

# THE UNDERSIDE OF THE COIN: ILLICIT FINANCE RISKS IN VIRTUAL ASSETS

BY RICHARD GOLDBERG AND ALEX LEVITOV

FEBRUARY 16, 2023

## INTRODUCTION

With the implosion of FTX and the arrest of its founder, Sam Bankman-Fried, Washington is finally waking up to the need for more effective regulation of cryptocurrency. Despite the “crypto winter” and scandals in the industry, institutional interest in cryptocurrency remains high, with the potential for crypto usage to increase steadily.<sup>1</sup> This reveals a glaring gap in regulation. The United States and like-minded countries have built regulatory frameworks to protect the traditional banking system from illicit finance, but Washington needs to update these frameworks for the “Web3” era, in which decentralized tools like cryptocurrency are increasingly prominent.

The indictment of Bankman-Fried on charges of securities and commodities fraud underscores the need to protect consumers while regulating cryptocurrency investments and trading. Yet as Washington takes up the challenge of crypto regulation, national security should also be front and center. Regulatory frameworks for the traditional banking system include strong anti-money laundering and combating the finance of terrorism (AML/CFT) measures. There is an urgent need to adapt AML/CFT frameworks to address cryptocurrency use in cybercrime, terror finance, drug trafficking, human trafficking, sanctions busting, and domestic extremism.

The relative anonymity (or pseudonymity) of certain blockchain-based transactions made cryptocurrency naturally attractive to those seeking to avoid government oversight and intervention, including criminals, terrorists, and the states that sponsor them.<sup>2</sup> Blenders, mixers, and other services that enhance the anonymity of cryptocurrency transactions have only increased their appeal to illicit actors. Further, poor cybersecurity has left digital currency exchanges and related entities open to attack, including hacks resulting in the cumulative theft of billions of dollars, much of it by state-sponsored hacking groups. Troublingly, many companies in the crypto sector either do not have — or do not want to have — effective compliance and prevention programs to mitigate these risks.

---

1. Jared Blikre, “Bitcoin interest surged in 2022 as ‘crypto winter’ arrived: Morning Brief,” *Yahoo! Finance*, December 22, 2022. (<https://finance.yahoo.com/news/bitcoin-interest-surged-in-2022-as-crypto-winter-arrived-morning-brief-103134240.html>)

2. Greg Myre, “How Bitcoin Has Fueled Ransomware Attacks,” *NPR*, June 10, 2021. (<https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks>); “Crypto Money Laundering Rises 30%, Report Finds,” *BBC* (UK), January 26, 2022. (<https://www.bbc.com/news/technology-60072195>)

The absence of a coordinated regulatory or legislative response from the U.S. government is a gap that America's adversaries can exploit. To be sure, both government and industry need to balance protections of national security, privacy, and free speech in the regulation of digital assets.<sup>3</sup> But the complexity of this task should not be a pretext for delay.

In March 2022, President Joe Biden issued an executive order calling for a national security strategy for digital assets. In August, the Treasury Department unveiled an action plan to address the illicit financing risks of digital assets. The plan called for an assessment of risks and gaps within the existing U.S.-based AML/CFT regulatory regime; improvement of regulations and enforcement in foreign jurisdictions; updating U.S. banking regulations as needed; holding illicit actors accountable; and engaging the private sector to share information and raise the virtual asset (VA) industry's awareness of illicit finance. These steps moved the national security-related cryptocurrency policy debate in the right direction. But they were only a start. Now is the time to take additional steps to defend our national security.<sup>4</sup>

This memo seeks to inform the efforts of both the executive and legislative branches to address the national security challenges posed by cryptocurrencies while modernizing AML/CFT-related statutes and regulations. Some of the recommended measures will be analogous to steps taken previously to help traditional financial institutions bolster their compliance programs. This memo also focuses on challenges specific to the Web3 ecosystem, such as unique protocols intended to conceal identities and the question of how to prevent illicit activity without undercutting legitimate use.

## CRYPTOCURRENCY TRAITS THAT ILLICIT ACTORS CAN EXPLOIT

Cryptocurrencies, the most common form of virtual assets, are most vulnerable to abuse because of three characteristics or tools illicit actors can exploit:

- **Decentralization and Borderless Transactions:** Many cryptocurrencies facilitate near-instantaneous peer-to-peer financial transactions across borders without the involvement of regulated intermediaries, such as traditional banks. Other cryptocurrencies use intermediaries that operate in jurisdictions without sufficient counter-illicit finance standards. The exclusion of regulated intermediaries or third parties enables illicit actors to sell or purchase goods and services without oversight. Despite the public visibility of these transactions on the blockchain, the permissionless, open-source nature of the technology serves to lower barriers to entry for licit and illicit actors alike.
- **Pseudo-anonymity:** The structure and design of the cryptocurrency economy make it possible for a VA owner to avoid the disclosure of his or her true identity. Parties transacting on the blockchain do not need to trust, or even know, each other. Transactions registered on the blockchain typically include only non-personal identifiers, such as a wallet address, so parties to the transaction enjoy pseudo-anonymity (or pseudonymity). This affords less protection than true anonymity, yet certain cryptocurrencies, including “privacy coins,” further enhance

.....  
3. Rich Goldberg, “To Regulate or not to Regulate, that is the Question,” *Cryptonite*, September 6, 2022. (<https://ricochet.com/podcast/cryptonite/to-regulate-or-not-to-regulate-that-is-the-question>)

4. The White House, Press Release, “FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets,” March 9, 2022. (<https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets>); U.S. Department of the Treasury, “Action Plan to Address Illicit Financing Risks of Digital Assets,” September 20, 2022. (<https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf>)

anonymity; non-public or private blockchains make it more difficult to trace or attribute transactions. As a result, a VA owner may only have to reveal his or her true identity when converting between VAs and fiat currencies. This lack of customer and counterparty identification is especially concerning given the cross-border nature of many transactions and the inadequate regulation and supervision of VA activities. Finally, concealment of identity can also be a concern when individuals anonymously join together to mine cryptocurrencies — creating new coins by solving advanced mathematical equations — in “mining pools.” Without AML due diligence, mining pool operators could help enrich illicit actors.

- **Anonymizing Services:** Many blockchains are entirely public. All transactions to and from a particular wallet are open to public scrutiny (even if the wallet owner’s true identity remains unknown). To prevent even this limited scrutiny, VA users employ anonymizing services, also known as mixers or tumblers, which use tactics such as distributing VAs to thousands of accounts and then re-aggregating them and sending them back to their original owners or onward to their ultimate recipient. In August 2022 and again in November 2022, the Treasury Department imposed sanctions on the virtual currency mixer Tornado Cash, which has been used to launder more than \$7 billion worth of virtual currency since its creation in 2019 — including more than \$455 million stolen by a North Korean state-sponsored hacking group.<sup>5</sup>

Some cryptocurrencies and other types of VAs limit decentralization and anonymity. They rely on a centralized authority that controls participation in the network and access to the blockchain. This authority may conduct customer due diligence on key participants, at least in jurisdictions subject to effective regulation and supervision.

## THE CRYPTOCURRENCY-ILLICIT FINANCE NEXUS

VAs, just like cash, can be used to move or store value for a range of illicit activity, from simple fraud to the proliferation of weapons of mass destruction. A survey from the Financial Action Task Force (FATF) — an intergovernmental organization focused on countering illicit finance — found the use of VAs was most common in the sale of narcotics and other controlled goods, such as firearms. Cases involving computer-based fraud and extortion saw the second-most frequent use of VAs.<sup>6</sup> U.S. and British authorities have also linked virtual assets with drug trafficking and cybercrimes, such as ransomware attacks,<sup>7</sup> as well as arms-length criminal transactions in which the parties seek a high degree of anonymity, such as purchases from “dark web” marketplaces.<sup>8</sup> Recent reporting reveals the potential for billions of dollars to flow through the crypto economy via high-risk and highly sanctioned jurisdictions like Iran.<sup>9</sup> North Korea has already stolen hundreds of millions of dollars of cryptocurrency, which Pyongyang has occasionally repatriated via conversion to anonymity-enhanced virtual currencies, making

5. U.S. Department of the Treasury, “U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash,” August 8, 2022. (<https://home.treasury.gov/news/press-releases/jy0916>); U.S. Department of the Treasury, “Frequently Asked Questions,” November 8, 2022. (<https://home.treasury.gov/policy-issues/financial-sanctions/faqs/updated/2022-11-08>)

6. Financial Action Task Force, “Virtual Assets Red Flag Indicators of Money Laundering And Terrorist Financing,” September 2020. (<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf>)

7. U.S. Department of the Treasury, “U.S. National Money Laundering Risk Assessment,” 2018. ([https://home.treasury.gov/system/files/136/2018NMLRA\\_12-18.pdf](https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf))

8. His Majesty’s Treasury and The Home Office (UK), “National risk assessment of money laundering and terrorist financing,” December 2020. ([https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/945411/NRA\\_2020\\_v1.2\\_FOR\\_PUBLICATION.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf))

9. Angus Berwick and Tom Wilson, “Crypto exchange Binance helped Iranian firms trade \$8 billion despite sanctions,” *Reuters*, November 7, 2022. (<https://www.reuters.com/business/finance/exclusive-crypto-exchange-binance-helped-iranian-firms-trade-8-billion-despite-2022-11-04>)

tracking extremely difficult.<sup>10</sup> Terrorist groups have openly solicited contributions in the form of VAs and have moved these assets through multiple wallets or accounts before ultimately selling them for cash.<sup>11</sup>

## CYBERCRIME

Attacks on Colonial Pipeline and JBS meat plants in 2021 demonstrated the increasing demand for cryptocurrency as a means for ransom payments (though in the case of Colonial, the U.S. government clawed back \$2.3 million after the ransom was paid).<sup>12</sup> As National Public Radio observed, “Bitcoin and other cryptocurrencies made it possible to extort huge ransoms from large companies, hospitals, and city governments. And if the cyber thieves live in countries like Russia — which many do — there’s virtually no chance of getting caught.”<sup>13</sup> Well before its 2022 invasion of Ukraine, Russia emerged as a haven for cybercriminals.<sup>14</sup> The country is a hub for “ransomware-as-a-service” providers that help criminal cyber actors breach companies’ networks with malware.<sup>15</sup> Meanwhile, North Korea is responsible for some of the largest thefts to date.<sup>16</sup> In one instance, North Korea stole \$622 million from the Axie Infinity game through spearfishing.<sup>17</sup>

## TERRORISM

In 2019, Hamas, a U.S.-designated foreign terrorist organization, issued a call for donations in Bitcoin; Reuters reported the group was experimenting with various crypto fundraising schemes.<sup>18</sup> In 2020, the U.S. Justice Department seized \$2 million across 30 digital wallets tied to al-Qaeda, ISIS, and Hamas.<sup>19</sup> In December 2021, Israel’s defense minister ordered the seizure of \$830,000 in cryptocurrency from a money exchange run by Hamas in Gaza.<sup>20</sup> And in February 2022, Israel’s defense minister announced Israeli authorities seized “tens of thousands

10. United Nations Security Council, “Midterm report of the Panel of Experts submitted pursuant to resolution 2464 (2019) (S/2019/691),” August 30, 2019. (<https://undocs.org/S/2019/691>)

11. U.S. Department of the Treasury, “2022 National Terrorist Financing Risk Assessment,” February 2022, page 22. (<https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf>)

12. “The Colonial Pipeline CEO Explains The Decision To Pay Hackers A \$4.4 Million Ransom,” *NPR*, June 3, 2022. (<https://www.npr.org/2021/06/03/1003020300/colonial-pipeline-ceo-explains-the-decision-to-pay-hackers-4-4-million-ransom>); Jacob Bunge, “JBS Paid \$11 Million to Resolve Ransomware Attack,” *The Wall Street Journal*, June 9, 2021. (<https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781>); U.S. Department of Justice, “Justice News,” June 7, 2021. (<https://www.justice.gov/opa/pr/departments-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>)

13. Greg Myre, “How Bitcoin has Fueled Ransomware Attacks,” *NPR*, June 10, 2021. (<https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks>)

14. John Hardie, “U.S. Steps up Pressure Against Russian Crypto Abuse,” *Foundation for Defense of Democracies*, September 30, 2020. (<https://www.fdd.org/analysis/2020/09/30/us-pressure-against-russian-crypto-abuse>)

15. Rich Goldberg, “Is my Crypto Secure?,” *Cryptonite*, April 19, 2022. (<https://cryptopod.substack.com/p/is-my-crypto-secure>)

16. Samantha Ravich and Annie Fixler, “The Attack on America’s Future,” *Foundation for Defense of Democracies*, October 28, 2022. (<https://www.fdd.org/analysis/2022/10/28/the-attack-on-americas-future-cyber-enabled-economic-warfare>)

17. Daniel Van Boom, “A Fake Job Offer Reportedly Led to Axie Infinity’s \$600M Hack,” *CNET*, July 6, 2022. (<https://www.cnet.com/personal-finance/crypto/a-fake-job-offer-reportedly-led-to-axie-infinitys-600m-hack>)

18. AFP and TOI Staff, “Send us Bitcoin, Cash-Strapped Hamas Pleads,” *The Times of Israel* (Israel), January 30, 2019. (<https://www.timesofisrael.com/send-us-bitcoin-cash-strapped-hamas-pleads>); Tom Wilson and Dan Williams, “Hamas Shifts Tactics in Bitcoin Fundraising, Highlighting Crypto Risks,” *Reuters*, April 26, 2019. (<https://www.reuters.com/article/us-crypto-currencies-hamas/hamas-shifts-tactics-in-bitcoin-fundraising-highlighting-crypto-risks-research-idUSKCN1S20FA>)

19. Amanda Macias, “U.S. seizes \$2 million from more than 300 cryptocurrency accounts used by terror groups,” *CNBC*, August 13, 2020. (<https://www.cNBC.com/2020/08/13/us-seizes-2-million-dollars-from-crypto-accounts-used-by-terror-groups.html>)

20. Ahmad Abu Amer, “Hamas Plans to Continue Using Cryptocurrencies for Operations,” *Al-Monitor*, January 7, 2022. (<https://www.al-monitor.com/originals/2022/01/hamas-plans-continue-using-cryptocurrencies-operations>)

of shekels” from 30 Hamas-affiliated digital wallets linked to six accounts tied to a cryptocurrency exchange based in Gaza.<sup>21</sup>

Last fall, the Joint Counterterrorism Assessment Team (JCAT) — a collaboration of the National Counter Terrorism Center, Department of Homeland Security, and the Federal Bureau of Investigation — issued a memorandum on terrorists’ use of cryptocurrency.<sup>22</sup> According to JCAT, “a prominent Telegram channel that promotes violent extremist related material [likely white supremacist] posted a graphic, with corresponding text, promoting the use of Monero cryptocurrency.” JCAT said the “same channel previously published a 34-page guide, titled “Cryptocurrency - A Privacy & Security Goys [non-Jew] Practical Guide.” Privacy coins like Monero, Dash, and Zcash, topped the JCAT team’s concerns, alongside obfuscation techniques and technology like mixing and layering.<sup>23</sup> These privacy coins have also been linked to Islamist violent extremist groups like ISIS.<sup>24</sup>

## DRUG AND HUMAN TRAFFICKING

In March 2022, the United Nations-affiliated International Narcotics Control Board warned that the Mexico-based Jalisco New Generation cartel and the Sinaloa cartel were using Bitcoin to avoid traditional anti-money laundering programs in the United States.<sup>25</sup> In 2020, the U.S. Drug Enforcement Agency (DEA) asserted that a steady drop in seizures of hard currency suggested increasing use of cryptocurrency by cartels. The DEA called it a “trend to launder illicit proceeds” and claimed both Mexican and Colombian Transnational Criminal Organizations were “increasing their use of virtual currency because of the anonymity and speed of transactions.”<sup>26</sup>

In January 2022, the U.S. Government Accountability Office (GAO) confirmed a spike in the use of cryptocurrency by drug and human traffickers. “Virtual currency’s anonymizing features can attract criminals’ use to avoid detection when paying for illicit activities such as human and drug trafficking,” according to the GAO. “[T]he number of suspicious activity reports filed with the Financial Crimes Enforcement Network (FinCEN) that involve virtual currency and drug trafficking increased fivefold (from 252 to almost 1,432) from calendar year 2017 to 2020.”<sup>27</sup>

.....  
21. Emanuel Fabian, “Israel seizes 30 crypto wallets allegedly used to fund Hamas,” *The Times of Israel* (Israel), February 28, 2022. (<https://www.timesofisrael.com/israel-seizes-30-crypto-wallets-allegedly-used-to-fund-hamas>)

22. “Identifying and Preventing Illicit Use of Cryptocurrency by Terrorists,” *First Responders Toolbox*, accessed November 21, 2022. ([https://www.odni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/119s\\_-\\_First\\_Responders\\_Toolbox\\_-\\_Identifying\\_and\\_Preventing\\_Illicit\\_Use\\_of\\_Cryptocurrency\\_by\\_Terrorists.pdf](https://www.odni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/119s_-_First_Responders_Toolbox_-_Identifying_and_Preventing_Illicit_Use_of_Cryptocurrency_by_Terrorists.pdf))

23. U.S. Department of the Treasury, “National Money Laundering Risk Assessment,” February 2022. (<https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf>)

24. Counter Extremism Project, Press Release, “Extremist Content Online: ISIS Releases A New Video Titled ‘The Epic Battles Of Attrition 3’ And Neo-Nazi Telegram Channel Removed,” June 29, 2020. (<https://www.counterextremism.com/press/extremist-content-online-isis-releases-new-video-titled-epic-battles-attrition-3-and-neo-nazi>)

25. “Mexican cartels turn to bitcoin, internet, e-commerce,” *Associated Press*, March 10, 2022. (<https://apnews.com/article/business-caribbean-mexico-crime-drug-cartels-1bb5ebf84fbf71baf6a845648bad4990>)

26. Diego Ore, “Latin American crime cartels turn to cryptocurrencies for money laundering,” *Reuters*, December 8, 2020. (<https://www.reuters.com/article/mexico-bitcoin-insight/latin-american-crime-cartels-turn-to-cryptocurrencies-for-money-laundering-idUSKBN28I1KD>)

27. Government Accountability Office, “Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking,” January 10, 2021. (<https://www.gao.gov/products/gao-22-105462>) The data on suspicious activity reports does not, however, reveal the number of confirmed trafficking cases and may be correlated to an increase in industry oversight.

## SANCTIONS EVASION

Last year, Treasury published its first guidance on sanctions compliance for the digital asset industry and has since targeted wallets and exchanges tied to ransomware attacks.<sup>28</sup> In April 2022, the department imposed sanctions on a crypto miner in Russia, and in May it announced its first-ever sanctions targeting a “virtual currency mixer” — a technology that makes it harder to track the origin, destination, and counterparties of blockchain transactions.<sup>29</sup> Last August, Treasury imposed sanctions on a notorious mixer called Tornado Cash — with additional sanctions in November — for its role in activities that ultimately supported North Korea’s missile proliferation efforts.<sup>30</sup>

In January 2022, Iran directed its sanctioned central bank to expand its use of cryptocurrency.<sup>31</sup> Then, in August, Tehran announced it approved cryptocurrency regulations, a sign that digital assets would pay for otherwise sanctionable imports.<sup>32</sup> In fact, the regime pledged to use cryptocurrency as a medium for foreign trade to evade U.S. sanctions.<sup>33</sup> This was reminiscent of 2018, when Venezuela launched the oil-backed Petro virtual currency to skirt U.S. sanctions.<sup>34</sup> The coin was a flop but provided other rogue actors with a blueprint and lessons to learn.<sup>35</sup>

Treasury is now pressuring virtual currency exchanges to prevent exploitation by sanctions evaders. In October 2022, the Bitnexus exchange agreed to pay more than \$50 million in fines for failing to prevent actors in Syria, Iran, Sudan, Cuba, and Russian-occupied Crimea from using its platform.<sup>36</sup> In November, the Kraken exchange agreed to pay more than \$360,000 to settle its potential civil liability for violating Iran sanctions.<sup>37</sup> Earlier that same month, Reuters reported that the “crypto exchange Binance helped Iranian firms trade \$8 billion despite sanctions.”<sup>38</sup>

28. U.S. Department of the Treasury, “North Korea Designation Update,” April 14, 2022. (<https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220414>); Lauren Fiener, “US Treasury Sanctions Cryptocurrency Exchange for Alleged role in Ransomware Attacks,” *CNBC*, September 22, 2021. (<https://www.cnn.com/2021/09/21/us-treasury-sanctions-cryptocurrency-exchange-suex.html>)

29. Ryan Browne, “Sanctions threaten to cripple Russia’s multibillion-dollar crypto industry,” *CNBC*, April 22, 2022. (<https://www.cnn.com/2022/04/22/sanctions-could-hurt-russias-multibillion-dollar-crypto-industry.html>); U.S. Department of the Treasury, “U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats,” May 6, 2022. (<https://home.treasury.gov/news/press-releases/jy0768>)

30. U.S. Department of the Treasury, “U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash,” August 8, 2022. (<https://home.treasury.gov/news/press-releases/jy0916>); U.S. Department of the Treasury, “Treasury Designates DPRK Weapons Representatives,” November 8, 2022. (<https://home.treasury.gov/news/press-releases/jy1087>)

31. “Central Bank of Iran to Aid Traders Making Sanction-Busting Crypto Payments,” *Pymnts*, January 12, 2022. (<https://www.pymnts.com/cryptocurrency/2022/central-bank-of-iran-to-aid-traders-making-sanction-busting-crypto-payments>)

32. “Iran Approves Cryptocurrency Regulations, Raising Fears Of Skirting Sanctions,” *Radio Free Europe/Radio Liberty*, August 29, 2022. (<https://www.rferl.org/a/iran-cryptocurrency-regulations-skirting-sanctions/32009292.html>)

33. @SGhasseminejad, *Twitter*, August 9, 2022. (<https://twitter.com/SGhasseminejad/status/1557039271386685442?s=20&t=bS1fwyWz8srlxSv60kWdjw>)

34. “Petro Ignited: Venezuela Launches Pre-Sale Of Oil-Backed National Cryptocurrency,” *CoinTelegraph*, February 21, 2018. (<https://cointelegraph.com/news/petro-ignited-venezuela-launches-pre-sale-of-oil-backed-national-cryptocurrency>)

35. Yaya J. Fanusie, “Crypto Rogues,” *Foundation for Defense of Democracies*, July 11, 2019. (<https://www.fdd.org/analysis/2019/07/11/crypto-rogues>)

36. U.S. Department of the Treasury, “Treasury Announces Two Enforcement Actions for over \$24M and \$29M Against Virtual Currency Exchange Bittrex, Inc.,” October 11, 2022. (<https://home.treasury.gov/news/press-releases/jy1006>)

37. U.S. Department of the Treasury, Enforcement Release, “OFAC Settles with Virtual Currency Exchange Kraken for \$362,158.70 Related to Apparent Violations of the Iranian Transactions and Sanctions Regulations,” November 28, 2022. ([https://home.treasury.gov/system/files/126/20221128\\_kraken.pdf](https://home.treasury.gov/system/files/126/20221128_kraken.pdf))

38. Angus Berwick and Tom Wilson, “Crypto exchange Binance helped Iranian firms trade \$8 billion despite sanctions,” *Reuters*, November 7, 2022. (<https://www.reuters.com/business/finance/exclusive-crypto-exchange-binance-helped-iranian-firms-trade-8-billion-despite-2022-11-04>)

## DOMESTIC EXTREMISM

Since being denied access to traditional financial products following the 2017 “Unite the Right” rally in Charlottesville, Virginia, white supremacists increasingly accept “cryptocurrency donations to support content they produce, such as video streams, podcasts, and radio shows,” and “as payment for merchandise they produce and sell, such as apparel, books, and various accessories.”<sup>39</sup> Cryptocurrency also helps fund legal defenses and supplies for extremist groups. Last year, a Foundation for Defense of Democracies report warned that domestic extremists would exploit privacy coins like Monero, along with techniques such as mixing and “coinjoining” (bundling together multiple transactions to add an additional layer of anonymity). The report also warned of self-executing “smart contracts” (a computerized protocol that automatically executes the terms of a contract) to “outsource criminal activities, potentially including [terrorist] attacks.”<sup>40</sup>

## 51% ATTACKS

Other challenges loom. Economists and investors warn that Beijing (or possibly other adversaries) could also amass enough supercomputing power to attack a blockchain and upend its ledger system through so-called “51% attacks.” In such an attack, a rogue actor can use majority control of the computer power of some particular cryptocurrency or blockchain to manipulate data and change an official on-chain record.<sup>41</sup> This would result in severe disruptions to U.S.-based transactions.

## GAPS IN THE REGULATION OF VIRTUAL ASSET SERVICE PROVIDERS

Following the terrorist attacks of September 11, 2001, Congress passed legislation, and the executive branch issued regulations, to strengthen AML/CFT standards for domestic and foreign financial institutions. A wave of congressionally mandated sanctions targeted banks doing business in places like Iran, and the Treasury Department began to employ targeted sanctions authorities more aggressively. These changes led the financial industry to invest more in compliance and risk management programs, software, systems, and personnel. By contrast, virtual asset services providers (VASPs), by virtue of their youth and the immature regulatory environment, lack comparable AML/CFT and sanctions compliance programs. Although FATF has called for greater AML/CFT compliance, few jurisdictions have robust AML/CFT laws and regulations in place that govern VASPs and other VA sector participants.<sup>42</sup>

In fact, the industry has often pushed back against nascent efforts to strengthen regulation. While the cost of compliance is a valid concern, the industry does not fully appreciate — or even denies — the risk of illicit finance. Last year, a U.S. lobbying group representing more than 70 crypto platforms told the media that Russian oligarchs “aren’t using (and can’t use) crypto to evade sanctions” despite the demonstrated use of cryptocurrency for sanctions

.....  
39. Daveed Gartenstein-Ross, “Crypto-Fascists,” *Foundation for Defense of Democracies*, March 15, 2022, page 6. (<https://www.fdd.org/analysis/2022/03/15/crypto-fascists>)

40. Daveed Gartenstein-Ross, “Crypto-Fascists,” *Foundation for Defense of Democracies*, March 15, 2022, pages 6 and 14-16. (<https://www.fdd.org/analysis/2022/03/15/crypto-fascists>)

41. Rich Goldberg, “Risky Business,” *Cryptonite*, February 24, 2022. (<https://cryptopod.substack.com/p/risky-business>)

42. Financial Action Task Force, “Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers,” June 2022. (<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf>)

evasion, as noted above.<sup>43</sup> While there is no evidence yet of large-scale transactions by the Russian government, the Justice Department announced charges in October 2022 against a criminal network alleged to have provided funds to the Russian military, including cryptocurrency transfers worth millions of dollars.<sup>44</sup>

In its efforts to downplay cryptocurrency risks, the industry emphasizes that the traditional banking system is exploited by the same criminal enterprises that abuse cryptocurrency platforms. Yet crypto presents unique risks. First, certain cryptocurrencies are designed to offer increased anonymity, thereby making life easier for the illicit financier and more difficult for law enforcement authorities. Second, cryptocurrency is new, and our process of understanding how to counter illicit finance in the crypto domain is still in its infancy.

In terms of risk, one may think of VASPs as similar to financial institutions that service cash-based businesses, albeit with greater ability to trace transactions on-chain. It is a risky enterprise by nature. What's more, traditional financial institutions' relationships with VASPs amplify illicit finance vulnerabilities, since VASPs connect these institutions to their own customer base.

Strengthening the oversight of VASPs requires addressing three deficiencies:

- **Weak Global Regulatory and Supervisory Architecture:** Virtual assets and VASPs have entered the mainstream faster than countries have been able to develop regulatory standards. The existence of unregulated VASPs raises risk across the virtual asset sector, and the newness of regulatory regimes for VASPs means that banks and other actors cannot assume VASPs have effective oversight. If bad actors can access VASPs subject to insufficient regulation, they can often gain access to other, better-regulated VASPs and, ultimately, the traditional financial sector.
- **Insufficient Preventive Measures:** VASPs themselves — especially in jurisdictions with weak or nonexistent regulatory frameworks — often lack effective preventive and risk-mitigating measures. VASPs in jurisdictions with stronger or more mature regulatory regimes may still lack experienced compliance staff and/or have insufficient compliance budgets. And even VASPs with experienced compliance staff and robust programs may not fully account for real risk, in part because of a lack of clear regulatory guidance. For example, certain exchanges may limit the number of transaction hops (i.e., previous entries in the transaction chain) they review as part of their due diligence and monitoring processes and, as a result, may miss prior transactions involving sanctioned wallets or protocols (such as Tornado Cash). This is not necessarily a failure on the part of the entity but rather a result of unclear guidance.
- **An Underdeveloped Culture of Compliance in the Industry:** Some individuals or communities involved with the operation of VASPs may be ideologically opposed to government intervention. They view virtual assets as a

.....  
43. Brian Schwartz, "Cryptocurrency group lobbies Congress against bills that target Russian oligarchs," *CNBC*, April 29, 2022, (<https://www.cnbc.com/2022/04/29/cryptocurrency-group-lobbies-congress-against-bills-that-target-russian-oligarchs-.html>); Rich Goldberg, "Crypto, Russia, and Ukraine," *Cryptonite*, March 7, 2022. (<https://cryptopod.substack.com/p/crypto-russia-and-ukraine>); United Nations Security Council, "Letter dated 26 February 2020 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council." (<https://undocs.org/S/2020/151>)

44. Angus Berwick and Tom Wilson, "Crypto exchange Binance helped Iranian firms trade \$8 billion despite sanctions," *Reuters*, November 7, 2022. (<https://www.reuters.com/business/finance/exclusive-crypto-exchange-binance-helped-iranian-firms-trade-8-billion-despite-2022-11-04>); U.S. Department of Justice, "Justice Department Announces Charges and Arrests in Two Cases Involving Export Violation Schemes to Aid Russian Military," October 19, 2022. (<https://www.justice.gov/opa/pr/justice-department-announces-charges-and-arrests-two-cases-involving-export-violation-schemes>)

privacy-focused alternative to the traditional financial sector, making them reluctant to impose measures they perceive as excessive, despite the requirements of international AML/CFT standards. This dogmatic approach to privacy can create opportunities for terrorists and other criminal actors to exploit.

### **GRAPPLING WITH WEB3**

Cryptocurrency exchanges face compliance challenges similar to those of traditional financial services providers. Both require “know your customer” (KYC) protocols to ensure customers are who they say they are — not money launderers or sanctions evaders. Exchanges also need effective transaction monitoring and screening using Treasury Department sanctions and other illicit finance databases. Putting in place such measures is difficult, but traditional financial institutions have done so for years.

Yet cryptocurrency also presents challenges with solutions that do not fit within the existing regulatory toolkit. These new challenges often stem from so-called “Web3” applications that facilitate peer-to-peer transactions of various kinds while sidelining the intermediaries often responsible for risk management. Policymakers must consider how to regulate this activity without banning entire classes of products or services that have legitimate uses.

The Treasury Department’s designation of Tornado Cash highlights the challenge.<sup>45</sup> Treasury asserted that Tornado Cash was widely used to facilitate illicit activity. There was ample cause to shut it down. Yet Tornado Cash is a freely available open-source protocol, not owned by one individual or company whose assets can be frozen. As a result, many in the crypto sector are unsure what to do with funds that passed through Tornado Cash following its designation. Compliance professionals could certainly freeze all funds that come directly from Tornado Cash. But what if the mixing of cryptocurrency happened three transactional hops in the past? How far back on the blockchain must a VASP go? And what are the implications for transactions that passed through mixing services that pose similar risks but remain unsanctioned? This is where clear regulatory guidance would be helpful.

Policymakers should consider three larger questions posed by the challenges of Web3 technology:<sup>46</sup>

- Should regulators accept that mixers are just protocols while ignoring the people behind the protocols?
- Should regulators shut down protocols because of abuse by illicit actors, even if other users have legitimate purposes (for example, ensuring anonymity for transactions in authoritarian countries)?
- Is there a way to ensure developers build certain AML/CFT controls and functionality into the code of their protocols (e.g., automatically prohibiting transactions with certain persons under sanctions)?

Without answering these questions, the security challenges associated with Web3 will remain.

### **CONCLUSIONS AND RECOMMENDATIONS**

While President Biden’s March 2022 executive order and Treasury’s subsequent action plan helped address the risks posed by digital assets, other steps are necessary.

.....  
45. U.S. Department of the Treasury, “U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash,” August 8, 2022. (<https://home.treasury.gov/news/press-releases/jy0916>)

46. Daniel Kuhn, “What Happens when you try to Sanction a Protocol like Tornado Cash,” *Coindesk*, August 10, 2022. (<https://www.coindesk.com/layer2/2022/08/10/what-happens-when-you-try-to-sanction-a-protocol-like-tornado-cash>)

## 1. Implement FATF Recommendations

A compliance system is only as strong as its weakest link. The United States should launch a concerted effort, consisting of both diplomacy and enforcement actions, to ensure FATF members adopt the organization's guidance for crypto regulation. In October 2018, FATF recommended that all member states establish AML/CFT regulations for both cryptocurrency firms and other entities involved in the crypto business, including those facilitating the administration and storage of virtual currencies.<sup>47</sup> In June 2019, FATF issued additional guidance for implementing AML/CFT requirements for VASPs and VAs.<sup>48</sup> This guidance included requirements for gathering customer data for transactions, for developing a risk-based approach for the operations of VASPs and other companies, and on the “travel rule” for virtual currency.

The U.S. Bank Secrecy Act “travel rule” requires all financial institutions to pass on certain information, in certain situations, to the financial institution to which it transmits funds. Subsequent FATF updates in 2020 and 2021 refined the travel rule, focusing on value/asset transfer regulation to crypto firms. However, few foreign jurisdictions have implemented the travel rule, and VASPs that operate in less strict regulatory environments may not be aware of or feel obligated to comply with such regulations.<sup>49</sup> The United States should work to ensure VASPs and foreign regulators follow the travel rule. Washington should encourage crypto firms to adopt technologies that facilitate the transfer of data regarding cryptocurrency senders and recipients and virtual asset transactions. If necessary, the U.S. government can mandate adoption of the rule as a precondition for a firm to operate legally in the United States.

Concurrently, the administration (including the Treasury Department's Office of Terrorist Financing and Financial Crimes) and Congress can assist in standardizing cryptocurrency terminology across foreign jurisdictions. This is one of the biggest challenges facing the cryptocurrency market, as terminology associated with crypto products varies significantly from one jurisdiction to another. The United States should make clear to jurisdictions with insufficient AML/CFT regimes for VASPs that Washington will consider sanctions, the use of Section 311 “special measures,” and other enforcement actions against entities that threaten the integrity of the U.S. financial system.

While implementing FATF's requirements is challenging for the crypto sector, it will ultimately increase trust in cryptocurrency and virtual assets as a safe and effective means to transfer value.

## 2. Regulate By Enforcement When Necessary

In recent years, U.S. regulatory authorities have taken to regulating digital assets by enforcement. While regulating by enforcement is not ideal in the first instance, it may become increasingly necessary to drive

.....  
47. Financial Action Task Force, “Regulation of Virtual Assets,” accessed November 22, 2022. (<https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html>)

48. Financial Action Task Force, “Public Statement on Virtual Assets and Related Providers,” accessed November 22, 2022. (<https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html>); Financial Action Task Force, “Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,” accessed November 22, 2022. (<https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>)

49. Financial Action Task Force, “Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers,” June 2022. (<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf>)

industry-wide change. The Treasury Department’s Office of Foreign Assets Control (OFAC) has a long history of using enforcement actions to communicate key compliance messages in “teachable moments.”

In its enforcement action against wallet platform BitGo in December 2020, OFAC alleged that BitGo collected IP address information but did not screen that information to determine its geographic origins. As a result, persons in comprehensively sanctioned jurisdictions were able to benefit from BitGo’s services. This action underscored OFAC’s expectation that if companies have data, including location data, they must screen it for sanctions risk. OFAC reinforced this lesson in its October 2021 guidance for the virtual currency industry and in more recent actions against Bittrex and Kraken, which OFAC found had users located in sanctioned countries based on IP data the firms failed to adequately screen.<sup>50</sup>

3. Consider Regulations Governing Privacy Coins, Virtual Currency Mixers, and Mining Pools

Privacy coins like Monero and virtual currency mixers like Tornado Cash can undermine the legitimacy of the cryptocurrency industry and frustrate the purpose of the global AML/CFT framework. They must be better regulated. Transparency in mining pools may also be necessary to prevent the use of these tools for AML/CFT or sanctions evasion.

Policymakers and the crypto community need to strike a balance between security and privacy. This means finding the right solutions to ensure that even privacy-enhancing tokens, entities, and protocols address the risks of illicit finance. If risk management features are technically feasible, regulators will have to determine the extent to which they can require these features in products/protocols without violating free speech.

4. Require Minimum Standards for Cybersecurity

Some of the greatest threats to VA holders today comes from cyberattacks, hacks, and ransomware attacks. The failure of VASPs to invest in cybersecurity measures leaves the public vulnerable. The administration and Congress should consider minimum standards for cybersecurity for a VASP to maintain its legal status.

5. Invest in Blockchain Analysis Tools and Software

Ample analytic tools and software can track — and potentially interdict — illicit activity on the blockchain. The administration and Congress should work together to ensure all appropriate federal, state, and local agencies have access to such tools. Congress should consider legislation requiring exchanges to build these tools and software into their compliance frameworks, with penalties applied to platforms that do not comply. In April 2022, New York State’s Department of Financial Services advised all virtual currency business entities to use blockchain analytics to augment KYC-related controls and to conduct both transaction monitoring and sanctions screening of on-chain activity.<sup>51</sup> Federal regulators should consider similar measures.

.....  
50. U.S. Department of the Treasury, Office of Foreign Asset Control, “Sanctions Compliance Guidance for the Virtual Currency Industry,” October 2021. ([https://home.treasury.gov/system/files/126/virtual\\_currency\\_guidance\\_brochure.pdf](https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf)); U.S. Department of the Treasury, “Treasury Announces Two Enforcement Actions for over \$24M and \$29M Against Virtual Currency Exchange Bittrex, Inc.,” October 11, 2022. (<https://home.treasury.gov/news/press-releases/jy1006>); U.S. Department of the Treasury, “OFAC Settles with Virtual Currency Exchange Kraken for \$362,158.70 Related to Apparent Violations of the Iranian Transactions and Sanctions Regulations,” November 28, 2022. ([https://home.treasury.gov/system/files/126/20221128\\_kraken.pdf](https://home.treasury.gov/system/files/126/20221128_kraken.pdf))

51. State of New York Department of Financial Services, “Virtual Currency Guidance,” April 28, 2022. ([https://www.dfs.ny.gov/industry\\_guidance/industry\\_letters/il20220428\\_guidance\\_use\\_blockchain\\_analytics](https://www.dfs.ny.gov/industry_guidance/industry_letters/il20220428_guidance_use_blockchain_analytics))

## 6. Establish Due Diligence Regulations for Crypto Exchanges in Higher Risk Jurisdictions

Exchanges in higher-risk jurisdictions require little or no user identity verification to transfer crypto assets or convert crypto assets to a fiat currency. These exchanges often have limited payment transparency standards and weak transaction monitoring and sanctions screening controls. VASPs in well-regulated jurisdictions should be required to apply specific and enhanced due diligence standards to crypto service providers in jurisdictions with systemic AML/CFT deficiencies. Traditional financial institutions are expected to apply a higher standard of scrutiny to foreign correspondent relationships in high-risk jurisdictions. VASPs must be no different.

In the years ahead, bipartisan leadership will be needed to weigh the costs and benefits of regulatory and legislative measures, with an eye toward strengthening our country's AML/CFT architecture and defending U.S. national security interests in the Web3 world. Ignoring glaring problems simply invites a national security version of the FTX implosion.

## Foundation for Defense of Democracies (FDD)

FDD is a Washington, DC-based nonpartisan research institute focusing on national security and foreign policy.

## FDD's Center on Economic and Financial Power (CEFP)

FDD's Center on Economic and Financial Power (CEFP) studies national economic security, with a focus on how the United States can leverage its economic and financial power to achieve its national security objectives. CEFP promotes greater understanding of how the U.S. government can best employ its economic and financial authorities to counter its adversaries.

---

**Richard Goldberg** is an FDD senior advisor. He previously served as a White House National Security Council official, as deputy chief of staff and national security advisor for Senator Mark Kirk, as founding staff director of the bipartisan House U.S.-China Working Group, as chief of staff for Illinois Governor Bruce Rauner, and as a Navy reserve intelligence officer. **Alex Levitov** is an Associate Managing Director at K2 Integrity, where he advises financial institutions, technology firms, and jurisdictional authorities on assessing and managing financial crime risks. He holds a Ph.D. in politics from Princeton University and has held fellowships at the Princeton Institute for International and Regional Studies and Stanford University's Center for Ethics in Society.

---

*FDD values diversity of opinion and the independent views of its scholars, fellows, and board members. The views of the authors do not necessarily reflect the views of FDD, its staff, or its advisors.*