cyberIdaho Financial Innovation Lab

Emerging Technology Advisory Committee Report

Digital Forensic Tools & Evidence Locker Audits are Necessary to Identify & Account for Illicit Crypto Assets in Seizure/Forfeiture Programs

Executive Summary

A massive increase in illicit activity leveraging crypto assets (e.g., cryptocurrencies such as Bitcoin, Ethereum, Monero etc.) is leading to a surge in criminal/national security cases involving crypto seizures/forfeitures that makes it vital for federal, state, and local stakeholders to adopt an effective audit function to properly identify and account for these assets to ensure victim restitution, protect against misconduct, and stop bad actors from maintaining access to their illicit assets. **Known illicit crypto activity reached an all-time high in 2025 totaling $154 billion, while crypto cybercrime losses grew approximately 3677% since 2020 in the United States.** Various factors including the digitization of society, pseudonymous nature of crypto assets, short transaction settlement cycles, and rising adoption/value of crypto assets is causing more illicit actors to use crypto in their operations. Concurrently, limited government crypto expertise and outdated asset seizure/forfeiture processes are highlighting the need for government stakeholders to adopt new crypto auditing policies, solutions, and tools. Additionally, since numerous seizures/forfeitures of electronically stored information (e.g., digital storage devices, electronic records, and digital evidence etc.) have not been properly searched for crypto assets in the past many evidence lockers contain unidentified illicit crypto assets that would be uncovered with a proper audit.

The combination of growing crypto crime and evidence lockers that have not been thoroughly audited for crypto assets is making it crucial for key stakeholders to facilitate and design an audit strategy to identify and account for crypto assets in an effort to frustrate illicit operations, prevent custodial misconduct, alleviate digital evidence processing backlogs, and most importantly return funds to victims. To accomplish these goals federal and state policymakers should design policies that require annual crypto asset audits of seized/forfeited electronically stored information in evidence lockers, direct custodians to establish strong crypto storage and access safeguards, enable the procurement of necessary audit tools/services, provide access to crucial training, and stipulate that government agencies proactively conduct research for victim restitution purposes when illicit crypto assets are seized/forfeited.

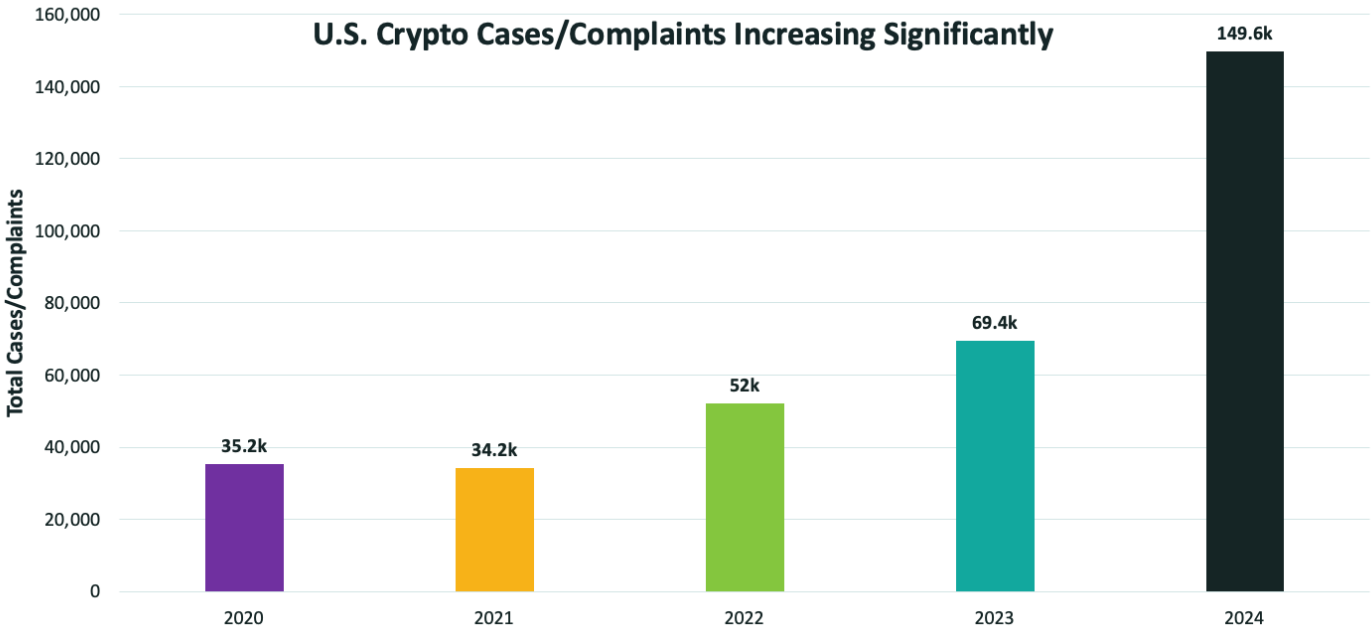
[1] [2]

Investigations Involving Crypto Assets are Growing Exponentially in the United States

The increasing adoption and market value of crypto assets over the past decade is causing illicit actors to embrace crypto into their operations and is driving the large growth of investigations and asset seizures/forfeitures involving crypto assets that make a robust audit function necessary. Conservative estimates suggest that approximately 600 million people are currently using crypto assets globally with research also highlighting that crypto is used by nearly 20% of adults in the U.S.[3] [4] This strong adoption of crypto assets combined with its growing acceptance as a payment mechanism (e.g., Home Depot, Gucci, and Burger King accept payments at select locations etc.) and its rising value (the market cap for crypto assets reached over $4 trillion in 2025) is both enabling and motivating both good and bad actors to operate more freely and consistently in the crypto space leading to an increase in investigations containing these assets.[5] [6]

Accompanying the mainstream adoption and legitimization of crypto assets is a rise in illicit crypto transactions, cybercrime, and investigations. Between 2020 - 2024 approximately $200 billion in known illicit crypto transactions have occurred including everything from dark web transactions, hacks, and money laundering operations to scams, terrorist finance transactions, and thefts.[7] The U.S. is currently experiencing a cybercrime

epidemic with cases often possessing a crypto element. Crypto fraud accounted for $9.3 billion of the $16.6 billion worth of known cybercrime losses last year in the U.S., which represents over half of all known U.S. cybercrime losses.[8] This surge in illicit crypto activity and cybercrime correlates with the nearly 325% increase in crypto cases/complaints the Federal Bureau of Investigation's (FBI) Internet Crimes Complaint Center (IC3) has received since 2020 (see chart below). [9]



These factors showcase that the growing adoption and use of crypto in illicit activity is leading to a significant increase in investigations that lead to the seizure/forfeiture of electronically stored information (ESI) containing crypto assets. This reality makes the development of a properly functioning crypto asset audit function vital to identifying and returning stolen victim funds and stopping bad actors from controlling/accessing their illicit gains.

Digital Value, Quick Transaction Speeds, & Unique Crypto Attributes Makes Crypto Asset Seizure/Forfeiture Tools and Audits Essential

The growing use of digital technology in financial transactions is making both society and illicit actors comfortable with the idea of digital value, which is leading to a surge in illicit operations using crypto. The convenience and portability digital financial transactions and crypto assets present are a major reason approximately 3 billion people globally are using digital payments and nearly 90% of Americans are using financial technology.[10] [11] COVID-19 acted as a catalyst to this trend as more people began using digital financial technology, internet connectivity, and mobile services for business, shopping, entertainment, and personal purposes.[12] For illicit actors, the mobility, convenient access, and global reach crypto assets provide is an upgrade over more tangible and analog methods of exchanging value such as using cash or precious metals (e.g., gold) that share similar bearer instrument characteristics. These more traditional financial assets are also much easier to identify and account for during seizures/forfeitures and audits than crypto assets.

Furthermore, the benefits crypto assets provide in the form of transaction speeds, one-way payments, decentralized control, and cryptographic privacy make it a useful tool for bad actors in their operations. Crypto transactions can settle in a matter of seconds or minutes and once they are sent to a beneficiary's wallet the transaction cannot be reversed since there is no centralized entity with control over a transaction. Additionally, the use of asymmetric cryptography (mathematical algorithms that use public and unique private keys to

complete transactions) eliminates the need for names in transactions like those found in the traditional financial system's account-based architecture. These unique attributes help illicit actors hide their identities and move money quickly, which can make seizures/forfeitures, custodial oversight, and victim recoveries difficult without proper investigative and auditing tools and processes.

Lack of Digital Forensic Tools & Annual Audits Will Lead to Missed Victim Recovery Opportunities, Enable Misconduct, & Allow Bad Actors to Maintain Illicit Gains

While physical evidence such as cash can easily be seized by law enforcement anyone with access to private keys or copies/backups of crypto wallets (including illicit actors) can recover assets within seconds or minutes, and this makes it important for law enforcement and evidence custodians to have access to the tools/services they require to immediately seize assets and create a trustworthy chain of custody for audit trails to guarantee the safety of these assets. The inability to immediately identify crypto assets on devices during seizures/forfeitures presents illicit actors and their networks with an opportunity to move and maintain control of their ill-gotten gains before they can be identified, seized, or formally accounted for during the forfeiture process.

The absence of annual audits or delays in processing digital evidence opens an avenue for bad actors and corrupt officials to steal funds if they are not properly processed and accounted for during an investigation. Many law enforcement officials and evidence custodians lack critical crypto knowledge, so it is crucial for them to build this knowledge to develop effective processes for storing, managing, and auditing crypto assets that are seized and forfeited. In 2022, the Department of Justice (DOJ) highlighted the need for the U.S. Marshall Service (USMS) to update their policies regarding the custody, management, and disposal of crypto assets.[13] By adopting the tools and processes required for crypto asset seizures/forfeitures a trusted chain of custody can be established that can prevent misconduct by corrupt officials (e.g., the high-profile Silk Road case where Drug Enforcement Administration Agent Cal Force and Secret Service Agent Shaun Bridges were caught stealing $800,000 worth of crypto assets).[14]

Since crypto assets, wallets, seed phrases, and private keys can be found in all types of ESI (phones, computers, servers, emails, cloud accounts etc.) it is critical that all seized/forfeited devices in evidence lockers are analyzed during annual audits to identify potential illicit crypto assets that may have been missed, so they can be returned to victims and taken away from illicit actors. Furthermore, many law enforcement agencies and evidence custodians are just starting to make crypto audit practices a priority, which means there are likely billions of dollars sitting in evidence lockers right now that could be uncovered via a crypto asset evidence locker audit of all ESI. This would accomplish the dual goal of supporting victim restitution efforts, while also preventing bad actors from regaining control of their illicit assets.

Key Policy Solutions for Crypto Asset Seizure/Forfeiture Programs: Audits, Tool Procurement, Updated Processes, Training, & Victim Restitution Research

The surge in legal cases involving crypto asset seizures/forfeitures requires policymaker attention to account for the unique features of crypto assets to ensure that illicit proceeds are identified, seized, and properly custodied to improve victim recovery, prevent misconduct, and make sure bad actors lose control of their crypto. To create an efficient and effective crypto asset seizure/forfeiture audit process policymakers should take the following steps:

> **Authorize Annual Crypto Asset Audits of all ESI in Evidence Lockers** – Congress and state legislatures should draft legislation that requires annual crypto specific audits of all seized ESI being held in law enforcement agencies, DOJ, Department of Defense (DoD)/Department of War (DoW), and

the Intelligence Community (IC) evidence lockers to better identify, safeguard, and account for seized crypto assets. In the absence of legislation, the White House and state governors should immediately issue Executive Orders to relevant agencies authorizing annual ESI audits to identify crypto assets to assist with victim recovery efforts, deter custodial misconduct, and deny bad actors access to illicit funds.

Allocate Budget Resources for Crypto Digital Forensic Tools/Services – Congress, state legislatures, and government agencies should allocate budget resources for the procurement of digital forensic investigation tools and services that can ensure successful crypto asset seizures/forfeitures and audits. Access to digital recovery scanning tools (e.g., CAT Labs Recovery CAT), backup tools (e.g., CAT Labs Security CAT), and blockchain analytic tools (e.g., Chainalysis, TRM, Merkle Science etc.) are essential for a properly functioning crypto asset seizure/forfeiture and audit program.

Review and Update Processes for Managing Seized Crypto Assets – Policymakers should require leadership in agencies overseeing seizure/forfeiture programs to review and update their processes annually to address and identify potential vulnerabilities in the ever-changing crypto ecosystem. Due to the unique attributes of crypto assets, they can be difficult to track and price (e.g., price volatility or forking events) and because they are digital bearer instruments (e.g., if someone controls the private keys for a crypto wallet they control the crypto assets in that wallet) these assets require strong inventory reconciliation practices and storage/access controls.

Provide Key Stakeholders with Crypto Asset Trainings– Agencies involved in crypto asset investigations and seizures/forfeitures should use a portion of their training budgets to enhance the knowledge of their investigators and evidence custodians by sending them to targeted trainings focusing on crypto assets. Understanding crypto asset features, cybersecurity issues, and novel financial crime methodologies will help increase crypto seizures/forfeitures, while concurrently building strong safeguards for the storage, management, and custody of crypto assets. Since the crypto landscape is constantly evolving it is important for stakeholders to obtain the knowledge and training they require to successfully adapt to changes in the crypto ecosystem to responsibly fulfill their missions.

Ensure Victim Restitution Research is Conducted After Crypto Asset Seizures – Policymakers should require agencies to conduct research in key federal and state databases, such as the FBI's IC3 database, to identify potential victim restitution opportunities when illicit funds are seized. Since crypto assets operate on distributed ledger technology (e.g., blockchain) investigators can use digital forensic tools (see above) and the transparency of these ledgers to track and trace transactions back to victims if they file law enforcement or regulatory complaints in federal or state databases.

When victims cannot be identified government agencies should continue to place forfeited assets into victim and law enforcement support funds such as the DOJ Asset Forfeiture Fund, the Treasury Forfeiture Fund, and similar state funds. A provision that enables a portion of these forfeited assets to be allocated to nonprofits that are assisting with ancillary victim support services (e.g., mental health services and other support mechanisms) would also be beneficial. However, government agencies should proactively seek to identify victims when funds connected with their cases are recovered and seized.

The development of reliable federal and state crypto asset seizure/forfeiture and audit programs will help make

more victims whole and disrupt the operations and financial well-being of bad actors. The adoption of the policy solutions above will create the foundation for a successful crypto asset seizure/forfeiture program that can properly handle the rising number of investigations/cases involving crypto assets by providing the critical authorities, evidence locker audit functions/processes, resources, tools, and knowledge needed to better serve victims and the public at the expense illicit actors.

Endnotes

[1] https://finance.yahoo.com/news/illicit-crypto-hits-time-high-130000148.html (refers to the $154 billion worth of illicit crypto activity stat mentioned in the callout box).

[2] https://www.ic3.gov/annualreport/reports (the percentage change metric in the callout box is from IC3's annual and state reports between the years 2020 - 2024).

[3] https://coingate.com/blog/post/how-many-people-will-use-crypto-in-2026#:~:text=How%20Many%20Crypto%20Users%20Are,hold%20crypto%20beyond%20mere%20speculation.

[4] https://nca.org/2025%20State%20of%20Crypto%20Holders%20Report.pdf

[5] https://finance.yahoo.com/news/walmart-starbucks-more-accepting-crypto-202205775.html

[6] https://finance.yahoo.com/news/crypto-sector-breaches-4-trillion-194622641.html#

[7] https://www.blockchain-investigation-agency.com/post/200-billion-in-cryptocurrency-illicit-transactions-from-2020-to-2025-a-deep-dive-into-financial-cr#:~:text=The%20staggering%20$200%20billion%20in,stay%20ahead%20of%20evolving%20threats.

[8] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[9] https://www.ic3.gov/annualreport/reports (the percentage change metric and chart is based on the complaint stats found in IC3's annual reports between the years 2020 - 2024).

[10] https://rootdigital.co.uk/blog/fintech-trends-and-statistics/#

[11] https://plaid.com/the-fintech-effect-2021-mass-adoption/

[12]https://pmc.ncbi.nlm.nih.gov/articles/PMC9759262/#:~:text=In%20this%20paper%2C%20we%20provide,occurred%20in%20the%20pandemic's%20absence.

[13] https://oig.justice.gov/sites/default/files/reports/22-082.pdf

[14] https://www.bbc.com/news/technology-32124251#:~:text=Two%20former%20US%20special%20agents,in%20Bitcoin%20from%20the%20operation.