presumption that people must be shielded from potential mistakes—based solely on their income or financial standing—undercuts this principle. While ensuring investor protections is important, denying access to opportunities based on wealth or salary assumes a uniform lack of judgment or competence that is neither fair nor accurate. Such restrictions inadvertently undermine the ideals of meritocracy and the "American Dream."

Together, these pathways prioritize financial literacy and informed decision-making over arbitrary wealth requirements. This proposal reflects a commitment to democratizing access while maintaining a focus on investor protection.

---

[53] SEC Commissioners are classified under Level IV of the Executive Schedule, with an annual salary of $191,900. The SEC Chairman is classified under Level III, which only surpassed the $200,000 threshold in 2024. Since the Commissioners are located in the D.C. area, they receive a 33.26% locality pay adjustment. *See generally U.S. Government Policy and Supporting Positions (Plum Book)*, S. Prt. No. 118-27 (2024), https://www.govinfo.gov/content/pkg/GPO-PLUMBOOK-2024/pdf/GPO-PLUMBOOK-2024.pdf; *U.S. Government Policy and Supporting Positions (Plum Book)*, S. Prt. No. 116 (2020), https://www.govinfo.gov/content/pkg/GPO-PLUMBOOK-2020/pdf/GPO-PLUMBOOK-2020.pdf.

IX. Classification Of Specific Digital Assets

The classification chart of specified digital assets is located in Exhibit 1. In that chart, we identify which of the twelve digital asset classes each identified digital asset fits, or may fit, within.

X. Identifying Appropriate Legal And Regulatory Regimes

In developing a comprehensive regulatory framework, it is important to identify which of the twelve asset classes naturally fall within the jurisdiction of a specific existing regulatory regime. Below are the most salient federal regulatory regimes for purposes of the digital asset classifications; however additional regulatory regimes may be applicable, including state law. With regard to state law, it is important to consider whether federal preemption should be extended to the extent it does not apply given the borderless nature of digital assets and implications for interstate commerce.

As an initial matter, society members are held to certain standards of conduct. One standard is the reasonable person standard,[54] which is a foundational principle in tort law and serves as a benchmark to evaluate whether an individual's actions meet the level of care required under specific circumstances. This standard embodies the hypothetical behavior of an ordinary, prudent person acting with rationality, caution, and foresight in comparable situations. The primary purpose of the standard is to establish an objective measure for assessing negligent conduct. It enables courts to determine whether a party breached their duty of care by failing to act as a reasonable person would under similar conditions and proximately caused harm to others that resulted in damages.

In addition, U.S. federal laws prohibit lying, cheating, and stealing to generally uphold fairness and integrity. These laws include key provisions against fraud, theft, and misrepresentation in both civil and criminal contexts. For example, the Wire Fraud Act and Mail Fraud Act criminalize deceit or false statements used to gain financial or personal advantage. Similarly, laws addressing embezzlement and larceny target the illegal appropriation of property or funds. These regulations ensure accountability and protect individuals, businesses, and the government from unethical behavior, reinforcing a broader commitment to trust and justice in society.

No additional regulatory regime is required to prohibit unreasonable and negligent actions, lying, cheating, or stealing.

[54] *See Blyth v. Company Proprietors of the Birmingham Water Works*, 11 Exch. 781, 156 Eng. Rep. 1047 (1856).

A. Securities And Exchange Commission

The SEC is the U.S. regulatory body responsible for enforcing federal securities laws and overseeing the securities industry. Its jurisdiction is limited to securities. Its stated mission is to protect investors, ensure fair, orderly, and efficient markets, and promote capital formation.[55] The primary federal statutes governing the federal securities law most relevant to this discussion are the Securities Act and the Exchange Act.[56] Generally, the Securities Act regulates the initial issuance and sale of securities, including registration, anti-fraud, and civil liability provisions. The Exchange Act regulates the secondary trading of securities, including trading on exchanges and over-the-counter markets. The SEC regulates traditional securities intermediaries, including securities brokers, exchanges, and clearing agencies.

The SEC has jurisdiction only over transactions involving securities, meaning its authority extends only to digital assets that implicate or fall under the purview of the securities laws. The securities laws generally require that the offer and sale of a security either be registered or conducted pursuant to an exemption from registration. Even if exempted from registration, certain disclosures from the issuer to the purchaser may be required, as well as other limitations on the transactions. Even when securities transactions are exempt, they are subject to the anti-fraud rules.

B. Commodity Futures Trading Commission

The jurisdiction of the Commodity Futures Trading Commission ("CFTC") is first defined by the bounds of the definition of "commodity" under the CEA. A "commodity" includes an enumerated list of agricultural products and "all other goods and articles . . . and all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in."[57] "[T]he existence of futures trading within a certain class" is sufficient for all items in that class to be considered commodities.[58]

The CFTC has enforcement, as opposed to regulatory, jurisdiction over the cash or "spot" commodity market. That means the CFTC does not have a regulatory and registration regime for commodity spot markets, but it can bring enforcement actions for fraud and market manipulation in connection with interstate commerce involving spot commodity markets.

The CEA grants the CFTC exclusive jurisdiction over various financial instruments related to commodities, including commodity options, swaps, futures contracts, and foreign exchange

---

[55] *About*, U.S. Sec. & Exch. Comm'n (Jun. 29, 2024), https://www.sec.gov/about.
[56] There are additional federal securities laws, such as the Trust Indenture Act of 1939, Investment Company Act of 1940, Investment Advisers Act of 1940, Sarbanes-Oxley Act of 2002, and Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.
[57] 7 U.S.C. § 1a(9).
[58] *CFTC v. My Big Coin Pay, Inc.*, 334 F. Supp. 3d 492, 498 (D. Mass. 2018) (applying a "middle of the ground" statutory reading that because futures contracts of bitcoin exists, all digital assets in the same class as bitcoin are also commodities, including the token, MBC).

trading.[59] The CFTC is charged with promoting markets that are open, competitive, and financially sound while protecting the public from fraud, manipulation, and abusive practices.

- **Commodity Options**: Financial contracts that give the holder the right, but not the obligation, to buy or sell a commodity (e.g., oil, gold, or agricultural products) at a predetermined price on or before a specified date.

- **Swaps**: Contracts in which two parties agree to exchange cash flows based on underlying assets or indices, such as interest rates, foreign currencies, or commodity prices. These can be complex financial products like interest rate swaps or credit default swaps.

- **Futures Contracts**: Agreements to buy or sell a commodity at a predetermined price on a specific future date. These contracts are widely used for hedging risks and speculating on price movements in markets such as agriculture, energy, and metals.

- **Foreign Exchange ("Forex") Trading**: The trading of one currency for another. These contracts are used to settle cross-currency payments and hedge currency risk.

The CFTC also regulates participants in the derivatives markets, including futures commission merchants ("FCMs"), exchanges, clearinghouses, and swap dealers/major swap participants.

The CEA, Securities Act, and Exchange Act do not expressly state that jurisdiction of the CFTC and SEC are mutually exclusive, but in practice it has been treated as such.[60] Crypto has presented a somewhat rare circumstance in which the SEC has treated a cryptocurrency as a security while the CFTC has treated that same cryptocurrency as a commodity.[61]

C. Federal Trade Commission

The Federal Trade Commission ("FTC") is primarily responsible for enforcing consumer protection and antitrust laws. Its regulations prohibit "unfair or deceptive acts or practices in or affecting commerce," which includes fraud.[62] The FTC's jurisdiction covers interstate commerce and applies to individuals, businesses, and entities engaging in commerce. Additionally, the FTC oversees issues in privacy, digital transactions, and deceptive marketing practices, ensuring consumer rights are upheld in an evolving digital economy. The FTC has already used its authority

---

[59] 7 U.S.C. § 2(a)(1)(A).
[60] Section 2(a)(1) of the CEA states that "nothing contained in this section shall (I) supersede or limit the jurisdiction at any time conferred on the Securities and Exchange Commission or other regulatory authorities . . . or (II) restrict the Securities and Exchange Commission . . . from carrying out their duties and responsibilities . . . ." 7 U.S.C. § 2(a)(1). The definition of "security" in both the Securities Act of 1933 and the Exchange Act begin with "unless the context otherwise requires." Securities Act, 15 U.S.C. § 77b(a)(1); Securities Exchange Act of 1934, 15 U.S.C. § 78c(3)(a)(10).
[61] Teresa Goody Guillén and Joanna Wasick. *DOJ, CFTC and SEC Bring Separate Actions for the Same Conduct: Alleged Digital Asset Manipulation and Fraud Scheme on Mango Markets Platform*. BakerHostetler Client Alert (Feb. 24, 2023), https://www.bakerlaw.com/insights/doj-cftc-and-sec-bring-separate-actions-for-the-same-conduct-alleged-digital-asset-manipulation-and-fraud-scheme-on-mango-markets-platform/.
[62] 15 U.S.C. § 45(a)(1).

in the crypto space, including in actions related to fake celebrity endorsements, scams, and misleading advertisements.

D. U.S. Department of the Treasury

The U.S. Department of the Treasury safeguards against financial crimes, leveraging its authority to promote global stability and maintain the integrity of the financial system. Through its specialized agencies—such as the Office of Foreign Assets Control ("OFAC"), the Financial Crimes Enforcement Network ("FinCEN"), and the Internal Revenue Service ("IRS")—the Treasury enforces laws on sanctions, anti-money laundering ("AML"), and tax compliance. Each agency plays a distinct yet interconnected role in combating illicit activities and ensuring adherence to federal regulations.

Sanctions Enforcement: OFAC administers and enforces economic and trade sanctions against targeted individuals, entities, and jurisdictions. These sanctions are designed to restrict financial transactions and deter activities that threaten national security, such as terrorism financing, nuclear proliferation, and human rights abuses.

AML and Know Your Customer ("KYC") Regulations: FinCEN combats money laundering and other financial crimes by implementing the Bank Secrecy Act ("BSA"). Under these regulations, financial institutions are required to implement KYC protocols, monitor suspicious transactions, and file reports on activities that raise red flags. These efforts target illicit financial flows and aim to prevent the misuse of financial systems for criminal activities, including drug trafficking and organized crime.

Tax Enforcement: The IRS focuses on ensuring compliance with tax law by detecting and addressing unreported income, tax evasion, and fraud.

E. Banking Regulators

The U.S. banking regulators oversee and regulate financial institutions to ensure the stability, safety, and fairness of the banking system. There are several key regulators with varying responsibilities and authority:

1. The Federal Reserve

As the central bank, the Federal Reserve ("Fed") has broad authority over the U.S. banking system. It supervises and regulates commercial banks, bank holding companies, and savings and loan associations. The Fed plays key roles in monetary policy, setting interest rates and controlling the money supply. It supervises financial institutions to ensure sound practices and adequate capital. Additionally, as a lender of last resort, the Fed provides emergency funds to financial institutions during crises to maintain stability.

2. The Office of the Comptroller of the Currency

The Office of the Comptroller of the Currency ("OCC") is responsible for regulating and supervising national banks and federal savings associations, focusing on their capital requirements, risk management, and compliance mechanisms. The OCC plays a key role in chartering national banks and overseeing their compliance with banking laws. It is tasked with ensuring banks operate safely, manage risks effectively, and maintain financial stability.

3. The Federal Deposit Insurance Corporation

The Federal Deposit Insurance Corporation ("FDIC") regulates and supervises state-chartered banks that are not members of the Federal Reserve System and provides deposit insurance to protect consumers. The FDIC insures deposits up to $250,000 per depositor, supervises banks for safety and compliance with consumer protection laws, and manages the resolution of failed banks to protect depositors.

F. Department of Justice

The DOJ is tasked with prosecuting financial crimes such as securities fraud, commodities fraud, crypto-related fraud, money laundering, and sanctions violations. The department collaborates with other regulators, including the SEC, CFTC, FTC, and Treasury, to enforce laws like the Securities Act, Exchange Act, CEA, the BSA, and the Racketeer Influenced and Corrupt Organizations Act ("RICO"). Its criminal enforcement role is central to upholding the law and maintaining integrity in financial systems.

XI. Considerations For Coordinated Comprehensive Regulation

After the initial digital asset classification and assessment of the regulatory regimes that are implicated for the various assets, we next identified issues that need to be addressed and proposed solutions. A few of the prominent issues are set forth below with relevant considerations.

A. Coordinated Agency And Legislative Action

In light of the significant setbacks faced by the digital asset industry,[63] it is crucial to develop an expedited, coordinated, and comprehensive regulatory regime. While numerous bills have been proposed in both the House and Senate, enacting major new legislation may not be necessary—there is likely a more swift approach. The SEC has broad exemptive authority under Section 28 of the Securities Act and Section 36 of the Exchange Act, which provides the agency the discretion to "conditionally or unconditionally exempt any person, security, or transaction, or any class or classes of persons, securities, or transactions" from the Acts and any rules and regulations

[63] *See* Hester M. Peirce, SEC Commissioner, *The Journey Begins*, U.S. Securities and Exchange Commission (Feb. 4, 2025), https://www.sec.gov/.

thereunder, as long as it deems the exemption to be in the public interest and consistent with the protection of investors.

Likewise, the CFTC has broad exemptive authority under Section 4(c) of the CEA, which allows the agency to exempt certain "agreement[s], contract[s], or transaction[s], (or classes thereof)" from regulation under the CEA if it determines that doing so is in the public interest or if it believes such an exemption would promote "responsible economic or financial innovation and fair competition." Notably, this could not be used to grant the CFTC additional regulatory authority over the spot commodities markets, which would require Congressional action.

However, the SEC and CFTC could align with other stakeholders, including Congress and the Executive branch, to arrive at a collaborative regulatory framework that can be established using their broad, respective exemptive authority. Through collaborative efforts, these agencies can implement light-touch regulatory approaches in a way that is adaptable and conducive to the assets and technology, which avoids comprehensive new legislation that may take many years to implement. The collaborative agreements could then be codified into law, ensuring their long-term stability. While additional legislation may be necessary to grant additional authority, such legislation could be significantly limited in scope to provide a potentially more nimble and swift approach.

This is not a new approach; the SEC and CFTC took a similar approach to jurisdictional coordination[64] in the 1981 jurisdictional accord, known as the Shad-Johnson Accord, which was formalized into legislation in 1982.[65] The Accord effectively divided jurisdiction over derivative products between the two agencies based on the nature of the products. Specifically, the SEC retained jurisdiction over securities-related products, such as options on securities and securities indices, while the CFTC took jurisdiction over commodity futures.

While tax implications are not the primary focus of this discussion, they play a critical role in the industry's growth, particularly in developing its infrastructure. Unfavorable or impractical tax treatments can hinder progress, making it essential to consider tax incentives and policies that support sustainable development while remaining practical and reasonable for industry participants.

B. Considerations For Regulatory Oversight Of Digital Asset Centralized Exchanges

Drawing from the lessons of the Pecora Commission, exchanges can play a pivotal role in safeguarding consumer protection and maintaining market integrity. "The function of an exchange is to maintain an open market for [assets], where supply and demand can freely meet at prices

---

[64] Bevis Longstreth, SEC Commissioner, *The SEC-CFTC Accord: Accommodation in the Public Interest, Remarks to the Securities and Commodities Laws Committees of the Chicago Bar Association*, U.S. Securities and Exchange Commission (Apr. 16, 1982), https://www.sec.gov/news/speech/1982/041682longstreth.pdf.
[65] Futures Trading Act of 1982, Pub. L. No. 97-444, 96 Stat. 2294 (1983).

uninfluenced by manipulation or control."[66] This principle is especially pertinent as we consider the future of cryptocurrency exchanges. With the rapid evolution of digital assets, there is substantial potential to create a framework that fosters innovation while addressing the unique challenges posed by these markets, which can be facilitated by various market participants. Centralized exchanges are uniquely positioned to implement listing disclosures, monitor for fraud and manipulative conduct, and promote competition to enhance market participation and growth.

Workable regulation must take into account several considerations:

- Trading some digital assets is not possible or practical under current regulations, such as digital asset securities on national securities exchanges. While legacy exchanges should be updated to accommodate digital assets, it may be more expedient and efficient to facilitate the trading of digital assets on existing (and future) digital asset exchanges, with new or modified regulations to the extent necessary.
- To best capture efficiencies and reduce overly burdensome and costly duplicative regulatory compliance, to the extent possible, different classes of digital assets should be available to trade on the same platform.
- To the extent possible, existing registration and reporting regimes should be considered whether they are practical for, and provide relevant information regarding, digital assets and associated transactions. Disclosures should provide purchasers with information that is relevant to their purchase, e.g., value regarding a digital asset as opposed to the value of the equity of a company associated with developing the digital asset. Disclosures required by listing persons or issuers must be feasible on permitted exchanges.
- To the extent existing regulatory frameworks are ill-suited for digital assets and DLT, such as for digital asset securities, new regulatory frameworks should be created. The new frameworks should leverage technologies (e.g., DLT-enabled clearing), enhance efficiencies, and provide flexibility to adapt to new technologies and products. Notably, the SEC took a similar approach when promulgating Regulation ATS for alternative trading systems. These new, simplified, nimble, forward-looking frameworks and approaches can be a template that is followed to improve our existing regulatory frameworks for traditional assets and legacy markets.
- Market participants, including intermediaries, should not have to be subject to regulation by multiple regulators for the same conduct. Full registration with one regulator with notice registration to any others should suffice.
- Assets may transform over their life cycle, but the exact moment of transformation would be difficult to define and should not force a shift in regulatory oversight.

[66] *Stock Exchange Practices Report of the Committee on Banking and Currency*, S. Res. 84, 72d Cong., 76 Cong. Rec. 5241 (1932); S. Rep. 73-1455, at 81 (1934), https://www.senate.gov/about/resources/pdf/pecora-final-report.pdf.

- Technology and automation should be used to the benefit of market participants, increasing reliability and lowering both barriers to entry and ongoing cost of compliance. For example, AI tools can be deployed for advanced auditing and monitoring.

C. Considerations For Regulatory Oversight Of Spot Digital Assets Markets

Certain digital asset markets are particularly vulnerable to manipulation, fraud, and unfair trading practices. Markets operating outside established securities and derivatives regulatory frameworks often lack adequate disclosures, creating information asymmetry between issuers/promoters and purchasers. Specifically, the spot market for digital assets that are neither securities nor derivatives are not subject to the SEC or CFTC regulatory registration and reporting regime. Instead, the trading of those assets may be subject to Treasury Department regulations for AML and counter-terrorism financing and banking or money transmission licensing and regulations. Even in the absence of a specific regulatory regime, the government has the authority to bring enforcement actions for fraudulent or manipulative conduct, as well as unfair and deceptive practices. In conversations with industry participants, many expressed a preference for a light-touch regulatory framework for the spot market of non-security digital assets. Such an approach would offer protections for purchasers, particularly in terms of disclosures, thereby enhancing market integrity, without imposing burdensome or excessive regulation. The goal is not rigid control but a forward-thinking, practical approach that considers the industry's trajectory. As the digital asset market rapidly expands, its economic impact will only continue to grow. A proposed initial summary of certain market participants, consumer protection and market considerations, and potential regulatory considerations is annexed as Exhibit 2.

One potential approach is for spot digital assets to be subject to certain regulatory requirements based on the characteristics of their respective markets. Indicia that some regulatory oversight is warranted could be guided by retail access to the market, market depth, and trading volume. That is, some regulatory oversight may be triggered when secondary market trading of an asset is available to retail investors on a centralized or decentralized exchange or the asset is otherwise traded with significant volume and liquidity. While large volumes and deep liquidity are signs of a healthy trading environment, these also may make the market more susceptible to manipulation, fraud, and other abuses if left unchecked. Without regulatory oversight, the market could be exploited by bad actors, and these markets may warrant additional, minimal consumer protections.

Certain concerns related to the integrity of digital asset markets should be considered in evaluating the necessity or appropriateness of regulation.

1. **Fair and Independent Price Discovery**: Prices should be determined equitably by the forces of supply and demand across multiple independent and unaffiliated trading venues. Price manipulation or biased pricing mechanisms can erode market integrity. If prices are shaped by a single entity or a small group of actors, it can result in artificial price levels and market distortions that disproportionately harm participants, especially retail investors. Independent price discovery is essential to guarantee that market prices accurately reflect the true supply and demand for assets.

In digital asset markets, where volatility and decentralized structures can make price discovery more complex, ensuring that prices reflect actual market activity is particularly crucial. This is often best achieved with transparency, surveillance, and rules that promote market fairness across all trading venues.

2. **Low Slippage and Tight Spreads**: Large trades should not significantly impact asset prices, and bid-ask spreads must remain narrow across platforms. Slippage, the difference between the expected and actual trade price, is particularly problematic in digital asset markets due to volatility and liquidity issues. Platforms should maintain sufficient liquidity to prevent large orders from causing price disruptions, allowing both retail and institutional traders to execute transactions with minimal price movement. Consideration should be given to mechanisms that incentivize competition, liquidity, and efficiency in the market, such as encouraging market makers to provide liquidity, using liquidity pools, and facilitating transparent pricing.

3. **Consumer Protection and Risk Disclosure**: Digital assets often carry high levels of risk due to their volatility and technological complexities. There are often information asymmetries associated with affiliated persons and entities who own significant amounts of the digital assets and/or effectively control the protocol or any part of the ecosystem as well as plans of operations.

   Consideration should be given to clear and consistent risk disclosure standards that are relevant to the specific asset and its characteristics so that retail investors understand the potential risks associated with investing in digital assets. This could include warnings about price volatility, the speculative nature of many assets, and the potential for loss of capital. Educating retail investors about these risks can help them make more informed choices and reduce the likelihood of market manipulation targeting less experienced investors. To the extent a disclosure regime is created for non-security digital assets, or digital asset securities that do not represent a debt or equity instrument or transaction, regulators should consider adapting the disclosure requirements from SEC Regulation CF and tailoring them to digital asset securities. To the extent there are securities that are not typically classified as debt or equity instruments, there must be a clear, consistent methodology to determine how to treat the assets. Returning to first principles, to the extent an investor transfers their money or assets for the right to receive something in the future, that generally implies a debt obligation or evidence of indebtedness.

   Relevant information for users of trading platforms includes financial health, trading volumes, and asset-backed reserves for platforms dealing with stablecoins or other asset-backed tokens.

4. **Auditability and Compliance**: Given the importance of technical security to prevent loss and protect privacy, consideration should be given to periodic, but not overly invasive, audits of smart contracts, financial records, and platform operations to detect potential vulnerabilities and prevent fraudulent activities, such as wash trading and market manipulation. Smart contract audits and any AI or automation should be audited to ensure that code is free of flaws or exploits that could compromise user funds. On-chain data could be leveraged to monitor for irregularities, such as unusual trading patterns or suspicious transactions, which would trigger targeted investigations. Combining automated, on-chain monitoring with light-touch regulatory oversight could effectively reduce the risk of fraud, improve market integrity, and ensure investor protection without stifling innovation in the sector.

When considering market monitoring or technological auditing requirements, it is important to strike a balance between consumer protection, cost-effectiveness, and competitive fairness. Excessive compliance costs can create barriers to entry, stifling innovation and reducing market competition.

To mitigate these concerns, policymakers should explore flexible regulatory approaches. This could include a combination of government-provided monitoring and auditing services as well as alternative compliance pathways for companies that prefer to limit direct disclosure to government entities. For instance, entities could meet certain regulatory requirements through approved third-party audits or certification programs. By offering multiple avenues for compliance, regulation can uphold consumer protection and market integrity without imposing undue financial burdens or inhibiting competition.

For digital assets without regulatory oversight, it is recommended that a clear, concise risk disclosure be required, similar in length and format to health warnings on products like cigarettes. The warning could read:

> ***Warning**: Purchasing digital assets is highly speculative and involves significant risk. Prices can fluctuate wildly, and you may lose all your money. These assets have limited regulatory oversight, and risks like fraud, market manipulation, or technical failures may result in financial loss. Only purchase what you can afford to lose.*

XII. Conclusion And Next Steps

Achieving clarity in digital asset regulation requires a nuanced approach that fosters innovation while ensuring accountability. This discussion framework emphasizes the need for comprehensive classification of digital assets, aligning regulatory oversight with their unique characteristics, and developing adaptable policies to promote transparent, fair, and resilient markets. Regulatory strategies should draw from traditional business structures, considering DLT's decentralized and borderless nature, to provide agile yet effective oversight.

The next phase necessitates collaboration among regulators, industry leaders, policymakers, and academics to refine these proposals. Policymakers are encouraged to use this framework as a foundation for open dialogue, aiming to streamline regulatory processes while safeguarding consumer and market interests. Stakeholders across the digital asset ecosystem are invited to offer feedback, share insights, and identify gaps, ensuring the framework remains practical and responsive to emerging technologies.

By uniting efforts, we can establish a regulatory environment that fosters growth, innovation, and trust in the future of digital assets. Now is the time to synchronize strategies and create a robust, forward-thinking structure that empowers a dynamic and democratic digital economy.

Exhibit 1

Key:
✅: Classification applies
➖: Classification may apply
Blank: Classification unlikely to apply

Proposed Digital Asset Classification Chart

*Depending on the structure and facts and circumstances of the asset and transaction, the classification is subject to change.

Digital Asset	Digital Payment Units	Primary Digital Currencies	Functional Digital Assets	Digital Asset Commodities	Digital Asset Securities	Asset-Backed Stablecoins	Tokenized Real-World Assets	Non-Fungible Digital Assets	Tribal & Social Assets	Non-Functional Inert Assets	Other
Cryptocurrencies (BTC, ETH, & Altcoins)	➖	➖	➖	➖	➖				✅		
Fiat-Backed Stablecoins	✅					✅					
Asset-Backed Stablecoins	✅					✅					
Algorithmic Stablecoins	✅										
Non-Fungible Tokens (NFTs)								✅	✅		
Meme/Community Tokens				➖					✅	✅	
Fundraising Token (ICO)	➖	➖	➖		✅				✅		
Tokenized Security Tokens					✅				➖		
Tokenized Real-World Assets				➖	➖		✅		➖		
Decentralized Finance (DeFi) Tokens	➖	➖	➖	➖	➖	➖			✅	➖	
Access Tokens		➖	✅	➖					✅		
Privacy Coins		➖	✅	➖					✅		
Carbon Credits & Environmental Assets		➖	✅	➖					✅		

Exhibit 1

Digital Asset	Digital Payment Units	Primary Digital Currencies	Functional Digital Assets	Digital Asset Commodities	Digital Asset Securities	Asset-Backed Stablecoins	Tokenized Real-World Assets	Non-Fungible Digital Assets	Tribal & Social Assets	Non-Functional Inert Assets	Other
Identity / Reputation Tokens			✅					—	✅		
Governance Tokens		—	✅	—	—				✅		
Central Bank Digital Currencies (CBDCs)	✅					✅					
Synthetic Assets (Synths)			—	—	—		—				✅ Derivative
Virtual or Metaverse Assets		—	✅	—	—			—	✅		
Gaming Assets / Play-to-Earn Tokens		—	✅	—				—	✅		
Layer 2 Tokens (Overlaps with Cryptocurrencies, e.g., Altcoins)	—		✅	—	—				✅		
Yield-bearing Tokens	—	—	✅	—	—	—			✅		
Staking Rewards	—	—	—	—	—			—	✅	—	
Liquidity Provider (LP) Tokens			✅	—	—						
Tokenized Intellectual Property (IP)			✅				✅				
Tokenized Fund Shares / Investment Tokens					✅		—				
Social Media and Content Creation Tokens	—	—	✅	—	—			—	✅		
Cross-chain Assets	—	—	✅	—	—	—	—	—	✅		

Exhibit 2

Market Participant Chart

Category	Description & Role	Consumer Protection & Market Considerations	Potential Regulatory Considerations
Retail Participants	• Individual, non-professional participants. • Limited access to private markets (when in investor capacity).	• Market volatility and information asymmetry. • Risk of investing in fraudulent or unsustainable projects. • Increased exposure to market manipulation, insider trading and token dumping concerns.	• Disclosure of risks and information. • Monitoring and fraud detection.
High-Net-Worth Participants	• Access to private placements, hedge funds, and venture capital. • Bring large amounts of liquidity. •	• Market manipulation risks, and lack of transparency. • Risk of investing in fraudulent or unsustainable projects. • Increased exposure to market manipulation, insider trading and token dumping concerns. • May have influence over governance mechanisms in DAOs or DeFi projects through size of holdings.	• Disclosure of risks and information. • Monitoring and fraud detection. • Transparency and disclosure for large/controlling digital asset holdings. • Limits on concentration of ownership for governance tokens.
Institutional Investors	• Organizations investing on behalf of others. Includes pension funds, mutual funds, insurance companies, and endowments. • Bring liquidity and sophistication to the market, contributing to market maturity.	• Counterparty risk when dealing with unregulated exchanges or custodians. • Risk of market disruption if large positions unwind suddenly. • Risk of investing in fraudulent or unsustainable projects. • Increased exposure to market manipulation, insider trading and token dumping concerns. • May have potential conflicts in token projects or if institutions also operate exchanges, custodians, or DeFi protocols. • May have influence over governance mechanisms in DAOs or DeFi projects through size of holdings.	• Transparency and disclosure for large/controlling digital asset holdings. • Risk management and disclosure. • Disclosure of potential conflicts. • Third-party custody requirement for large institutional holdings.

Exhibit 2

Category	Description & Role	Consumer Protection & Market Considerations	Potential Regulatory Considerations
Private Market & Alternative Investors	• Individuals or firms that invest in digital asset companies and DLT projects, offering capital in exchange for equity or tokens. Often focus on high-risk, high-reward investments in private markets. Includes venture capitalists (VCs), private equity (PE) firms, and hedge funds. • Provide funding and strategic guidance to DLT projects, fostering innovation and growth.	• Counterparty risk when dealing with unregulated exchanges or custodians. • Risk of market disruption if large positions unwind suddenly. • Risk of investing in fraudulent or unsustainable projects. • Increased exposure to market manipulation, insider trading, and token dumping concerns. • May have influence over governance mechanisms in DAOs or DeFi projects through size of holdings.	• Transparency for investors regarding token allocations and vesting schedules. • Limits on pre-sale allocations to prevent undue control. • Disclosure of potential conflicts.
Centralized Digital Asset Exchange (CEX)	• An exchange that is operated by a centralized entity that retains custody of crypto assets of customers. • Act as intermediaries, providing liquidity and often offering additional services, such as staking, margin trading, or futures.	• Risks related to hacking, insolvency, and fraud risks. • Potential for smart contract vulnerabilities. • Lack of consumer protection for lost or stolen funds. • May have conflicts of interest if exchange also acts as custodian, lender, market maker, or issuer. • May possess dominance over price discovery. • Potential self-dealing or preferential treatment of specific tokens.	• Licensing/registration and compliance requirements. • Transparency and standards related to listings, de-listings, order book, and liquidity. • Disclosure of information and risks. • Disclosures and mitigation to address vertical integration, conflicts of interest, potential for anticompetitive behavior. • Facilitate alternatives and user choice for certain services to avoid anti-competitive bundling. • Monitoring for fraud and manipulation detection.
Decentralized Digital Asset Exchange (DEX)	• A DeFi application enabling users can trade directly with each other, without an intermediary or central authority. • Users retain full custody of their assets and interact through smart contracts or peer-to-peer (P2P) mechanisms.	• Risks related to hacking, insolvency, fraud risks, illicit finance. • Potential for smart contract vulnerabilities. • Lack of consumer protection and recourse for lost or stolen funds and lack of accountability. • Lack of transparency and disclosures around platform functioning and design (fees, governance, token listings and de-listings).	• Due to decentralized nature, certain regulatory and reporting requirements generally are not feasible. • Licensing, registration, and/or compliance requirements on DEX front-ends or core developers (differing requirements depending on governance structure). • Transparency and standards related to listings, de-listings, order book, liquidity, smart contract risks,

Exhibit 2

Category	Description & Role	Consumer Protection & Market Considerations	Potential Regulatory Considerations
	• May use liquidity pools (AMMs) or on-chain order books to facilitate trading. • Typically allows permissionless access (anyone can trade without KYC/AML). • Supports trading many digital assets (not available on CEX).	• Lower liquidity leading to high slippage, increased volatility, fragmented and disadvantageous pricing.	and fees (potentially smart contract auditing AI apps). • Disclosures of risks (potentially automated). • If governance is centralized, ensuring transparency of conflicts of interest. • Monitoring for fraud and manipulation detection (potentially vendor agreement through DAOs, etc.).
Miners & Validators	• Entities responsible for securing DLT networks by validating transactions and maintaining the ledger. • Ensure the integrity and security of DLT networks, rewarded with new coins or tokens.	• Centralization risks in mining pools or validator networks (51% attack, double-spending, transaction censorship, cartelization). • MEV (maximal extractable value) exploits, as validators can front-run, sandwich attack.	• Disclosure of mining pool concentration, validator ownership, governance models, and staking delegation. • Incentivize validator participation to reduce centralization of efforts and encourage competition. • Ensuring transactions are processed fairly, preventing discriminatory treatment or censorship by miners or validators.
DLT Developers	• Developers creating and maintaining DLT platforms and smart contracts. • Contribute to the expansion of the digital asset space by improving scalability, security, and usability of DLT networks.	• Legal liability for flawed code leading to financial losses. • Developers controlling both infrastructure and applications could lead to anti-competitive behavior.	• Security audits for major DLT upgrades. • Open-source best practices. • Clear liability standards and safe harbors. • Disclosure and transparency of deployment of certain autonomous agents.
Digital Assets Custodians **(Custodial Wallets)**	• Third-party services providing secure storage and management of digital assets, especially for institutional participants. • Securely store large amounts of digital assets for individuals and institutions, reducing risk of theft or loss.	• Custodial failures leading to asset loss (fraudulent or mismanagement of client funds). • If provides other service, potential conflicts of interest could arise (e.g., asset security, lending). • Risk of liquidity shortfalls if custodian lends, stakes, or reinvests customer (pooled) assets. • Dominance of a few large custodians reducing competition. • Potential for smart contract vulnerabilities leading to loss of user funds.	• Licensing and asset reserve transparency and requirements. • Periodic security audits and risk assessments. • Segregation of customer funds from proprietary funds. • Standards and ownership clarity for omnibus accounts.

Exhibit 2

Category	Description & Role	Consumer Protection & Market Considerations	Potential Regulatory Considerations
DeFi Protocols and Platforms	• Platforms enabling peer-to-peer services like lending (including collateralized), borrowing, trading (including derivatives), and yield farming without centralized intermediaries. • Create new financial products, enabling global access to services like loans, insurance, and DEXs. • Uses liquidity pools, staking, or lending protocols to provide assets for activities.	• Risks related to hacking, insolvency, fraud, illicit finance. • Lack of consumer protection and recourse for lost or stolen assets and lack of accountability. • Lack of transparency and disclosures around platform functioning and design, including reward structure and recipients. • Lower liquidity leading to high slippage, increased volatility, fragmented and disadvantageous pricing. • Potential for smart contract vulnerabilities leading to loss of user funds. • Difficulty verifying absence of centralized control. • Potential market manipulation by large liquidity providers.	• Due to decentralized nature, certain regulatory and reporting requirements generally are not feasible. • Security and operations audits for DeFi platforms. • Risk disclosures for DeFi users (the extent feasible, potentially by front-ends, potentially automated, or initial disclosure from core developers). • Transparency regarding governance, incentives and rewards, liquidity. • If governance is centralized, ensuring transparency of conflicts of interest. • Monitoring for fraud and manipulation detection (potentially vendor agreement through DAOs, etc.).
Digital Assets Wallet Providers (Noncustodial)	• Providers offering software or hardware solutions for securely storing and managing digital assets. • Enable users to store private keys and interact with DLT networks.	• Risk of hacking, phishing attacks, lack of recovery mechanisms if private keys are lost. • Conflicts of interest if offering vertical services and potential for anti-competitive conduct. • Centralization risks in wallet providers affecting ecosystem security.	• Security certification standards for wallet providers. • Fraud protection measures for compromised wallets.
Digital Assets Payment Services	• Services allowing businesses to accept digital asset payments. • Bridge the gap between digital assets and fiat currencies, promoting broader digital asset adoption.	• Consumer protections for refund disputes and chargebacks. • AML/KYC compliance concerns. • Risk of preferential treatment if payment processors prioritize affiliated merchants. • Dependence on intermediaries for transaction processing. • Potential for smart contract vulnerabilities.	• Licensing and compliance requirements for payment processors. • Consumer protection rules for dispute resolution. • Transparency of affiliates and transparency and mitigation of conflicts of interest.
Digital Assets Payment Card Providers	• Provide credit or debit cards that allow users to spend digital assets at merchants. • Facilitate the use of digital assets in real-world transactions.	• Loss of funds due to fraud or improper card management. • If major exchanges also issue cards, there may be conflicts in transaction routing. • Market dominance by a few large issuers.	• Licensing and compliance standards (including fraud prevention measures). • Clear consumer refund and recourse mechanisms. • Transparency of affiliates and transparency and mitigation of conflicts of interest.

Exhibit 2

Category	Description & Role	Consumer Protection & Market Considerations	Potential Regulatory Considerations
Stablecoin Issuers	• Entities that create and maintain stablecoins pegged to real-world assets. • Provide stability in the volatile digital asset market.	• Lack of reserves transparency, redemption mechanisms, systemic risk in case of failure (risk of de-pegging leading to financial instability). • If vertical integration potential for conflicts of interest and liquidity manipulation (e.g., exchanges issuing their own stablecoins) • Few issuers controlling large portions of digital asset liquidity.	• Licensing and compliance requirements. • Reserve transparency and requirements, and audit requirements. • Consumer protections for refunds, dispute resolution, and redemption (including in the case of failure). • Interoperability standards to facilitate interoperability across networks.
Digital Asset Managers	• Firms or individuals managing digital asset portfolios on behalf of clients. • Help clients manage their digital asset investments by constructing diversified portfolios and providing strategy advice.	• Potential conflicts of interest when managing client assets. • Conflicts of interest if integration with other services (e.g., asset managers own trading platforms can front-run order). • Market dominance by a few large players reducing competition.	• Registration and licensing requirements for asset managers. • Duties to clients similar to traditional finance. • Transparency requirements for fund holdings.
Digital Assets Hedge Funds	• Hedge funds specializing in investments in digital assets associated with DLT, using strategies like active trading and arbitrage. • Seek to generate high returns (e.g., capitalizing on price volatility, market inefficiencies, and emerging DLT network opportunities).	• High-risk investment strategies may lead to substantial losses, especially in volatile and illiquid markets. • Lack of investor protections for digital asset investments. •	• Applicable disclosure requirements for risks, hedge fund holdings, strategies, and conflicts of interest. • Transparency of fees and expenses. • Secure custody solutions.
Decentralized Autonomous Organizations (DAOs)	• Community-governed entities that enable community decentralized decision-making (rather than centralized entity) within DLT-based projects. Often operate autonomously through smart contracts and collective decision-making structures.	• Governance attacks where a small group gains control. • Legal ambiguity regarding DAO liability and enforcement. • Large token holders disproportionately influencing decisions. • Potential for smart contract vulnerabilities leading to loss of user funds (e.g., hacks or	• DAO legal entity frameworks for liability clarity. • Transparency requirements for governance votes. Anti-manipulation mechanisms so voting power is not unduly influenced by few large stakeholders (e.g., vote caps, delegation restrictions). • Some DAOs may need verification that participants are not known bad actors. • Dispute resolution mechanisms. • Security and smart contract audits.

Exhibit 2

Category	Description & Role	Consumer Protection & Market Considerations	Potential Regulatory Considerations
	• Token holders vote on proposals related to governance, development, or financial decisions.	exploitation of the DAO's funds or governance mechanisms).	
Digital Asset Staking Providers	• Platforms allowing users to stake digital assets to participate in proof-of-stake (PoS) consensus mechanisms. • Enable participation in PoS networks and reward users for supporting the network, often pooling funds for efficiency.	• Custodial risks if staking providers mismanage user funds (includes slashing). • Potential misleading claims about staking rewards. • If staking pools become too large, they could dominate consensus mechanisms. • Centralization risks if a few staking providers dominate governance.	• Disclosure and transparency requirements for staking service providers (fees, rewards, terms). • Disclosures (including risks) about staking lock-up periods and yield expectations. • Security standards and audits. • Consumer protection and illicit finance requirements (e.g., if custodial or facilitate large-scale staking pools).
NFT Platforms and Marketplaces	• Platforms facilitating the creation, buying, and selling of NFTs. • Help creators and collectors engage in the digital economy by enabling the trading of unique, DLT-based assets.	• Risk of fraud and counterfeit NFTs. • Lack of intellectual property protections. • If NFT platforms also issue NFTs, they could manipulate pricing. • Market manipulation via wash trading and artificial scarcity.	• IP verification standards for NFTs. • Fraud and manipulation prevention. • For certain transactions, transparency around NFT origin and history (creator, transaction history, and asset ownership).
Token Issuers	• Organizations or projects creating and issuing new digital tokens or digital assets. • Introduce new assets to the digital asset market, potentially offering investment opportunities in new projects.	• Risk of fraud and information asymmetry (scams, rug pulls). • Information asymmetry (lack of disclosures). • Conflicts of interest if combined with other business activities, e.g., exchanges issuing tokens (price manipulation, preferential listing), could distort market fairness (liquidity price discovery). • Market manipulation if issuers control token supply and price dynamics.	• Disclosures for token issuance (risks, goals, token functionality, milestones, control, token supply, allocation, token limits and vesting, whitepaper standards, financial reviews or audits). • Consumer protection measures for token pre-sales (application of securities laws to securities transactions, modified appropriately for digital assets). • Fraud and manipulation prevention.

Exhibit 2

Category	Description & Role	Consumer Protection & Market Considerations	Potential Regulatory Considerations
DLT Auditors & Security Firms	• Firms conducting security audits for smart contracts and protocols. • Ensure DLT security and prevent vulnerabilities.	• Conflicts of interest in auditing firms providing consulting services to projects they review. • Lack of standardization in security audits. • Lack of legal recourse if an audited project is later exploited. • Influence over market confidence in projects if a few firms dominate auditing.	• Standardized security auditing requirements (code review, penetration testing, stress testing). • Liability frameworks for security auditors if negligence leads to financial harm. • Accreditation and certification for auditors. • Disclosures in reports (methodologies, limitations and risks of audit, unresolved vulnerabilities).
Digital Assets Market Makers	• Liquidity providers ensuring smooth transactions on exchanges by placing buy and sell orders. • Facilitate liquidity and reduced volatility by consistently placing buy and sell orders for assets.	• Market manipulation (wash trading) and front-running concerns. • Conflicts of interest if affiliated with exchanges (price manipulation). • Market dominance by a few large market makers could lead to unfair pricing.	• Transparency requirements for market-making activities (e.g., fee disclosures, trading volumes, order limits, other practices impacting price discovery). • Monitoring to detect manipulative practices (e.g., spoofing, wash trading). • Disclosure requirements (e.g., relationships with exchanges).
Digital Assets Oracles	• Providers of external data to DLT networks; acting as intermediaries between off-chain data sources and on-chain smart contracts. • Enable decentralized applications to access reliable data, triggering smart contract actions.	• Risk of inaccurate or manipulated data impacting smart contract outcomes. • Single points of failure. • Centralization risks if a few oracle providers dominate the space. • Privacy concerns for hacked or misused data.	• Security and redundancy standards for oracle providers. • Disclosure requirements on data sources and methodologies, conflicts of interest, verification of data, and other issues impacting validation of data. • Depending on type of oracle, verification or auditing of data standards, data privacy and compliance requirements. • Transparency in governance of oracles.
Cross-Chain Bridge Providers	• Platforms enabling asset transfers between different DLT networks. • Facilitate interoperability between DLT ecosystems, unlocking liquidity and cross-chain use cases.	• Potential for smart contract vulnerabilities leading to loss of user funds. • Fraud risks in bridge operations. • Centralization risks if bridges become dominant intermediaries for interoperability. • Cross-chain consensus failures and scalability limitations (failed transaction, assets stuck in limbo, increased transaction fees).	• Security and audit requirements for cross-chain protocols. • Consumer recourse mechanisms in case of exploits. • Disclosure related to security, operations, governance, risks (transaction failures, security flaws, network issues). • Depending on circumstances, potential requirements related to prevention of illicit finance.
Lending Platforms	• Platforms allowing users to lend digital assets for interest or	• Counterparty risk if the platform collapses or mismanages funds. • Over-leverage risks leading to liquidations.	• Capital adequacy requirements for lending platforms.

Exhibit 2

Category	Description & Role	Consumer Protection & Market Considerations	Potential Regulatory Considerations
	rewards or borrow assts by providing collateral. • Provide liquidity and generate passive income for users while offering loans for borrowing purposes.	• Dominance by a few platforms may distort lending rates. • Potential for smart contract vulnerabilities leading to loss of user funds.	• Transparency of platform operations (collateralization ratios, loan terms, fees, interest rate algorithms) and risks (liquidation, over-leverage). • Fraud prevention, usury protection. • Security, data privacy protections.
Digital Assets Tokenization Platforms	• Platforms for converting real-world assets into DLT-based tokens. • Enable fractional ownership and liquidity for traditional assets.	• Legal enforceability of tokenized ownership, counterparty risk. • Centralization risks/lack of competition if one platform dominates tokenization. • Market liquidity and price volatility risks. • Fraud and manipulation, particularly by token issuer.	• Clarity on ownership rights for tokenized assets. • Disclosure requirements for certain tokenized assets (underlying asset information, verification, and custody). • Fraud and manipulation prevention.
Crowdfunding Platforms	• Platforms facilitating fundraising for digital assets projects through token sales, ICOs, or Initial DEX Offerings (IDOs). • Help digital assets projects raise capital by offering early access to tokens or digital assets in exchange for funding.	• Risk of fraud and information asymmetry (scams, rug pulls). • Price volatility. • Potential monopolization of the fundraising space by large platforms.	• Investor protection regulations for token sales (e.g., escrow requirements, disclosure standards). • Disclosure requirements for securities transactions that are tailored to the digital asset (as opposed to equity and debt). • Fraud and manipulation protection. • Licensing and reporting for platforms.