Cryptocurrency Sanctions: Compliance, Enforcement & Impacts

Josephine Wolff and Daniel Drezner
The Fletcher School, Tufts University

Beginning in 2018, the United States has used sanctions to target an increasing number of cryptocurrency actors as part of its efforts to combat financial cybercrime and foreign terrorism. This paper provides a historical overview of the evolution of those sanctions as the government's focus shifted from individual wallet addresses to centralized exchanges to decentralized cryptocurrency mixers. Through more than two dozen interviews with cryptocurrency firm compliance officers, regulators, former regulators, compliance consultants, and blockchain analysis tool providers, we offer insights into the motivations behind these shifts in the targets of U.S. cryptocurrency-related sanctions as well as how firms have adjusted their compliance practices in response to the sanctions and associated enforcement actions. We find that the sanctions and enforcement actions directed at cryptocurrency intermediaries drove significantly more investment in compliance among cryptocurrency firms beginning around 2019, but that these firms also often struggled with resolving ambiguities around how exactly they were supposed to comply with these sanctions.

1. Introduction

In November 2018, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) announced targeted sanctions against two Iranian individuals who had helped the operators of the SamSam ransomware convert their extorted cryptocurrency payments into fiat currency. For the first time, as part of its actions, OFAC identified two digital currency addresses for bitcoin wallets belonging to the two men. OFAC stated that the wallets had been used to process more than 7,000 transactions, totaling millions of dollars' worth of bitcoin. "Regardless of whether a transaction is denominated in a digital currency or traditional fiat currency, OFAC compliance obligations are the same," the Treasury Department stated in its press release about the sanctions.[1]

This marked the beginning of the U.S. government's efforts to include digital assets in its sanctioning practices. Over the next six years, U.S. officials ramped up enforcement of sanctions in the cryptocurrency sector, moving from individual wallets to exchanges like Bittrex to mixers like TornadoCash. By the end of 2024, OFAC had added more than 600 cryptocurrency addresses to its Specially Designated Nationals and Blocked Persons (SDN) list.[2]

As regulators rapidly expanded the list of cryptocurrency-linked sanctions, however, it was not always clear whether cryptocurrency firms were taking their compliance obligations seriously. After all, one of the animating ideas behind cryptocurrencies has been to obviate any need for a government role in the issuance of money by facilitating decentralized peer-to-peer exchange.[3] As with other information technologies, the cryptocurrency sector would be expected to have a wary attitude about government regulation. This attitude meshes with a broader tech sector skepticism about the ability of government officials to acquire the requisite technical knowledge to properly monitor, enforce, or regulate complex innovations.[4]

This study looks at the evolution of cryptocurrency-related sanctions since 2018 and how private sector compliance measures evolved alongside them to better understand how the increasing regulatory effort directed at cryptocurrencies interacted with and impacted both the sector's libertarian leanings as well as the technology's inherent decentralization. Through interviews with regulators, compliance officers, and blockchain analysis tool vendors, we aim to understand what steps crypto firms took to comply with sanctions over the six-year period from 2018 through 2024, and to what extent regulators and private sector compliance workers viewed these steps as effectively stopping, or at least slowing, financial flows to sanctioned entities. The

---

[1] "Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses" (U.S. Department of the Treasury, November 28, 2018), https://home.treasury.gov/news/press-releases/sm556.

[2] "OFAC and Crypto Crime: Every OFAC Specially Designated National with Identified Cryptocurrency Addresses" (Chainalysis, August 10, 2023), https://www.chainalysis.com/blog/ofac-sanctions/.

[3] It is worth remembering that for majority of American history, the federal government neither coined nor printed money. The dollar merely served as a unit of account; commercial banks issued their own banknotes that served as currency. Not until the Federal Reserve Act of 1913 did the United States have a modern central bank responsible for issuing a single currency.

[4] Marion Fourcade and Kieran Healy, *The Ordinal Society* (Cambridge: Harvard University Press, 2024), To be fair, this skepticism also exists in some parts of the political science literature on regulation. See, for example, Nolan McCarty, "The regulation and self-regulation of a complex industry," *Journal of Politics* 79 (October 2017): 1220-1236.

central research questions we aim to address are: How have U.S. cryptocurrency-related sanctions evolved since 2018? What motivated these changes? How has compliance with cryptocurrency-related sanctions changed and what role have enforcement actions against crypto firms played in those changes? And, how do public and private sector stakeholders perceive the effectiveness of these sanctions at achieving their aims?

Due to the inherent decentralized properties of digital assets, as well as private sector resistance to regulation, one could hypothesize that state efforts to extend sanctions enforcement to the crypto sector would encounter fierce resistance. In this scenario, we would expect that official efforts to extend sanctions enforcement to cryptocurrencies would not be successful and that the cryptocurrency sector would resist or bypass any effort by government officials to extend sanctions enforcement to cryptocurrencies.

However, as multiple observers have noted, cryptocurrencies have not actually developed in a decentralized manner.[5] Indeed, the industrial organization of cryptocurrencies has begun to resemble the very financial sector it was supposed to supplant. Instead of an ecosystem dominated by decentralized blockchain ledgers, large corporate exchanges like Binance and Coinbase have become the dominant mechanism through which cryptocurrencies are traded. Similarly, the demand for stablecoins to peg digital assets to the dollar further centralizes the crypto sector. As with traditional finance, these critical nodes provide a gateway through which governments can enforce economic sanctions. Just as OFAC and the Securities and Exchange Commission (SEC) could use large fines on large banks to improve adherence by traditional finance, the prosecutions of Binance and FTX could have a similar effect on the crypto sector.

At the same time, there are reasons to believe that at least some parts of the crypto sector might have an incentive to cooperate more with government officials, particularly with respect to anti-money laundering and countering the financing of terrorism (AML/CFT) policies and sanctions enforcement. The volatility and fraud that have plagued crypto since its beginning—perfectly encapsulated by the collapse of FTX—has been an impediment to expanding the size of its customer base. Demonstrating cooperation with federal authorities is one way to signal that the crypto sector is evolving into a more stable, mature industry. Additionally, the emergence of more predatory actors has also been a wake-up call for some in the sector. North Korea's ability to steal billions of dollars every year in crypto assets has helped to fund its nuclear program.[6] The surge of malicious activity might incentivize crypto firms to cooperate more closely with the U.S. government to prevent further fraud. These dynamics might lead us to expect that official efforts to extend sanctions enforcement to cryptocurrencies would be as successful as similar efforts in traditional finance, and that the cryptocurrency sector would, over time, cooperate with efforts by government officials to extend sanctions enforcement to cryptocurrencies.

---

[5] Fourcade and Healy, *The Ordinal Society*, p. 20; Henry Farrell and Abraham Newman, "Binance and the End of Crypto's Dream to Escape From Government," *Wall Street Journal*, November 24, 2023; Henry Farrell, "The Rise and Fall of Economic Statecraft," *Foreign Affairs* 104 (January/February 2025): 168-174.

[6] Morgan Meaker, "How U.S. Adversaries Are Using Cryptocurrency to Evade Sanctions," *World Politics Review*, September 29, 2020, accessed at https://www.worldpoliticsreview.com/how-sovereign-cryptocurrency-could-weaken-sanctions-and-the-u-s-dollar/.

This study is intended in part as an attempt to understand which of these two trajectories the cryptocurrency sector has more closely followed between 2018 and 2024, as well as the factors that significantly shaped the relationship between cryptocurrency firms and the government during that period. Section 2 describes our methods and analytical approach. Section 3 maps out how cryptocurrency-related sanctions changed over the six-year period covered in our study and what motivated these changes on the part of U.S. regulators. Section 4 looks at the compliance measures that crypto firms implemented during this same period and how compliance shifted with the introduction of new tools, rules, and guidance. Section 5 considers the role of enforcement actions against crypto firms and how those actions influenced the larger compliance landscape in the industry. Finally, Section 6 analyzes perspectives from the public and private sectors on the effectiveness of cryptocurrency sanctions and the possible paths forward for such efforts in the future.

2. Approach

This project relies on a series of semi-structured interviews with 25 individuals conducted between July 2024 and February 2025. Of those 25 participants, at the time of their interviews, three were regulators, five worked for blockchain analytics tool vendors, five worked for think tanks and as independent consultants, and 12 worked for cryptocurrency firms as compliance officers. Additionally, of the 21 people we interviewed who were not regulators, 16 of them had previously spent time working for the U.S. government in the Treasury Department, Justice Department, or intelligence community.

To identify potential interview subjects, we reached out to representatives of the ten largest cryptocurrency exchanges by volume in 2024, as identified by Statista, as well as individuals at the three largest blockchain analytics firms, and regulators who were named in Treasury press releases and guidance about cryptocurrency-related sanctions. Additionally, we contacted individuals who were referred to us by our professional contacts, and asked all of our participants for their suggestions for additional people we should interview.

The interviews for this study ranged from thirty minutes to one hour and were conducted via synchronous video call. All participants were granted anonymity to encourage them to speak candidly about their experiences and perspectives, and the interviews were not recorded to further facilitate a frank exchange of opinions. However, at least one interviewer provided note taking services during each interview to capture the participants' responses. The study protocol was approved by the IRB at Tufts University.

Given the relatively small community of crypto sanctions compliance experts, the reluctance of many current regulators to offer even anonymous interviews, and the fact that many of our participants had worked in the industry in several different capacities, we found that 25 interviews provided a useful window into the inner workings of the industry as well as the regulators who oversee it.

3. Cryptocurrency-Related Sanctions: Timeline and Motivations

In this section, we offer some brief background on U.S. reliance on sanctions as well as the different stages of cryptocurrency-related sanctions during the 2018-2024 timeframe.

3.1 Background on Sanctions

Economic sanctions have been an integral part of foreign policy for more than a century.[7] After the globalization of the 1990s, however, the United States increasingly utilized financial statecraft as a means of threatening and implementing economic sanctions. The Clinton administration's financial abuse initiative led the Treasury Department to enhance its anti-money laundering (AML) capacities, including notifying banks of jurisdictions suspected of having lax AML standards. In the wake of the September 11, 2001 terrorist attacks, the passage of the USA Patriot Act gave Treasury officials considerable discretion to take aggressive actions to counter foreign terrorism (CFT).[8] This included Section 311, which empowered the Treasury secretary power to designate "primary money laundering concerns" and apply countermeasures to specially designated individuals, entities, and jurisdictions without needing to prove criminal culpability. [9]

For multiple foreign policy reasons, over the past quarter-century the United States has relied on financial measures more than trade restrictions to implement economic sanctions.[10] First, for American policymakers, using the financial channel to impose sanctions plays to U.S. strengths: the dollar's role as the global reserve currency and the centrality of U.S. capital markets. As Henry Farrell and Abraham Newman have noted, the global need for dollars to conduct cross-border exchange allows U.S. officials to use corresponding banking accounts in the United States as a chokepoint to restrict access to targeted entities and jurisdictions.[11] The extension of U.S. control over the Society for Worldwide Interbank Financial Telecommunication (SWIFT), the dominant messaging mechanism for traditional finance, increased U.S. coercive power.

Second, financial sanctions can be imposed on specially designated individuals and targeted entities without necessarily curtailing broader financial flows. Financial sanctions like asset freezes can be designed to harm elites in targeted jurisdictions. Financial measures hurt holders of capital—i.e., the elites—which increases the likelihood of successful coercion.

Third, in contrast to trade sanctions, financial restrictions can be amplified rather than undercut by the private sector. The incentive to bust trade sanctions through black-market activity makes sense for local traders with minimal interest in accessing U.S. markets. The same cannot be said for banks that must be concerned about their global reputations and their access to dollars.

---

[7] See Nicholas Mulder, *The Economic Weapon* (New Haven: Yale University Press, 2022), for a relevant history.
[8] Juan Zarate, *Treasury's War* (New York: PublicAffairs, 2013); Henry Farrell and Abraham Newman, *Underground Empire* (New York: Henry Holt, 2023).
[9] Zarate, *Treasury's War*. See also Edward Fishman, *Chokepoints: American Power in the Age of Economic Warfare* (New York: Penguin, 2025).
[10] Daniel Drezner, "Global Economic Sanctions." *Annual Review of Political Science* 27 (2024): 9-24
[11] Farrell and Newman, Underground Empire. See also Henry Farrell and Abraham Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44 (Summer 2019: 42-79.

Private sector de-risking and AML/CFR enforcement therefore can act as a force multiplier for sanctions.

The rise of U.S. financial sanctions has been matched by an increase in the compliance structures of traditional financial institutions. Both the federal government and the financial sector have moved down the learning curve in terms of monitoring and enforcement. Treasury, particularly OFAC, learned that high-profile enforcement actions—also referred to as "whale-hunting"—could incentivize financial firms to adhere to AML/CFT guidelines, including fines in the billions of dollars.[12] Traditional financial institutions reacted to this by developing in-house compliance departments and contracting third-party tools to ensure that they did not knowingly facilitate financial crime or terrorist activity. Over time, commercial banks and other significant financial institutions have invested considerable sums in know-your-customer measures.[13] By the 2010s, systemically financially important institutions were routinely cooperating with Treasury to enforce U.S. sanctions, providing real-time information about financial transactions.[14]

This de-risking concomitantly increased the cost of legitimate cross-border transactions with some countries, such as Somalia or Yemen. Ironically, the rising costs of such transactions was one of the original motivations for cryptocurrencies. The original 2008 paper proposing bitcoin noted the increase in transaction costs as stifling economically beneficial exchanges: "Merchants must be wary of their customers, hassling them for more information than they would otherwise need." The use of blockchain technology would enable "a system for electronic transactions without relying on trust."[15]

While cryptocurrencies can enable transactions without concern for fraudulent double-spending, their very anonymity also facilitates illicit exchanges beyond the purview of traditional finance.[16] Indeed, sanctioned countries such as Russia have legalized cryptocurrencies precisely to facilitate sanctions-busting.[17] Over time, the federal government has expanded its sanctioning and enforcement activities with respect to cryptocurrencies, beginning with individual wallets, moving to cryptocurrency exchanges, and then mixers.[18]

3.2 Sanctioning Wallets (2018-2020)

---

[12] Bryan Early and Christopher Preble, "Going Fishing versus Hunting Whales: Explaining Changes in how the U.S. Enforces Economic Sanctions," *Security Studies* 29 (March 2020): 231-267.
[13] Julia Morse, *The Bankers' Blacklist* (Ithaca: Cornell University Press, 2021); Grégoire Mallard and Jin Sun, "Viral governance: How unilateral US sanctions changed the rules of financial capitalism," *American Journal of Sociology* 128 (July 2022): 144-188.
[14] See Daniel McDowell, *Bucking the Buck: US Financial Sanctions & the International Backlash against the Dollar* (New York: Oxford University Press, 2023).
[15] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, accessed at https://static.upbitcare.com/931b8bfc-f0e0-4588-be6e-b98a27991df1.pdf.
[16] Alex O'Neill and Amanda Wick, "Sounding the Alarm on Digitally Enabled Sanctions Evasion," *Lawfare*, October 16, 2024.
[17] Gleb Bryanski, "Russia to allow crypto payments in international trade to counter sanctions," Reuters, July 30, 2024; Bryanski, "Russia is using bitcoin in foreign trade, finance minister says," Reuters, December 25, 2024.
[18] U.S. Government Accountability Office, "Economic Sanctions: Agency Efforts Help Mitigate Some of the Risks Posed by Digital Assets," GAP-24-106178, December 13, 2023, accessed at https://www.gao.gov/products/gao-24-106178.

OFAC began laying the groundwork for cryptocurrency-related sanctions as early as March 2018, when it added a series of questions to its online FAQ related to cryptocurrencies.[19] Following its initial designation of the two bitcoin wallet addresses associated with the Iranian men in November 2018, the Treasury Department ramped up its cryptocurrency sanctions slowly for the next two years during the latter half of the first Trump administration. In August 2019, the United States issued only one set of sanctions that included digital currency addresses when it designated 12 cryptocurrency addresses associated with three Chinese individuals who were sanctioned for international narcotics trafficking.[20] In 2020, three sets of U.S. sanctions came out that included digital currency addresses: one in March that listed 20 wallet addresses associated with Chinese nationals who had helped launder stolen cryptocurrency for North Korea,[21] one in September that designated 23 wallet addresses associated with Russians accused of interfering in U.S. elections,[22] and another in September that included 12 addresses linked to Russians accused of stealing cryptocurrency from exchanges.[23]

Within the government during this period, there was some disagreement over whether it was important to include digital currency addresses in sanction actions and about how best to do so. One former regulator recalled, "It was a struggle to get the addresses on the SDN list at all—my boss at the time equated cryptocurrency with Beanie Babies, just a fad that was going to go away. It was a very low priority."[24]

Another former regulator who worked at Treasury during the announcement of these initial digital currency address sanctions noted that there was a lot of debate within the government about how best to add these addresses to the SDN list and whether it made sense to treat them in the same manner as bank accounts. "I wanted to create an entirely separate list of cyber identifiers to include IP addresses, email addresses, bitcoin wallets—things that we knew were associated with malicious activity but we didn't know exactly who they were associated with," the former regulator recalled. "That was ultimately shot down, but I still think that's where we should go, so you can update the list more easily and not need to know first name, last name, date of birth—things that you can't know in the cyber context."[25]

Regulators involved in issuing these initial sanctions also acknowledged that the early sanctions were unlikely to have a major impact given how easy it was for the sanctioned entities to simply

---

[19] See, "560. Are My OFAC Compliance Obligations the Same, Regardless of Whether a Transaction Is Denominated in Digital Currency or Traditional Fiat Currency?" (Office of Foreign Assets Control, March 19, 2018), https://ofac.treasury.gov/faqs/560. "561. How Will OFAC Use Its Existing Authorities to Sanction Those Who Use Digital Currencies for Illicit Purposes?" (Office of Foreign Assets Control, March 19, 2018), https://ofac.treasury.gov/faqs/561. "562. How Will OFAC Identify Digital Currency-Related Information on the SDN List?" (Office of Foreign Assets Control, March 19, 2018), https://ofac.treasury.gov/faqs/562.

[20] "Treasury Targets Chinese Drug Kingpins Fueling America's Deadly Opioid Crisis" (U.S. Department of the Treasury, August 21, 2019), https://home.treasury.gov/news/press-releases/sm756.

[21] "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group" (U.S. Department of the Treasury, March 2, 2020), https://home.treasury.gov/news/press-releases/sm924.

[22] "Treasury Sanctions Russia-Linked Election Interference Actors" (U.S. Department of the Treasury, September 10, 2020), https://home.treasury.gov/news/press-releases/sm1118.

[23] "Treasury Sanctions Russian Cyber Actors for Virtual Currency Theft" (U.S. Department of the Treasury, September 16, 2020), https://home.treasury.gov/news/press-releases/sm1123.

[24] Interview with crypto compliance officer #8, August 19, 2024.

[25] Interview with crypto compliance officer #6, August 2, 2024.

open new digital currency wallets. Still, several of them indicated that sanctioning individuals' cryptocurrency wallet addresses was an important first step for issuing cryptocurrency-related sanctions. "The Iranian wallets that were listed in 2018, sure, these same guys just opened up another wallet," one former regulator said, adding, "Maybe it was sort of simplistic, but it was the beginning."[26]

3.3 Ramping Up: Sanctioning Exchanges & Darknet Markets (2021-2022)

In 2021, cryptocurrency sanctioning activity accelerated and expanded with the introduction of sanctions directed at cryptocurrency intermediaries, rather than individual wallets associated with sanctioned entities. The first of these intermediaries to be sanctioned were cryptocurrency exchanges that the Treasury Department had linked to illicit activities, beginning in September 2021 with the designation of Russian exchange SUEX for facilitating transactions linked to ransomware.[27] Later that year, in November 2021, Treasury sanctioned peer-to-peer exchange Chatex, also for facilitating transactions for the perpetrators of ransomware.[28]

Several former regulators highlighted the significance of the Colonial Pipeline ransomware attack in May 2021 in driving the federal government's focus on ransomware that year and the subsequent sanctions on SUEX and Chatex. Ransomware had been on the Treasury Department's radar for a while—the 2018 sanctions that listed the first digital currency addresses had also been intended to target ransomware groups—but the high-profile attack on a critical infrastructure provider shifted the federal government's perception of ransomware. Instead of being treated as a cybercrime issue, ransomware instead began to be regarded by the Biden administration as a serious national security threat.[29] One former regulator said, "The Colonial Pipeline experience really scared the federal government. That was a huge wake-up call— the fact that ransomware actors were targeting hospitals, schools, infrastructure. We were like, 'What tools do we have to go after this?' And then it was like, 'Hey, Treasury, can we at least stop the money from moving?' "[30]

Growing concerns about the risks associated with ransomware helped spur more aggressive sanctions that targeted entire exchanges, rather than just individual wallets. In large part, this shift was motivated by regulators' fears that sanctions on individual wallet addresses were easily circumvented by criminals opening new wallets as quickly as their old ones were added to the SDN list.[31] One former regulator explained, "As we learned more about the space it became evident that there's a lot of wallets, so sometimes the best thing to do was go after the entire intermediary."[32] Another former regulator noted that these attempts to go after intermediaries with sanctions were the result of significant pressure on the Treasury Department from other

[26] Interview with crypto compliance officer #4, December 17, 2024.
[27] "Treasury Takes Robust Actions to Counter Ransomware" (U.S. Department of the Treasury, September 21, 2021), https://home.treasury.gov/news/press-releases/jy0364.
[28] "Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange" (U.S. Department of the Treasury, November 8, 2021), https://home.treasury.gov/news/press-releases/jy0471.
[29] Interview with regulator #1, December 20, 2024.
[30] Interview with crypto compliance consultant #2, July 9, 2024.
[31] Interview with crypto compliance officer #4.
[32] Interview with crypto compliance consultant #2.

parts of the U.S. government to do something about ransomware at the time. “Treasury is always asked to do something when other agencies can’t or won’t,” the former regulator explained. “With ransomware, there was a lot of pressure coming down from the National Security Council.”[33]

3.4 Sanctioning Mixers (2022-2024)

In May 2022, OFAC sanctioned its first mixer service, Blender.[34] Mixers provide cryptocurrency users with a way to mix together cryptocurrency funds from different wallets and then disperse the funds out to new wallets so that it is more difficult to track the origins of the cryptocurrency involved in the post-mixing transactions. The Blender sanctions were linked to the North Korean Lazarus Group, responsible for the theft of hundreds of millions of dollars’ worth of cryptocurrency. The Treasury Department highlighted in its announcement of the 2020 sanctions that the funds stolen by the Lazarus Group had “allow[ed] the North Korean regime to continue to invest in its illicit ballistic missile and nuclear programs.”[35]

Reports on the ties between North Korea’s cryptocurrency and its weapons programs dated back to a 2019 U.N. report that found North Korea had funded its weapons of mass destruction program by using “cyberspace to launch increasingly sophisticated attacks to steal funds from financial institutions and cryptocurrency exchanges to generate income” totaling roughly $2 billion.[36] That was followed up by another U.N. report in February 2022 that reiterated that North Korea’s stolen cryptocurrency was an “important revenue source” for its continued development of nuclear and ballistic missiles.[37] While it was well known by 2022 that North Korean hackers stole and laundered cryptocurrency, these reports were some of the first to explicitly draw a connection between those stolen funds and the country’s weapons program, leading to a renewed interest in issuing sanctions directed at North Korean hackers, like the Lazarus Group, and the intermediaries they relied on to launder their funds, like Blender. Later in 2022, OFAC sanctioned another mixer service that it had linked to North Korean activity, Tornado Cash,[38] and in November 2023, Treasury issued sanctions against a third mixer service linked to North Korea, Sinbad.[39]

“Preventing North Korea from using its stolen assets to fund its nuclear weapons program is the key,” one regulator said of the efforts to target mixers with sanctions.[40] One former regulator agreed that “the DPRK threat is the animating threat” but added that it was not a threat that made

---

[33] Interview with crypto compliance consultant #4, December 24, 2024.
[34] “U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats” (U.S. Department of the Treasury, May 6, 2022), https://home.treasury.gov/news/press-releases/jy0768.
[35] “Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group.”
[36] Michelle Nichols, “North Korea Took $2 Billion in Cyberattacks to Fund Weapons Program: U.N. Report,” *Reuters*, August 5, 2019, https://www.reuters.com/article/world/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-un-report-idUSKCN1UV1ZX/.
[37] “North Korea: Missile Programme Funded through Stolen Crypto, UN Report Says” (BBC, February 6, 2022), https://www.bbc.com/news/world-asia-60281129.
[38] “U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash” (U.S. Department of the Treasury, August 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.
[39] “Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency” (U.S. Department of the Treasury, November 29, 2023), https://home.treasury.gov/news/press-releases/jy1933.
[40] Interview with regulator #1.

a strong impression on everyone in the industry, explaining, "There's fundamentally just people who do not see this as a national security threat—the idea that North Korea is going to nuke Guam, it doesn't register with people."[41] But other compliance officers and former regulators disagreed, in some cases saying North Korea was the one enemy they felt everyone in the industry could unify against. One former regulator said that emphasizing the North Korean threat had helped forge closer relationships between the regulators and the crypto industry, explaining, "If anything has helped bring people together it is Lazarus Group."[42]

The shift to targeting mixers with sanctions seemed to some regulators like a logical extension of sanctioning addresses and exchanges, with several comparing mixers to tools used to launder fiat currency. "People used to talk about shell companies the same way we talk about mixers today," one former regulator pointed out, adding, "there's value in sanctioning those because you are adding friction to that process of laundering stolen funds."[43] On the other hand, some participants noted that this analogy sometimes made it harder for stakeholders within the government to get on board with mixer service sanctions. "There's a lot of people in Congress who are like, 'I've got 15 shell companies stood up in the Caymans! What's the big deal?' " a different former regulator recalled of pushback to some of the early mixer sanctions.[44]

Of the three mixer services that Treasury targeted, Tornado Cash was the most complicated and controversial to sanction because it was a decentralized service that made use of smart contracts to mix funds, rather than operating via a centralized organization or "custodial mixer" like Blender or Sinbad. This meant that there was no way for Treasury to "shut down" Tornado Cash, because it could operate without any organizational infrastructure or oversight. One former regulator highlighted this difference as a reason the government should have been more careful about going after Tornado Cash with sanctions. "If we consider behavior change as the measure of success, then Iran and North Korea could conceivably change their behavior, but we can't change the behavior of Tornado Cash—it's an autonomous system, it can never get delisted," the former regulator explained.[45]

Other former regulators noted that the Tornado Cash sanctions were especially complicated because of the risk that legitimate actors using the service would be affected by them. "Going after Tornado Cash—it took almost two years to get that through counsel because we knew that licit actors could get caught up in that," one former regulator recalled.[46] Multiple former regulators criticized the Tornado Cash sanctions as poorly designed, difficult to enforce, and inviting lawsuits by legitimate actors whose funds were impacted. "Treasury moved a little too fast before it really understood the tech," one former regulator said of the decision to sanction Tornado Cash.[47] Another former regulator agreed, saying, "I think the designation of Tornado Cash was probably a mistake. Treasury overshot it, spooked people, and caused firms to go dark.

[41] Interview with crypto compliance consultant #4.
[42] Interview with crypto compliance officer #2, January 7, 2025.
[43] Interview with blockchain analytics vendor #1, July 15, 2024.
[44] Interview with crypto compliance consultant #2.
[45] Interview with crypto compliance officer #2.
[46] Interview with crypto compliance consultant #2.
[47] Interview with crypto compliance consultant #3, January 7, 2025.

That was what we feared when I was [in government] and why we declined to do it, because we thought it would push people to go dark instead of getting them to build compliance."[48]

4. Compliance with Cryptocurrency Sanctions

There was a clear consensus among the interview subjects that compliance at crypto firms had gotten more rigorous and better funded beginning around 2019, especially at larger crypto firms. They attributed this change to three interlocking trends: ongoing guidance from the government about how to comply, firms hiring former regulators to lead their compliance teams, and improved blockchain analytics tools. Several compliance officers stressed that crypto firms had to ramp up compliance programs that had taken banks years to build out. "Banks have had 120 years to build up their compliance programs and then you have crypto that crops up so quickly and you're expected to be at that same level and it's not easy," one compliance officer said, adding "How do you comply given that we are not a bank and we haven't put hundreds of millions of dollars into a program?"[49]

Others also stressed the considerable costs of building out compliance programs. "Compliance used to be an afterthought, now it's becoming incredibly expensive because compliance is incredibly manual when it comes to the crypto industry and anything that's manual is expensive to maintain," one compliance officer explained.[50] The manual work required of compliance officers included a growing need to monitor any cryptocurrency addresses and accounts linked to those that were sanctioned, beyond those that had been explicitly added to the SDN list, to shield against indirect exposure to sanctioned entities. "It went from just 'we're blocking the addresses on the list' to the point where it became clear we could do indirect exposure blocking," one compliance officer explained.[51]

In particular, compliance officers pointed to blockchain analytics tools as an important piece of ramping up their compliance programs, but also a source of many subjective decisions about how to use the information and act on the alerts that those tools provided. The hiring of compliance officers out of the government was another driver of more mature compliance programs, participants agreed, but there were sometimes culture clashes between the libertarian ethos of crypto firms and the perspectives and attitudes of former regulators. And even as the compliance expertise within these firms expanded, there was still considerable uncertainty about some of the ambiguities surrounding cryptocurrency sanctions. Three areas of uncertainty that compliance officers highlighted included questions about whether they had to continue monitoring and flagging past transactions in perpetuity, how far back they had to trace each transaction before clearing it, and what they were expected to do when it came to monitoring their clients for VPN usage.

4.1 Reliance on blockchain analytics tools

[48] Interview with crypto compliance officer #2.
[49] Interview with crypto compliance officer #3, August 1, 2024.
[50] Interview with crypto compliance officer #6.
[51] Interview with crypto compliance officer #2.

All of the compliance officers we interviewed at crypto firms used tools from at least one of the three primary blockchain analytics firms, Chainalysis, TRM, and Elliptic, for tracking and flagging suspicious transactions. One compliance officer said the existence of these tools helped drive the maturation of compliance programs not just because they made it simpler for crypto firms to outsource some of the work associated with sanctions compliance, but also because "as it became more known what Chainalysis, Elliptic, and TRM could do, firms couldn't deny that it was possible" to comply with sanctions.[52]

The tools sold by these firms typically identify suspicious wallet addresses and transactions that are linked to sanctioned entities and flag those transactions for clients, who can then decide whether or not to allow them. One blockchain analytics tool vendor explained, "While just a few crypto addresses may be included as identifiers in a designation, a sanctions compliance team is still responsible for any additional addresses that are owned by that sanctioned entity. This is where blockchain analytics can capture this risk efficiently. The benefit of our tools is they can use clustering to turn just a few addresses in a designation into hundreds of thousands, if not millions."[53]

This clustering can be done in a variety of different ways, not just by tracking the transactions between different entities on the blockchain, but also by looking at public announcements by people soliciting contributions to their digital currency wallets, analytics vendors said. "If Farrukh Fayzimatov [a sanctioned Al Qaeda financial facilitator] is soliciting donations for motorbikes via cryptocurrency, then all I have to do is monitor his social media for the address he's telling people to send funds to and add it to the list," one vendor explained, saying that this made it less effective for sanctioned individuals to constantly change their wallet addresses. "I liken it to escaping prison and setting up a fire at night half a mile from the prison boundary," the vendor said. "There's really no way to collect donations at scale while also being public and also being sanctioned."[54]

Expanding a short list of sanctioned digital currency addresses to a list of millions, however, can create headaches and additional work for compliance officers, several of them said. "When I first got here we had about 25,000 alerts a month from Chainalysis," one compliance officer said. "Do you think a team of 12 has time to look at 25,000 alerts?"[55] To help prioritize these alerts, blockchain analytics tools often categorize or color code the alerts into high- medium- and low-risk (or red/yellow/green) labels to differentiate between transactions that are definitely and directly linked to sanctioned entities, those that have some indirect link to sanctioned entities, and those that appear to be completely legitimate. Almost everyone blocks transactions that are directly linked to sanctioned wallets and allows those that have no indirect ties, but the trickiest category is that "yellow" or medium-risk group of transactions and individuals that appear to have some indirect exposure to sanctioned entities, compliance officers said. "There are crypto firms that see someone flagged as yellow that they just want to completely deny their transactions, there are companies where that prompts a more in-depth analysis of the individual to try to figure out what's this person's background and then they can say, 'we've done our own

[52] Interview with crypto compliance officer #2.
[53] Interview with blockchain analytics vendor #2, July 10, 2024.
[54] Interview with blockchain analytics vendor #2.
[55] Interview with crypto compliance officer #6.

analysis, we're comfortable with them, but we're just going to screen them more regularly.' In general, though, we've seen less willingness by clients to accept customers in that yellow zone over time," one compliance consultant said. [56]

This category of transactions with some indirect exposure to sanctioned entities grew significantly with the introduction of sanctions on intermediaries, several participants noted, since these intermediaries often touched a wide range of cryptocurrency users. In some cases, sanctioned intermediaries could even be used deliberately to try to disrupt legitimate users' transactions, as in the 2022 incident where a user "dusted" celebrities' crypto wallets by sending them small amounts of Ethereum funds from Tornado Cash wallets. "It becomes a problem if there are larger intermediaries being sanctioned because you'll see that the wallet you're receiving funds from has some indirect exposure to Tornado Cash, but how do you differentiate the Tornado Cash funds from the rest? Blocking any wallet that has touched Tornado Cash — that's an easy decision but it doesn't really work," one compliance officer explained.[57]

Several compliance officers emphasized that when they saw indirect exposure of this nature to sanctioned entities they had to make "risk-based decisions" about which transactions and clients to allow on their platforms. In fact, 2021 OFAC guidance explicitly encouraged "a risk-based approach to sanctions compliance" on the grounds that "there is no single compliance program or solution suitable to every circumstance or business. An adequate compliance solution for members of the virtual currency industry will depend on a variety of factors, including the type of business involved, its size and sophistication, products and services offered, customers and counterparties, and geographic locations served."[58] One compliance officer said of this advice from OFAC, "I applaud them for putting out the virtual currency guidance, but I don't think the guidance is very clear at all."[59]

As one example of how a firm might tailor its compliance approach, one compliance officer explained that at their firm the scrutiny of different yellow alerts depends on the size of the transaction and how much of the transacted funds are "tainted," or linked to a sanctioned entity. "I only want to see those middle levels when it's a large dollar amounts," the compliance officer explained about which of the many blockchain analytics tool alerts they manually review. The officer continued, "Ninety-nine percent of what I see is someone in the UK sending $10 to their brother in Iran. It's a waste of time in my opinion, to monitor that, and we're not going to get rid of those clients unless they keep doing it again and again after we've blocked the transaction. If it's 90 percent taint or above, we will take a look at it no matter what the dollar amount is. If it's 80 percent taint, we'll take a look if it's over $2,000. If it's 60 percent taint, I don't want to take a look at it until it's over $10,000. If it's 20 percent taint, then I don't want to see it until it's over $20,000."[60]

[56] Interview with crypto compliance consultant #1, July 29, 2024.
[57] Interview with crypto compliance officer #8.
[58] "Sanctions Compliance Guidance for the Virtual Currency Industry" (Office of Foreign Assets Control, October 2021), https://ofac.treasury.gov/media/913571/download?inline.
[59] Interview with crypto compliance officer #6.
[60] Interview with crypto compliance officer #6.

Purchasing analytics tools can also be an important signal for crypto firms to show regulators that they are taking compliance seriously, some vendors and compliance officers said. "It can become a reputational branding exercise," one consultant explained, adding, "You signal to Treasury, 'hey, we've bought Chainalysis, we're good.' "[61] A former vendor also noted that when working for a blockchain analytics vendor, "we saw companies buy our product just so they could check the box and say 'we have a transaction monitoring tool,' but they didn't actually do anything with it."[62]

Vendors also said that they had seen firms moving in the direction of tailoring their tools to their own risk appetites and approaches. "I've been at [a blockchain analytics vendor] a little over two and a half years now, and when I started almost everyone was at a 'How do we do this? If [our tool] says it's bad then it's bad' stage of compliance, but since then many more of them are taking a more nuanced approach," one vendor said.[63] Compliance officers at larger exchanges echoed this sentiment, with one saying, "We moved from 'we're just going to rely on a screening provider to do [sanctions compliance]' in 2018 to 'no, we actually need to be committed to complying with sanctions, not just relying on what the screening provider says or does' by 2021."[64]

4.2 Hiring regulators into compliance positions, cultural fit

In addition to the uptake of more sophisticated blockchain analytics tools, another important factor driving the maturation of crypto firm compliance processes was the hiring of numerous former regulators into the industry around 2020, several participants said. "In 2019 and 2020 more people from government were going to crypto firms—people from DOJ, people from Treasury—you've got veterans of these organizations going to the private sector in droves," one compliance officer said.[65] Some participants were skeptical that these hires really reflected a strong commitment to compliance. "I would be wary of the reputational laundering going on—you hire a bunch of former Treasury and Justice people and then your reputation is obviously improved, because they couldn't possibly be turning a blind eye to illicit behavior," one consultant said.[66]

Several former regulators and compliance officers flagged that there was a bit of a culture clash between the people coming out of government and the ones who ran cryptocurrency companies especially in the early days of the compliance hiring. "There was a period where it was very much, 'hey, you are the cops, we don't need a narc hanging out here,' and that is very much past," one former regulator turned compliance officer said.[67] A compliance consultant put it more bluntly, "Running under all of crypto is the pink sludge of libertarianism—they do not think laws apply to them, period."[68]

---

[61] Interview with crypto compliance consultant #4.
[62] Interview with crypto compliance consultant #3.
[63] Interview with blockchain analytics vendor #2.
[64] Interview with crypto compliance officer #8.
[65] Interview with crypto compliance officer #4.
[66] Interview with crypto compliance consultant #5, January 27, 2025.
[67] Interview with crypto compliance officer #2.
[68] Interview with crypto compliance consultant #3.

Another former regulator echoed a similar sentiment but said it was less true of the largest firms, explaining, "There is a cultural issue here—there are people within the cryptocurrency community who fundamentally do not want to comply with a bunch of US laws. Sure, there are companies that do want to invest in compliance, but they are a very small minority and they're a little bit disproportionate in terms of their economic power because they tend to be the biggest firms."[69] Even the largest crypto firms that hired significant numbers of former regulators seem to have somewhat mixed sentiments when it comes to compliance, one consultant said. "Coinbase has invested substantially in compliance, they've taken the slow and expensive route, and they have hired a number of my former colleagues to be able to have a serious compliance team," the former regulator said. "But they're the funders of the Tornado Cash litigation—they're actively funding litigation to undermine the architecture of the sanctions."[70]

Several participants noted that given this culture clash, working in compliance for crypto firms requires a unique and somewhat contradictory set of skills and beliefs. "Those of us who work in crypto sanctions, we are an interesting bunch," one former regulator turned compliance officer said. "We believe in the technology, we believe in privacy and economic freedom and getting these technologies into the hands of people who need them, but we also understand the importance of national security and complying with laws and the need to balance those things."[71]

4.3 Monitoring past transactions

Despite a clear consensus that crypto sanctions compliance had matured considerably since 2018, there were several points where compliance officers noted considerable divergence in how firms approached compliance. One area that was raised repeatedly by compliance officers was the question of how much monitoring they were required to do of past transactions and when they were required to report such transactions if they were later flagged as suspicious. OFAC's 2021 guidance suggests that "virtual currency companies may consider conducting a historic lookback of transactional activity after OFAC lists a virtual currency address on the SDN List to identify connections to the listed address."[72]

In general, compliance officers expressed a strong sentiment that it was unfair that crypto firms were seemingly expected to monitor their past transactions in perpetuity due to the volume of data available about blockchain transactions. "Compliance officers are constantly barraged with alerts about a client who looked fine the day they came in and then it turns out, years down the road, they might be sanctioned," one compliance consultant explained. "The visibility in crypto is a double-edged sword. On the one hand, look at how traceable it is, we can go back seven years! But also, now you can go back seven years, so you have to report all this stuff that wasn't a problem at the time."[73]

Compliance officers said they routinely learn that transactions are related to sanctioned entities after they have been processed. "One of the biggest issues we have is late attribution—we settle

[69] Interview with crypto compliance consultant #2.
[70] Interview with crypto compliance consultant #4.
[71] Interview with crypto compliance officer #9, January 17, 2025.
[72] "Sanctions Compliance Guidance for the Virtual Currency Industry."
[73] Interview with crypto compliance consultant #3.

transactions with multiple clients today and I don't find out that they're related to Garantex until 3 or 5 days later," one compliance officer said.[74] Another compliance officer echoed this concern, saying that on average, it took 120 days for their multiple blockchain analytics tools to attribute a wallet to Garantex because of how the exchange obfuscated its addresses.[75]

It is unclear when these flagged past transactions have to be reported and how frequently, compliance officers said. "The industry has been discussing do we need to file a voluntary self-disclosure if we learn about an alert after the transaction is processed—and at what cadence? Daily? Quarterly?" one compliance officer said.[76] Another compliance officer expressed frustration with regulators at having to report data to them that's already publicly available. "They want us to send them all of these post facto alerts in a report," the compliance officer said, "I ask myself, what is the value of my sending you data that's already on a public blockchain?"[77]

Additionally, a few people pointed to the lack of clarity on how regularly firms are supposed to rescreen their customer data in light of new sanctions. "OFAC says you should screen customers at onboarding and occasionally afterwards, and what that actually translates to is a wide range of approaches: daily, weekly, monthly, quarterly. So if I screen a customer today and OFAC sanctions them tomorrow I may not know until three months from now," one tools vendor said.[78]

There were also some concerns about whether the reports of past activity made by crypto firms were actually useful to law enforcement. "Companies do get frustrated when they report a bunch of activity and there's absolutely no activity from enforcement officers," one consultant said, adding, "I think it's worth asking, 'Compliance for what?' If law enforcement isn't doing anything with it, or enforcing any of these, then does it matter if we report them?"[79]

4.4 How far do you trace back transactions?

A related compliance concern was the question of how many "hops" a crypto firm is required to trace a transaction back to previous wallets before clearing it of any links to sanctioned entities. "In the tradfi [traditional finance] space you basically just see one hop out; in crypto you can see basically infinite hops out not only before a transaction but also after," a crypto compliance officer explained. "How far back are we supposed to go looking for a link to a sanctioned wallet? Do we stop at ten hops or twenty? Do we keep monitoring the transaction after we accept it? We could track your transactions basically forever."[80]

In part, regulators said, the ambiguity around how far back firms are expected to trace transactions is intentional. One former regulator noted, "When I was at OFAC we thought about should we do an FAQ for how many hops you have to go back, and we decided definitely no, because the bad guys would just go one hop more than that."[81] Another former regulator said, "I

[74] Interview with crypto compliance officer #6.
[75] Interview with crypto compliance officer #9.
[76] Interview with crypto compliance officer #1, December 18, 2024.
[77] Interview with crypto compliance officer #9.
[78] Interview with blockchain analytics vendors #4 and #5, February 11, 2025.
[79] Interview with crypto compliance consultant #5.
[80] Interview with crypto compliance officer #2.
[81] Interview with crypto compliance officer #6.

think it would be really irresponsible to put a number of hops in formal guidance, I have no idea what the number of hops would be. Let's go back until we're not really concerned about it anymore."[82]

Current regulators echoed these sentiments, saying it was up to individual institutions to set appropriate thresholds for their transactions. "I don't think that ten or twenty hops is something we can ask for," one regulator said, adding, "it's more that the thresholds that the institution sets have to make sense. It's more like a descriptive set of rules, you have to make sure you can detect such transactions."[83] The descriptive, or flexible, nature of this compliance guidance is both a feature and a bug, another regulator said, in that it forces firms to develop more tailored compliance regimes but also allows room for variable standards of compliance. "We have to have a risk-oriented focus and not a checklist mindset in order to really comply with these rules. There's not a one-size-fits-all approach, but we have been pushing especially in recent years to consider sanctions compliance from ground zero, early on in the process," the regulator explained.[84]

4.5 VPN Monitoring

One final area of ambiguity that compliance officers flagged in cryptocurrency sanctions compliance was what they were supposed to do to monitor virtual private network (VPN) use by sanctioned entities. The 2021 OFAC guidance states that one risk indicator for transactions may be individuals who "Attempt to access a virtual currency exchange from an IP address or VPN connected to a sanctioned jurisdiction." It further recommends that firms use geolocation tools to "identify IP misattribution, for example, by screening IP addresses against known virtual private network (VPN) IP addresses and identifying improbable logins (such as the same user logging in with an IP address in the United States, and then shortly after with an IP address in Japan)."[85]

Some compliance officers said they saw a disparity in what was expected of them versus traditional banks when it came to VPNs. "No bank in America cares that you're on a VPN," one compliance officer said. "I asked a colleague in traditional finance, 'Are banks looking at who's spoofing their location to make sure they're not servicing individuals in sanctioned locations?' And the guy looked at me and said, 'we're not the NSA.' "[86]

Another compliance officer highlighted the irony of the cryptocurrency industry trying to prevent people from using privacy-enhancing technologies like VPNs. "We're not going to not let people use VPNs, I mean come on, we're in the crypto industry," the compliance officer said, adding, "We're trying to figure out how to appease regulators with no clear guidance on what to do in the VPN space."[87]

[82] Interview with blockchain analytics vendor #1.
[83] Interview with regulator #2, July 10, 2024.
[84] Interview with regulator #1.
[85] "Sanctions Compliance Guidance for the Virtual Currency Industry."
[86] Interview with crypto compliance officer #9.
[87] Interview with crypto compliance officer #6.

Regulators again insisted that it was up to individual firms to develop a protocol for monitoring VPN use and suspect IP addresses tailored to their customer base and risk-based approach. "No one is trying to forbid the use of VPNs," one regulator said, adding, "we're just saying if someone seems to be moving between two countries in a way that is physically impossible—jumping continents in a matter of seconds—maybe take a closer look at that user."[88]

5. Enforcement Actions

The enforcement actions taken by the U.S. government against crypto firms for failing to institute sufficient sanctions compliance checks helped drive more investment in compliance programs, many participants agreed. One Treasury official stated that they viewed OFAC enforcement actions as a means of communicating and messaging to the cryptocurrency sector about compliance.[89] However, interviewees differed on their perspective as to whether these enforcement actions helped clarify expectations for crypto firms and whether the resulting penalties were sufficient to deter careless compliance practices.

"Before 2020, I think there was an early period of head-in-the-sand, plausible deniability and there were a lot of consultants in the AML crypto space that for literally like $500 would give you a compliance opinion and they'd be like, 'I don't think you're a bank, so you don't need to do anything,' " one compliance officer explained, adding, "Then, after enforcement actions started, it became clear that those opinions weren't worth anything."[90]

5.1 Binance Enforcement Action

The enforcement actions helped draw the attention of crypto firm leadership to the issue of compliance, one consultant said. "When these enforcement actions happen, they're going to look at the people in charge," the consultant explained. "So now we're not just having calls or conversations with the business folks, it's jumped up to c-suite execs. With Binance getting the largest money laundering penalty ever, it's like, this is serious now, this is D Day."[91]

But several participants said the penalties were not sufficiently severe to really motivate firms to invest more heavily in compliance. They pointed, in particular, to the Binance enforcement action in November 2023, when the exchange's CEO pleaded guilty to failing to maintain an effective AML program and the company agreed to pay $4 billion in fines and penalties.[92] One compliance officer said, "Binance seems to have rebounded pretty quickly after having some really serious compliance vulnerabilities. I don't think that's a good lesson learned."[93] Another compliance consultant echoed that opinion, saying, "Binance got off pretty well—it's a lot of

[88] Interview with regulator #2.
[89] Interview with Treasury official #1.
[90] Interview with crypto compliance officer #2.
[91] Interview with crypto compliance consultant #1.
[92] "Binance and CEO Plead Guilty to Federal Charges in $4B Resolution" (U.S. Department of Justice, November 21, 2023), https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.
[93] Interview with crypto compliance officer #12, February 27, 2025.

money to us but it's not a lot of money to them, and their primary concern was keeping their CEO out of jail. He got a slap on the wrist for some really serious criminal behavior."[94]

One of the points made by participants about the Binance enforcement action was how blatant Binance's disregard of sanctions compliance was. For instance, regulators pointed out that Binance had never filed a suspicious activity report with FinCEN, and that compliance employees at the company made jokes, internally, about how easy it was to use the service for laundering illicit funds, with one writing in a chat message, "we need a banner 'is washing drug money too hard these days – come to binance we got cake for you.' "[95] This meant that it was difficult for well-intentioned exchanges to really learn anything from the enforcement, since Binance hadn't been taking any measures to enforce sanctions in the first place. "Binance was egregious; you read the enforcement order and they're saying, 'come here and you can use our platform to launder money,' " one compliance officer pointed out.[96] Still, some participants said, it was important to send the signal that blatant disregard for sanctions would not go unpunished. "The importance to me of the Binance case was that it was so egregious and everyone knew it was happening," one former regulator said, adding, "we would go to an exchange and say, 'you shouldn't do this' and they would say, 'how can that possibly be a problem? Binance has been doing this for years.' So it was helpful in setting a baseline, but it didn't clarify an edge case."[97] Another compliance officer said of the enforcement action, "Binance was such a no-brainer that everyone was like, 'well, it's about time.' "[98]

Another compliance officer pointed out that going after a company that was not headquartered in the United States was also an important signal to the industry. "What that enforcement action did was it let the industry know that the façade of not being incorporated here—that isn't legit, that's not going to shield you from OFAC and the DOJ," the officer explained, adding, "The Binance action showed that if you're highly liquid and you're banking sanctioned actors, the U.S. is going to go after you however it can."[99]

5.2 Bittrex and BitPay Enforcement Actions

While participants largely disregarded the possibility of learning anything about compliance best practices from the Binance enforcement action, they did point to other, smaller actions, as valuable in clarifying what sanctions compliance should look like. For instance, multiple compliance officers raised the case of Bittrex, an exchange that was fined in 2022 by both OFAC and FinCEN for failing to adequately comply with sanctions.[100]

---

[94] Interview with crypto compliance consultant #1.
[95] "Acting Assistant Attorney General Nicole M. Argentieri Delivers Keynote Speech at the American Bar Association's 39th National Institute on White Collar Crime" (U.S. Department of Justice, March 8, 2024), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-nicole-m-argentieri-delivers-keynote-speech-american.
[96] Interview with crypto compliance officer #5, August 7, 2024.
[97] Interview with crypto compliance officer #2.
[98] Interview with crypto compliance officer #8.
[99] Interview with crypto compliance officer #4.
[100] "Treasury Announces Two Enforcement Actions for over $24M and $29M Against Virtual Currency Exchange Bittrex, Inc." (U.S. Department of the Treasury, October 11, 2022), https://home.treasury.gov/news/press-releases/jy1006.

In the resulting consent order, FinCEN noted that despite processing thousands of transactions every day, in 2016 Bittrex had not used transaction monitoring tools and had instead relied on "two employees with minimal AML training and experience to manually review all of the transactions for suspicious activity. These manual transaction monitoring responsibilities were in addition to their other duties." When Bittrex finally began using third-party software to screen transactions for compliance with OFAC sanctions, the consent order further noted, it "only screened transactions to identify potential matches on the OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List") and other lists. The vendor's software did not begin screening some customers or transactions for a nexus to sanctioned jurisdictions" until the following year.[101]

These details helped signal to exchanges that they needed to be using blockchain analytics tools to flag transactions, and that they needed to use those tools not just to look for links to sanctioned entities but also ties to any sanctioned jurisdictions more broadly, compliance officers said. "Bittrex was seminal on the compliance side—there was nuance to it," one compliance officer said, adding, "it was really treating a crypto exchange like a financial institution."[102]

The Bittrex action also flagged for exchanges that ramping up compliance was not sufficient to protect themselves from enforcement unless they applied those changes retroactively as well. For instance, in the consent order, FinCEN notes that, "In December 2017, Bittrex hired a qualified AML compliance officer with significant BSA/AML experience. That same month, Bittrex paused new customer registrations for four months and used the pause to bolster its AML compliance program. To date, Bittrex has continued to increase compliance staffing and training, and it continues to develop and implement new policies and procedures, including the purchase and integration of several automated transaction monitoring systems."[103] But despite these improvements, since the company did not apply its new compliance regime to its past transactions as well, it was still subject to enforcement. This was a wake-up call for some exchanges, one compliance officer said, explaining, "Bittrex showed that you have to apply everything retroactively as well every time you implement a new sanctions compliance policy or control."[104]

Another enforcement action that some compliance officers said they found helpful was the 2021 OFAC settlement with cryptocurrency payment processor BitPay for failing to sufficiently screen the location of buyers who purchased things from merchants who used BitPay's services.[105] While BitPay screened its own customers—the merchants who were using their payment processing services to sell things—they did not adequately screen the customers of those clients who were purchasing goods from the merchants they supported. One compliance officer explained, "BitPay was doing KYC on their customer, the mom-and-pop shop that wanted a

[101] "In the Matter of Bittrex, Inc. Consent Order Imposing Civil Money Penalty" (FinCEN, 2022), https://www.fincen.gov/sites/default/files/enforcement_action/2023-04-04/Bittrex_Consent_Order_10.11.2022.pdf.
[102] Interview with crypto compliance officer #2.
[103] "In the Matter of Bittrex, Inc. Consent Order Imposing Civil Money Penalty."
[104] Interview with crypto compliance officer #1.
[105] "Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and BitPay, Inc." (Office of Foreign Assets Control, February 18, 2021), https://ofac.treasury.gov/recent-actions/20210218.

crypto interface, but then it turns out that Iranian actors and other sanctioned actors were buying things from that shop and BitPay wasn't screening them because they're not BitPay's customers, they're just the business's customers. So they got a slap on the wrist, but that enforcement action actually helped clarify what companies needed to be doing, and it showed that compliance was not as sophisticated, not as thorough as it needed to be."[106]

One of the main purposes of enforcement actions is to clarify for industry actors what compliance should—and should not—look like, regulators and former regulators said. "We do look at our enforcement actions as important ways to engage with the industry and indicate lessons learned," one regulator noted.[107] But several compliance officers said they felt the enforcement actions to date had been too few, and too small, to elicit any real attention from their executives. "Compliance officers are constantly looking for leverage to get more resources and convince leadership to let them enforce compliance," one compliance officer said, adding, "if you're not going to penalize the bad actors and reward the good ones you make our job impossible."[108] A compliance consultant echoed a similar sentiment, saying, "My clients ask me what is the cost of non-compliance, and I have a hard time telling them that the cost of compliance is lower than the cost of non-compliance."[109]

6. Impacts & Effectiveness of Crypto Sanctions

Participants offered a varied set of opinions about how cryptocurrency-related sanctions had impacted their industry, sanctioned entities, and legitimate cryptocurrency users. Many noted that it was difficult to measure these impacts in any meaningful way because of how many different avenues bad actors had for shifting their digital currency infrastructure in the aftermath of sanctions, but nearly all of them said they thought that the sanctions had at least some impacts on the sanctioned actors, even if those impacts were likely to be short lived in the absence of continual monitoring and updating of the sanctioned address lists.

One former regulator pointed out that part of what made it difficult to assess the effectiveness of sanctions was the lack of clarity surrounding their intended goals. "You can only measure the effectiveness of sanctions if the goal is stated clearly and generally, the goal is not stated clearly because policymakers do not want to be measured against goals," the regulator-turned-compliance-officer explained. "There's often a lofty goal ascribed to sanctions—the goal is to change the regime or end human rights abuses—but really the goal generally is to punish and make lives more difficult for those engaging in a certain set of behaviors," the compliance officer added.[110] Overall, participants referred to three different types of impacts of the sanctions: the impacts on legitimate cryptocurrency users whose funds were caught up in the sanctions, the impacts on sanctioned actors, and the impacts on the crypto industry itself.

6.1 Impacts on legitimate cryptocurrency users

[106] Interview with crypto compliance officer #4.
[107] Interview with regulator #1.
[108] Interview with crypto compliance officer #7, August 5, 2024.
[109] Interview with crypto compliance consultant #1.
[110] Interview with crypto compliance officers #10 and #11, February 4, 2025.

Several compliance officers highlighted the impacts that sanctions compliance could have on legitimate users of cryptocurrency. "There's real people on the other end of this," one compliance officer said. "If I take a janitor who works at the city council in Venezuela and I block all of his funds and he can't eat, did that really move the needle with the Maduro regime? People are trying to send remittances to their family in these war-torn places and they're innocent people and their money gets tied up in this. Are we really supposed to offboard the client who sent their grandma $10 through Garantex?"[111]

One regulator emphasized that the intention of cryptocurrency sanctions was to narrowly target bad actors and avoid as much collateral damage as possible. "Something that we have certainly striven to message is that we aren't targeting the legitimate use of digital currency," the regulator said.[112] Still, many compliance officers said that as sanctions expanded to intermediaries, they saw more and more legitimate actors get caught up in the resulting screening and compliance efforts. Several officers called out the Tornado Cash sanctions as being especially damaging in this regard. "The Tornado Cash sanctions absolutely terrified open source developers who began wondering, 'Am I going to jail because I contributed one element on GitHub to some code used in Tornado Cash?' " one compliance officer said.[113]

6.2 Impacts on sanctioned entities' ability to launder funds

Participants largely agreed that the sanctions had some impact on the ability of sanctioned actors to launder and offramp their cryptocurrency funds, though they were often uncertain how large that impact was. One blockchain analytics vendor said that the sanctions had noticeably slowed North Korea's ability to cash out its stolen funds. "Adding any friction slows them down to the point where we can get there first," the vendor said, noting, "We're still seeing funds on the blockchain from North Korea that they haven't been able to cash out."[114]

Other participants also highlighted the importance of making the laundering process slower and more expensive for the targets of these sanctions. One regulator said that sanctions have made using mixers "very expensive" for actors like North Korea, to the point that when they "go through that cycle of laundering they're losing anywhere from 30-50 percent of their funds."[115] Some compliance officers were skeptical that these increased costs of laundering were significant to the sanctioned parties. "North Korea doesn't care about cost—they're stealing billions of dollars' worth of crypto. What do they care how much it costs to launder?" one compliance officer said, adding, "They're incredibly sophisticated, they'll move it out a million hops if they need to."[116]

Participants also differed on whether it mattered if sanctioned entities were unable to cash out their stolen funds and turn them into fiat currency. "There have been a lot of instances where you

[111] Interview with crypto compliance officer #9.
[112] Interview with regulator #1.
[113] Interview with crypto compliance officer #2.
[114] Interview with blockchain analytics vendor #1.
[115] Interview with regulator #3, February 13, 2025.
[116] Interview with crypto compliance officer #6.

see actors just keep things in crypto and they don't offramp those funds, but that's because North Korea can't do very much with fiat because it's so heavily sanctioned, so they just keep it in crypto," one compliance consultant noted. "The assumption that they're never going to be able to convert these into dollars doesn't matter if you can buy uranium with crypto," the consultant continued, referencing the possibility that North Korea might be able to fund its weapons program directly with cryptocurrency rather than needing to find a way to offramp it and exchange it for fiat currency.[117]

But at least a few participants were doubtful that sanctioned entities would be able to do much with crypto funds. "Having funds sit in a wallet that is being monitored by a government is not going to be helpful to you if you're trying to make a payment for oil," one blockchain analytics vendor said.[118] The importance of restricting how sanctioned actors could use stolen cryptocurrency also underlined the need for going after darknet markets, where people could use cryptocurrency to purchase illicit goods, participants noted.

One former regulator highlighted that sanctioning wallets also enabled other types of law enforcement actions that could further hurt sanctioned entities. "To my mind sanctions are most effective when paired with other actions," the former regulator said. "If you sanction an individual or wallet then that allows law enforcement to pile on to their ongoing investigation because now there's been identified money laundering. Once law enforcement gets involved, that opens up new tools and authorities like asset seizure and forfeiture—things Treasury can't do by itself. So when you target a wallet with sanctions you're freezing that money, then law enforcement can seize it and give that money back to the victim."[119] Several participants emphasized the importance of freezing funds in the sanctioned wallets. "You have illicit actors who can't access these funds that they were relying on—that's an immediate effect," one consultant said.[120]

In spite of these immediate effects, several participants said it was unclear to them how long-lasting the impacts of many cryptocurrency-related sanctions will be given the ability of sanctioned actors to switch to new wallets and intermediaries. For instance, several noted that it was unclear that the impacts of the Tornado Cash sanctions stayed consistent after the initial announcement. "With Tornado Cash we saw immediate drop off after the designation because it was very public, so users thought, 'I can get in trouble if I do this,' " one blockchain analytics vendor noted, adding that usage of the mixer service began to increase again a few months later, possibly due to the lack of any serious enforcement action.[121]

One compliance officer argued that this sort of "whack a mole" approach to updating sanctions as sanctioned entities shifted their infrastructure was not a sign of failure, but simply "how things work."[122] One blockchain analytics vendor offered a similar perspective on the impact of cryptocurrency-related sanctions, urging for realistic expectations in what they could achieve. "If

[117] Interview with crypto compliance consultant #3.
[118] Interview with blockchain analytics vendor #2.
[119] Interview with crypto compliance consultant #2.
[120] Interview with crypto compliance consultant #4.
[121] Interview with blockchain analytics vendor #2.
[122] Interview with crypto compliance officer #4.

you can name and shame, add friction to the laundering process, and take a few bad actors out of the ecosystem, then I think that's success," the vendor said.[123]

6.3 Impacts on the crypto industry

Finally, several participants noted that cryptocurrency sanctions had impacted their industry, in some cases encouraging crypto firms to move out of the United States. "We've had clients that have come to us and said, 'Look, we've reviewed the guidance and we just can't comply with it.' And we say to them, 'Our advice is you have to comply with sanctions law.' So we've had clients that have left the U.S. because they couldn't comply with U.S. sanctions," one compliance consultant said.[124]

But other consultants said they thought this threat was overblown, especially since crypto firms were confident in a much lighter regulatory touch under a second Trump administration. "A lot of [venture capital firms] are saying the U.S. is no longer a friendly place for the development of this technology that is the future of finance, so we are going overseas to develop this—which also diminishes US national security," one consultant said, adding, "But I think they're actually still investing in the U.S. and after the election they see the tides fundamentally changing, so they're scuttling those plans to go overseas."[125]

7. Conclusion

From 2019 onward, cryptocurrency sanctions have expanded to include a broader range of intermediaries and actors. The U.S. government came to regard the threats of ransomware and cryptocurrency theft as being linked to major national security risks, including attacks on U.S. critical infrastructure and nuclear proliferation by North Korea. The government's implementation of cryptocurrency sanctions expanded over time, from wallets to exchanges to mixers. During that same period, cryptocurrency exchanges made significant strides in developing their compliance programs but many nuances of compliance remained unclear to even seasoned compliance officers. These ambiguities included how long firms are required to continue to monitor past transactions, how far back on the blockchain they are required to trace transactions for any interaction with sanctioned entities, and how they are supposed to monitor for VPN usage in sanctioned jurisdictions.

The enforcement actions brought by the US government in some cases served to help clarify these ambiguities, but in others were viewed as merely giving a slap on the wrist to the most egregious offenders in the industry and offering little insight into how best to actually comply with sanctions. The participants in our study varied in their perceptions of whether the cryptocurrency sanctions had any meaningful impacts on the sanctioned entities, but almost all agreed that such impacts were likely to be relatively short lived in the absence of continuous updating and monitoring of sanctioned addresses. Overall, several participants expressed some skepticism that sanctions compliance in the industry would continue to mature or even be

[123] Interview with blockchain analytics vendor #1.
[124] Interview with crypto compliance consultant #1.
[125] Interview with crypto compliance consultant #4.

maintained at its current level. “There’s a shift in the risk appetite with the Trump administration coming in,” one compliance officer noted, adding, “the sense is, ‘no one’s going to touch us now.’ ”[126]

The cryptocurrency lobby invested heavily in Donald Trump’s 2024 presidential campaign—as well as crypto-friendly members of Congress.[127] This led to Trump reversing his position on crypto, from describing it as “like a scam” in 2021 to proposing a national bitcoin reserve during the campaign. The *New York Times* concluded, “the mere fact that a Bitcoin stockpile is under consideration is a sign of how drastically the political winds have shifted after a yearslong regulatory crackdown on the crypto industry.”[128] Several participants said they believed Trump’s victory would lead to much less regulation and enforcement directed at the cryptocurrency industry, including with regard to sanctions.

Another significant setback for proponents of cryptocurrency-related sanctions was a November 2024 legal defeat in the Fifth Circuit. The Treasury Department was defending its Tornado Cash sanctions against a group of Tornado Cash users, including Joseph Van Loon, who had sued the government on the grounds that the government does not have authority to sanction open-source self-executing software like Tornado Cash. In a November 26, 2024, ruling, the Fifth Circuit sided with the plaintiffs, writing that “Tornado Cash’s immutable smart contracts (the lines of privacy-enabling software code) are not the ‘property’ of a foreign national or entity, meaning (1) they cannot be blocked under IEEPA, and (2) OFAC overstepped its congressionally defined authority.”[129]

Several participants perceived the sanctions on Tornado Cash as going too far in trying to target intermediaries and backfiring on the Treasury Department by handing them a resounding defeat. “The combination of the *Van Loon* decision and Trump’s election make this an inflection point,” one compliance officer said, adding, “now everyone is pulling back on their OFAC screening.”[130] Others, however, noted that there was still some uncertainty about exactly how far the Trump administration’s friendliness towards the crypto industry would extend. “For as pro crypto as they nominally say they are, you do not want to cross the line with Iran and North Korea in this administration,” one compliance officer said.[131]

The ongoing tension between the libertarian culture of technologists and the compliance culture of regulators and financial professionals persists. Interview subjects were cautious about whether Trump’s 2024 election would tip the scales back towards less compliance. The potential for that reversal, however, hints at how uneasy the fit between crypto firms and regulatory compliance teams has been from the start. It suggests that even as crypto firms began investing

---

[126] Interview with crypto compliance officer #9.
[127] Jemima Kelly, “Crypto lobbyists are polluting the US election,” *Financial Times*, June 30, 2024; Josh Dawsey, “Wealthy industry donors fuel Trump’s conversion on cryptocurrency,” *Washington Post*, July 15, 2024; Andrew Chow, “How the Crypto World Learned to Love Donald Trump, J.D. Vance, and Project 2025,” *Time*, July 17, 2024; Jasper Goodman, “A wave of crypto-friendly lawmakers is about to crash Congress,” Politico, October 22, 2024.
[128] Kelly, “Crypto lobbyists are polluting the US election”; David Yaffe-Bellamy, “A First Day Trump Order: A Federal Stockpile of Bitcoin?” *New York Times*, January 16, 2025.
[129] Van Loon v. Department of the Treasury, No. 23-50669 (5th Cir. November 26, 2024).
[130] Interview with crypto compliance officer #9.
[131] Interview with crypto compliance officer #2.

in compliance programs and hiring former regulators in the late 2010s and early 2020s, leaders at many of those companies never fully bought into these programs. As quickly as the crypto sector has built up a compliance apparatus, they might be able to just as quickly dismantle it.