



**STATE OF NEW YORK
OFFICE OF THE ATTORNEY GENERAL**

**LETITIA JAMES
ATTORNEY GENERAL**

Statement for the Record of the New York State Office of the Attorney General

**Before the
United States House Financial Services Committee
Public Hearing - American Innovation and the Future of Digital Assets: From Blueprint to
a Functional Framework**

June 6, 2025

Thank you for the opportunity to present this statement for the record to the United States House Financial Services Committee on behalf of the People of the State of New York regarding the Digital Asset Market Clarity Act ("CLARITY"). We would like to thank the Chair, the Honorable French Hill, for convening this hearing, the Ranking Member, the Honorable Maxine Waters, for inviting our office to make this submission, and all the members of the committee for holding this very important hearing.

The Office of the Attorney General is the statutory regulator for both securities and commodities in the State of New York. Among other things, it is my Office's job to protect nearly 20 million people from all manner of investment fraud. While my Office remains agnostic in the debate regarding the uses and benefits of digital assets, the last decade has made clear that this asset class subjects the public to a number of serious risks. If digital assets are to flourish and reach their potential, it is critical that they be safe and trustworthy.

All who care about this industry, including the many good actors in the industry, should share in my office's desire to protect the public and thwart bad actors. In April of this year, my Office [wrote to Congress](#) identifying certain risks to America's national interests posed by digital assets and suggested tenets of responsible regulation to guard against them.¹ We now make this submission to raise concerns that CLARITY, as currently drafted, does not do enough to protect America's interests, investors, and national security.

¹ Letitia James, *Letter to Congress on Digital Asset Regulation*, Att'y Gen. N.Y., [letter-to-congress-on-digital-asset-regulation-letter-2025.pdf](#).

A. CLARITY Does Not Contain the Regulatory Guardrails Necessary to Protect America's Investors from Bad Actors Seeking to Exploit and Defraud Them

The public is best served when Congress takes a technology-neutral approach — as my office has — and requires similar investment products which carry similar risks to follow the same laws. When an entrepreneur seeks to raise capital from the public, they are subject to the securities laws. To the extent that same entrepreneur chooses to issue cryptocurrency as a mechanism to fund their innovation, that is their choice, but that choice should be accompanied by regulations that ensure investors understand the unique risks and are protected from fraud and manipulation,² as would be the case in the traditional securities markets.

Rather than taking a technology-neutral approach, the proposed legislation creates a technology-specific loophole that upends almost one hundred years of securities laws meant to protect America and its investors. We are concerned that under the proposed law, promoters could raise money from mom-and-pop investors, senior citizens, and inexperienced investors without transparency, disclosure, or protection simply by shrouding their call for public funding in a digital asset. By contrast, our current securities laws provide numerous protections for investors in connection with capital being raised by known companies backed by major banks and other financial institutions. Such protections are all the more necessary in the digital assets space, where many of the players are anonymous, unregistered, and located overseas.

In today's environment, cryptocurrency has become the primary tool used by scammers to defraud their victims. In some cases, such as those involving scam tokens that have no value, for example, the digital asset itself is the crux of the fraud. Other crypto frauds can involve billion-dollar pyramid schemes. And in some cases, criminals use digital assets to anonymously launder the proceeds of their schemes and hide them in locations that are outside any American law enforcement jurisdiction.² Any legislation addressing digital assets must include regulations to protect against crypto's inherent features (such as their anonymity and purported decentralization) from being exploited by fraudsters, organized crime, and terrorists.

B. CLARITY Allows Bad Actors to Hide Behind the Façade of Decentralization

Under the proposed legislation, the distinguishing line between a commodity and a security is determined by the “maturity” or “decentralization” of a digital network. The concept of decentralization is rooted in the crypto industry's claim that no one controls these complex financial products worth billions. And, therefore, no one can be called to account in the event of fraud, manipulation, bribery, and outright theft.

² Tonantzin Carmona, the Brookings Institute, *Protecting the American Public from Crypto Risks and Harms*, (June 2, 2025)

<https://www.brookings.edu/articles/protecting-the-american-public-from-crypto-risks-and-harms/#:~:text=Principle%20%232%3A%20Protect%20retail%20investors%20from%20market%20manipulation%2C%20fraud%2C%20and%20scams%2%A0>

The concept of decentralization, however, is simply another way for bad actors to avoid accountability. The proposed law would subject American investors to more risky and complex products with little or no recourse in the event of a bug, theft, fraud, hack, or other attack. Promoters would be permitted to — and in fact encouraged — to disavow all responsibility for products and platforms that hold billions of dollars of investor funds. Should there be a malfunction in the code or a hack by criminals, implementing a fix would effectively require control over the code, which would be an admission that the digital network is not “decentralized.”³ Criminals already take advantage of decentralization because they know that stolen funds can almost never be clawed back and returned.⁴ Decentralization must not become a loophole that can be used to foster fraud.⁵

At the same time, many in the industry hold themselves out as being decentralized when in reality they are engaged in mere decentralization theater. While some may claim their applications are decentralized because they do not take custody of investor funds, these applications necessarily take control of customer funds to execute transactions. Creators of these products and platforms include a way to profit from them, which inherently signals a level of control. Nonetheless, the proposed bill carves out these applications from regulation, creating enormous risks for investors and our markets.

C. Digital Identity Must be Required to Ensure America’s National Security

Any legislation that is serious about the enforcement of our anti-money laundering laws and the Bank Secrecy Act must include a mandate for digital identity and a framework for associating real-world identities with online anonymous transactions. In today’s world, the anonymity provided by cryptocurrency has made it the medium of choice for illicit finance, bribery, sanctions evasion, and terrorism funding. North Korea has stolen more than \$6 billion in cryptocurrency to fund its

³ *When Smart Contracts are Outsmarted: The Parity Wallet “Freeze” and Software Liability in the Internet of Value*, Proskauer (December 22, 2017) [https://corpgov.law.harvard.edu/2023/05/22/anatomy-of-a-run-the-terra-luna-crash/#:~:text=The%20collapse%20of%20Terra%20in,DeFi%29%20architecture](https://www.proskauer.com/blog/when-smart-contracts-are-outsmarted-the-parity-wallet-freeze-and-software-liability-in-the-internet-of-value#:~:text=On%20November%208%2C%20Parity%20Technologies%C2%A0announced%C2%A0that,over%20%2430%20million%20in%20Ether; Jiageng Liu et al., Anatomy of a Run: The Terra Luna Crash, H.L.S. F. on Corp. Governance (May 22, 2023), <a href=).

⁴ “Victims of investment fraud, specifically those involving cryptocurrency, reported the most losses—totaling over \$6.5 billion.” *FBI Releases Annual Internet Crime Report*, <https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report>; See also *Federal Bureau of Investigation Internet Crime Report 2024* https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf at 35.

⁵ Bruno Mazorra et al., *Do not rug on me: Zero-dimensional Scam Detection* (2022); Jennifer Sor, *Decentralized cryptocurrency exchanges are awash in fake trades, research report says*, Bus. Insider (Sep. 12, 2023 at 12:10 ET), <https://markets.businessinsider.com/news/currencies/defi-crypto-exchange-token-wash-trading-fraud-price-manipulation-2023-9>.

nuclear program,⁶ making it the third largest holder of Bitcoin.⁷ Russia is using cryptocurrency in its oil trade with China and India to evade sanctions, following Venezuela's move to do the same in 2024.⁸ Our laws must ensure that when an investor buys Bitcoin on a platform in New York they are not unwittingly funding a terrorist organization or an enemy state's nuclear program. Indeed, enemy state actors, terrorists, and organized crime organizations use cryptocurrency to move at least \$50 billion annually in illicit money and to avoid sanctions imposed by our government.⁹

Digital identity is an exciting area of innovation that is compatible with blockchain and smart contracts and enables cost-effective compliance to meet our national security needs while preserving privacy and civil liberties. With breakthroughs in a technology called zero-knowledge proofs, it is now possible to verify key identity and transaction attributes without the need to share or expose underlying personal identifying information. The industry has been developing interoperable standards for digital identity credentials, which can be associated or attached to digital wallets. However, there is currently no impetus to adopt this technology at scale unless crypto companies and projects are required to do so. Legal requirements should also ensure a fair playing field for all actors in the U.S. to prevent compliant actors from losing market share.

Importantly, identifying information would be kept private from the general public, *e.g.*, hidden from block explorers, and revealed only to the appropriate parties under the law. Privacy is maintained by allowing verifiers to receive only the information they need without unnecessary exposure to sensitive or personally identifiable information. In most instances, verifiers only need to know that certain attributes are met *i.e.*, that a person is a U.S. person, at least 18 years old, and has a valid government-issued identification and a recent address.¹⁰

D. Market Structure Legislation Should Mandate a Closed Loop of Know-Your-Customer Rules and Price Transparency to Protect American Investors

Comprehensive regulation of the digital assets industry requires a closed loop of traceable transactions and identifiable market participants, which is the critical missing piece to crypto

⁶ Patricia Kowsmann & Timothy W. Martin, *How North Korea Cheated Its Way to Crypto Billions*, WALL STREET J. (Apr. 3, 2025), https://www.wsj.com/world/asia/north-korea-cryptocurrency-580d7d3f?mod=saved_content.

⁷ Yoon Min-Sik, *North Korea's Bitcoin Reserve Thought to be 3rd Largest in World: Report*, THE KOREA HERALD (Mar. 18, 2025), <https://www.koreaherald.com/article/10443993>.

⁸ Anna Hirtenstein & Chen Aizhu, *Russia leans on Cryptocurrencies for Oil Trade, Sources Say*, REUTERS (Mar. 14, 2025), <https://www.reuters.com/business/energy/russia-leans-cryptocurrencies-oil-trade-sources-say-2025-03-14/>.

⁹ *Id.*

¹⁰ Personal identifying data could be stored in a decentralized manner or locally with the stablecoin holder to minimize security risks and require the use of cryptographic key-pairs for access (similar to how transactions are signed on the blockchain).

market infrastructure. In the U.S. national market system, fraud and money laundering are detectable because participating institutions must collect know-your-customer (“KYC”) information. Exchanges and dark pools are required to know the identities of their member broker-dealers and subscribers. Broker-dealers are, in turn, required to know their customers. These rules create a closed loop of regulated institutions over which regulators have investigative authority, allowing them to identify patterns of anomalous behavior and ultimately find those who engage in fraud, manipulation, and illegality. Sound cryptocurrency regulations must leverage and enforce existing anti-terrorism and money laundering laws to create a closed loop of compliance and disrupt illicit uses of cryptocurrency.

Requiring a closed loop will also allow for actual price discovery. Anonymous trading, manipulative trading, and speculation, especially by those overseas, have resulted in market manipulation to the benefit of crooks and our enemies.¹¹ Such trading has dominated as much as 60% of Bitcoin price discovery, or lack thereof.¹² In the securities markets, the national market system enforces price integrity across institutions by requiring that trades occur at or better than the national best bid and offer (“NBBO”). Most cryptocurrency platforms do not abide by rules governing the prices they quote.¹³ Further, because of the global nature of cryptocurrency, prices on certain centralized platforms where KYC information is collected are influenced by prices on anonymous decentralized and centralized platforms without adequate KYC. Without KYC information, these platforms do not know who is submitting orders and the extent to which prices are the product of wash trading¹⁴ and other manipulation. Accordingly, effective cryptocurrency legislation should include requirements that orders be filled at or better than an NBBO price that is the product of reliable order information provided by firms that know who placed those orders.

We also cannot ignore the fact that crypto prices are not based on underlying economic activity. In traditional capital markets, capital is allocated to productive activity and asset prices are ultimately rooted in fundamentals. For example, stock prices are based on factors like a company’s projected earnings and bond prices are based on assessments of risks. In contrast, the price of Bitcoin fluctuates based on speculation and supply and demand, which could be artificial or

¹¹ “Frequently the prices of securities on such exchanges and markets are susceptible to manipulation and control, and the dissemination of such prices gives rise to excessive speculation, resulting in sudden and unreasonable fluctuations in the prices of securities which (a) cause alternately unreasonable expansion and unreasonable contraction of the volume of credit available for trade, transportation, and industry in interstate commerce, (b) hinder the proper appraisal of the value of securities and thus prevent a fair calculation of taxes owing to the United States and to the several States by owners, buyers, and sellers of securities, and (c) prevent the fair valuation of collateral for bank loans and/or obstruct the effective operation of the national banking system and Federal Reserve System.” *The Securities Exchange Act of 1934, Necessity for Regulation* (15 USCS § 78b(3)).

¹² Carol Alexander & Daniel Heck, *Price Discovery in Bitcoin: The Impact of Unregulated Markets*, 50 J. OF FIN. STABILITY 2 (Oct. 2020), <https://www.sciencedirect.com/science/article/abs/pii/S1572308920300759>.

¹³ *Statement on Potentially Unlawful Online Platforms for Trading Digital Assets*, U.S. SEC. & EXCH. COMM’N (Mar. 7, 2018), <https://www.sec.gov/newsroom/speeches-statements/enforcement-tm-statement-potentially-unlawful-online-platforms-trading-digital-assets>.

¹⁴ Lin William Cong, Xi Li, Ke Tang & Yang Yang, *Crypto Wash Trading*, (Nat’l Bureau of Econ. Rsch., Working Paper No. 30783, 2022), https://www.nber.org/system/files/working_papers/w30783/w30783.pdf.

manipulated. No economic activity explains why the price of Bitcoin can drop by 30% one day and increase by 30% the next.¹⁵

For the crypto industry to mature in a way that benefits America and its investors, crypto platforms need to rise to the same standard as regulated national exchanges to ensure free and fair markets where wrongdoers may be held accountable, features that make our current securities markets the envy of the world. Failure to do so will mean that American investors will not be able to tell whether the prices they see are the product of true supply and demand or the product of market manipulation.¹⁶ Rigged markets are not free markets.

E. Congress Must Not Interfere with States' Investor Protection Laws.

Congress must ensure that this legislation does not reduce the number of cops on the beat. State anti-fraud and registration laws are intended to prevent and remedy fraud and must be preserved. In order to prevent and effectively prosecute fraud, states must retain their ability to enforce state laws and registration provisions as recognized under federal securities and commodities laws today.

We call upon Congress to protect Americans and American institutions that have made this country great. While digital assets are certainly exciting, our country's markets have fostered many innovations over the last century - but have done so within the framework of our securities and banking regulations in order to protect America's investors, the economy, and national security. Failures to regulate new financial products adequately have repeatedly resulted in financial crises that required the U.S. government to spend tens, and even hundreds, of billions of dollars on bailouts, most recently in 2008 (due to subprime loans and mortgage-backed securities) and in 2023 (resulting from overexposure to digital assets). We urge Congress to ensure that market structure legislation includes appropriate guardrails to safeguard America's investors, economy, and national security. Indeed, it is such guardrails that will protect our financial system from a future crash.

¹⁵ See <https://www.google.com/finance/quote/BTC-USD?window=YTD>.

¹⁶ *Market Manipulation: Suspected Wash Trading on Select Blockchains May Account for Up To \$2.57 Billion in Trading Volume*, CHAINALYSIS (Jan. 29, 2025), <https://www.chainalysis.com/blog/crypto-market-manipulation-wash-trading-pump-and-dump-2025/>.