TESTIMONY OF

Carole House[1]

BEFORE THE

United States House Financial Services Committee

Hearing on American Innovation and the Future of Digital Assets: From Blueprint to a Functional Framework (Continuation)

June 6, 2025

Thank you Chairman Hill, Ranking Member Waters, and distinguished members of the Committee for holding this hearing continuation and the honor of the invitation to testify on the future of digital assets. I applaud your leadership in convening the Committee on this important issue and continuing the years-long efforts of this Committee across several Congresses to evaluate and build legislation around a clear, comprehensive, and competitive cryptocurrency regulatory framework. I hope my testimony will be helpful in considering some of the most important aspects of frameworks needed to drive innovation in a secure, competitive, safe, and sound digital finance ecosystem that reinforces national security interests, defends consumers, and preserves personal liberty.

I have spent my career working at the intersection of national, economic, and technological security. I have spent two tours at the National Security Council (NSC) leading cryptocurrency initiatives; led crypto and cybersecurity policy at the U.S. Financial Crimes Enforcement Network (FinCEN), the U.S. anti-money laundering and countering financing of terrorism (AML/CFT) regulator; and served on advisory boards for the U.S. Commodity Futures Trading Commission (CFTC), the Idaho Department of Finance, and the New York Department of Financial Services (NYDFS). Over recent years, I have observed massive growth, collapses[2], experimentation[3], exploitation[4], and innovation

---

[1] Nonresident Senior Fellow, Atlantic Council GeoEconomics Center. *Previous Advisory Roles:* Chair, Commodity Futures Trading Commission (CFTC) Technology Advisory Committee; Member of the Emerging Technology Advisory Committee (ETAC) to the Idaho Department of Finance (IDOF); Member of the Virtual Currency Advisory Board (VCAB) to the New York Department of Financial Services (NYDFS); Advisory Board Member, Third Way U.S.-China Digital World Order Initiative; Advisory Board Member, Digital Dollar Project. *Previous Government Roles:* Special Advisor for Cyber and Critical Infrastructure & Director of Cybersecurity and Secure Digital Innovation, White House National Security Council; Senior Strategic Policy Officer for Cyber and Emerging Technology, U.S. Financial Crimes Enforcement Network; Presidential Management Fellow (PMF) and Policy Advisor, White House Office of Management and Budget and U.S. Senate Homeland Security and Governmental Affairs Committee; Captain, U.S. Army. The views I express are my own and do not represent those of the Atlantic Council.

[22] *For example, see* Sallee Ann Harrison, AP News, "A Timeline of the Collapse at FTX," (May 8, 2024); Anton Badev and Cy Watsky, Federal Reserve, "Interconnected DeFi: Ripple Effects from the Terra Collapse," (May 9, 2023).

[3] *For example, see* SWIFT, "Swift Unlocks Potential Tokenization with Successful Blockchain Experiments", (August 31, 2023).

[4] *For example, see* FinCEN, Advisory FIN-2019-A003, "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 9, 2019); EUROPOL, "Cryptocurrencies: Tracing the Evolution of Criminal Finances," (2021); Olga Kharif, Bloomberg, "Wash Trading is Rampant on Decentralized Crypto Exchanges," (September 12, 2023).

across the digital asset market. Of course, innovation *and* exploitation in finance are not unique to digital assets, and the risks and benefits of one blockchain system are not equivalent across all assets --- they depend significantly on the design and features of specific systems. To make best use of the benefits and mitigate the critical risks, we need to ensure that technology, operations, and policy are aligned along critical safeguards and also with driving competitive and liquid U.S. markets.

That brings us to this critical juncture – the current alignment and implementation of protections in digital assets is not working. The status quo has not benefited consumers, markets, or national security. As just one example, *the largest heist in history just occurred in February of this year targeting this sector*, perpetrated by North Korean actors as part of their revenue generation to fund activities like their proliferation program.[5] This incident also was not in a vacuum but instead was yet another cyber theft as part of a years-long building trend in this industry exploiting both pervasive cybersecurity and AML/CFT vulnerabilities. This is just one example, which sits alongside highly volatile markets that have lost trillions and defrauded consumers, but also an environment that is reportedly set to drive the best developers abroad rather than inspiring them to stay here and build to agreed upon guardrails. Inaction by both government and industry will not achieve desired outcomes for protecting consumers or businesses.

I applaud Congress for continuing to elevate the issue of digital asset legislation to ensure appropriate regulation in the United States. Despite calls from some to avoid regulation of digital assets that may seemingly legitimize an immature sector, I maintain that regulation is critical to give a north star that *demands legitimate and responsible activity* within an industry with many actors who aim to bring positive evolutions in finance and cryptocurrency. Regulation also provides *legitimate authorities and levers* to supervisors and enforcement agencies to hold accountable illicit actors that seek to defraud consumers, launder criminal proceeds, and undermine the integrity of the U.S. financial system. As I have testified to previously, clear and comprehensive guardrails are necessary to protect consumers, national security, and U.S. competitiveness in financial innovation.[6] While timely progress is critical after several Congresses being unable to establish a comprehensive approach, these frameworks must also be deliberate, thoughtful, and comprehensive of the real and present risks, as well as opportunities, that we have observed in the digital asset ecosystem and broader financial system.

---

[5] *See* Federal Bureau of Investigation, Alert I-022625-PSA, "North Korea Responsible for $1.5 Billion Bybit Hack," (February 26, 2025).

[6] *See* Carole House, testimony before the House Financial Services Committee Subcommittee on Digital Assets, Financial Technology, and Inclusion, "Hearing on Crypto Crime in Context Part II: Examining Approaches to Combat Illicit Activity," (February 2024); *and* Carole House, testimony before the House Financial Services Committee, "Hearing on Navigating the Digital Payments Ecosystem: Examining a Framework for Payment Stablecoins and Consequences of a U.S. Central Bank Digital Currency," (March 11, 2025).

The stated goals of the Digital Asset Market CLARITY Act of 2025 (the "Clarity Act")[7] to help address regulatory gaps and to provide clarity for an industry seeking it are laudable. Unfortunately, the tenets of the proposed legislation as drafted appear to be overly complex, forging notable gaps for coverage under consumer and market protections rather than closing them; leave insufficiently or unaddressed key areas like meaningful implementation and enforcement measures, countering illicit finance, and cybersecurity; and depart from the long bipartisan-stated principles of technology-neutrality that would enable regulations to persist in the face of technological innovations.

In my testimony, I briefly offer opportunities for addressing those issues and preserving a framework built on the key pillars of sound market regulation and national security interests. I draw many of these recommendations from the groundbreaking work of the Commodity Futures Trading Commission (CFTC) Technology Advisory Committee (TAC), where I co-chaired a group of 19 incredible industry, government, and academic experts to produce a first-ever comprehensive review of risks and opportunities in decentralized finance (DeFi), with outlined steps for policymakers to take build the framework for DeFi.[8] I encourage legislators to consider these measures especially where existing digital asset market structures differ from traditional financial market structure, and urge you to be extremely deliberate when choosing to depart from long-tested principles needed to preserve integrity of markets, such as consumer protections, resilience against exploitation and shocks, and addressing separations of functions and conflict of interests.

Regulatory Gaps and Potential for Confusion

As I mentioned above, seeking to provide regulatory clarity, in both authority and application, are important at this critical juncture. It will establish clear rules of the road for responsible actors to engage and innovate in the space as well as ensure strong footing for regulators and enforcement agencies to oversee markets and investigate wrongdoing. A clear framework will also (finally) help level the playing field for U.S. firms that have long been more compliant than many foreign-operating cryptocurrency businesses that exploited their savings in non-compliance as a competitive advantage against more responsible U.S. companies.

The Clarity Act as currently written attempts to provide clarity through defining regulatory jurisdictional bounds between the Securities Exchange Commission (SEC) and CFTC as well as defining key terms of assets to establish scope of coverage as securities versus digital commodities. The bill also includes some important protection measures, specifically around areas like segregation of customer assets, limited disclosures such as around token structure and conflicts of interest, and registration requirements.

[7] *See* Bill H.R. , 119th Congress, "Digital Asset Market Clarity Act of 2025," (2025).
[8] *See* CFTC TAC, "DeFi Report," (January 2024).

However, the Clarity Act is still absent many important protections that we have observed to be critical to protect consumers and markets in the wake of a crisis. Within the 236 pages of the bill are confusing and ambiguous definitions and missing elements that pave the way for regulatory arbitrage and exploitation:

- *No Clear Non-Securities Spots Market Authority:* This bill does not appear to clearly outline authority over spots markets for assets that are not securities. The definition of "digital commodity" may be restrictive insofar as to only cover a limited set of tokens, which would leave potentially hundreds of tokens unregulated and/or without clear guidance on its applicability even if they function as financial assets.
- *Unclear Definitions and Impacts on Securities Laws:* There are various definitions in the bill whose challenges with clarity may subvert the drafters' intent to provide clarity and defend against regulatory arbitrage. Some definitions may be seen to be crafted to frame large exemptions from responsibility decentralized finance, such as in defining concepts like groups and common control in a a "decentralized governance system," which in the bill is a system where participation (not even active involvement, just the pretext of participation) is "not limited to or under the effective control of, any person or group of persons under common control." In another example, the bill treats assets called "investment contract assets" as digital commodities, though "investment contracts" have generally been a key element of securities laws.
- *Conflating Decentralization and Maturity:* The test for decentralization in the bill is described as a test of blockchain maturity. In a sector where projects that are (or at least claim to be) decentralized are being targeted and exploited for weaknesses in their code, cybersecurity, and irrevocability of mistakes or illicitly acquired assets, it is confusing on why a greater extent of decentralization --- a concept that is also vague in the bill --- inherently means maturity rather than other markers of good governance and operations. The decentralization test also introduces some confusion that may challenge real-world implementation, and is unclear on how such a feature impacts an asset functioning like a commodity versus a security. Current and former regulatory leadership has warned against arbitrary carve-outs of protections like under securities laws simply based on complex issues like decentralization that so far have largely been met with convoluted definitions that risk exemption significant amounts of high-risk investment-related activity.[9]
- *Departing from Technology Neutrality:* The approach in the Clarity Act departs from an economic function-centric approach to create a technology-bespoke framework, which unfortunately lends toward attempts to draft overly complex definitions and frameworks for coverage that change the nature of market protections simply due to the type of technology used to implement the system.

[9] *See* Timothy Massad, Testimony before House Financial Services Committee, "American Innovation and the Future of Digital Assets," (June 4, 2025) ;" Hester Peirce, SEC Statement, "New Paradigm: Remarks at SEC Speaks," (May 19, 2025).

This also threatens potentially creating the opposite of a future-proofed regulatory approach that cannot keep up with future technological innovation.

National Security and the Critical Role of Enforcement

In the wake of serious national security threats like billion+ dollar hacks by rogue nations[10], growing integration of cryptocurrency as a tool for transnational organized crime[11], market manipulation and fraud that can threaten system integrity and stability, as well as pressure from adversarial nations seeking to develop and leverage alternative financial systems to weaken and circumvent the dollar[12], it is clear that strong safeguards, including for U.S. competitiveness, are needed. This framework also demands we ensure policy and enforcement approaches both domestically and internationally create a level playing field for U.S. firms – often the most compliant firms in the world – to be able to compete fairly. Otherwise, the foundation we build these systems on risk faltering, with the potential to not only reap significant harms but also prevent us from harnessing the greatest positive potential that is possible from a secure and innovative digital finance ecosystem.

There is limited discussion of either illicit finance or cybersecurity in the Clarity Act --- many more pages are honed on establishing large regulatory carve-outs than on establishing expectations, driving needed industry standards or sponsoring research and development, or appropriating necessary resources to ensure appropriately scaled and timely enforcement of these critical requirements. Also important to note, especially in light of recent changes in enforcement posture – beyond just creating the policy framework, the government and industry must work to apply and *enforce* the framework. A policy that isn't enforced or implemented does nothing to benefit consumers nor U.S. firms with stronger compliance programs that have been operating at higher costs and less competitive advantages than many foreign-operating firms.

I have testified previously[13] to the critical needs for strengthening AML/CFT and sanctions authorities in the cryptocurrency space, which generally have been suggested to be saved for "comprehensive market legislation." Such enhanced protections like appropriations for skilled enforcement and investigative personnel, sharpening tools like 9714/311 designation authorities, ensuring extraterritorial application of regulations

[10] *See* Federal Bureau of Investigation (FBI), Public Service Announcement, I-022625-PSA, "North Korea Responsible for $1.5 Billion Bybit Hack," (February 26, 2025).
[11] *See* TRM Labs, "Understanding the Use of Cryptocurrencies by Cartels," (January 22, 2025); *and* Douglas Farah and Marianne Richardson, Georgetown University Journal of International Affairs, "The Growing Use of Cryptocurrency by Transnational Organized Crime Groups in Latin America," (March 20, 2023).
[12] *See* Hippolyte Fofack, Atlantic Council, "Piece by Piece, the BRICS Really Are Building a Multipolar World," (August 23, 2023).
[13] *See* Carole House, testimony before the House Financial Services Committee Subcommittee on Digital Assets, Financial Technology, and Inclusion, "Hearing on Crypto Crime in Context Part II: Examining Approaches to Combat Illicit Activity," (February 2024).

and/or through designations of entities of high national security risk, creation of an enforcement strategy to scale timely enforcement against the most egregious violators, or resourcing public-private partnerships like the Illicit Virtual Asset Notification (IVAN) program are missing from the legislation but could be easily added in to help strengthen the holistic cryptocurrency framework. In the face of disbanding of the Department of Justice (DOJ) National Cryptocurrency Enforcement Team (NCET)[14] and significant downsizing and weakening of enforcement offices and personnel across the U.S. Government, the legislation could help ensure that tools are being honed to better address the worst actors in the space. Only with meaningful enforcement can policy be truly impactful and can we reward the best actors in the space, which are typically American companies.

An Alternative Approach for Consideration – Joint, Targeted, Adaptable, and Balanced

I support calls for a legislative solution that enables nuance and distinct treatment across various assets based on their economic *function* and which will ensure persistent clarity and flexibility for regulators to address significant risks of fraud, manipulation, and investor exploitation that we have seen in the space. The legislation should also guide regulators with key principles, many of which are similar to those outlined in the Clarity Act, and should be done in full view of the benefits that some aspects of digital assets uniquely provide, such as an unprecedented level of market transparency for on-chain financial activity to enable greater market surveillance and oversight.

An alternative approach may help meet the intent of the drafters while giving time for greater exploration and experimentation while meeting near-term calls for the most beneficial transparency needs of the market, which I have observed to most consistently be calls for a clear pathway to registration. I encourage policymakers to consider a much more streamlined approach if a more complex bill proves too difficult to reconcile:

- *Dual Rulemaking:* Similar to efforts undertaken in the wake of the 2008 Financial Crisis and pursuant to the joint rulemaking efforts directed in Title VII of Dodd Frank, Congress could again direct the SEC and CFTC to jointly develop a framework and rulemakings to give greater specificity and adaptability to approaches to ensure appropriate coverage but at least one of the markets regulators.
- *Mandate for Sandboxes and Clear Registration Pathways:* In the interim while the SEC and CFTC craft their approach, Congress could direct a near-term establishment via sandboxes, provisional registrations, and other requirements with clear guardrails to help ensure clear near-term coverage while giving the time needed to thoughtfully evaluate the more complex issues like dual-registered

[14] *See* Department of Justice, Memorandum, "Ending Regulation by Prosecution," (April 7, 2025).

entities, defining tokens, defining the jurisdictional hand-off, and how to address DeFi. Policymakers should consider looking to the United Kingdom's current joint efforts between the Bank of England and the FCA under the Digital Securities Sandbox[15] for inspiration.

- *Clarify Commodity Spots Market Authorities:* The legislation should specify clearly authority to the CFTC over commodity spots markets, or at a minimum digital commodity spots markets.
- *Clear Principles for the Framework:* To ensure the regulators meet the intent of Congress, legislators should outline for regulators clear principles to be followed. These will draw significantly from existing markets regulation and the principles in the Clarity Act, and must especially include market and investor protection measures like against conflicts of interest, market transparency, capital requirements, and risk management like for AML/CFT and cybersecurity.
- *Explicit Appropriations and Mandate for Additional AML/CFT and Cybersecurity Initiatives:* The legislation would also optimally integrate near-term resourcing, not just authorizations, to ensure the ability to effectively police bad actors in the system, which should include the earlier-referenced initiatives like expanded targeting authorities, appropriations, public-private partnerships, and cybersecurity and information sharing standards.
- Undertake Steps to Address the Regulatory Perimeter and Controls with DeFi: Finally, legislators should direct the SEC and CFTC to jointly undertake the steps recommended by the CFTC TAC in evaluating how to evolve market structure in addressing issues like the unique constructs in DeFi. These steps include mapping ecosystem players, processes, and data; assessing compliance and requirements gaps; identifying risks; evaluating options, benefits, and costs of changes to the regulatory perimeter, and surging research and development and standards partnerships.[16]

With guardrails established and more consistent oversight by Congress, this approach, implemented through administrative procedure and thoughtful regulation with public engagement, I think is likely the best way to achieve a comprehensive and enduring framework.

In closing, I'd like to again underscore my gratitude for the honor of the opportunity to speak with you all today. It is critical that the United States make timely progress on establishing and implementing cryptocurrency regulatory frameworks, which should leverage years of effort on defining critical holistic protections that also reinforce the central role in the financial system and as a leader in technological innovation.

Thank you.

[15] *See* Bank of England, "Digital Securities Sandbox."
[16] *See* CFTC TAC, "DeFi Report," (January 2024).