Digital Asset Crime

Are we still early?

WRITTEN BY **CARLO D'ANGELO** AND **CARLOS GARCIA**

"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution."

—Satoshi Nakamoto[1]

It's likely no coincidence that the pseudonymous person, or group of persons, known as Satoshi Nakamoto unveiled the plan for bitcoin—a purely decentralized peer-to-peer electronic cash system—just as the world plunged into the depths of the 2008 global financial crisis. But despite all the financial carnage that resulted from the 2008 collapse, crypto has been slow to gain mass-adoption.

Although Web3 and decentralized blockchains offer seemingly limitless opportunities for consumers and businesses, critics continue to push the narrative that crypto is only good for facilitating Ponzi schemes and fueling Dark Web marketplaces. But recent reports of rising inflation, bank failures, and currency debasement—ironically similar to the headlines we saw back in 2008—may well draw new users to crypto who see it as a hedge against these institutional risks. And this potential increase in crypto adoption will inevitably draw the continued attention of criminal enterprises and other bad actors who seek to capitalize on unsuspecting new users of this technology.

There is no denying that blockchain technology is rapidly disrupting many sectors of the world economy. However, with new technological advancements, come new risks. And the blockchain is no exception. In particular, cryptocurrencies and non-fungible tokens, or NFTs, have been mainstays as newsworthy headlines with opposing opinions that are as divided as partisan politics during an election cycle.

This article is intended to hit the critical points of digital asset crime while providing fellow attorneys with a more cogent idea of what to look for as the need for knowledgeable defense attorneys and prosecutors increases.[2]

Blockchain crimes are primarily observed in three categories: (1) the use of digital assets to pay for illicit goods, (2) financial crimes including money laundering and tax evasion, and (3) consumer-focused scams colloquially referred to as "rug pulls." Common in nearly every criminal situation is the anonymous nature of digital wallets, identities, and transactions, which can make it difficult to hold the correct bad actors accountable. Although the vast majority of peer-to-peer digital asset transactions facilitate the lawful and efficient transfer of funds without the need for slow and costly intermediaries, bad actors have seized upon this technological revolution to come up with new and creative ways to defraud consumers.

For a thief to steal one's digital assets, they must first gain access to a user's wallet. Digital assets are generally either stored on a decentralized or a centralized exchange wallet. A decentralized exchange, or DEX, is a type of cryptocurrency exchange wallet that operates on a peer-to-peer network, rather than relying on a centralized authority to manage and execute trades. A DEX can offer greater privacy and security, since users retain control of their private keys and funds, rather than entrusting them to a centralized intermediary. However, DEXs can also be more complex to use than centralized exchanges and generally have no identity verification protocol, such as Know Your Customer, or KYC, or Anti-Money Laundering, or AML, standards. On the other hand, major centralized crypto exchanges that do business in the United States are required to comply with some measures of KYC and AML standards under the federal Bank Secrecy Act and applicable state money transmitter licensing laws. Although crypto advocates believe that it is essential to preserve the decentralized and pseudonymous nature of digital asset transactions, these aspects of blockchain technology can also be abused by bad actors because they frustrate a government's ability to investigate and prosecute fraud and tax evasion schemes.

Different from a DEX, platforms like Coinbase and Kraken provide investors with a centralized exchange, or CEX, that holds custody of their digital assets and allows users to access those assets via the platform's hosted wallet accounts. Decentralization advocates warn that the use of "hosted" wallets via a CEX, of course, runs afoul of crypto rule number one—namely "not your keys, not your crypto." A person who holds their digital assets in a CEX wallet sacrifices self-custody benefits that come with a DEX because the exchange maintains control over the private user key to that wallet. Consumers therefore entrust the CEX to custody their digital assets rather than being themselves responsible for holding the private key to the account. The benefit of holding your crypto on a CEX is it presumably provides a more robust layer of institutional security to protect against hackers and fraudulent schemes. The downside is that if the CEX is hacked, collapses, or is mismanaged, then investor assets are at risk of being stolen, lost, or mishandled. Conversely, the downside to self-custody on a DEX is that you, as the wallet holder, are responsible to secure your own private key to your account as opposed to letting the CEX secure the assets for you. If, for example, a DEX user falls prey to a phishing scam or clicks on a bad link, then they are at risk of losing all the digital assets in their wallet.

Blockchain crime scams target both cryptocurrency and NFT holders[3] with equal impunity and have recently drawn increased attention from law enforcement and prosecuting entities across the globe. In 2020, for example, the U.S. Department of Justice published the first-ever Crypto Currency Enforcement Framework. The DOJ noted that although "cryptocurrency represents a transformative way to store and exchange value" this technology also plays a "role in many of the most significant criminal and national security threats our nation faces."[4]

Generally, blockchain crime schemes follow a very simple roadmap. Bad actors first steal the digital assets through some

form of a wire fraud scheme. Bad actors then attempt to conceal those digital assets through software protocols that enable them to "tornado" the crypto assets across multiple wallets. The process of "tumbling" or "mixing" the crypto assets across these multiple wallets is done to cover the bad actor's tracks and frustrate law enforcement's ability to trace victim funds. Once the crypto assets have been scattered across these multiple wallets, thieves must then try to off-ramp the crypto on a CEX and convert it to fiat currency. This phase of the blockchain crime scheme generally involves the recruitment of unlicensed or illicit money changing services to assist in laundering the crypto funds so they can be converted to a fiat currency that the bad actors can then spend on goods and services.

According to Chainalysis, in 2021, there was an estimated $15.8 trillion in reported cryptocurrency transactions.[5] This volume represents a 567% increase in transactions over the previous year.[6] And with this increase in transaction volume, we have seen a significant uptick in digital asset related crimes.[7] Chainalysis also noted that in 2021, blockchain criminal activity reached an estimated all-time high of $18 billion.[8] This figure represents a significant rise from the $7.8 billion estimate reported for the previous year.[9] Chainalysis further noted in its recently published 2023 Crypto Crime Report that despite a market downturn in 2022, "illicit transactions rose for the second consecutive year, hitting an all-time high of $20.6 billion."[10] In response to this alarming trend, the White House recently released an executive order directing the DOJ to prepare a report on recommendations for combating digital asset crimes.[11] The DOJ's report confirms that blockchain crime presents a significant threat to the United States and offers a comprehensive outline of the role law enforcement should play "in detecting, investigating and prosecuting criminal activity related to digital assets."[12] Although we are still at the very early stages of this enforcement initiative, there have been several recent noteworthy criminal prosecutions by the DOJ, including the $4.5 billion Bitfinex bitcoin hack and money laundering case,[13] the FTX collapse and indictment of its founder Sam Bankman-Fried,[14] the OpenSea NFT[15] and Coinbase[16] "insider trading" fraud schemes, and the Frosties NFT "rug-pull" prosecution.[17]

If you spend enough time around digital asset and Web3 enthusiasts, you will no doubt hear the phrase "we are still early." And although we are indeed still very early to the party when it comes to the innovative and transformative possibilities of digital assets, its continued growth and mass adoption is very much dependent on consumers being able to securely and safely conduct blockchain transactions. **TBJ**

NOTES

1. *Re: Bitcoin P2P e-cash paper,* The Mail Archive (2008), https://www.mail-archive.com/cryptography@metzdowd.com/msg09971.html.
2. When referencing "digital assets" throughout this article, we are referring to cryptocurrencies and NFTs within the context of blockchain technology. This is NOT a reference to other non-blockchain or non-cryptographically verified assets such as identities, video game skins, or the like, which may also be called "digital assets."
3. Daniel Van Boom, *Seth Green Loses $200K Bored Ape Yacht Club NFT in Phishing Scam,* CNET (2022), https://www.cnet.com/personal-finance/seth-green-loses-200k-bored-ape-yacht-club-nft-in-phishing-scam/.
4. *Cryptocurrency Enforcement Framework,* Attorney General's Cyber-Digital Task Force Cryptocurrency Enforcement Framework (2020), https://www.justice.gov/archives/ag/page/file/1326061/download.
5. Chainalysis Team, *Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High Value, All-Time Low in Share of All Cryptocurrency Activity,* Chainalysis (Jan. 6, 2022), https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/.
6. *Id.*
7. *Id.*
8. The 2023 Crypto Crime Report, Chainalysis (2023), https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf.
9. *Supra* note 7.
10. *Supra* note 8.
11. "Executive Order on Ensuring Responsible Development of Digital Assets," Joseph R. Biden, The White House, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/.
12. *The Role of Law Enforcement In Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets,* The Report of Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067, U.S. Department of Justice (2022), https://www.justice.gov/d9/2022-12/The%20Report%20of%20the%20Attorney%20General%20Pursuant%20to%20Section.pdf.
13. *Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency,* United States Department of Justice, Office of Public Affairs (Feb. 8, 2022), https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.
14. *FTX Founder Indicted for Fraud, Money Laundering, and Campaign Finance Offenses,* U.S. Department of Justice, Office of Public Affairs (Dec. 13, 2022), https://www.justice.gov/opa/pr/ftx-founder-indicted-fraud-money-laundering-and-campaign-finance-offenses.
15. *Former Employee of NFT Marketplace Charged in First Ever Digital Asset Insider Trading Scheme,* U.S. Department of Justice, U.S. Attorney's Office, Southern District of New York (June 1, 2022), https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-charged-first-ever-digital-asset-insider-trading-scheme.
16. *Three Charged in First Ever Cryptocurrency Insider Trading Tipping Scheme,* U.S. Department of Justice, U.S. Attorney's Office, Southern District of New York (July 21, 2022), https://www.justice.gov/usao-sdny/pr/three-charged-first-ever-cryptocurrency-insider-trading-tipping-scheme.
17. *Two Defendants Charged in Non-Fungible Token ("NFT") Fraud and Money Laundering Scheme,* U.S. Department of Justice, U.S. Attorney's Office, Southern District of New York (March 24, 2022), https://www.justice.gov/usao-sdny/pr/two-defendants-charged-non-fungible-token-nft-fraud-and-money-laundering-scheme-0.

CARLO D'ANGELO
is a criminal defense lawyer, former law professor, and crypto and NFT enthusiast with 25-plus years of experience defending individuals charged with state and federal crimes. In 2022, D'Angelo was a featured speaker at NFT.NYC, where he spoke on the subject of "The Growing Threat that Crypto Criminal Enterprises Pose to NFTs." In a poll conducted by NFT.NYC in 2022, he was nominated as one of the top five lawyers in the category of "Most Expert Handling of the Law and NFTs." D'Angelo is also the co-host of Lex Line, a crypto and blockchain legal podcast available on Apple and Spotify. For more information about D'Angelo, go to www.DAngeloLegal.com.

CARLOS GARCIA
is a criminal defense lawyer and technology enthusiast. He is the former American Bar Association subcommittee chair for NFTs and intellectual property and has been featured as a speaker at numerous conferences including the 2022 ABA Intellectual Property Symposium. Garcia is currently a managing partner for the Texas office of the Defense Firm (GG Law Group) and focuses on the company's federal criminal defense portfolio. He has represented several NFT and crypto projects in complex regulatory and IP issues. Prior to entering private practice, Garcia spent over 16 years in the Army JAG Corps. For more information, go to www.DefenseFirm.Law.