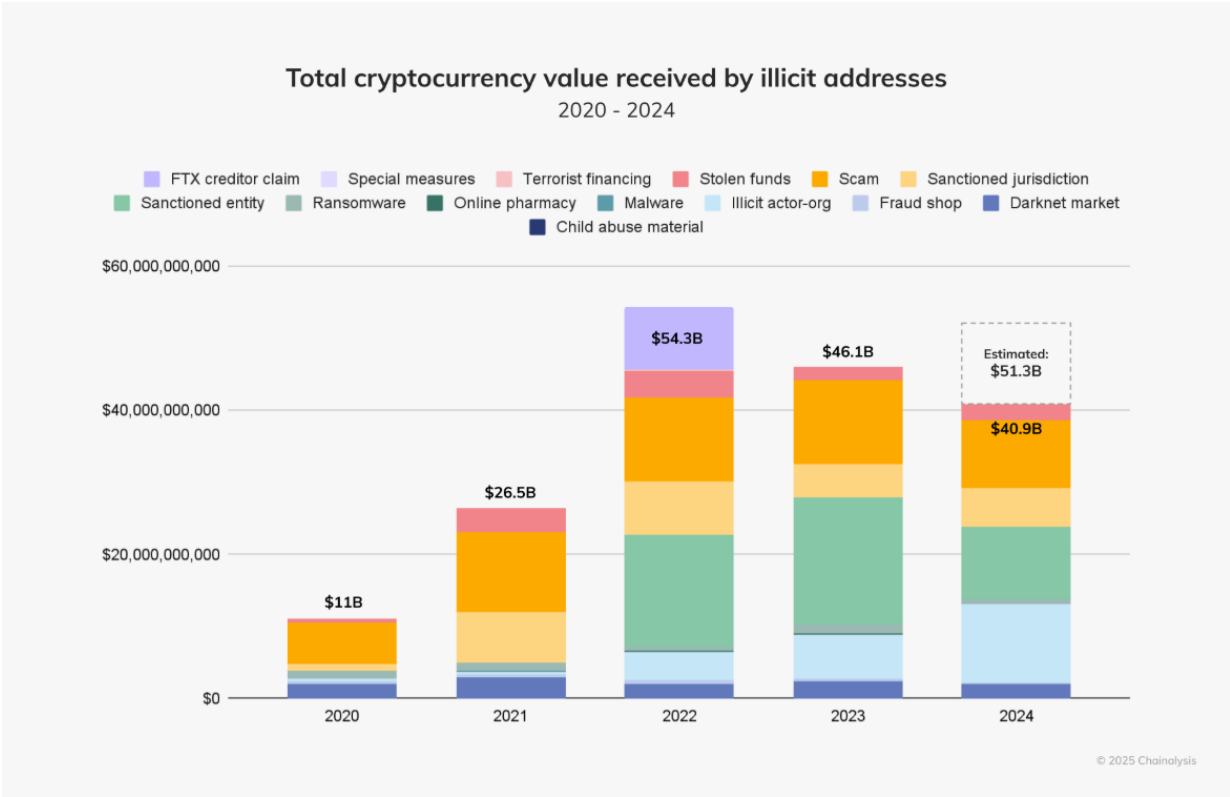



# A Golden Age of Crypto Crime?

By Benjamin Schiffrin | *Director of Securities Policy*  
February 10, 2025

Crypto crime likely broke [records](#) in 2024. Chainalysis, a cryptocurrency tracking firm that publishes an annual report on crypto crime, has already identified the receipt of over \$40 billion by illicit cryptocurrency addresses, and it estimates that the total amount will be over \$50 billion once it completes its tracking for the year. Even this number is likely to underestimate the amount of crypto crime, as Chainalysis counts only the illicit transactions it can confirm. Regardless, 2024 was already the third consecutive year where the total cryptocurrency value received by illicit addresses exceeded \$40 billion.



On February 11, 2025, the Digital Assets, Financial Technology, and Artificial Intelligence subcommittee of the House Financial Services Committee will hold a hearing entitled “A Golden Age of Digital Assets: Charting a Path Forward.” While Congress ponders a path forward for crypto regulation, it should consider that all too often “standing with crypto”



means [standing with fraudsters](#). As detailed below, crypto’s criminal uses continue to proliferate, and **Congress must not adopt a regulatory regime that allows an intended “Golden Age of Digital Assets” to instead become a Golden Age of Crypto Crime.**<sup>1</sup>

## Ransomware

[Ransomware](#) is a type of malicious software that prevents users from accessing their computer files, systems, or networks unless the users pay the attackers a ransom. In 2024, ransomware attacks [surged](#) both in frequency and sophistication. [Cryptocurrency](#) “remains the dominant form of payment in these attacks, enabling cybercriminals to receive payments anonymously and execute cross-border transactions.”

These attacks often target U.S. cities and prevent their residents from receiving basic services. For example, Dallas [suffered](#) a ransomware attack that hindered the city’s 911 emergency services and court systems. A ransomware attack in Baltimore [prevented](#) residents from paying their water bills or parking tickets. And Oakland suffered a ransomware attack that resulted in outages to the city’s systems that were so [severe](#) that the city administrator declared a state of emergency to fast-track the restoration process.

Smaller towns that have fewer cybersecurity resources are even more vulnerable to having their most crucial systems attacked. The San Bernardino County Sheriff’s Department was [forced](#) to pay hackers a \$1 million ransom to recover access to its computer systems, including email, in-car computers, and some law enforcement databases, including a system that deputies use for background checks. Similarly, ransomware attackers held the Plainfield, Connecticut police department’s computer systems [hostage](#).

Police Chief Mario Arriaga called the incursion a “complete system failure” that could potentially affect officer safety and response times. “Dispatchers can’t access information on criminal histories or on addresses we’re sending officers to,” he said. “We can’t tell if a motor vehicle has a suspended registration or tell how many times we’ve been dispatched to a certain residence.” The department is down to two working phone lines.

Ransomware attacks that impact real people are not limited to government services. Ransomware attacks routinely force [hospitals](#) to divert ambulances and cancel appointments. For example, last May, a ransomware attack hit Ascension, a St. Louis-based nonprofit that oversees 140 hospitals across 19 states.

“It’s putting people’s lives in danger,” said a nurse who works at Ascension Providence Rochester Hospital, a 290-bed facility about 25 miles north of

---

<sup>1</sup> Of course, while criminal conduct is the most egregious, it is not the only illegal, unlawful, and predatory conduct that victimizes hard-working Main Street Americans. For example, crypto’s refusal to follow the securities and commodities laws exposes Americans to conflicts of interest and illegal behavior that needlessly threaten their investments.

downtown Detroit. “People have too many patients for what is safe. Nurses are taking on five or six patients dealing with all of this paper charting.”

Another nurse, who works at a 409-bed Ascension hospital in Birmingham, Alabama, told CNN: “It’s frightening how many safety guardrails [have been] out of service without any computers.”

With crypto “[continuing to play a central role in extortion](#)” through ransomware attacks, Congress should consider the dangers of a lax regulatory regime.

## Meme Coins

A [meme coin](#) is a cryptocurrency that is inspired by a meme or other internet trend. Recently, there has been an [explosion](#) of meme coins tied to celebrities and politicians. These meme coins are [highly volatile and speculative assets](#) that are susceptible to fraud.

Scams involving meme coins are so common that they have a name: [rug pulls](#).


While the tokens have no value as currency, their price can soar upon release, as speculators jump on the new offering. That allows insiders who held the coins before their public debut to turn a quick profit, with some top tokens achieving multibillion-dollar valuations in a matter of minutes. But the coins are also likely to crash just as quickly, leaving latecomers with steep losses.

Essentially, these meme coin rug pulls are [pump and dumps](#), where insiders buy up a large percentage of the tokens in advance and then dump them after the price soars, leaving regular investors with tokens that are essentially worthless.

One recent and prominent example is the case of Haliey Welch, who gained internet fame after a TikTok video of her went viral. After [parlaying her newfound fame](#) into a merchandise line and podcast, she launched a meme coin in December 2024. The meme coin initially surged in price, but its value quickly [plummeted](#) by over 90% [after](#) a small group of owners sold off more than 80% of the token’s supply. One investor wrote on X that she was a fan of Welch but [as a result](#) of her purchase of the meme coin “you took my life savings.”

This is just the latest example of ordinary investors suffering harm from meme coins. Caitlyn Jenner, Iggy Azalea, and Jason Derulo have [all](#) also launched meme coins that have been incredibly volatile. Most celebrity meme coins have lost more than [90%](#) of their value since their launch. Azalea’s meme coin was relatively more successful—as of last month, it had lost only about [80%](#) of its value since the high it reached two weeks after its launch.

Even President Trump’s meme coin is not immune from this volatility. Although there are no allegations that its debut involved a rug pull, it has lost [75%](#) of its value since its launch. The president’s meme coin has [also sparked a flood of imitators, leading to warnings that investors risk being duped](#). Investors buying the copycat coins are at ““[enormous risk](#).””



The fact that meme coins [do not generate revenue or cash flow](#) means that they are mostly for speculation. This makes them a [paradise for gamblers and grifters](#). As a result, meme coins are the perfect example of why lax crypto regulations will endanger investors.

## Illicit Transfers

Unfortunately, investment frauds are both [prolific](#) and also just one of the many ways in which criminals use crypto to victimize ordinary Americans. Another increasingly prevalent fraud involves scammers [impersonating](#) a legitimate business to get the victims to transfer their assets into crypto. Criminals prefer crypto for these types of scams because crypto allows them to quickly move large sums of money across borders without having to engage with the traditional financial system. Crypto also offers criminals a level of anonymity. The nature of crypto transactions makes their real identity often impossible to ascertain.

America's most vulnerable citizens appear particularly susceptible to these scams. For example, Lawrence and Ling-Ling Liu, an elderly married couple, [lost \\$18.5 million](#) after they were tricked into transferring their assets to a cryptocurrency exchange. The Lius had accounts at Schwab, and Lawrence Liu received a pop-up warning on his computer telling him those accounts were under attack. Liu also received a phone number ostensibly for a Schwab employee who could help him protect his assets. The fake Schwab employee told Liu to move his and his wife's assets to other institutions for safekeeping. The scammer persuaded the Lius to open an account at crypto exchange Unchained Trading. Eventually, the Lius sold almost \$30 million of stock and transferred the money to their Unchained Trading account. Of the money transferred to Unchained Trading, most of it was used to purchase crypto. The crypto was then sent to an online address believed to be maintained by the scammer who posed as the fake Schwab employee. Ultimately, \$18.5 million was converted into crypto and sent to the scammers, making it most likely unrecoverable.

Similarly, Marjorie Bloom, a retired civil servant, lost [her life savings](#) of \$661,000 after transferring her funds into cryptocurrency at the urging of someone claiming to be a fraud investigator at PNC Bank, where she was a customer. The scammer persuaded Bloom that criminals were in the process of stealing her funds. He said that to protect her money she had to move it quickly. So the scammer had Bloom wire funds from her PNC Bank account to an account at now-defunct Signature Bank in New York. Her funds were then transferred to an account at Coinbase, converted to cryptocurrency, and then moved to an offshore account on the Binance crypto trading platform in the Cayman Islands. When Bloom tried to access the funds that she thought she had worked to secure, she couldn't.

'All of a sudden, this grayness lifted,' said Bloom, who lives in Chevy Chase, Maryland. 'I realized I had been defrauded of everything.'

## Bitcoin ATMs

A variation on this type of scam involves the use of bitcoin ATMs. Again, fraudsters contact their victims through a message that looks like a legitimate alert, like a pop-up notification, claiming an urgent problem with an account. They eventually text the victims a QR code connected to a digital wallet and direct the victims to scan the code and deposit cash into a bitcoin ATM under the guise that this will protect the victims' money. The bitcoin ATM then converts the cash to bitcoin that immediately gets transferred to the scammer.

Joseph Buentello, 80, was [one such victim](#). He received a frantic call claiming his son had been arrested and needed \$5,000 for legal fees. Buentello said the caller instructed him to withdraw the money from his bank and deposit it into a Bitcoin ATM at his local grocery store. Buentello followed the instructions, only to realize later that he had been scammed. The money was instantly converted to Bitcoin and sent to a cryptocurrency wallet, making it unrecoverable.

Joe Samuels, an 84-year-old artist, was another [victim](#). He received a call from someone claiming to be in the IT department of his computer company. They told him they had mistakenly deposited \$20,000 into his checking account and demanded that he send it back through a bitcoin ATM. He complied and never saw the money again. Marilyn LoCascio, another senior citizen, [similarly lost money](#) after receiving what looked like a security alert on her iPad. She lost \$31,500 to a fraud group that included people posing as an Apple tech support specialist, a bank representative, and two government officials.

The Federal Trade Commission [reports](#) that consumers reported \$114 million in losses from scams involving bitcoin ATMs in 2023. This was a nearly 900% increase over the preceding three years. Losses through June 2024 were around \$66 million, with the median amount of loss \$10,000—a sign the trend in bitcoin ATM fraud is only growing.

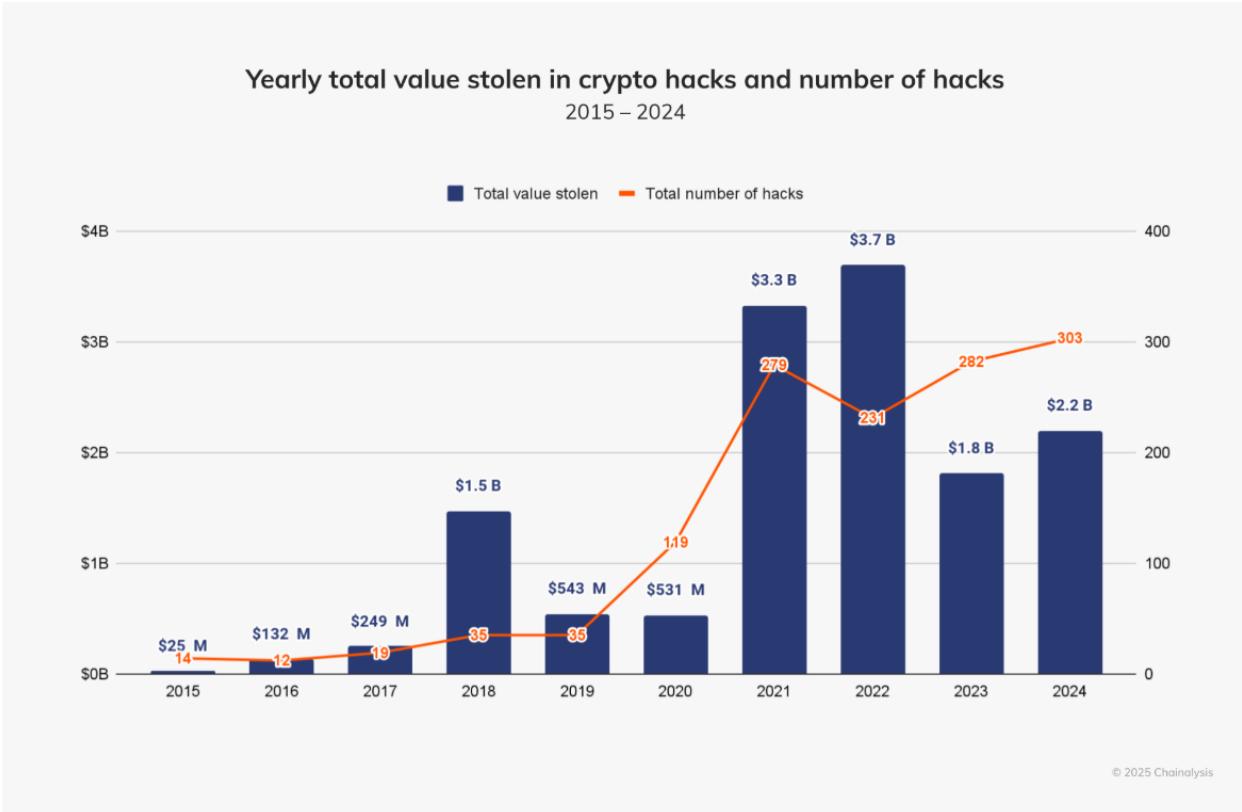
## Hacking

Crypto criminals also defraud investors by hacking their accounts. For example, [just last week](#), the Department of Justice charged Andean Medjedovic with exploiting vulnerabilities in two decentralized finance protocols to fraudulently obtain about \$65 million.

Medjedovic exploited the vulnerabilities in the automated smart contracts used by the KyberSwap and Indexed Finance protocols. Ultimately, Medjedovic was able to withdraw millions of dollars of investor funds from the protocols at artificial prices. Medjedovic also schemed to open accounts with digital asset exchanges using false and borrowed identifying information to conceal the source and true ownership of the proceeds. This criminal conduct rendered the victims' crypto investments essentially worthless.


Medjedovic’s scheme is emblematic of the rise of investor losses through crypto hacks. In 2024, criminals stole [\\$2.2 billion](#) from crypto platforms through hacking. This was the fourth straight year that more than a billion dollars’ worth of crypto was stolen.

2024 also set a [record](#) in terms of the number of individual hacking incidents. The number of individual hacking incidents increased from 282 in 2023 to 303 in 2024. This is why regulations that are designed to safeguard investors’ crypto assets are so essential.



## Market Manipulation

The crypto markets have long been plagued by manipulative activity. For example, in October, DOJ [charged](#) four crypto companies and four crypto financial services firms with market manipulation and wash trading. The defendants who created the crypto companies made false statements about their tokens and executed wash trades in those tokens to create the appearance of trading activity that would make the tokens look like good investments. The crypto companies also hired financial services firms to wash trade their tokens in exchange for payment. These wash trades attracted new investors and purchasers, which resulted in an increase in the tokens’ trading prices. The defendants then sold their tokens at the artificially inflated prices. The scheme involved millions of dollars of wash trades for approximately 60 different cryptocurrencies.



Reports estimate that, in total, there was [\\$2.57 billion](#) in potential crypto wash trading activity in 2024. So market manipulation remains a critical concern in the crypto space.

The complex and dynamic nature of market manipulation, compounded by crypto's unique characteristics—such as its pseudonymity and decentralization—heightens the challenge.

A regulatory regime for crypto must respond to this challenge. Without sufficient regulation, wash trading could cause untold damage to crypto investors.

## Conclusion

It is clear that the crypto industry is full of fraudulent, unlawful, illegal, and criminal behavior. Unfortunately, that sordid record does not appear to have any influence on those seeking to deregulate and unleash crypto on the American people. For example, recent news reports [indicate](#) that the SEC is reducing the number of enforcement personnel dedicated to crypto cases. This means there will be fewer “securities cops on the beat” to monitor crypto lawbreakers. The same seems to be happening at the CFTC and at other regulators and prosecutors. Hardworking Americans stand to suffer as a result. These Americans don't have millions of dollars to donate to political campaigns, unlike the millions of dollars the crypto industry [spent](#) during the 2024 election. But these ordinary Americans are the ones who suffer from the rampant fraud and abuse in the crypto sector. Congress needs to ensure that any regulatory regime for crypto protects these Americans.



Better Banks | Better Businesses

Better Jobs | Better Economic Growth

Better Lives | Better Communities

**Better Markets** is a public interest 501(c)(3) non-profit based in Washington, DC that advocates for greater transparency, accountability, and oversight in the domestic and global capital and commodity markets, to protect the American Dream of homes, jobs, savings, education, a secure retirement, and a rising standard of living.

Better Markets fights for the economic security, opportunity, and prosperity of the American people by working to enact financial reform, to prevent another financial crash and the diversion of trillions of taxpayer dollars to bailing out the financial system.

By being a counterweight to Wall Street's biggest financial firms through the policymaking and rulemaking process, Better Markets is supporting pragmatic rules and a strong banking and financial system that enables stability, growth, and broad-based prosperity. Better Markets also fights to refocus finance on the real economy, empower the buy-side and protect investors and consumers.

For press inquiries, please contact us at [press@bettermarkets.com](mailto:press@bettermarkets.com) or (202) 618-6430.



[SUBSCRIBE](#) to Our Monthly Newsletter

FOLLOW US ON SOCIAL



2000 Pennsylvania Avenue NW | Suite 4008 | Washington, DC 20006 | 202-618-6464 | [www.bettermarkets.org](http://www.bettermarkets.org)

© 2024 Better Markets, Inc. All Rights reserved.