FACTCOALITION
Financial Accountability & Corporate Transparency

November 3, 2022

To: Jon Fishman, Assistant Director, Office of Strategic Policy, Terrorist Financing and Financial Crimes

Submitted electronically via www.regulations.gov.

Re: Ensuring Responsible Development of Digital Assets; Request for Comment (87 FR 57556)

Dear Assistant Director Fishman,

This letter responds to the request by the Department of the Treasury ("Treasury") for comment on its notice regarding how to ensure responsible development of digital assets in the United States ("Notice").[1] Treasury is to be commended for deepening its analysis of illicit finance and national security risks posed by the misuse or improper development of digital assets and related technologies, helping to coordinate U.S. regulatory and enforcement policies involving digital assets, and inviting public comment on its actions to date, including issuance of its 2022 action plan to guide next steps.[2]

The FACT Coalition strongly supports Treasury's plans to focus on combating illicit financing and national security risks relating to digital asset technologies[3] that facilitate anonymous or difficult-to-trace digital transactions.[4] Digital asset proponents often praise the public nature of blockchains as a way to minimize fraud, increase efficiencies, lower costs, and ensure fair dealing, but the facts show that too many blockchain operators and users work to develop and exploit digital asset technologies that conceal their identities and digital transactions. If digital assets are to play a positive role in financial markets, financial regulators need to take strong action to apply comprehensive anti-money laundering (AML), countering-financing-of-terrorism (CFT), and reporting protocols to the digital asset ecosystem; apply a

[1] Treasury, "Ensuring Responsible Development of Digital Assets; Request for Comment," Treasury Notice, 87 Fed. Reg. 57556 (Sept. 20, 2022). For the purpose of this comment, FACT will generally rely on and use the definitions used by Treasury in its Action Plan to Address Illicit Financing Risks of Digital Assets, (Sept. 20, 2022), https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf (hereinafter "2022 Action Plan").
[2] See 2022 Action Plan supra note 1.
[3] While FACT recognizes the distinction that Treasury has drawn between "virtual" and "digital" assets, this letter uses the broader term "digital assets" to encompass both types of assets, unless referring specifically to virtual asset service providers. See 2022 Action Plan supra note 1 at p.2.
[4] Related to these risks are risks regarding tax evasion and aggressive tax avoidance that are posed by certain digital asset technologies, including in light of the various intersections between illicit financial flows and tax evasion. See, e.g. IMF, The IMF and the Fight Against Illicit and Tax Avoidance related Financial Flows (Mar. 8, 2021), https://www.imf.org/en/About/Factsheets/Sheets/2018/10/07/imf-and-the-fight-against-illicit-financial-flows#:~:text=Illicit%20financial%20flows%20refer%20to,use%20(e.g.%20terrorist%20financing). These risks should be considered in concert, and FACT will note particular areas where Treasury might advance reforms that address any combination of illicit financing, national security, and tax evasion risks.

more aggressive approach to regulating anonymity-enhancing technologies; and continue to prosecute those who misuse those technologies to commit crimes, swindle investors, evade taxes, or engage in other wrongdoing.

In response to Treasury's request for comments on additional steps that can be taken by the U.S. government, including Treasury, to ensure responsible development of digital assets in the United States in light of illicit financing and national security risks, FACT respectfully recommends that U.S. regulators take at least the following steps as explained in more detail later in this letter:

(1) **Anonymity-Enhancing Technologies:** Prohibit U.S. financial institutions from using or transacting with mixers and other anonymity-enhancing technologies for digital assets and from handling, using, or transacting with digital assets that have been anonymized by those technologies. Commit additional resources to monitor and support enforcement actions combatting existing and emerging anonymity-enhancing technologies.

(2) **Opaque Blockchains and Privacy Coins:** Prohibit U.S. financial institutions from handling, using, or transacting with digital assets on opaque blockchains, privacy coins, or digital assets using similar cryptotechnologies.

(3) **Digital Asset Rulemakings:** Complete four rulemakings related to digital assets, including (i) the proposed rule seeking to strengthen the travel rule for digital transactions; (ii) the proposed rule applying currency transaction reporting requirements to digital assets and requiring certain U.S. financial institutions to comply with customer identification, recordkeeping, and information reporting requirements for certain transactions involving unhosted wallets or hosted wallets in identified foreign jurisdictions; (iii) the proposed rule implementing 26 U.S.C. 6050I tax reporting requirements for digital asset transactions exceeding $10,000; and (iv) the proposed rule implementing 26 U.S.C. 6045 information return requirements regarding digital assets, including defining covered brokers to encompass a broad cross-section of service providers based on facilitating activities performed to effectuate digital asset transactions.

(4) "**Decentralized" Technologies:** Issue guidance on the application of the definition of "money service businesses" to enterprises employing decentralized technologies involving digital assets, ensuring coverage of a broad cross-section of service providers based on facilitating activities performed to effectuate digital asset transactions.[5]

[5] FACT recognizes that Treasury has stated that "certain persons despite characterizing themselves as P2P service providers or DeFI protocols may constitute a VASP and thus have AML/CFT obligations." See 2022 Action Plan at 5. FACT agrees with this conclusion, and encourages Treasury to issue clear guidance addressing this critical problem. FACT's recommendation here is meant to offer one potential solution, but is not meant to limit the United States government in implementing and enforcing effective and consistent AML/CFT protections across the U.S. financial system, including the digital asset sector.

(5) **Public and Private Keys:** Require virtual asset service providers (VASPs) to obtain for each digital asset they handle the relevant client's public and private keys as part of the provider's mandatory Know Your Customer (KYC) information for digital assets, and require production of that information to law enforcement in response to an appropriate request.

(6) **AML/CFT Examination Teams:** Establish specialized AML/CFT examination teams for MSBs that handle digital assets, similar to the AML/CFT examination teams for banks, and conduct periodic examinations of MSBs that currently do not undergo them. Consider whether and under what circumstances bank AML/CFT examination teams should prioritize review of a bank's digital asset activities.

(7) **Beneficial Ownership Registry:** Provide guidance to the digital asset community on what entities must file reports with the new U.S. beneficial ownership registry; as well as what U.S. and non-U.S. law enforcement and regulatory agencies handling digital asset matters can access registry information and how they can request specific data.

(8) **FSOC and OFR:** Explicitly enlist both the Financial Stability Oversight Council and the Office of Financial Research in the work to monitor and analyze the risks and threats posed by digital assets, and consider directing them to analyze the extent to which higher capital requirements should apply to high-risk digital asset activities.

This letter proceeds in five parts. First, it provides a brief background on the digital asset risks identified by Treasury. Second, this letter commends Treasury for its efforts to create and implement an international framework for protecting against the AML/CFT, national security, and tax evasion risks associated with digital assets, and offers recommendations to strengthen those endeavors. Third, this letter explains in more detail FACT's eight recommendations, listed above, for additional steps to ensure responsible development of digital assets in the United States. Fourth, this letter acknowledges and makes recommendations with respect to the outreach by Treasury to private industry. Finally, it counters claims by some critics that Treasury lacks authority to take enforcement actions and issue effective AML/CFT and tax reporting rules related to digital assets.

The Financial Accountability and Corporate Transparency (FACT) Coalition is a non-partisan alliance of more than 100 state, national, and international organizations working toward a fair tax system that addresses the challenges of a global economy and promoting policies to combat the harmful impacts of corrupt financial practices. As part of our initiative, FACT provides this comment letter to clarify, strengthen, and encourage strong enforcement of AML/CFT and reporting requirements in the digital asset sector.

A. Background

As Treasury has demonstrated and explained, mounting evidence shows that digital assets are frequently used to commit wrongdoing. Instances include digital assets being used

to: (i) fund rogue regimes, such as via the multi-million-dollar thefts perpetrated by the North Korean-affiliated Lazarus Group; (ii) finance terrorism; (iii) launder money; and (iv) otherwise enable illicit financial flows.[6] Even industry advocate Chainanalysis has estimated that over $8.6 billion was laundered through cryptocurrencies in 2021, of which a significant portion was moved through decentralized protocols.[7]

Allowing digital asset users to employ technologies that enable them to avoid U.S. anti-money laundering/countering-the-financing-of-terrorism (AML/CFT) safeguards creates dangerous loopholes in the U.S. financial regulatory system. Those loopholes can enable the proliferation of weapons of mass destruction, international drug-trafficking, corruption, human-trafficking, tax evasion, and other illicit activity that may ultimately destabilize democracy at home and abroad. The failure to effectively regulate digital assets in light of illicit finance risks creates a pressing national security risk that cannot be ignored.

Treasury must move quickly to apply current U.S. AML/CFT safeguards to digital assets without creating loopholes or unintended consequences that may subject U.S. markets to abuse by corrupt or criminal actors. Treasury's ongoing work with other federal agencies, state regulators, and other jurisdictions to strengthen regulatory practices and resolve cross-jurisdictional pitfalls or inconsistencies involving digital assets also merits priority consideration. To the extent Treasury believes that it does not have the tools necessary to apply the U.S. AML/CFT framework in an effective way to existing and emerging digital assets, Treasury should clearly and publicly identify any legal or statutory limitations so that Congress can act.

The remainder of this letter responds to Treasury's current efforts related to digital assets, provides recommendations in response to certain questions posed by the Notice, and rejects concerns raised by some digital asset proponents regarding the constitutionality of U.S. actions to counter anonymity-enhancing technologies that compromise U.S. national security, financial, and tax systems.

a. Treasury is Correct to Identify, Prioritize, and Address Illicit Finance Risks Posed by Digital Assets (Question A.1)

FACT commends Treasury for identifying a wide range of illicit financing risks associated with digital assets, including money laundering, ransomware, proliferation financing, sanctions evasion, malicious cybertattacks, and terrorist financing.[8] In addition, Treasury has identified important vulnerabilities in U.S. and global digital asset safeguards, including gaps in controls applicable to cross-border digital asset transfers; uneven and often inadequate regulation and

[6] See, e.g., 2022 Action Plan supra note 1; Treasury, National Money Laundering Risk Assessment (February 2022), https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf.
[7] See Gertrude Chavez-Dreyfuss, *Crypto Money Laundering Rises 30% in 2021-Chainanlysis*, Reuters (Jan. 26, 2022), https://www.reuters.com/technology/crypto-money-laundering-rises-30-2021-chainalysis-2022-01-26/.
[8] See 2022 Action Plan, supra note 1, at pp. 2-4. Other Treasury reports also note tax evasion and aggressive tax avoidance risks posed by digital assets. See, e.g., Treasury, "The American Families Plan Tax Compliance Agenda," (5-2021), Treasury report, at 20-21, https://home.treasury.gov/system/files/136/The-American-Families-Plan-Tax-Compliance-Agenda.pdf. See also IMF supra note 4.

supervision of digital asset transactions across jurisdictions; the increasing use of anonymity-enhancing and allegedly autonomous digital technologies; gaps in the regulation of digital transactions involving unhosted wallets; the failure to apply AML/CFT controls to financial institutions functioning as intermediaries in some digital asset transactions; distributed operations in which digital asset service providers register in one country, locate personnel in another, and offer services in multiple countries with differing rules; and virtual asset service providers that fail to comply with their registration, AML/CFT, recordkeeping, and reporting obligations.[9]

Treasury should continue to prioritize these issues as they are essential in analyzing, mitigating, and deterring existing and emerging money laundering and terrorist financing practices in the digital sector, facilitated by the use of anonymity-enhancing technologies. The use of mixers, chain-hopping, and decentralized financial services, among other factors, are enabling malicious actors to continue their criminal activity with few to no repercussions.

FACT recommends that Treasury commit to regularly reviewing and publicly updating trends in and the status of digital asset illicit finance risks and the anonymity-enhancing technologies that threaten U.S. interests.

b. Treasury Should Continue its Active Role in Global Implementation of Consistent, Comprehensive AML/CFT Standards and Tax Reporting Requirements, Including Through Its Participation at OECD and FATF (Questions C.1 and C.2)

Treasury is correct to prioritize multilateral and bilateral engagement to promote the effective implementation of AML/CFT regulation and enforcement best practices, including to (i) support coordinated, comprehensive and robust international AML/CFT regulation and enforcement with respect VASPs and other parties engaged in a digital asset transactions; (ii) improve information collection, storage, and sharing best practices in the digital asset ecosystem; and (iii) support capacity building to assist countries implementing international AML/CFT standards for digital assets and related service providers. FACT recommends that this work include continuing to advocate for best practices at the FATF and OECD levels, as well as working to ensure that the United States is regulating digital assets and related service providers and users in line with international best practices. This work should also include continuing to monitor the advancement of best practices occurring in our partner jurisdictions, such as with respect to the recent EU AML 6 directive, in which the EU reached an agreement to advance a travel rule more consistent with FATF best practices.[10] To the extent that Treasury identifies jurisdictions that are particularly risky or subject to abuse, Treasury should pursue appropriate action to restrict the ability of U.S. persons to conduct digital transactions within those jurisdictions.

[9] See 2022 Action Plan, supra note 1 at pp. 4-7.
[10] European Council, Anti-money laundering: Provisional agreement reached on transparency of crypto asset transfers, EU (Jun. 29, 2022), https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/.

As part of Treasury's annual risk assessment obligations relating to SARs, or otherwise, FACT recommends that Treasury identify actions Treasury is taking, as necessary, to implement international best practices in AML/CFT protocols based on its work internationally and emerging trends. Treasury should also identify any additional authorities it may need to regulate, exchange information, or support capacity building in developing countries to advance international best practices in AML/CFT controls related to digital transactions.[11]

B. Recommendations for Additional Steps by Treasury to Ensure Responsible Development of Digital Assets in the United States

Financial innovation should be encouraged within the confines of U.S. regulatory and enforcement regimes, and disallowed when designed to circumvent safeguards intended to protect U.S. markets, financial systems, and national security. For decades, Congress and U.S. financial regulators have limited or prohibited financial innovations or design choices found to be incompatible with the public interest. For example, the Corporate Transparency Act recently banned the creation of bearer share entities in the United States due to the illicit finance risks associated with entities whose owners cannot be easily determined.[12] The Dodd-Frank Act of 2010 banned unregulated swap markets, instead requiring swap dealers and swap exchanges to comply with registration, recordkeeping, reporting, margin, anti-manipulation, conflict of interest, and other limits, due to the financial risks posed to the U.S. economy by unregulated swaps.[13] The Patriot Act of 2001 prohibited U.S. financial institutions from opening accounts for foreign shell banks, due to the money laundering risks posed by foreign banks operating without any physical presence.[14] Bearer shares, unregulated swaps, and shell bank accounts were financial design choices that were promoted as innovations, but later subjected to tighter regulation to protect U.S. markets, financial systems, and national security. "Innovative" digital asset technologies should be treated the same way.

---

[11] The United States government is also behind as it relates to reciprocal information exchange with partner jurisdictions for tax purposes, such as under the Foreign Account Tax Compliance Act (FATCA), which may accompany and increase illicit financing and national security risks. See, e.g., Statement of Ryan Gurule Before the European Parliament Re: The Exchange of Information, FACT Coalition (Mar. 28, 2022), https://www.europarl.europa.eu/cmsdata/246386/Ryan%20Gurule%20Statement.pdf. This is particularly relevant in light of the recent efforts by the OECD to create a new global tax transparency framework with respect to the exchange of information relating to crypto-assets, the ownership of which has not previously been the subject to Common Reporting Standard exchange. See OECD, OECD presents new transparency framework for crypto-assets to G20 (Oct. 10, 2022), https://www.oecd.org/newsroom/oecd-presents-new-transparency-framework-for-crypto-assets-to-g20.htm. As proposed by President Biden in his 2023 Budget, the United States should move forward with advancing truly reciprocal tax information exchange with partner jurisdictions, including relating to the exchange of information with respect to digital assets. Department of the Treasury, General Explanations of the Administration's Fiscal Year 2023 Revenue Proposals (Mar. 2022), https://home.treasury.gov/system/files/131/General-Explanations-FY2023.pdf. In the same vein, it is essential that forthcoming rules regarding access to the beneficial ownership directory being created pursuant to the Corporate Transparency Act, which will require reporting with respect to the beneficial ownership of certain decentralized autonomous organizations (DAOs) in the United States, should guarantee uncomplicated access to partner jurisdictions, as further discussed below. See, e.g., FACT Coalition, Re: Beneficial Ownership Reporting Requirements (Feb. 7, 2022), https://thefactcoalition.org/corporate-transparency-acts-draft-rule-applauded-by-fact-coalition/.

[12] 31 U.S.C. § 5336(f).

[13] Dodd-Frank Act, Part 2, § 721 et seq.

[14] 31 U.S.C. § 5318(j).

The 2022 Treasury Action Plan identifies a number of anonymity-enhancing digital asset innovations that raise illicit financing concerns including enhanced cryptography and anonymity-enhanced cryptocurrencies, mixers, tumblers, chain hopping (including, through cross chain bridges),[15] and opaque blockchains.[16] Each is designed to reduce transparency in digital asset transactions, either by making it more difficult to trace the origin or movement of those assets or obscuring the identities of the parties involved in the transactions. For example, in March 2022, the so-called Lazarus Group – a malicious cyber gang associated with North Korea – used mixers to steal about $620 million in digital assets from a blockchain, cloak the movement of those assets, and make the assets available for money laundering and other wrongdoing by its gang members or North Korea.[17]

The anonymity-enhancing technologies identified in the Treasury Action Plan appear to offer no legitimate financial or efficiency benefits to U.S. markets, financial systems, or the public, while at the same time facilitating a variety of illicit financing activities. As a result, those anonymity-enhancing technologies warrant greater regulatory scrutiny, increased enforcement actions, and additional restrictions to limit the risks posed to U.S. financial institutions, markets, and the public.

The 2022 Treasury Action Plan also identifies disintermediation and lax registration and AML/CFT compliance by virtual asset service providers (VASPs) as a key sources of illicit financing and national security risks for digital assets.[18] These factors also create tax evasion risks, contributing to and occurring alongside illicit financing and national security risks, as discussed above. Treasury is correct to note that some digital asset transactions may distribute effectuating activities in a manner that makes it difficult to apply and enforce current AML/CFT and tax evasion protocols against actors that have not historically been identified as MSBs or other regulated parties.[19] At the same time, some experts insist that, in most cases, characterizing digital asset transactions as occurring solely between two persons without any other person involved in effectuating the identified transaction, is inaccurate and generally misleading.[20] It is important that steps be taken by Treasury, and the U.S. government more generally, to counter all attempts to evade U.S. AML/CFT, national security, and tax evasion controls and ensure that the same safeguards that constrain wrongdoing in other financial sectors also apply in the digital asset sector.

---

[15] See Cross-chain Crime: More Than Half a Billion Dollars has Been Laundered Through a Cross-chain Bridge, Elliptic (Oct. 8, 2022), https://hub.elliptic.co/analysis/cross-chain-crime-more-than-half-a-billion-dollars-has-been-laundered-through-a-cross-chain-bridge/.
[16] See, e.g., 2022 Action Plan at 2-3, 6.
[17] See 2022 Action Plan at 3; Treasury, "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats," (May 6, 2022), Treasury press release, https://home.treasury.gov/news/press-releases/jy0768.
[18] See, e.g., 2022 Action Plan supra note 1 at 4-6.
[19] See id.
[20] See, e.g., Nicholas Weaver, "OFAC Around and Find Out," (Aug. 19, 2022), Lawfare, https://www.lawfareblog.com/ofac-around-and-find-out.

The Notice requests comment on additional steps that can be taken by the U.S. government to "deter, detect, and disrupt the misuse of digital assets and digital asset service providers by criminals" (Question B.1); "better mitigate illicit financing risks associated with digital assets" (Question B.4); "address the illicit finance risks related to mixers and other anonymity-enhancing technologies" (Question B.7); "mitigate the illicit finance risks related to DeFi" (Question B.8); "improve AML/CFT and sanctions compliance" by private sector entities using digital assets (Question D.4), "disrupt illicit finance associated with digital assets" (Question D.4); "maximize the development and use of emerging technologies like blockchain analytics, travel rule solutions, or blockchain native AML/CFT solutions" to "strengthen AML/CFT compliance related to digital assets" (Question D.7); and encourage financial institutions to "better integrate" their AML/CFT controls for fiat currency into their "digital asset transaction monitoring and customer identification" and better "identify, mitigate, and report illicit finance risks" (Question D.8).

The 2022 Treasury Action Plan already identifies multiple steps that the U.S. government expects to take to address those issues, all of which FACT supports, subject to the recommendations in this letter. In addition, FACT respectfully recommends the following additional actions that could be taken to address illicit finance, national security, and tax evasion risks related to digital assets.

Anonymity-Enhancing Technologies. FACT recommends that Treasury, working with other U.S. financial regulators, take action to prohibit U.S. financial institutions from using or transacting with mixers and other anonymity-enhancing technologies for digital assets and from handling, using, or transacting with digital assets that have been anonymized by those technologies. These prohibitions merit consideration because the primary purpose and effect of those technologies is to make it more difficult to trace the origin and movement of digital assets and identify the persons involved with the transactions. The U.S. Department of Justice (DOJ), working with the Internal Revenue Service (IRS) and Financial Crimes Enforcement Network (FinCEN), has already demonstrated how some digital asset businesses use mixer and tumbler technologies to conceal, transfer, and launder hundreds of millions of dollars in illicit funds generated by illegal activities.[21]

Earlier this year, for example, Treasury's Office of Foreign Assets Control (OFAC) imposed sanctions on Tornado Cash, an open-source software protocol which allegedly operates as an automated mixer, pooling certain digital assets, mixing and anonymizing them, and then transmitting the resulting assets to designated persons.[22] OFAC determined that Tornado Cash had been used to launder more than $7 billion in digital assets since its creation in 2019, including over $455 million in assets stolen by the North Korean-sponsored hacking

[21] See, e.g., DOJ, "Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin 'Mixer' That Laundered Over $300 Million," (8-18-2021), DOJ press release, https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million; Treasury, "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats," (May 6, 2022), Treasury press release, https://home.treasury.gov/news/press-releases/jy0768.

[22] Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," Treasury press release (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.

gang, the Lazarus Group. After OFAC imposed sanctions, many users stopped employing or providing services with respect to the software. Tornado Cash developers and others have since challenged OFAC and Treasury in court, claiming that the software is fully automated, functions only to ensure the privacy of digital asset users, and can't be sanctioned under U.S. law in the same way as an individual, entity, or property.[23] As discussed below, these claims are not substantiated.

In addition, FACT respectfully recommends that Treasury commit additional resources to monitor and support enforcement actions combatting existing and emerging anonymity-enhancing technologies related to digital assets.

Opaque Blockchains and Privacy Coins. Some digital asset industry participants have designed new technologies to conceal or otherwise obscure digital asset transaction information on a more system-wide basis, making blockchain analysis more difficult for digital asset users, financial institutions, and law enforcement.[24] Some of those technologies conceal transaction amounts, the origin or destination of asset transfers, or the identity of various parties involved with specific transactions. The technologies offer new ways to reduce transparency in digital asset transactions – financial innovations which will inherently benefit wrongdoers seeking to use blockchains for illicit purposes. It is no surprise that those technologies are being developed at the same time U.S. law enforcement has strengthened its ability to analyze blockchains and trace illicit proceeds.[25] Treasury, working with other U.S. financial regulators, should prohibit U.S. financial institutions from handling, using, or transacting with digital assets on opaque blockchains, privacy coins, or digital assets using similar cryptotechnologies.

Complete Digital Asset Rulemakings. Right now, Treasury and its component agencies are considering four rulemakings related to digital assets, all of which would strengthen U.S. digital asset safeguards and should be finalized as soon as possible.

Travel Rule. In October 2020, FinCEN proposed a rule that would strengthen the travel rule by lowering its applicable threshold and clarify its application for certain digital asset transfers.[26] Yet, this rule remains unfinalized. Because this rule will produce transaction data vital to detecting, stopping, and deterring illicit financing through digital assets, FACT urges Treasury to issue the final rule as soon as possible, preferably by the end of the first quarter of 2023.

---

[23] Coin Center, "Coin Center is suing OFAC over its Tornado Cash sanction," (Oct. 12, 2022), Coin Center press release, https://www.coincenter.org/coin-center-is-suing-ofac-over-its-tornado-cash-sanction/.
[24] See, e.g., Farid Elwailly, "Sword: An Opaque Blockchain Protocol," (Sept. 26, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3699925.
[25] See, e.g., DOJ, "Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency," (Feb. 8, 2022), DOJ press release, ("In a futile effort to maintain digital anonymity, the defendants laundered stolen funds through a labyrinth of cryptocurrency transactions. Thanks to the meticulous work of law enforcement, the department once again showed how it can and will follow the money…."), https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.
[26] See FinCEN Proposed Rule, 85 FR 68005 (Oct. 27, 2020), https://www.federalregister.gov/documents/2020/10/27/2020-23756/threshold-for-the-requirement-to-collect-retain-and-transmit-information-on-funds-transfers-and.

Value Transaction Reports and Unhosted Wallets. In December 2020, FinCEN proposed a rule to extend currency transaction (CTR) reporting obligations to banks and money service businesses (MSBs) handling digital transactions, requiring them to file a Value Transaction Report with FinCEN for digital asset transactions valued in excess of $10,000.[27] The rule also introduced certain recordkeeping procedures with respect to transactions involving unhosted wallets or wallets hosted by financial institutions in jurisdictions to be identified by FinCEN.[28] After Congress provided additional statutory support for the rulemaking by modifying the Bank Secrecy Act to contemplate digital assets,[29] FinCEN updated the rule in January 2021, and separately extended the comment period for the two different aims of the rule.[30] FinCEN has yet, however, to complete the rulemakings. Because these rules will address a critical vulnerability in U.S. digital asset safeguards, FACT urges Treasury to issue final rules as soon as possible, preferably by the end of the first quarter of 2023.

Section 6045 Returns and 6050I Reports. In 2021, as part of the Infrastructure Investment and Jobs Act, Congress strengthened federal tax reporting requirements for digital asset transactions under 26 U.S.C. §§ 6045 and 6050I. The law requires digital asset brokers to submit annual information returns under Internal Revenue Code (IRC) Section 6045 to the IRS reporting certain digital asset transactions and client identifying information.[31] The law also requires brokers to begin filing those returns in 2024. In addition, the same 2021 statute amended IRC Section 6050I to require reporting on trade or business digital asset transactions valued in excess of $10,000.[32] Both of the new provisions raise issues requiring clarification from Treasury, including with respect to the definition of "brokers" that must file 6045 returns and details regarding which digital business transactions are subject to 6050I reporting. Because both reporting requirements will produce transaction data vital to detecting, stopping, and deterring illicit financing through digital assets, including tax evasion, FACT respectfully recommends that Treasury complete rulemakings to implement the new provisions as soon as possible and no later than the end of 2023. FACT also recommends that Treasury clarify in the section 6045 rules that covered "brokers" encompass a broad cross-section of

[27] See FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," (Dec. 23, 2020), 85 FR 83840, FinCEN proposed rule, https://www.federalregister.gov/documents/2020/12/23/2020-28437/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets.
[28] See id.
[29] Congress amended the Bank Secrecy Act's definition of "monetary instruments" in 31 U.S.C. § 5312(a)(3)(D) so that it would include digital assets. See section 6102(d) of the Anti-Money Laundering Act of 2020, enacted as Division F of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. Law No. 116-283 (Jan. 1, 2021).
[30] Compare 86 FR 7352, https://www.federalregister.gov/documents/2021/01/28/2021-01918/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets#footnote-1-p7352; with 86 FR 3897, https://www.federalregister.gov/documents/2021/01/15/2021-01016/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets#footnote-1-p3898.
[31] Infrastructure Investment and Jobs Act, Pub. Law No. 117-58, Section 80603(b)(1) and (2). Section 6045 also requires brokers to send copies of the returns to affected clients.
[32] Id., Section 80603(b)(3). Congress should also clarify that reciprocal reporting requirements under the Bank Secrecy Act with respect to cash transaction reporting requirements under section 6050I also apply for digital assets. Cf. 31 U.S.C. 5331; 26 U.S.C 6050I(d).

service providers based on facilitating activities performed to effectuate digital asset transactions.

"**Decentralized" Technologies:** Different technologies within the digital asset ecosystem can be used to disaggregate the various activities that effectuate digital asset transactions. Nonetheless, like any financial ecosystem, digital asset ecosystems require some method of promoting trust between users so that the system functions and transactions may occur.[33] In simplistic terms, the U.S. dollar is backed by the full faith and credit of the United States, and financial intermediaries are utilized to validate and clear transactions between independent third parties. Some digital asset users also rely on more traditional financial intermediaries, but others choose to rely on a series of activities – in some cases, governed by one or more mutually agreed to software programs – to prove that a particular transaction occurred, verify and protect (or store, alter or communicate) rights with respect to asset ownership or control, effectuate a given transaction, or ensure the functionality of the system.[34]

MSBs and other financial institutions should be subject to consistent U.S. AML/CFT, sanctions, and tax reporting requirements whether they facilitate cash transactions, wire transfers, or activities that effectuate digital asset transactions. Treasury is already working with other federal agencies, the fifty states, and internationally to apply the existing AML/CFT, sanctions, and tax reporting frameworks to MSBs, other financial institutions, VASPs, and other actors engaging in or facilitating the activities that effectuate digital asset transactions. At present, however, some digital asset actors are claiming they can operate beyond the reach of U.S. laws.[35]

Treasury has stated that, "certain persons despite characterizing themselves as P2P service providers or DeFI protocols may constitute a VASP and thus have AML/CFT obligations."[36] FACT agrees with this conclusion, and encourages Treasury to issue clear guidance addressing this problem. For example, Treasury should issue additional guidance on the application of the definition of MSB to businesses employing decentralized technologies involving digital assets, ensuring coverage of a broad cross-section of service providers based on facilitating activities performed to effectuate digital asset transactions. Clarification may be provided, for example, on whether certain decentralized autonomous organizations, bridge protocols, and certain digital asset miners or stakers qualify as MSBs subject to U.S. AML/CFT

[33] See, e.g., Matt Levine, *The Crypto Story*, Bloomberg (Oct. 25, 2022), https://www.bloomberg.com/features/2022-the-crypto-story/?leadSource=uverify%20wall.
[34] The often-centralized nature of the various actors that perform the activities necessary to effectuate digital asset transactions support the idea that "decentralized" systems are often not all that decentralized, after all. See, e.g., Weaver supra note 20; *see also* CFTC, "CFTC Imposes $250,000 Penalty Against bZeroX, LLC and Its Founders and Charges Successor Ooki DAO for Offering Illegal, Off-Exchange Digital-Asset Trading, Registration Violations, and Failing to Comply with Bank Secrecy Act," (Sept. 22, 2022), CFTC press release, https://www.cftc.gov/PressRoom/PressReleases/8590-22 (identifying controlling persons associated with the "decentralized" automated organization and potentially illegal marginal trading platform, Ooki DAO).
[35] See 2022 Action Plan supra note 1 at 6.
[36] 2022 Acton Plan supra note 1 at 5. To the extent that any additional clarification is needed to incorporate a consistent definition of VASP into U.S. law and otherwise ensure consistent AML/CFT, sanctions, and tax reporting requirements apply to protect the digital asset sector and the U.S. financial sector more broadly, FACT encourages Treasury to do so (or to work with Congress to achieve this purpose, as necessary).

requirements as a result of facilitating activities performed to effectuate digital asset transactions. Additional guidance may also be warranted to resolve any remaining confusion regarding the ability of the U.S. government to apply sanctions to all members of the digital asset ecosystem, including allegedly autonomous software systems.[37]

Designate Public and Private Keys as KYC Information. Virtual asset service providers (VASPs) currently provide a wide range of services to digital asset users, including validating, storing, and transferring digital assets, exchanging one form of virtual currency for another, cashing out digital assets for fiat currency, and operating or maintaining mixers and tumblers. As money service businesses, VASPs are already required to establish risk-based AML/CFT programs, know their customers, monitor customer transactions, and report suspicious activity to FinCEN. FACT respectfully recommends that, as part of their AML/CFT obligations, VASPs should also be required as a precondition for handling a particular digital asset for a client to obtain and record the relevant public and private keys held by that client with respect to that asset and to provide those keys – along with client identification information – to law enforcement upon an appropriate request. Other financial institutions like banks and securities firms already provide client account numbers to law enforcement when asked; VASPs should do the same with public and private keys. Treasury, working with other U.S. financial regulators, could propose requiring VASPS to obtain, record, and produce a client's public and private keys as part of their mandatory Know Your Customer (KYC) information when handling specific digital assets for that client.

AML/CFT Examination Teams. The 2022 Treasury Action Plan states that one of its priorities is to strengthen U.S. AML/CFT supervision of digital asset activities, including improving registration, examination, and state licensing of VASPs.[38] FACT strongly supports this objective in light of the many enforcement actions demonstrating that VASPs too often disregard or fail to meet their AML/CFT obligations. For example, in 2015, DOJ took a criminal enforcement action against a digital asset exchange for failing to establish an appropriate AML/CFT program.[39] In 2020, the CFTC imposed a $100 million civil monetary penalty against a digital asset futures exchange for failing to register with the CFTC and willfully violating its U.S. AML/CFT obligations.[40] In 2022, FinCEN imposed a $29 million civil monetary penalty against a digital asset exchange for willfully failing to maintain an effective AML/CFT program

[37] OFAC has already issued guidance on sanctions compliance when handling digital assets. See Office of Foreign Assets Control, Sanctions Compliance Guidance for the Virtual Currency Industry (Oct. 2021), https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf. But this guidance may need to be supplemented.
[38] 2022 Treasury Action Plan, supra note 1 Priority Action 4.
[39] DOJ, "Ripple Labs Inc. Resolves Criminal Investigation," (5-5-2015), DOJ press release, https://www.justice.gov/opa/pr/ripple-labs-inc-resolves-criminal-investigation.
[40] CFTC, "Federal Court Orders BitMEX's Three Co-Founders to Pay a Total of $30 Million for Illegally Operating a Cryptocurrency Derivatives Trading Platform and Anti-Money Laundering Violations," (May 5, 2022), CFTC press release, https://www.cftc.gov/PressRoom/PressReleases/8522-22#:~:text=Number%208522%2D22-,Federal%20Court%20Orders%20BitMEX's%20Three%20Co%2DFounders%20to%20Pay%20a,and%20Anti%2DMoney%20Laundering%20Violations.

and failing to file Suspicious Activity Reports, including with respect to transactions that violated U.S. sanctions.[41]

As part of this effort, FACT respectfully recommends the establishment of specialized AML/CFT examination teams for MSBs that handle digital assets, similar to the AML/CFT examination teams already employed by federal banking regulators for banks, and that these teams conduct periodic examinations of MSBs that currently do not undergo regular AML/CFT examinations. Regulatory AML/CFT examinations of MSBs are not only less resource-intensive than criminal proceedings, but can also prevent or remediate lax AML/CFT performance through regulatory directives and consent agreements. Establishing a system for conducting MSB AML/CFT examinations warrants immediate and sustained action by Treasury and FinCEN.

FACT also recommends that Treasury consider whether and under what circumstances bank AML/CFT examination teams should prioritize review of a bank's digital asset activities.

Provide Guidance on Beneficial Ownership Registry Reporting and Access. In 2021, Congress enacted the Corporate Transparency Act and required FinCEN to establish a registry containing beneficial ownership information for corporations, limited liability companies, and similar entities formed or registered to do business in the United States.[42] In September, FinCEN finalized the first of three rules to establish the beneficial ownership registry.[43] FACT respectfully recommends that, based upon the first final rule, Treasury issue guidance to the digital asset community on what types of entities – such as foreign-based VASPs or decentralized autonomous organizations handling digital transactions for U.S. persons, mining companies transferring coin ownership to U.S. clients, or bridge protocols transferring assets to a wallet held by a U.S. person – are required to file reports with the beneficial ownership registry as a result of being formed or doing business in the United States. In addition, once the second rule implementing the registry is finalized, Treasury should consider issuing guidance clarifying which U.S. and non-U.S. law enforcement and regulatory agencies handling digital asset matters can access U.S. registry information and how they can request specific data. FACT strongly supports rules that make registry access uncomplicated and useful for U.S. and non-U.S. law enforcement investigating illicit financing or other suspicious activity involving digital assets.

Enlist FSOC and OFR. The Financial Stability Oversight Council (FSOC), which is chaired by the Treasury Secretary, is charged with identifying "risks to the financial stability of the United States" and responding to "emerging threats" to the stability of the U.S. financial system.[44] Among other actions, FSOC is authorized to collect agency information and market

[41] FinCEN, "FinCEN Announces $29 Million Enforcement Action Against Virtual Asset Service Provider Bittrex for Willful Violations of the Bank Secrecy Act," (Oct.11, 2022), FinCEN press release, https://www.fincen.gov/news/news-releases/fincen-announces-29-million-enforcement-action-against-virtual-asset-service.
[42] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Title LXIV (entitled the Corporate Transparency Act), Pub. Law No. 116-283 (1-1-2021).
[43] FinCEN, "Beneficial Ownership Information Reporting Requirements," final rule, 87 Federal Register 59498 (Sep. 30, 2022).
[44] 12 USC § 5322(a)(1).

data, direct work by the Office of Financial Research (OFR), recommend federal regulatory supervisory priorities and principles, and establish special advisory, technical, or professional committees to help carry out its responsibilities.[45] Even though the misuse of digital assets to advance illicit finance poses the types of risks and threats that FSOC is designed to address, the 2022 Treasury Action Plan does not explicitly mention either FSOC or OFR, even when discussing specific plans to monitor emerging risks related to digital assets.[46] FACT respectfully recommends that Treasury explicitly enlist both FSOC and OFR in the work needed to monitor and analyze the risks and threats posed by digital assets, and consider directing them to analyze the extent to which higher capital requirements should apply to high-risk digital asset activities.

C. **A Private Sector That Routinely Indicates Its Willingness to Be Regulated Should Be Held Accountable Through AML/CFT Engagement and Broad Stakeholder Collaboration** (Questions D.1, .3-.5, .7-.8)

As many of the money-laundering risks relating to digital assets ultimately relate to design choices created, enabled, or perpetuated by the industry itself, as discussed above, we support the U.S. government's efforts to work with the private sector to address AML/CFT concerns. Any such engagement should be focused, first and foremost, on establishing principles for comprehensive AML/CFT and sanctions enforcement compliance that will impact development choices and encourage private industry compliance solutions. At each step of such engagement, it is important that the government consult and consider input from all private sector members, including not just industry, but other stakeholders as well including civil society, academics and technologists inside and outside of the blockchain industry.

In the wake of rising international tensions related to the abuse of digital assets by terrorists, organized crime, and other wrongdoers to move and launder illicit funds across borders, industry insiders have repeatedly signaled an openness to increasing regulation to promote trust in the digital asset ecosystem.[47] Indeed, as proponents of digital assets and blockchain technology point out, a compelling feature of blockchain technologies is that the technology is itself a public recordkeeping device that is intended to create a trustworthy financial ecosystem.

At the same time, many in the digital asset industry are expending significant resources to undercut and minimize blockchain transparency and trustworthiness, including by developing opaque blockchains or privacy coins, employing mixer and tumbler technologies to impede tracing of transactions, promoting other anonymity-enhancing technologies that make it difficult or impossible to link digital assets to specific individuals, and failing to develop efficient means to collect and share know-your-customer information across companies, industry sectors, and

[45] 12 USC §§ 5321(d), 5322(a)(1).
[46] 2022 Treasury Action Plan, Priority Action 1.
[47] *See, e.g.*, Phil Rosen, FTX's Sam Bankman-Fried called for firmer regulation of crypto in a new interview. 2 experts shared their predictions for what's to come in 2022 (Feb. 20, 2022), https://markets.businessinsider.com/news/currencies/sam-bankman-fried-ftx-crypto-regulation-experts-security-sec-markets-2022-2.

borders. Designing allegedly autonomous software to execute digital transactions while simultaneously claiming that software can operate outside of AML/CFT controls and accountability measures that apply broadly in other financial sectors is also problematic. Today, the proliferation of anonymity-enhancing technologies in the digital asset marketplace poses a direct challenge to industry claims of blockchain transparency and trustworthiness.

So, when Treasury asks private industry about additional steps that the U.S. government can take to promote innovative technologies designed to improve AML/CFT compliance with respect to digital assets, this inquiry must be addressed in the context of principled rules making it clear that innovations frustrating AML/CFT compliance are not only of no interest but will be strongly discouraged. Doing so is critical to maintaining a trustworthy financial ecosystem that is the underlying purpose of any blockchain, as well as to supporting U.S. financial markets, U.S. national security concerns, and U.S. democracy more broadly.

Assuming consensus can be reached on those principles, the private sector may be helpful in understanding current and emerging AML/CFT risks as well as crafting solutions to some of those risks. For example, private industry may be well positioned to identify technical problems with AML/CFT and sanctions compliance and may be motivated to craft innovative data practices for collecting, storing, and sharing information needed to carry out effective AML/CFT protocols and sanctions enforcement across multinational entities and international borders. To that end, Treasury might consider reframing portions of its outreach to the private sector to solicit solutions to AML/CFT problems that cross international borders, and making clear that in the absence of such solutions, more restrictive regulatory approaches may be pursued. It may also be useful to identify AML/CFT vulnerabilities inherent in certain design choices – such as with respect to certain "anonymity enhancing technologies" or disintermediation – and ask the private sector to provide design solutions in a way that addresses AML/CFT risks and effectively deters use of high-risk technologies. Again, in the absence of such solutions, Treasury should make clear that more restrictive regulatory approaches – such as those recommended in this letter – may be pursued.

It should also be made clear that stakeholders outside of industry – including civil society, academics, and technologists within and without the digital asset industry – are members of the private sector that is being consulted to encourage responsible innovation of digital assets. The digital asset ecosystem reached $3 trillion in combined market capitalization at its peak in late 2021, according to the White House.[48] Risks created by illicit financial flows in digital asset markets cannot be isolated to those markets, and the actors that may be best positioned to comment on ways to mitigate those risks are by no means limited to industry or even the business sector more broadly. As a result, it is important that Treasury does not narrow its lens when soliciting comments from or considering solutions to the illicit financing and national security risks related to digital assets. For example, we understand that a group of technologists and economists at the Digital Economist – focused on responsible tech innovation

[48] See E.O. 14067 (Mar. 9, 2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/.

to address global challenges – have made themselves available for consultation on a number of the issues that Treasury has flagged for the private sector.

D. Treasury Should Reject Claims that Virtual Asset Safeguards and Enforcement Actions Violate the Constitution or other Grants of Authority

In response to actions taken by Congress and Treasury, some industry advocates have raised claims challenging the government's ability to effectively regulate and take enforcement action to stop the illicit finance, national security, and tax evasion risks posed by digital assets. For example, Coin Center – a pro-industry group – has challenged the recent U.S. sanctions imposed on Tornado Cash raising First Amendment claims as well as claims that Treasury exceeded its powers under the International Emergency Economic Powers Act.[49] Coin Center has also challenged section 6050I federal tax reporting requirements, extended by Congress to trade or business transactions involving digital assets in excess of $10,000, raising First Amendment, Fourth Amendment, and Fifth Amendment claims.[50]

The U.S. government, including Treasury, should reject these claims and continue to pursue regulatory safeguards and enforcement actions that protect U.S. markets, the public, and U.S. democracy against illicit financing, national security, and tax evasion risks stemming from digital assets. This comment letter will highlight some of the key weaknesses with those Constitutional and statutory claims.[51]

a. First Amendment Claims Fail to Acknowledge the Public, Voluntary Use of Digital Assets

The First Amendment protects, among other fundamental rights, "the right of the people peaceably to assemble." Courts have interpreted that right as also guaranteeing the freedom of Americans to associate for expressive, often political purposes, free from undue government interference. *NAACP v. Alabama*, 357 U.S. 449 (1958). Digital asset proponents have claimed that this right is impeded by sanctions enforcement and regulations that might expose the political or expressive activities of a digital asset user whose transactions appear on a public blockchain ledger.[52] That is, that information reporting rules that identify a user of digital assets in connection with a specific transaction may reveal identifying information with respect to all expressive, or political activities of that user along the public blockchain ledger.

A separate claim is that U.S. government action to block digital asset users from using anonymity-enhancing technologies, like mixers, prevents users from being able to maintain the confidentiality of their political and expressive activities. For example, some claim that blocking anonymity-enhancing technologies enables the U.S. government – and the public more broadly

[49] See Complaint, Coin Center, et. al, v. Janet Yellen et. al (N.D.FL) (filed 10/12/22), https://www.coincenter.org/app/uploads/2022/10/1-Complaint-Coin-Center-10-12-22.pdf.
[50] See Complaint, Dan Carman et. al. v. Janet Yellen et. al (E.D.KY filed 6/10/222), https://www.coincenter.org/app/uploads/2022/06/1-Complaint.pdf.
[51] These responses are not meant be comprehensive.
[52] See Coin Center v. Yellen supra note 49; Carman v. Yellen supra note 50.

– to use transactions on a public blockchain to uncover an individual's charitable contributions or payment of membership dues to a political organization.

These First Amendment claims fail to take into account the voluntary, public nature of digital asset transactions. No individual is forced to buy, sell, or use digital assets or to make use of a public blockchain. Similarly, no individual is forced to use digital assets on a public ledger to make a charitable contribution or pay dues to a political organization. More fundamentally, blockchains are designed to execute and record financial transactions; they are not designed to help individuals engage in expressive or political associations. The argument that blockchain regulation and enforcement activities inherently impede associational rights is, therefore, difficult to justify.

Digital asset users that voluntarily participate in, and refuse to leave, the digital asset ecosystem can also arrange their affairs to maintain privacy in connection with their expressive or political associations without running afoul of any reporting requirements or sanctions enacted by Congress and implemented by U.S. agencies. Digital asset users do not have to use the same blockchain, wallet, or other readily available and voluntarily chosen digital asset tools for all of their business, personal, and political transactions, mixing them together for convenience. Instead, they can choose to keep these affairs separate. In other words, users can rely on different wallets, accessible via different public or private keys, and transact with different computers or other hardware with separate identifying protocols (whether owned or used at a public library) to carry out specific digital asset transactions. In so doing, users can completely separate, without any meaningful additional cost or burden, transactions that represent expressive or political associations from their other transactions.

More importantly, no law and no reform being contemplated would require any digital asset user to use digital assets in a way that would disclose their expressive or political associations. Any digital asset user may use any other form of currency to make a donation, join an organization, or pay expenses in connection with an association. In so doing, the digital asset user may entirely avoid having transactions related to their expressive or political speech made available on a public ledger.[53] Digital asset proponents raising First Amendment claims fail to show why any digital asset user cannot arrange their affairs to continue to engage in personal and political associations without inviting public scrutiny.

b. Digital Asset Information Reporting Regimes Do Not Violate Fourth Amendment Protections

For similar reasons, industry proponents cannot sustain challenges under the Fourth Amendment to information reporting regimes recently enacted by Congress or proposed by this letter. The Fourth Amendment protects against unreasonable searches and seizures by law enforcement. The Supreme Court has continually held that the Fourth Amendment does not

[53] Claims that certain expressive or political speech – such as donations to assist Ukraine in its defense against Russia – may *also* be made by the use of digital assets confuse administrative convenience with the inability to keep certain types of associative activities confidential.

prevent lawful requests by law enforcement for information made available to third parties or intermediaries as a result of "voluntary" actions, like information provided by individuals using a bank account or making telephone calls. See, e.g., *United States v. Miller*, 425 U.S. 435 (1976)(upholding a lawful subpoena of a criminal defendant's bank records, observing that the defendant had voluntarily provided information to the bank which then produced the records).

Industry proponents have alleged that tax information reporting requirements enacted by Congress that identify users of digital assets in connection with certain specified transactions or circumstances might effectively allow the government to search the transaction history of the digital asset user in an unconstitutional manner. But finding a Fourth Amendment violation in the digital asset context would require a court to reverse decades of Fourth Amendment precedent or determine that digital asset users are somehow entitled to more privacy in their transactions than persons engaging in other transactions, despite the fact that digital asset users voluntarily choose to use systems that utilize public blockchains.

Recently, the Fifth Circuit addressed a Fourth Amendment challenge to a subpoena which obtained blockchain information and used that information to identify a criminal and indict him for procuring child pornography.[54] The appeals court upheld the subpoena, ruling that it obtained third party information that the individual had voluntarily provided, analogizing it to subpoenas that obtain telephone call records or banking information arising from voluntary transactions between an individual and the holder of those records. In addition, the court found that digital asset users could not realistically claim an expectation of privacy given the explicitly public and voluntary nature of virtual asset transactions which are invariably recorded on a public ledger.

Proponents making Fourth Amendment claims also fail to provide a compelling justification as to why information reporting requirements for digital assets merit more protection than reporting requirements related to cash transactions. For example, proponents have alleged that because digital asset transactions rely on private keys and pseudonyms, digital asset users are entitled to enhanced expectations of privacy under the Constitution. But nothing is more anonymous than cash, yet courts have repeatedly upheld reporting requirements under the Bank Secrecy Act and Internal Revenue Code for cash transactions. See, e.g., *United States v. Goldberger Dubin PC,* 935 F.2d 501(2nd Cir. 1991)(upholding the constitutionality of section 6050I's reporting requirements).

Some digital asset proponents nevertheless insist that the voluntary and continual disclosure of personal information on a public ledger somehow creates additional Fourth Amendment rights. This claim is wrong for two reasons. First, the ledger is public – not by virtue of government requirements, but by design of the blockchain users. Second, the voluntary surrender of identifying information (like a telephone number or a public digital asset address) to a central (and in the digital asset context, essential) intermediary or conduit – the blockchain – also undermines, rather than increases, Fourth Amendment rights. It is that public characteristic

[54] Gratkowski v. United States, 964 F.3d 307 (5th Cir. 2020).

of blockchain transactions that the Fifth Circuit highlighted in its Gratkowski ruling. If anything, digital asset users can and should expect less privacy in their transactions as a result of using digital assets in the first place, since the *public* validation of chain of title and transaction history is an inherent component of the technology. In short, court precedent finds no Fourth Amendment barriers to information reporting regimes that tackle illicit finance, national security and tax evasion risks stemming from digital assets.

c. Digital Asset Information Reporting Regimes Do Not Violate Fifth Amendment Protections

A final Constitutional claim is that certain aspects of particular digital asset information reporting regimes could violate the Fifth Amendment's due process clause. These claims essentially argue that as a result of certain digital asset technology design choices – namely establishing complex transaction protocols in a decentralized network – certain federal information reporting requirements may be unconstitutionally vague, making it unclear how virtual asset service providers and others should comply with them. These claims ignore clear precedent rejecting similar Fifth Amendment challenges to federal reporting regimes for cash transactions.[55] These claims also ignore the competency of Treasury in crafting rules to address transactions involving the original "peer-to-peer"[56] and potentially cross-border form of payment – cash, as well as rules to address the application of reporting requirements to emerging technologies and financial innovations.[57] Finally, these complaints seem to gloss over technologies that could instead aid in compliance with information reporting regimes.

These Fifth Amendment claims seem to be a smoke screen, trying to distract from the fact that Congress has been quite clear that voluntary design choices associated with digital currency shouldn't trump sound tax reporting or anti-money laundering rules.[58] Recent enactment of the Infrastructure Investment and Jobs Act, the Anti-Money Laundering Act, and other new laws repeatedly make clear that Congress expects voluntary digital asset design choices to conform with long-existing, principled, constitutionally-validated AML/CFT and tax reporting rules to protect the U.S. financial system.

d. Sanctions Enforcement Against Anonymity-Enhancing Technologies Does Not Violate the International Economic Powers Act

The key statutory challenge made by some digital asset proponents to recent U.S. enforcement actions involving digital assets is equally unconvincing. In response to the recent sanctions imposed by OFAC on Tornado Cash, some industry proponents have claimed that sanctions enforcement against anonymity-enhancing technologies exceeds Treasury's power

[55] See, e.g., Jensen v. United States, 69 F.3d 906 (8th Cir. 1995)(finding 26 U.S.C. § 6050I and 7203 "are not void for vagueness").
[56] While the U.S. dollar and other foreign currencies are obviously backed by respective governments, the exchange of cash does not require any centralized clearing mechanism that involves otherwise regulable intermediaries. Cash in circulation allows users to interact on a "peer-to-peer" basis.
[57] See, e.g., Treas Reg. 1.6050I-1.
[58] See, e.g., 26 U.S.C. 6045; 31 U.S.C. 5312(a)(3)(D).

under the International Economic Powers Act.[59] At the core of those arguments is that Tornado Cash – an allegedly autonomous digital asset mixer that enabled in excess of $7 billion in money laundering transactions since 2019 – can also be used by individuals to transfer funds among themselves or among parties that are not under sanction.

This argument ignores the "pooling" of licit and illicit digital assets through the software that powers the mixer and certain other anonymity-enhancing technologies to anonymize ownership of the pooled digital assets – regardless of who controls any particular token or other asset. This pooling creates a common enterprise with respect to the assets using the anonymity-enhancing technology. Additionally, as Treasury recently put it, the facts show that anonymity- enhancing tools "indiscriminately facilitate() anonymous [digital] transactions by obfuscating their origin, destination, and counterparties, with no attempt to determine their origin."[60] These facts support OFAC's decision to apply sanctions to stop the pooling activity.

It is evident that Tornado Cash has been used and can be used again by sanctioned individuals, entities, and countries to pool and mix their digital assets and impede law enforcement efforts to trace specific transactions and the persons responsible for them. Treasury has routinely used its powers under the International Economic Powers Act to sanction enterprises and actors on similar grounds.[61] Those sanctions remain valid even if the given institution or entity also facilitated many transactions unrelated to a sanctioned party.

In the case of Tornado Cash, the United States determined that North Korean-sponsored hackers laundered $455 million in stolen funds using this software. Other Tornado Cash users are voluntarily and willfully pooling their capital in a way known to pose enormous illicit financing and national security risks and create a common enterprise with potentially sanctioned actors. Treasury has ample authority to sanction the use of this software and other anonymity- enhancing tools to prevent the ongoing abuse of U.S. and global financial markets and to address national security risks created by state-sponsored bad actors like the Lazarus Group.

Conclusion

FACT commends Treasury for its sustained effort to address illicit financing risks posed by digital assets and to ensure responsible development of digital assets in the United States. Treasury should continue to pursue its identified priorities and the recommendations in this

[59] See 50 U.S.C. 1702(a)(1); Coin Center, "Coin Center is suing OFAC over its Tornado Cash sanction," (Oct. 12, 2022), Coin Center press release, https://www.coincenter.org/coin-center-is-suing-ofac-over-its-tornado-cash-sanction/.

[60] See Treasury supra note 22.

[61] See 50 U.S.C. 1702(a)(1)(A)(ii); see, e.g., U.S. Treasury Announces Unprecedented & Expansive Sanctions Against Russia, Imposing Swift and Severe Economic Costs (Feb. 24, 2022), https://home.treasury.gov/news/press-releases/jy0608 (levying sanctions on several Russian related institutions and enterprises, including privately owned entities).

letter. Thank you for the opportunity to comment on the Notice. Should you have any questions, please feel free to contact Ryan Gurule at rgurule@thefactcoalition.org.

Sincerely,

Ian Gary
Executive Director

Erica Hanichak
Government Affairs Director

Ryan Gurule
Policy Director