Written Testimony of Jonathan Levin
Chief Executive Officer
Chainalysis Inc.

Before the:
United States Senate Committee on Banking, Housing, and Urban Affairs
"From Wall Street to Web3: Building Tomorrow's Digital Asset Markets"
July 9, 2025

Chairman Scott, Ranking Member Warren, and distinguished members of the Committee. Thank you for inviting me to testify before you today on the regulation of digital asset market structure. We are in the early stages of a generational shift toward a new form of financial market infrastructure. The potential of public blockchains and other distributed ledgers lies not only in more inclusive and efficient financial services but also in fundamentally new approaches to compliance, regulation, and enforcement, enabled by the transparent nature of these systems.

The United States has an opportunity to ensure that this generational shift is guided by rigorous standards and strong supervision that protects consumers and enhances the health and integrity of the entire financial system. I support continued bipartisan efforts on this matter and commend the efforts underway across both chambers. This Committee's Crypto Market Structure Principles, the Senate's Responsible Financial Innovation Act (RFIA), and the House's Digital Asset Market Clarity Act (CLARITY) are all welcome developments that represent serious engagement with an issue that has long been left unaddressed.

My name is Jonathan Levin, co-founder and CEO of Chainalysis, the blockchain data platform that helps make blockchains safer and more secure, enabling banks, businesses, and governments to have the confidence and knowledge they need to support the growth of the digital asset economy. Leveraging the inherent transparency of blockchain, our tools and the data they are built upon are used daily to identify and understand digital asset activity. We provide this data and these tools to customers in both the private and public sectors, including the federal government.

In my testimony, I provide an assessment of the extent of illicit activity in the sector, the importance of establishing market structure rules, and how the use of blockchain analytics data and tools can reshape and enhance both compliance and regulation.

Key Takeaways

- **The urgency of a market structure framework is now:** The U.S. is the largest digital asset market, and leadership on regulation is necessary to drive secure growth.

- **Chanalysis supports the principles outlined by the Senate Banking Committee**: These are a sensible foundation to build on, including specifically the proposal to target illicit activity and extend anti-financial crime obligations to market intermediaries.
- **Digital assets can be abused for illicit purposes, but public blockchains provide us with the tools to combat this illicit activity:** Using specialist blockchain analytics, public sector agencies and private sector enterprises have a superior capability to prevent, detect, disrupt, and ultimately deter illicit activity in digital asset markets.
- **Regulation should lean into these new features of blockchain, rather than simply transposing existing obligations:** Data-first market regulation, characterized by proactive monitoring by government agencies and real-time compliance from businesses, is now a reality that a framework should acknowledge and embrace.

The urgency of a comprehensive framework for the United States

The United States is the world's largest digital asset market. Between July 2023 and June 2024, it accounted for nearly 20% of all on-chain value transferred, over three times that of the next largest market (Figure 1).

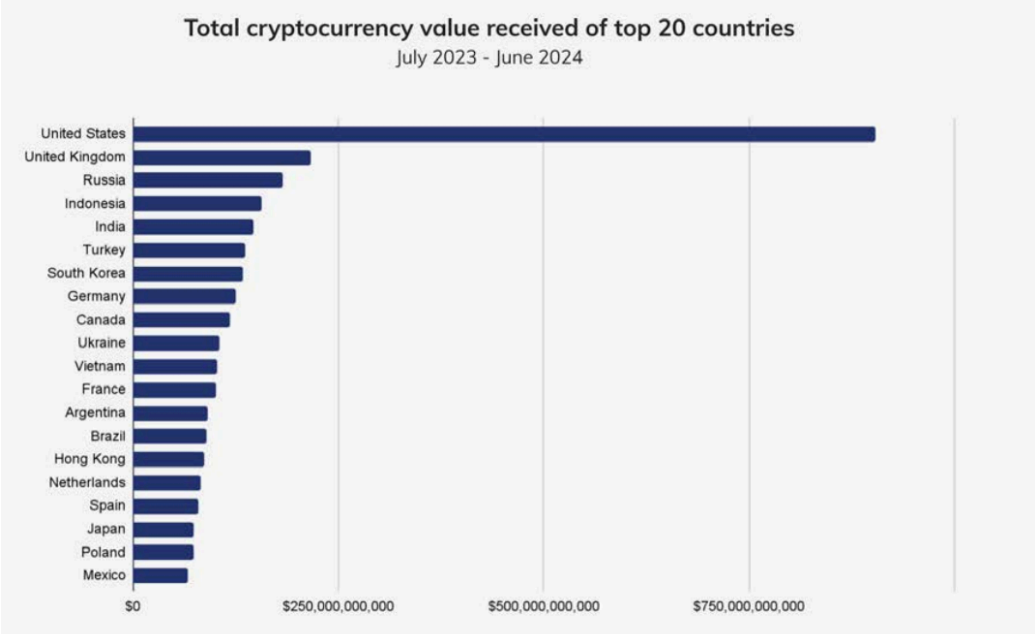

Figure 1

Institutional engagement is forming an increasing share of that market (Figure 2), likely due to the U.S.'s position as a global financial center.

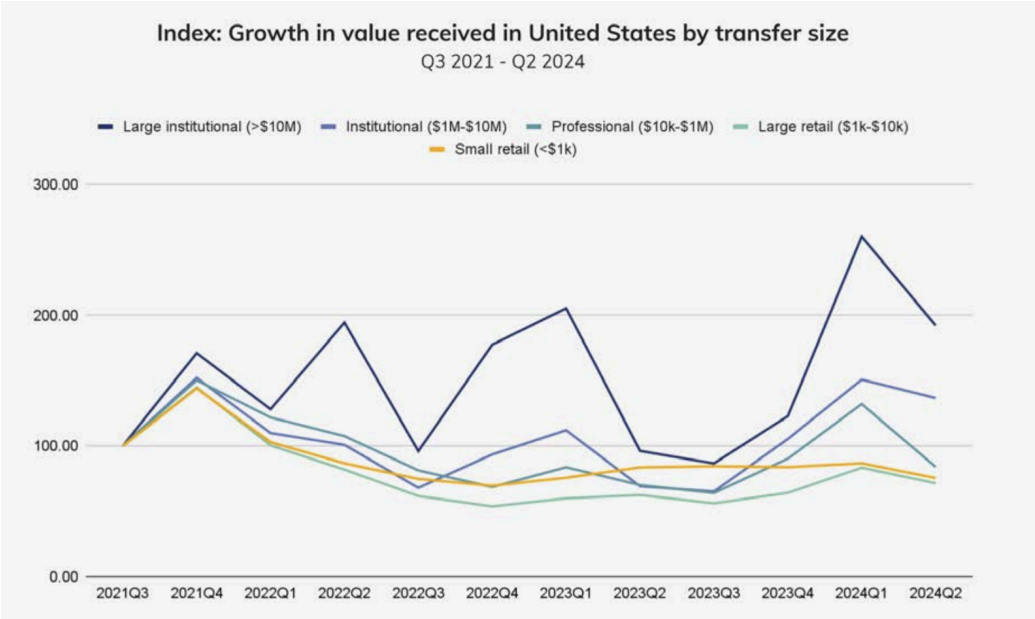

Figure 2

Against the backdrop of growing retail participation and institutional engagement, the absence of a federal regulatory framework for digital asset market structure creates risks for Americans and uncertainty for investors.

Other major financial centers are moving decisively to build a competitive edge. The European Union has enacted the Markets in Crypto-Assets Regulation to create a harmonized regime across 27 jurisdictions. The United Arab Emirates is capitalizing on digital assets as an engine of economic growth through a strategy of practical regulation and industry engagement. Singapore and Japan are iterating on pioneering frameworks that drew early lines in the sand on consumer protection and financial crime prevention.

It is not only friendly jurisdictions that have an agenda in mastering this space. Russia has openly sought to leverage digital assets to resist U.S. sanctions and preserve international financial connectivity. Iran's digital asset sector has been linked to the financing of state-sponsored terrorism. China appears to be, at the very least, tacitly supporting Hong Kong's ambitions as a hub for Web 3 and digital assets. And DPRK has successfully exploited digital asset businesses, stealing billions on behalf of the regime.

In summary, what is at stake is not simply a $3 trillion market, but the new global financial infrastructure. If we in the United States fail to provide legal clarity and strong enforcement, we risk ceding control over critical financial infrastructure to other jurisdictions.

Categories of illicit activity in digital assets

Like any form of value transfer, digital assets can be abused for illicit purposes. As digital asset markets scale, the scope for misuse grows in tandem. Indeed, digital assets can be observed in a broad range of illicit activity, from the manufacturing of fentanyl precursors supplied to Mexican drug cartels to the financing of entities affiliated with designated terrorist organizations, including proxies of Iran's Islamic Revolutionary Guard Corps (IRGC).

However, the public ledgers underpinning most digital asset activity also provide unprecedented levels of visibility into the sources and destinations of illicit finance, as well as the layering mechanisms in between.

Chainalysis research indicates that digital asset flows into known illicit addresses remain relatively small today, accounting for 0.14% of total on-chain value transferred in 2024 (Figure 3). This is a lower-bound estimate that does not comprehensively capture criminal activity that may have occurred off the blockchain, where fiat proceeds are converted into digital assets solely for laundering and are virtually indistinguishable from licit transactions.

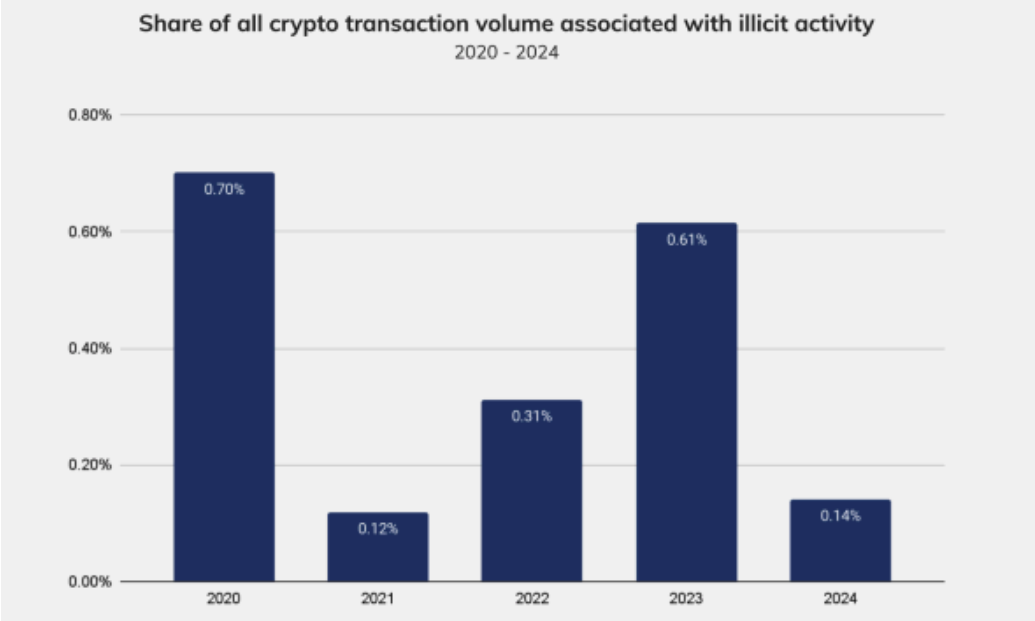

Figure 3

By the time we compile our next report, we expect the total value of digital assets received by illicit actors in 2024 to have risen to over $51 billion, as we identify more illicit addresses

and incorporate their historical activity into our estimates (Figure 4). Our current data reflects over $40 billion received by illicit actors, which, based on historical trends, will invariably increase as we identify more illicit transactions associated with activity in 2024.

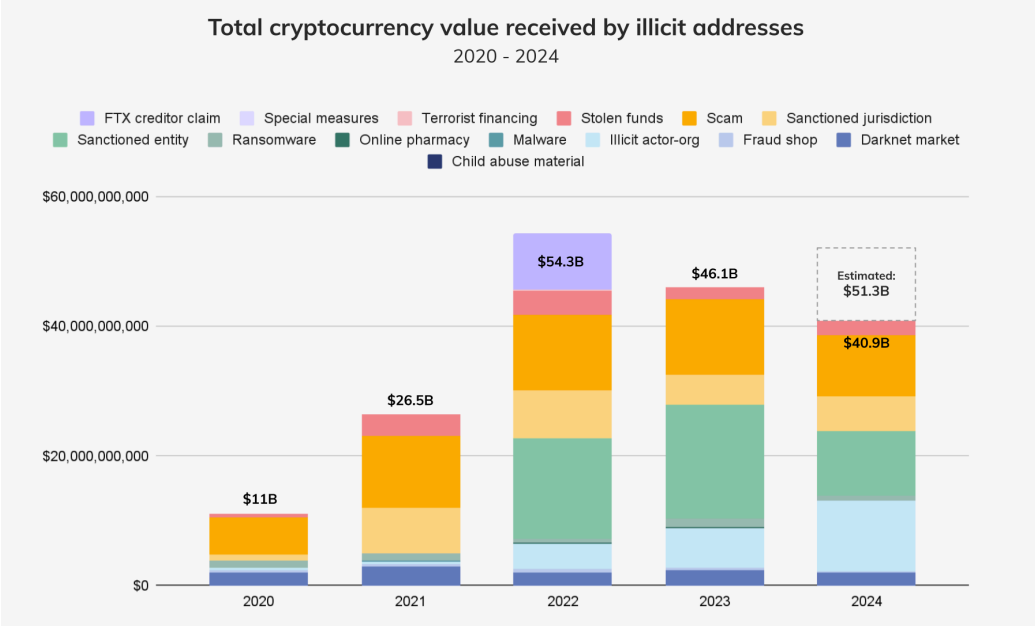

Figure 4

While the share of total digital asset flows that are illicit remains a small fraction—well under 1%—of all transaction activity on blockchain networks, we expect that as this market becomes more liquid and accessible, the appeal to threat actors will grow in tandem.

This is particularly concerning in a few key areas of national concern for the United States. Here, our data and tools are crucial in ensuring not only that there is effective insight into these threats but also that we are actively and robustly combating the activities of drug cartels, terrorists, cybercriminals, and others who leverage digital assets for illicit purposes.

1. **Narcotics trafficking**

Chainalysis research shows that between 2015 and 2023, over $250 million in digital assets were received by wallets affiliated with Chinese fentanyl precursor manufacturers, likely representing purchases of pharmaceutical chemicals, including fentanyl and MDMA precursors. For example, a recent civil forfeiture case in the Eastern District of Wisconsin highlighted the growing role of digital assets in the financial ties between Mexican cartels and Chinese chemical suppliers. The case resulted in the seizure of over $5.5 million in digital assets, illustrating how Chainalysis can help uncover hidden financial flows within organized crime. While the cartel may have benefited from speed, low transaction fees, and cross-border efficiency, its reliance on the blockchain allowed investigators to trace these

transactions more easily than would have been possible with traditional cash-based money laundering. Furthermore, it allows even greater disruptive potential because issuers and centralized services can typically freeze digital assets when necessary.

Further analysis identified that digital asset transaction volumes to Chinese chemical shops correlated with fentanyl seizures at the U.S.-Mexico border the following month. This reflects how blockchain analytics data, when used appropriately, can serve as a predictive indicator for law enforcement agencies to identify trafficking patterns and timings, as well as to build comprehensive networks of addresses associated with narcotics through behavioral analysis.

With the proper training and tools, agencies can effectively monitor sales on the darknet markets where criminals operate, identify individuals, and reduce trafficking into the U.S.

2. **Child Sexual Abuse Material (CSAM)**

While not all CSAM activities involve digital assets, and in many cases, users simply trade CSAM amongst themselves, there are well-publicized instances of law enforcement using Chainalysis data and tools as part of shutting down CSAM marketplaces, such as Welcome to Video (WTV), which almost exclusively accepted digital assets as payment. Using our tools, law enforcement was able to not only trace funds to the site's administrator but also site users and contributors, as they had personal Bitcoin addresses associated with WTV.

Collaboration amongst our investigators, partner agencies, non-profits, and our customers has enabled us to build a map of the CSAM ecosystem, identifying both vendors and buyers. According to our analysis, in 2023, over 10,000 digital asset wallets sent funds to CSAM vendor wallets. One trend that our research identifies is the increasing lengths to which CSAM actors go to hide their activity, increasing the difficulty of identifying CSAM-related activity with certainty. We believe these actors are increasingly using privacy coins, which deploy privacy-enhancing features, instant exchangers that facilitate crypto-crypto exchange directly between wallets, and platforms that don't require KYC. However, when equipped with sophisticated blockchain analytics tools and data capabilities and strong industry collaboration, agencies can remain effective in combating this abhorrent activity.

3. **Mixers**

One category of service that plays a key part in the privacy-enhancing technology infrastructure is mixers. Chainalysis data finds that, while there are legitimate use cases for these services, mixers are often associated with increased levels of illicit activity, receiving a significantly larger share of funds from wallets associated with illicit activity than other

categories tracked by Chainalysis. While these services have experienced significant disruption over recent years, with sanctions against Blender and Sinbad, as well as law enforcement takedowns of others, such as Chipmixer, illicit actors continue to utilize these types of services. Typically, a mixer will take a number of transactions, pool them together, "mix" them, and then redistribute the funds, complicating the process of identifying and following funds for investigators. Advances in blockchain analytics mean that transparency is achievable even where infrastructure and services are deployed to obfuscate activity.

4. Sanctions evasion

Sanctioned jurisdictions and entities received $15.8 billion in digital assets in 2024, accounting for approximately 39% of the total digital asset flows into illicit addresses.

i. Russia

The exploitation of digital assets to circumvent international financial sanctions is now official state policy in Russia. There is evidence that Russians are using digital assets to evade sanctions in an attempt to restore financial connectivity. From large exchanges within Russia processing billions of dollars in transactions, even post sanctions designation, to smaller Russian-language instant exchanges services that don't require KYC, offer on- and off-ramping on behalf of sanctioned Russian banks, and even facilitate commodities and weapons trade with IRGC proxies, Russia has sought unique mechanisms to evade sanctions. While sanctions, seizures, and takedowns have impacted the illicit Russian digital asset economy, rebrands and even the creation of alternative assets, such as a Russian ruble-backed stablecoin, continue to take form in the face of international sanctions.

ii. Iran

Digital assets have served as safe havens for ordinary citizens in countries like Iran, where local currencies have been volatile and economic conditions challenging. However, there is evidence that the state and its associated actors have also utilized the same channels to facilitate trade in contravention of sanctions. In 2024, outflows from Iranian services increased to $4.18 billion, representing a nearly 70% year-over-year rise.

An illustrative example is Iran's largest digital asset exchange, Nobitex. Nobitex facilitates transactions for a diverse range of users, including regular Iranians and ransomware actors linked to the IRGC, as well as the sanctioned Russian exchange, Garantex. The exchange's large inflows and connections to other sanctioned and illicit actors, both within and beyond Iran, underscore its significance in facilitating state-linked sanctions evasion. Recently, Nobitex was exploited in June 2025, resulting in the loss of over $90 million in digital assets.

Furthermore, the IRGC's proxy networks have sought to facilitate commodity trade, weapons procurement, and, more broadly, sanctions evasion through the use of digital assets. Sanctions have highlighted this usage, including an IRGC-connected Houthi financier who received over $178M in part to facilitate Iranian oil trade, a broader Houthi network facilitating nearly $1B in transactions, involved in Russian commodities and weapons procurement, and Hezbollah-linked financiers. Hamas has also sought to leverage digital assets to facilitate its activity, including donation campaigns, which have regularly been disrupted by law enforcement, including most recently, where over $200,000 was seized by the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI).

iii. DPRK

The Democratic People's Republic of Korea (DPRK) has developed a sophisticated, multi-pronged approach of using digital assets for sanctions evasion and to support its weapons of mass destruction program.

In 2024, DPRK-linked groups stole at least $1.3 billion in digital assets across 47 incidents. DPRK hackers have also been responsible for some of the most audacious digital asset thefts over the years (Figure 5). This includes the $600 million Ronin Bridge hack and this year's $1.4 billion theft from digital asset exchange Bybit, where malicious code successfully manipulated the approval of transactions that then distributed funds to the hackers.

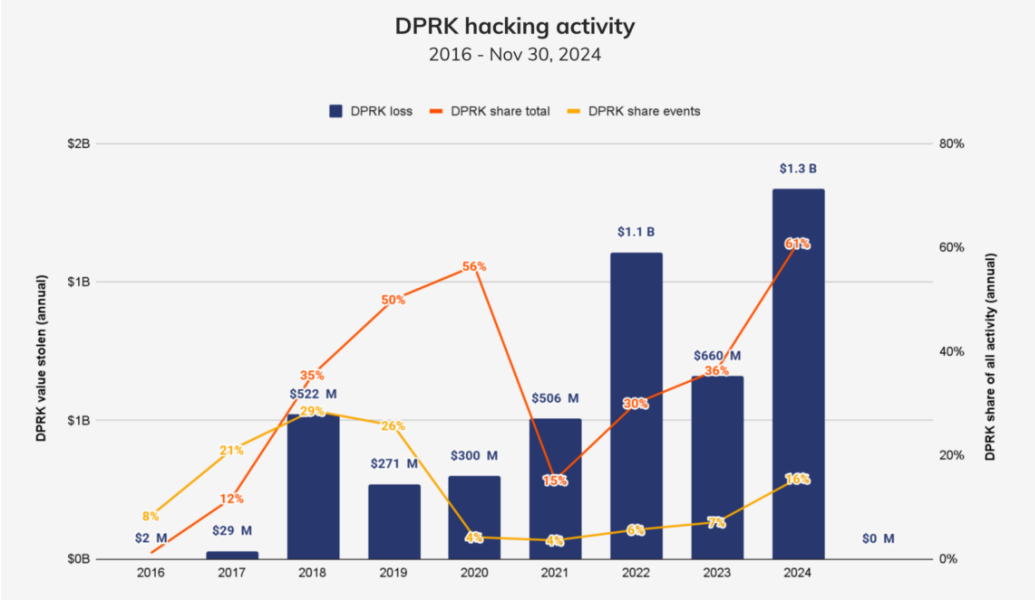

Figure 5

DPRK stolen funds are frequently laundered through a complex web of intermediary wallets, mixers, and cross-chain bridges. The Chainalysis graph below illustrates the complexity of

how hackers associated with the DPRK theft from Bybit attempted to move stolen funds through various wallets, mixers, and bridges to obfuscate transaction activity (Figure 6).

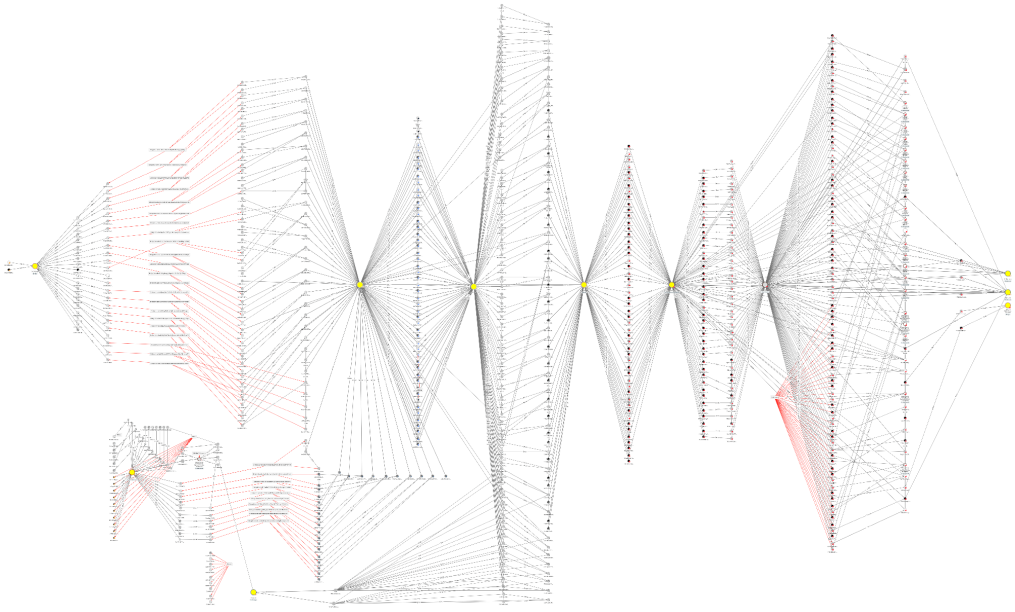

Figure 6

DPRK-linked actors also have a track record of infiltrating organizations by posing as remote IT workers. A recent DOJ indictment revealed 14 DPRK nationals who posed as remote workers, earning over $88 million while stealing proprietary data. These DPRK-aligned hacking groups create convincing employee profiles on professional networks and target roles at digital exchanges and Web3 companies. Using generative AI for facial and voice recognition, falsified documents, and technical interview assistance, they can infiltrate organizations to identify vulnerabilities and execute exploits.

The threat posed by the DPRK to the US and its allies is significant and critical to address for the health and viability of the digital asset ecosystem. Their track record of success in gaining access to and exploiting legitimate exchanges and web3 companies, as well as in a range of high-profile events, has enabled them to garner a significant war chest of digital assets for the regime to deploy. Combating this threat will require the public and private sectors to work together to implement security measures against DPRK intrusions, disrupt laundering and off-ramping efforts, and seize stolen funds after exploits have occurred.

Fraud and Scams

Americans face a growing threat from cyber-enabled and increasingly professional scammers who capably exploit technological developments such as social media, digital assets, and AI. Digital assets are just one vector for scam execution and laundering, but they are an important one.

Scams have consistently been one of the largest categories of illicit activity involving digital assets, accounting for over $10 billion in on-chain value transferred annually over the past four years. In 2024, scams accounted for approximately 25% of all illicit digital asset proceeds that we were able to trace, with over 80% of scam proceeds attributed to high-yield investment scams and so-called “pig butchering” scams, which are a combination of romance and investment scams (Figure 7). These involve victims being deceived into authorising a payment, causing financial and emotional harm to individuals and substantial financial and reputational costs to businesses that inadvertently facilitate the payments.

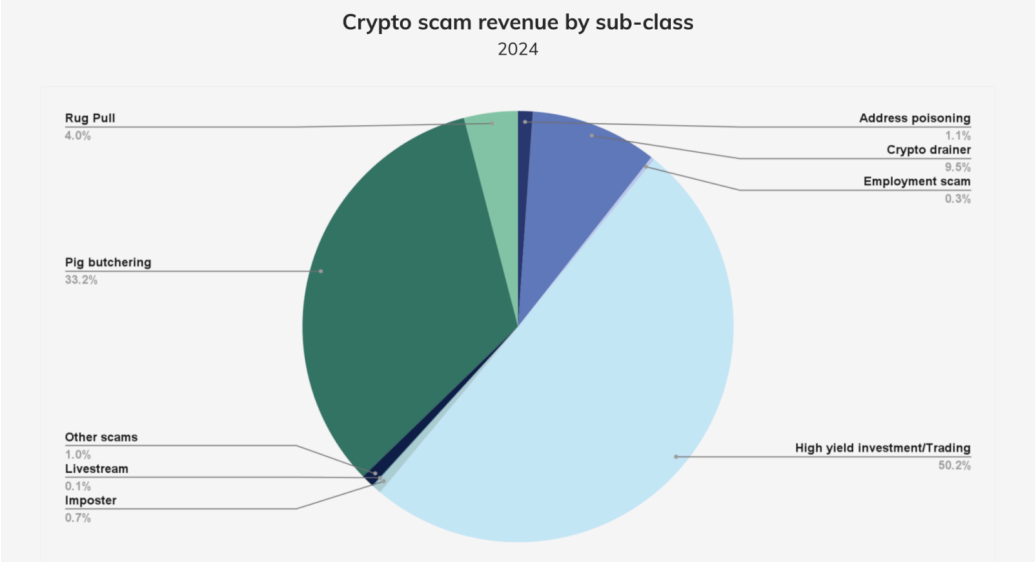

Figure 7

While our data is central to identifying the nature and scale of the problem, and our tools have been critical to the response, we recognize that reactive approaches are not sufficient to tackle scams at scale. The industry response needs to prioritize the prevention of illicit on-chain activity where possible by leveraging next-generation blockchain analysis and AI-driven tools that enable proactive monitoring and real-time threat detection.

Chainalysis: A trusted partner in combating illicit activity

Since Chainalysis was first founded in 2014, pioneering the field of blockchain analytics, our singular purpose has been to build trust in blockchains. The use of digital assets should place illicit actors at a disadvantage, given the traceable nature of these assets and their associated transactions; we strive to make that a reality.

We analyze transaction data from blockchain networks in conjunction with open-source intelligence and proprietary data to map the ecosystem of both benign and illicit

participants in these networks. Blockchain investigations and transaction monitoring, leveraging Chainalysis software and data, provide a clear and visual representation of criminal networks and illicit activities, offering a level of transparency unparalleled in traditional financial services. Building on this foundation, we have developed custom-made tools to map the blockchain, enabling us to identify potential suspicious activity, trace fund movements, and disrupt illicit activity across digital asset networks.

Over the past decade, our tools and data have become indispensable to the workflows of law enforcement and intelligence agencies in the US and globally, and have been utilized extensively to mitigate illicit activity and other risks within the digital asset ecosystem. For example, we have provided direct support on hundreds of cases involving seizures and freezing of digital assets. In partnership with government agencies worldwide, we have helped secure an estimated $12.7 billion worth of illicit proceeds in digital assets.[1] In addition to providing the most comprehensive blockchain tools, we also provide training to enforcement agencies and regulatory bodies worldwide.

These seizures were made possible by the transparency of blockchain and the availability of state-of-the-art Chainalysis tools and data.

- In late 2023, Chainalysis, Tether, and digital asset exchange OKX collaborated with the DOJ and U.S. Secret Service to investigate a major pig butchering romance scam compound in Southeast Asia. Using Chainalysis tools, investigators traced illicit transactions, allowing Tether to freeze approximately $225 million of USDT held in perpetrators' wallets, marking the largest ever freeze of USDT.[2] As of June 2025, this has been seized, making it the largest seizure of funds related to digital asset scams.[3]
- In November 2021, IRS-CI seized 50,676 bitcoin worth $3.36 billion from James Zhong, who pleaded guilty to wire fraud for stealing the funds from Silk Road in 2012, making it one of the largest digital asset seizures. Zhong exploited a flaw in

[1] "Asset Seizure and Cryptocurrency: How Chainalysis Creates Opportunities for Self-Sustaining Law Enforcement," *Chainalysis*, Mar. 26, 2025, https://www.chainalysis.com/blog/cryptocurrency-asset-seizure/.
[2] "Following Investigations by Tether, OKX, and the U.S. Department of Justice, Tether Voluntarily Freezes 225M in Stolen USDT Linked to International Crime Syndicate," *Tether* and *OKX*, Nov. 20, 2023, https://www.okx.com/en-eu/learn/tether-okx-investigation and https://tether.io/news/following-investigations-by-tether-okx-and-the-us-department-of-justice-tether-voluntarily-freezes-225m-in-stolen-usdt-linked-to-international-crime-syndicate/.
[3] Department of Justice, "Largest ever seizure of funds related to crypto confidence scams" https://www.justice.gov/usao-dc/pr/largest-ever-seizure-funds-related-crypto-confidence-scams, *Chainalysis*, Jun. 18 2024

Silk Road's withdrawal system, later using mixers and exchanges to launder funds. Agencies used Chainalysis tools to trace transactions and link Zhong to the crime.[4]

- In May 2021, Colonial Pipeline paid approximately $4.4 million worth of bitcoin in ransom to DarkSide, a Russia-based ransomware group, following a cyberattack that disrupted fuel supply across the southeastern U.S. Using Chainalysis tools, the FBI traced the ransom payment, identifying fund movements through DarkSide's network. This led to the seizure of $4.4 million of bitcoin from the attacker's wallet.[5]

These seizures are significant as they help dismantle criminal funding networks, making it harder for bad actors to continue operating and forcing them to identify new funding and cash-out streams. Seizures can also generate revenue, allowing the government to reinvest the seized funds into its operations, thereby reducing its reliance on taxpayer dollars.

Beyond these specific seizure examples, as evidence of our close and continuing approach to partnering with the public sector, we launched Operation Spincaster to disrupt and prevent scams through public-private collaboration.[6] Chainalysis proactively identified thousands of compromised wallets using our data and tools. This actionable intelligence formed the basis of a series of operational sprints across six countries (the US, the UK, Canada, Spain, the Netherlands, and Australia) with over 100 attendees, including 12 public sector agencies and 17 digital asset exchanges. Over 7,000 leads were disseminated during these sprints relating to approximately $162 million of losses. These leads were used to close accounts, seize funds, and build intelligence to prevent future harm to consumers.

Market Structure Principles: An important foundation

The Principles released by the Committee are an important foundation for developing a modernized digital asset market structure framework. We welcome the focus on responsible innovation while ensuring consumers are protected and illicit finance risks are addressed.

In transitioning from principles to legislation, we encourage the Senate to consider how risks and solutions in the digital asset sector differ from those in traditional finance. In our view, there are three main ways in which risks differ from those in traditional finance, and they relate directly to the nature of the underlying technological infrastructure:

[4] "Chainalysis in Action: Department of Justice Announces Second-Largest Ever Crypto Seizure, with $3.36 Billion in Bitcoin Seized from Silk Road Hacker" https://www.chainalysis.com/blog/james-zhong-silk-road-hack-seizure/

[5] "Chainalysis In Action: How FBI Investigators Traced DarkSide's Funds Following the Colonial Pipeline Ransomware Attack" https://www.chainalysis.com/blog/darkside-colonial-pipeline-ransomware-seizure-case-study/

[6] "Introducing Chainalysis Operation Spincaster: An Ecosystem-Wide Initiative To Disrupt and Prevent Billions in Losses to Crypto Scams," *Chainalysis*, Jul. 18, 2024, https://www.chainalysis.com/blog/operation-spincaster/.

- **First, illicit finance.** As evidenced in this testimony, the illicit finance risks associated with digital assets are, in some cases, accentuated by the scale and speed of blockchain transactions. The Principles appropriately highlight the need for a common-sense package of measures aimed at preventing money laundering and sanctions evasion. The framework must emphasize the importance of new tools for detecting illicit activity, including on-chain transaction monitoring and the utilization of blockchain analytics to assess the riskiness of on-chain exposures.
- **Second, market integrity and fraud.** The structure of digital asset markets can facilitate new forms of misconduct, including rug pulls and oracle manipulation. There are also new vectors for carrying out familiar forms of misconduct, such as insider trading, wash trading, and market manipulation. These activities can occur on centralized trading venues or decentralized platforms, or bridge both, making them harder to detect. To ensure investor protection, any eventual legislation must take into account how businesses and enforcement agencies can foster cleaner markets.
- **Third, cybersecurity.** In no other sector is cybersecurity so closely entwined with prudential soundness and the safety of customer assets. This is aptly demonstrated by the billions of dollars' worth of digital assets that have been stolen from both centralized and decentralized businesses. The Senate should consider requiring the establishment of standards for cyber risk management in a blockchain environment.

In each of the above examples, the fundamental risks associated with digital assets are similar to those in traditional finance, but they materialize in slightly different ways. More importantly, new technological solutions exist that enable businesses to effectively manage their risks by drawing on the transparency of blockchains. These include:

- AML/CFT risk management tools that have become fundamental elements of businesses' risk management programs and compliance with requirements under the BSA, including transaction monitoring, enhanced due diligence, and, when appropriate, enhancing SAR filings. Chainalysis Know-Your-Transaction (KYT) and Address Screening are tools that allow businesses to monitor incoming and outgoing digital asset transactions, wallet addresses, and liquidity pools in real time to assess risk and raise alerts for potential compliance issues;
- Bespoke blockchain analytics that detect suspicious patterns of behaviour suggestive of different types of market manipulation and fraud. When it comes to detecting and disrupting fraud, Alterya, a Chainalysis company, utilizes AI to identify scammers before they target victims, gathering data from multiple sources, including direct engagement with criminals. This intelligence integrates with customers' transaction

monitoring platforms to provide real-time analysis of scams, enabling risk assessment and preventive action;

- Real-time smart contract monitoring and other on-chain security tools that go beyond the current approach, which centers around access and identity management and point-in-time audits. Hexagate, a Chainalysis company, enables users to monitor on-chain transactions and receive alerts when suspicious or unusual activity is detected. In many instances, this enables users to preempt threats and act swiftly to prevent losses.

We strongly encourage the Senate to leverage these new technological tools and their potential to improve regulatory outcomes in an efficient, pro-innovation manner.

Building regulatory and enforcement agency capability

In the same way that digital assets and the public ledger have reshaped compliance, they also provide an opportunity to reimagine approaches to regulation and investigation. In particular, by leveraging blockchains as a data source, regulators can go from reactive to proactive, such as through:

- **Data-driven policymaking.** Understanding the amount and nature of on-chain activity in the jurisdiction, particularly sources of illicit finance risk;
- **Real-time supervision:** Ongoing supervision of the AML/CFT defenses of registered businesses by understanding their sending and receiving exposure, and how these are changing over time;
- **Scam and mule detection:** AI-driven detection of likely scam and mule wallets, which criminal groups use to defraud American citizens in pig butchering scams and other forms of authorized fraud;
- **Automated detection of market abuse:** Detection and disruption of market abuse on blockchains, by identifying patterns of suspicious activity and investigating them through specialized blockchain tracing software; and
- **Cyber threat monitoring:** Real-time threat intelligence and monitoring of potential cyber exploits, particularly where they involve customer assets.

The Senate must ensure that agencies tasked with oversight are adequately resourced and equipped to discharge their responsibilities and that they are empowered to explore innovative solutions that enable them to do so in a business-friendly manner.

Conclusion

If we get the framework for regulating digital asset markets correct, the United States will lead the next generation of financial infrastructure. Blockchain technology and its inherent transparency introduce a fundamentally new way for government agencies to deliver oversight. This transparency also enhances our ability to identify and act against illicit actors at speed, in near real time.

Crucially, we need to equip government agencies with the appropriate resources and tools to leverage this new paradigm. Delivering the right regulation requires defining agency roles, understanding the risks associated with digital assets, leveraging real-time transparency for effective oversight, and designing compliance regimes that enable institutions to engage with these technologies.

Treating digital assets like traditional finance means missing the opportunity to build tomorrow’s digital asset markets better. With regulation that embraces blockchain's unique capabilities—transparency, speed, and programmability—we can achieve better, stronger outcomes for both market integrity and innovation.

At Chainalysis, we're proud to support the U.S. government in keeping the digital asset ecosystem safe. Thank you.