Genuine DeFi as Critical Infrastructure:
A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance

Rebecca Rettig, Michael Mosier & Katja Gilman[1]

January 29, 2024

Abstract

Combating illicit financial activity in permissionless blockchain-based financial systems — referred to as "decentralized finance" or "DeFi" — has challenged regulators and policymakers. Traditional financial integrity laws and regulations, comprised of anti-money laundering ("AML")/countering the financing of terrorism ("CFT") and sanctions, attach to intermediaries, including, with respect to AML/CFT obligations, those intermediaries the Bank Secrecy Act ("BSA") defines as "financial institutions." The current laws, however, are not amenable to intermediary-less systems like DeFi. This paper proposes a framework (*see* Section III) to effectively detect, deter and prevent illicit financial activity in DeFi, while preserving the technology as permissionless, neutral infrastructure. The three-part proposal (1) sets forth a definition of "independent control" in order to identify smart-contract based financial protocols that do *not* constitute DeFi; (2) seeks to classify genuine DeFi protocols — neutral, decentralized software — as "critical infrastructure," subject to oversight and security coordination by the Treasury Department's Office of Cybersecurity and Critical Infrastructure Protection ("OCCIP"); and (3) suggests that new laws could require certain businesses that are (a) necessary to the transmittal of communications about DeFi transactions, (b) transmit a material portion of such communications and (c) offer the service as a business to take on additional illicit finance risk management practices, *without* becoming "financial institutions" subject to the BSA. This paper is intended to begin a meaningful conversation about how to achieve the policy goals of combating illicit financial activities while allowing for continued innovation in DeFi, a nascent technological sector.

[1] Rebecca Rettig is the Chief Legal & Policy Officer at Polygon Labs; Michael Mosier is a co-founder of Arktouros pllc, a partner at *ex/ante* and the former Acting Director of FinCEN, former Associate Director of OFAC and a former Deputy Chief of the U.S. Department of Justice's Money Laundering Section; Katja Gilman is the Senior Public Policy Lead at Polygon Labs.

Thank you to the following people for their review and thoughtful feedback: Miller Whitehouse-Levine, Kenneth Blanco, Jai Ramaswamy, Jai Massari, Gregory Lisa, Michele Korver, Marc Boiron, Reid Yager, David Silverman and Rodrigo Seira. Special thanks to Jarrod Watts for the DeFi Transaction Flow graphic in Section II and Appendix A; Kathryn Dunham for creating the (literal) space for this paper to be written; and our friends and colleagues — too numerous to name — who supported the efforts that went into this paper.

Introduction[2]

Global regulators and policymakers have long focused on how to regulate cryptocurrencies and the blockchain technology systems in which they operate.[3] Combating illicit financial activity in these systems has proven particularly challenging due to a novel feature: the systems run without traditional identifiable intermediaries. Decentralized finance or "DeFi" — an open source, blockchain-based, software-based system that empowers users to engage in economic transactions without the need for intermediaries — has challenged regulators and policymakers on the illicit finance question precisely for this reason.

In the U.S., a decades-old financial integrity regime — one that addresses concerns relating to anti-money laundering ("AML"), countering the financing of terrorism ("CFT") and sanctioning bad actors or countries that threaten the economic and national security of the U.S. — governs the way in which the traditional financial system ("TradFi") combats illicit activity. In TradFi, intermediaries — in particular, a special set of intermediaries defined as "financial institutions" under the Bank Secrecy Act ("BSA"), including banks, SEC-registered broker dealers, money services business ("MSBs"), among others — that engage in specific types of financial activity on behalf of third party customers must adhere to AML/CFT and sanctions requirements.

The reliance on intermediaries to combat illicit finance in TradFi creates challenges for lawmakers seeking to build similar regulation for an intermediary-less world. As the International Monetary Fund

---

[2] DeFi is an emerging technological system, and the scholarship on DeFi — from government regulators and policymakers, academics, legal scholars, industry advocacy groups and industry participants — continues to grow. We reviewed much of this scholarship — as cited throughout — to inform the concepts underpinning this paper. In addition, we consulted the following non-exhaustive list of literature: Matthias Nadler & Fabian Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers*, 105 Fed. Reserve Bank of St. Louis Rev. 122, (2023), https://doi.org/10.20955/r.105.122-136; Thomas Bourveau, Janja Brendel & Jordan Schoenfeld, *Decentralized Finance (DeFi) Assurance: Early Evidence*, (2023), https://papers.ssrn.com/abstract=4457936; Sanjeev Bhasker, Michael Grady & Kevin Mosley, *Cryptocurrency: Anti-Money Laundering Enforcement and Regulation*, 38 Am. Bar Assoc. Crim. Just. Mag., (2023),https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2023/summer/cryptocurrency-anti-money-laundering-enforcement-regulation/; Fabian Schär, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*, 103 Fed. Reserve Bank St. Louis Rev. 153, (2020), https://doi.org/10.20955/r.103.153-74; Nic Carter & Linda Jeng, *DeFi Protocol Risks: The Paradox of DeFi*, (2021), https://papers.ssrn.com/abstract=3866699; *Crypto Crime in Context: Breaking Down Illicit Activity in Digital Assets: Hearing Before the H. Subcomm. on Digit. Assets, Fin. Tech. and Inclusion*, 118th Cong. (2023) (testimony of Gregory C. Lisa); Raphael Auer et al., *The Technology of Decentralized Finance (DeFi)*, (2023), https://link.springer.com/10.1007/s42521-023-00088-8; Eur. Sec. and Mkts. Auth., *Decentralised Finance: A Categorisation of Smart Contracts*, (2023), https://data.europa.eu/doi/10.2856/398988; His Majesty's Treas., Future Financial Services Regulatory Regime for Cryptoassets: Consultation and Call for Evidence, (2023), https://www.gov.uk/government/consultations/future-financial-services-regulatory-regime-for-cryptoassets; Joseph Burleson, Michele Korver & Dan Boneh, *Privacy-Protecting Regulatory Solutions Using Zero-Knowledge Proofs*, a16z crypto, (2022), https://a16zcrypto.com/posts/article/privacy-protecting-regulatory-solutions-using-zero-knowledge-proofs-full-paper/.

[3] The U.S. Department of the Treasury recognized recently, however, "[M]oney laundering, proliferation financing, and terrorist financing most commonly occur using fiat currency or other traditional assets as opposed to virtual assets." *See* U.S. Dep't of the Treas., Illicit Finance Risk Assessment of Decentralized Finance, 36 (2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf [hereinafter DeFi Risk Assessment].

("IMF") and Financial Stability Board ("FSB") recognized, "In the case of DeFi . . . , the lack of intermediaries means that the traditional approach to AML/CFT regulation, in which AML/CFT requirements are imposed on a private sector entity and compliance is monitored by supervisors, *cannot be applied*."[4] The U.S. Department of the Treasury (the "Treasury Department") recognized the same in its Illicit Finance Risk Assessment of Decentralized Finance ("DeFi Risk Assessment"): "DeFi services that lack an entity with sufficient control or influence over the service may not be explicitly subject to AML/CFT obligations."[5]

It *is* possible, however, to address the policy goals underlying traditional financial integrity regimes in DeFi.[6] Consistent with the observations of the IMF/FSB and the Treasury Department, imposing existing laws and regulations is not the answer to achieving these goals. Any regulatory proposal in this regard must acknowledge the realities of DeFi technology, which is, at its heart, a communications system that allows users to transmit information about their desired economic transactions. In some instances, persons or entities maintain "independent control" over elements of the blockchain-based software system that allows for financial transactions (the "System"), and in others, the technology operates neutrally and autonomously — the former coined "on-chain CeFi" and the latter, "genuine DeFi" in a scholarly article by Katrin Schuler, Ann-Sophie Cloots and Fabian Schär.[7] With this distinction in mind, policy proposals must focus on parts of a DeFi System where transactions by illicit actors can be properly documented, detected and deterred. At the same time, policymakers must not undermine the significant advances of cryptographically secured, resilient and widely accessible networks that can enable their own democratic and financially inclusive policy goals, such as the Treasury Department-enabled humanitarian aid to 60,000 Venezuelan healthcare workers under an authoritarian government, which only succeeded because of the permissionless and non-intermediated nature of cryptocurrencies.[8]

---

[4] IMF & Fin. Stability Bd., *IMF-FSB Synthesis Paper: Policies for Crypto-Assets*, 14 (2023), https://www.fsb.org/wp-content/uploads/R070923-1.pdf (emphasis supplied).

[5] DeFi Risk Assessment, *supra* note 3 at 2.

[6] As discussed further below, the goals of the financial integrity regime in the U.S. are to document, detect, deter and prevent illicit activity and threats to national security. Crime prevention is defined as a set of actions intended to reduce or remove the risk of crime and harms associated with the commission of crime. To that end, this paper uses the term "deterrence" broadly to include both discouraging and wholesale preventing illicit activity. Notably, financial integrity standards are anchored in "reasonable risk management" and "reasonably designed" programs to mitigate risk, not prevent — *i.e.*, eliminate entirely — all risk. There is no "zero-risk" requirement to guarantee perfection that would likely cause meaningful collateral impact by aggressive de-risking, which the Treasury Department has pointed out in its excellent De-Risking Strategy report. *See* U.S. Dep't of the Treas., AMLA: The Department of the Treasury's De-Risking Strategy, 22 (2023), https://home.treasury.gov/system/files/136/Treasury_AMLA_23_508.pdf [hereinafter De-Risking Report].

[7] Katrin Schuler, Ann Sophie Cloots & Fabian Schar, *On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance*, (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4422473 [hereinafter On-Chain CeFi].

[8] *Circle Partners with Bolivarian Republic of Venezuela and Airtm to Deliver Aid to Venezuelans Using USDC*, Circle (Nov. 20, 2020), https://www.circle.com/blog/circle-partners-with-bolivarian-republic-of-venezuela-and-airtm-to-deliver-aid-to-venezuelans-using-usdc.

This paper intends to begin a conversation around the novel ways laws and regulations can achieve these goals in DeFi Systems. Section I of this paper provides a brief overview of the current financial integrity regime in the United States, focusing on the BSA, the laws and regulations relating to U.S. sanctions and the way in which financial institutions implement programs relating to both of these. Section II defines DeFi for purposes of this paper and discusses the sources of illicit finance risks in DeFi — cyber risk, system management risk and usage risk. Section III sets out a three-part conceptual framework for combating illicit finance risks in DeFi Systems. *First*, we propose a definition of "independent control" — grounded in the 2019 FinCEN Guidance (as defined below) — to allow for identification of Systems dependent on centralized actors ("System Control Persons"): these are on-chain CeFi. *Second*, we propose classifying Systems without System Control Persons — "genuine DeFi" — as "critical infrastructure" to be overseen by the Treasury Department's Office of Cybersecurity and Critical Infrastructure Protection ("OCCIP"). *Third*, for certain types of businesses that interact with genuine DeFi Systems but that are not System Control Persons, we propose creating a new category of persons — "critical communications transmitters" ("CCTs") — that would have regulatory obligations to aid in the protection of U.S. national and economic security, but *not* the same obligations as "financial institutions" subject to the BSA, with new, limited and tailored oversight by the Financial Crimes Enforcement Network ("FinCEN").

The proposal set forth in Section III balances government and industry interests on financial integrity in DeFi — a balance fundamentally necessary for any *effective* regulatory approach. This proposal seeks to build upon the Treasury Department's supervision over U.S. national and economic security; recognize the realities of the DeFi Transaction Flow (as shown in Section II below) to identify an appropriate regulatory focal point for combating illicit activity;[9] not subject mere software providers to regulation by virtue of software development activity alone, a concept antipodal to long-standing FinCEN guidance; and — critically — maintain base layer neutrality,[10] an ideal imperative to ensuring the continued development of permissionless blockchain networks as global infrastructure.

This paper does not endeavor to address all questions of illicit finance in the cryptocurrency context: it does not address questions of centralized cryptocurrency financial actors, many of whom are already subject to current financial integrity laws as MSBs, nor does it addresses questions relating to the base layer of the technology — that is, blockchain networks and their various components, including validators, which should remain credibly neutral as fundamentally global data infrastructure.[11] It also

[9] The proportion of DeFi transactions flowing through CCTs likely will continue to grow as blockchain networks scale, meaning that large-scale CCTs will be integral to high communications throughput.

[10] For an overview of base layer neutrality and its import, *see* Rodrigo Seira, Dan Robinson & Amy Aixi Zhang, *Base Layer Neutrality*, Paradigm (2022), https://www.paradigm.xyz/2022/09/base-layer-neutrality.

[11] *Id*.

does not address other regulatory questions in the cryptocurrency space, which have already been the subject of numerous scholarly articles and likely will be the subject of encyclopedic books in the future.[12] Finally, this paper is not addressing all (or even the illicit finance aspect) of "web3," which, as a cryptographically secured, shared data layer, has myriad important and novel non-financial uses, such as decentralized file storage, non-fungible token ("NFT") art, decentralized social media and identity-related tooling, among numerous others.

I. Current Illicit Finance Regulation & Implementation in the U.S.

This section briefly describes the U.S. AML/CFT regime under the BSA, which focuses on the regulation of "financial institutions" — not providers of software services — and then discusses the U.S. economics sanctions regime, which is the other key half of the U.S. legal approach to financial integrity. The section concludes with a practical description of how these regimes are implemented by financial institutions and those subject to U.S. sanctions requirements.

A. A Brief Summary of the Bank Secrecy Act and Related Legislation

1. *The BSA and Its Progeny*

The BSA was passed in 1970[13] to "promote financial transparency"[14] through improved financial recordkeeping and responsiveness to law enforcement inquiries.[15] Congress has subsequently amended the BSA a number of times: first in 1986 with the Money Laundering Control Act[16] to criminalize money laundering and deter complicit bankers, lawyers and accountants — for whom recordkeeping violation fines had not served as adequate deterrents — from participating in their clients' money laundering schemes;[17] then in 1992 with the Annunzio-Wylie Act,[18] to require financial institutions to file reports ("suspicious activity reports" or "SARs") with FinCEN detailing certain suspicious activity that could potentially indicate money laundering or other enumerated crimes and to implement procedures "reasonably designed" to maintain "minimum standards" for an AML program, including

[12] It further does not address the Constitutional matters relating to proposed cryptocurrency regulation that have been articulated and examined by others. *See e.g.*, Peter Van Valkenburgh, *Broad, Ambiguous, or Delegated: Constitutional Infirmities of the Bank Secrecy Act*, Coin Center (2023), https://www.coincenter.org/app/uploads/2023/11/BroadAmbiguousDelegated.pdf.

[13] 12 U.S.C. §§ 1829b, 1951-59; 31 U.S.C. §§ 5311-14, 5316-32.

[14] *The Bank Secrecy Act: A Supervisory Update*, Fed. Deposit Ins. Corp., https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum17/sisummer2017-article02.html (Apr. 6, 2023).

[15] *Id.* (noting that the BSA was passed to address "the lack of financial recordkeeping by financial institutions and the use of foreign bank accounts located in jurisdictions with strict secrecy laws.").

[16] Pub. L. No. 99-570 § 1351 *et seq.*, 100 Stat. 3207-18 (1986).

[17] *Id.*

[18] Pub. L. No. 102-550, 106 Stat. 4044 (1992).

verification and recordkeeping for wire transfers and a proactive detection and reporting regime;[19] again in 1994 and 1998, to, among other things, require bank regulatory agencies to develop procedures for AML examination of banks as well as to require the Treasury Department and other agencies to develop a national money laundering strategy;[20] and after the September 11, 2001 attacks, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the "USA PATRIOT Act")[21] "updated the law to reflect new technology and new threats,"[22] introduced customer due diligence ("CDD") requirements as well as information sharing requirements between financial institutions and the U.S. government and provided additional avenues for sanctioning illicit actors.

Most recently, Congress passed the Anti-Money Laundering Act of 2020 ("AMLA")[23] to "strengthen, modernize and streamline the existing AML regime by promoting innovation, regulatory reform and industry engagement."[24] According to the Congressional Research Service, "if fully implemented by the executive branch, AMLA may represent one of the most comprehensive efforts in recent decades to modernize the U.S. government's regulatory architecture for AML, combat the financing of terrorism (CFT) and detect other financial crime activity."[25] To enhance the BSA's existing illicit finance regulatory framework, the AMLA emphasized the need for financial institutions to implement risk-based AML programs — as opposed to programs primarily focused on blanket reporting — and explicitly expanded the statutory scope of the BSA to include businesses that provide covered financial services involving "value that substitutes for currency,"[26] whereas "convertible virtual currency" (including cryptocurrency) was previously captured only through FinCEN's own interpretation of its

---

[19] The minimum standards for an AML program — set forth in Annunzio-Wylie and codified at 31 U.S.C. § 5318(h) — include: "(A) the development of internal policies, procedures, and controls, (B) the designation of a compliance officer, (C) an ongoing employee training program, and (D) an independent audit function to test programs."

[20] *History of Anti-Money Laundering Laws*, Fin. Crimes Enf't Network, https://www.fincen.gov/history-anti-money-laundering-laws (last visited Jan. 21, 2024).

[21] Pub. L. 107-56, 115 Stat. 272 (2001).

[22] *The USA PATRIOT Act: Preserving Life and Liberty,* U.S. Dep't of Just., https://www.justice.gov/archive/ll/highlights.htm (last visited Jan. 21, 2024).

[23] Division F of the William M. (Mac) Thornberry National Defense Authorization Act ("NDAA") for FY2021, Pub. L. 116-283, 134 Stat. 4547 (2021); For a summary of AMLA, *see* Rachel G. Skaistis et al., *The Anti-Money Laundering Act of 2020*, Cravath, Swaine, & Moore LLP, (2021), https://www.cravath.com/a/web/6PUaNYoMmg8Xjmu8cMKYNV/2hjEvG/anti-money-laundering-act-of-2020.pdf.; For FinCEN's report on implementation of AMLA, *see* Liana W. Rosen & Rena S. Miller, Cong. Rsch. Serv., R47255, The Financial Crimes Enforcement Network (FinCEN): Anti-Money Laundering Act of 2020 Implementation and Beyond, (2022).

[24] Fin. Crimes Enf't Network, *AMLA FinCEN One Pager*, https://www.fincen.gov/sites/default/files/shared/20210615%20AMLA%20FinCEN%20One%20Pager_FINAL.pdf (last visited Jan. 21, 2024).

[25] Rosen and Miller, *supra* note 23 at 2.

[26] Fin. Crimes Enf't Network, FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, 3 (2013), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

authority through rulemaking and guidance.[27] The AMLA mandates reviews to identify the categories and characteristics of reports that best support law enforcement investigations and establishes innovation offices at the related regulators, to better understand innovative use of technologies both for themselves and covered institutions in combating illicit finance. Moreover, pursuant to the AMLA, FinCEN issued — for the first time — national AML/CFT priorities that included "cybercrime, including relevant cybersecurity and virtual currency considerations"[28] to guide how financial institutions should structure their risk-based AML programs to "reallocate resources from other lower-priority risks or practices to manage and mitigate higher-priority risks, including any identified as Strategic AML Priorities."[29]

2. *BSA's Regulation of Financial Institutions — Not Software Developers*

The BSA hinges on the regulation of "financial institutions" — a type of person or entity that conducts certain types of financial activity or otherwise facilitates those types of financial activities on behalf of others.[30] The statute defines "financial institution" by listing different types of "persons"[31] that provide services involving holding or storing funds on behalf of customers, exchanging currencies for customers or transferring funds from one person to another on behalf of a customer or otherwise facilitating funds transfers or payments for a customer[32] — a sensible focus for laws designed to prevent illicit financial transactions, as these types of entities have insight into the financial transactions of their customers. Specifically, under the BSA, "financial institutions" include a broad array of financial intermediaries, such as banks (insured, commercial or private), SEC-registered brokers or dealers, money services businesses (*e.g.*, money transmitters, currency exchangers, foreign exchange dealers), telegraph companies (*e.g.*, originally Western Union, which completed the first transcontinental telegraph service

---

[27] *See e.g.,* Fin. Crimes Enf't Network, Anti-Money Laundering and Countering the Financing of Terrorism National Priorities, (2021), https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf.

[28] *Id.*

[29] Anti-Money Laundering Program Effectiveness, 85 Fed. Reg. 58023 (2020) [hereinafter AML Program Effectiveness].

[30] *Banker Resource Center: Bank Secrecy Act*, *supra* note 14 ("By statute, individuals, banks, and other financial institutions are subject to the BSA recordkeeping requirements.").

[31] "Person" has the same meaning as in the BSA. *See* 31 CFR §1010.100(mm).

[32] Andrew P. Scott, Cong. Rsch. Serv., R46486, Telegraphs, Steamships, and Virtual Currency: An Analysis of Money Transmitter Regulation, 1 (2020) ("MSBs have three general functions: (1) receiving and sending money on behalf of consumers; (2) providing products that receive, store, or send money for consumers; and (3) providing an exchange for currencies."); Fin. Crimes Enf't Network & Internal Revenue Serv., Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses, 9 (2008) https://www.fincen.gov/sites/default/files/shared/MSB_Exam_Manual.pdf ("A money transmitter is defined as any person, whether or not licensed or required to be licensed, that engages as a business in accepting currency or funds denominated in currency and transmits the currency or funds, or the value of the currency or funds, by any means ...").

in 1861 and added the ability to transfer money via telegraph in 1871),[33] casinos and anyone subject to federal or state bank supervisory authority.[34]

Providers of software alone — who do not otherwise engage in the types of financial activity described above — are not "financial institutions." Indeed, in its seminal 2019 guidance, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (the "2019 FinCEN Guidance"), FinCEN states that its "regulations exempt from the definition of money transmitter those persons providing 'the delivery, communication, or network access services used by a money transmitter to support money transmission services.' This is because suppliers of tools (communications, hardware or software) that may be utilized in money transmission . . . are engaged in trade and not money transmission."[35]

2019 was not the first time that FinCEN staked out this position. The 2019 FinCEN Guidance includes reference to an earlier FinCEN Administrative Ruling that stated, "[t]he production and distribution of software, in and of itself, does not constitute acceptance and transmission of value, even if the purpose of the software is to facilitate the sale of virtual currency."[36] And that builds on earlier guidance, before FinCEN ever publicly discussed cryptocurrencies, in which FinCEN distinguished the provision of software and hardware services as *not* money transmission, even where the software and hardware services were used by others to conduct regulated money transmission services.[37] Indeed, it has always been that, under the BSA, persons engaged solely in software development activity are not financial institutions subject to regulation under the BSA nor are the software providers who simply offer services for communication or network access, even if those services are used by financial institutions for regulated activity. The same holds true for those persons providing access to software where users engage solely in peer-to-peer transactions and interactions.[38]

---

[33] Western Union also introduced "Metal Money," one of the first consumer charge cards, in 1914. *See* Cecilia Hendrix, *6 Fascinating Things about Western Union's History*, Western Union (Oct. 8, 2019), https://www.westernunion.com/blog/en/6-fascinating-things-about-western-unions-history/.

[34] 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).

[35] Fin. Crimes Enf't Network, FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, 20 (2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf [hereinafter 2019 FinCEN Guidance].

[36] Fin. Crimes Enf't Network, FIN-2014-R002, Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity, 2 (2014), https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R002.pdf.

[37] Fin. Crimes Enf't Network, FIN-2009-R001, Whether Certain Operations of a Service Provider to Prepaid Stored Value Program Participants is a Money Services Business, 2 (2009), https://www.fincen.gov/sites/default/files/administrative_ruling/fin-2009-r001.pdf ("When selling and marketing its software and hardware products to retailers, program managers, and issuing banks, the Company is providing data processing hardware and software and product networking services — not money transmitting services — to merchants and financial institutions.").

[38] *See* 31 C.F.R. § 1010.100(ff)(5)(2)(A); *see also* 2019 FinCEN Guidance, *supra* note 35 at 24.

B. A Brief Summary of U.S. Sanctions Laws

The U.S. government's ability to impose economic and trade sanctions forms the second key part of the financial integrity regime in the United States. Sanctions authority is delegated by Congress to the U.S. Office of Foreign Asset Control ("OFAC"), which "designates" various individuals, entities and jurisdictions in order to restrict — fully or in part — the ability of specified persons to engage in business, provide services or engage in other economic activities in order to protect the country's economic and national security interests and further U.S. foreign policy goals.[39] OFAC's administrative powers emanate from a series of laws and regulations, along with numerous Presidential Executive Orders ("E.O.s"), including but not limited to the International Emergency Economic Powers Act ("IEEPA"),[40] enacted by Congress in 1977, and the National Emergencies Act ("NEA"),[41] enacted a year earlier in 1976 — both of which empower the President to use special powers to combat economic threats during times of particular crisis.

OFAC has the ability to impose (1) primary sanctions on U.S. persons or entities or in situations where there is a connection to the U.S.; and (2) secondary sanctions — sanctions against non-U.S. persons relating to a specified activity that occurs outside the U.S. with certain sanctioned jurisdictions or entities. The former seek to protect U.S. economic and national security, while the latter seek to promote the U.S. foreign policy objectives by deterring non-U.S. actors from engaging with entities or jurisdictions the U.S. deems dangerous. OFAC's powers permit the imposition of "complete" sanctions — prohibitions for all trade and economic activity with a particular country — as well as "selective" sanctions — targeted prohibitions against particular persons or entities.[42]

OFAC issues sanctions by adding the names of an "entity" to the Specially Designated Nationals ("SDN") List, listing certain transactions on the Sectoral Sanctions Identification ("SSI") List or otherwise publishing information about sanctioned countries or entities.[43]

OFAC does not, however, have unlimited powers; they are curbed by various parts of the laws, regulations and E.O.s, including exemptions and enshrined principles such as humanitarian aid, as well

[39] Office of Foreign Assets Control, https://ofac.treasury.gov/ (last visited Jan. 21, 2024).
[40] 50 U.S.C. § 1701 *et seq.*
[41] 50 U.S.C. § 1601 *et seq.*
[42] *Id.*
[43] *See* Sanctions Lists, Office of Foreign Assets Control, Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists, https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists (Jan. 25, 2024).

as the free flow of information under the Berman Amendment[44] and General License D-2 covering communications software and services (including anti-censorship tools such as VPNs).[45]

That said, protecting U.S. national and economic security allows the government wide latitude and broad discretion in imposing sanctions to protect the country.

C. AML/CFT and Sanctions Programs In Practice

Under the BSA, financial institutions' AML/CFT programs focus on detection, documentation and deterrence of illicit financial activity. These programs are not intended to — and cannot entirely — prevent money laundering or terrorist financing. Indeed, the federal banking regulators and FinCEN have explicitly stated that the key to financial integrity in the United States under the BSA is for financial institutions to have a "reasonably designed" AML program with "effective processes to identify, measure, monitor and control risks," noting that "banks are encouraged to . . . mitigate risks . . . rather than declining to provide banking services to entire categories of customers."[46] FinCEN also states that "[u]nder any proposal to incorporate a requirement for an 'effective and reasonably designed' AML program, [it] understands that institutions may reallocate resources from other lower-priority risks or practices to manage and mitigate higher-priority risks, including any identified as Strategic AML Priorities."[47] Thus, the legal and regulatory standard is not zero tolerance or total elimination of risk (even if some financial institutions may articulate this overall aspiration) but rather reasonable control over and mitigation of risks that allocate attention to priorities while valuing the importance of giving consumers and businesses access to the financial system.[48] This latter point was underscored in the

---

[44] 50 U.S.C. § 1702(b)(3) ("The authority granted to the President by this section does not include the authority to regulate or prohibit, directly or indirectly— (1) any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value;... or (3) the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials.").

[45] Press Release, U.S. Dep't of the Treas., U.S. Treasury Issues Iran General License D-2 to Increase Support for Internet Freedom, (2022), https://home.treasury.gov/news/press-releases/jy0974.

[46] The Board of Gov.'s of the Fed. Res. Sys. et al., *Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision*, (2019), https://www.fincen.gov/news/news-releases/joint-statement-risk-focused-bank-secrecy-actanti-money-laundering-supervision.

[47] AML Program Effectiveness, *supra* note 29.

[48] William Fox, Director, Financial Crimes Enforcement Network, Presentation to the American Bankers Association (Oct. 25, 2004), https://www.fincen.gov/news/speeches/remarks-william-j-fox-director-financial-crimes-enforcement-network-united-states-0; *An Update on Money Services Businesses Under Bank Secrecy and USA PATRIOT Regulation: Hearing Before the S. Comm. On Banking, Housing, and Urban Affairs*, 109th Cong. 11 (2005) (statement of Julie Williams, Acting Comptroller of the Currency, Office of the Comptroller of the Currency), https://www.banking.senate.gov/imo/media/doc/ACF5BF.pdf ("The BSA has been the focus of regulatory, Congressional, and media attention for much of the last year. Clearly, these are very important issues to the banking industry, the OCC and the United States. This emphasis and attention on BSA has prompted the industry to feel that the regulators have adopted a 'zero tolerance' approach to BSA/AML supervision and enforcement — that any deficiency in a bank's BSA processes equates to a violation triggering a cease and desist order. At the OCC we take this assertion seriously — because it is flat wrong."); Monica C Meinert, *FinCEN to Launch Innovation Initiative*, A.B.A. J., (2018), https://bankingjournal.aba.com/2018/12/fincen-to-launch-innovation-initiative/ ("Blanco also discussed the agency's efforts for updating the BSA/AML framework, noting that 'we are committing to updating the regulations as necessary to ensure that the BSA regime is as effective and efficient as possible.' In the days ahead, FinCEN will work to

Treasury Department's recent report on De-Risking; results of surveys with bank officers and regulators demonstrated a misunderstanding on a "risk-based approach"[49] to compliance. Although banks may believe "they face a risk of large fines from regulators for *any* failure in banking controls," regulators "note that such fines are rare and that they are uniformly the result of *total failure* of AML/CFT compliance programs, not a result of more limited shortcomings that might result from a *reasonable* application of the *risk-based* approach."[50]

Financial institutions implement the BSA's requirements through a variety of processes and procedures aimed at enhancing "financial transparency" — ultimately, implementing a reasonable risk-based program based upon documentation, detection and deterrence of illicit financial activity.

Documentation. Most financial institutions are required to file various reports with FinCEN, including SARs for suspicious transactions above certain dollar thresholds for bank[51] and (non-bank) MSBs[52] and CTRs for cash payments over $10,000 and maintain copies of these reports and supporting documents for five years to aid any potential future law enforcement investigations.[53]

Detection. Financial institutions maintain programs through which they collect specific information about each customer (*e.g.*, verifying customers' identity), colloquially known as "know your customer" ("KYC") programs. Although KYC is often framed as a keystone in combating illicit financial activity, "KYC" as a term is never mentioned in the BSA, subsequent legislation or attendant regulations, and there is no singular regulatory concept of "KYC" itself. Today, bank and non-bank financial institutions primarily engage in versions of three types of "KYC": a Customer Identification Program ("CIP"), as well as Customer Due Diligence ("CDD") and Enhanced Due Diligence ("EDD") programs.

Covered financial institutions typically verify their customers' identity (CIP), usually via government ID, to be able to reliably assess (CDD) that the customer is safe to do business with, usually by ascertaining risks related to source and/or destination of funds and/or relationship to parties on high-risk lists (sanctions, Politically Exposed Persons ("PEPs") and so-called "negative news" searches). Financial institutions conduct EDD for persons or situations that present heightened illicit finance risk,

clarify the risk-based approach to the examination process; clarify that 'there is no zero-tolerance approach to BSA enforcement'; incentivize financial institutions to devote resources to priority illicit finance threats; and develop concrete ways to highlight the value of BSA data across stakeholders, he added.").

[49] De-Risking Report, *supra* note 6 at 22.

[50] *Id.* at 22-23 (emphasis supplied).

[51] *FFIEC BSA/AML Assessing Compliance with BSA Regulatory Requirements - Suspicious Activity Reporting*, Fed. Fin. Insts. Examination Council, https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/04 (last visited Jan. 23, 2024).

[52] *Money Services Business (MSB) Suspicious Activity Reporting*, Fin. Crimes Enf't Network, https://www.fincen.gov/money-services-business-msb-suspicious-activity-reporting (last visited Jan. 23, 2024).

[53] Illicit actors can, however, attempt to structure transactions in ways that do not trigger the reporting requirements.

e.g., those in certain "high risk" jurisdictions or lines of business. Institutions must then store this information for specified periods of time and provide it to law enforcement if or when requested.[54]

Deterrence. Covered financial institutions maintain written AML programs to reasonably address the specific illicit finance risks of its business and its customer base and implement procedures to address these risks. Institutions routinely audit their respective AML programs and/or are audited on this by their respective regulators; hire sufficient compliance personnel and appropriately train them to carry out the program; and ensure the program adequately detects suspicious activity to identify persons potentially engaged in illicit financial activity such that it can be investigated and, ultimately, deterred.

As with the BSA and financial institutions' AML/CFT programs flowing therefrom, U.S. sanctions programs also require a risk-based approach notwithstanding the strict liability standard for U.S. persons engaged in sanctions violations.[55] The standard for sanctions compliance in practice is also not "zero tolerance." Rather, any person or entity that is a U.S. person, majority owned by U.S. persons or conducts business in or with the United States must not engage in activity that "contributes or provides . . . funds, goods, or services by, to, or for the benefit of any" sanctioned party or "interests" of a sanctioned party or "facilitates" any of the foregoing. "Facilitation" is construed broadly — it frequently looks to whether the person or entity provided "material assistance" to those engaging in the sanctioned conduct with sanctioned parties, but also has been thought of generally as "making [sanctioned conduct] easier."[56] For U.S. persons who may have involvement in any way, the prohibition applies even where the person is "dealing with" sanctioned persons, which has been construed to include nearly any indirect benefit or service to or from a designated person, regardless of it being "material" or "substantial."[57] Thus, any sanctions programs for those persons or entities subject to the U.S. sanctions regime must ensure that appropriate measures are implemented to avoid not only direct sanctions violations but also the facilitation of those violations.

II. Illicit Finance in DeFi

This section provides an overview of the technical aspects of DeFi Systems and raises additional considerations relating to the practical ways in which the DeFi ecosystem has developed, including how

---

[54] The Right to Financial Privacy Act covers how such requests must be made.

[55] Dep't of the Treas., *A Framework for OFAC Compliance Commitments*, https://ofac.treasury.gov/media/16331/download?inline (last visited Jan. 23, 2024); Dep't of the Treas., *Sanctions Compliance Guidance for the Virtual Currency Industry*, (2021), https://ofac.treasury.gov/media/913571/download?inline.

[56] Exec. Order No. 13694, 80 Fed. Reg. 18077 (2015), *as incorporated in* Exec. Order No. 13757, 82 Fed. Reg. 1 (2017).

[57] *See e.g.,* Exec. Order No. 13608, 77 Fed. Reg. 26409, 26409 (2012) (Regarding Iran and Syria: "[T]he Secretary of the Treasury may prohibit all transactions or dealings, whether direct or indirect, involving such [designated] person, including any exporting, re-exporting, importing, selling, purchasing, transporting, swapping, brokering, approving, financing, facilitating, or guaranteeing, in or related to (i) any goods, services, or technology in or intended for the United States, or (ii) any goods, services, or technology provided by or to United States persons, wherever located.").

certain DeFi Systems are governed. It then discusses the sources of illicit finance risks in DeFi Systems. This background provides the necessary foundation for the framework on combating illicit finance in DeFi proposed in Section III.

A. Defining DeFi

There is no widely agreed-upon definition of "DeFi."[58] This confusion has arisen, in part, because the term "DeFi" has been used to describe a number of different types of smart contract-based Systems, including to describe — in our opinion, wrongly — certain centralized businesses that offer distinctly non-decentralized services through blockchain-dependent applications, including some that are custodial. This co-opting of the term "DeFi" conflates the systems providing centralized and/or custodial software services — in which intermediaries have authority over the System or users' funds — with open source software systems comprised entirely of code ("smart contracts") that work autonomously upon a condition being met, without the need for intermediaries.[59] Schuler et al. have labeled the former, "on-chain CeFi,"[60] and the latter, "genuine DeFi," which they define as "independent, neutral infrastructure."[61] This paper builds on Schuler et al.'s definition of "genuine DeFi."

> "Genuine DeFi" refers to a technological System comprised only of open source software — typically smart contracts — in which
>
> 1. users engage in financial transactions in a self-directed manner without reliance on intermediaries (*e.g.*, no bank, broker, etc.),
> 2. users maintain independent control over their own assets at all times through maintenance of the "private key" for their wallets and
> 3. all elements of transactions occur on a permissionless blockchain network.[62]

---

[58] *See, e.g.*, Mariana de la Roche W. & Mirko Zichichi, *Bringing Clarity to the DeFi Sector: A Cross-Sector Proposal for a Unified DeFi Definition*, IOTA Foundation (2023), https://www.eublockchainforum.eu/news/new-report-bringing-clarity-defi-sector-cross-sector-proposal-unified-defi-definition [hereinafter DeFi Definitions]; On-Chain CeFi, *supra* note 7 at 1; DeFi Risk Assessment, *supra* note 3 at 1; The Bd. of the Int'l Org. of Sec. Comm'ns, *Consultation Report: Policy Recommendations for Decentralized Finance (DeFi)*, 1 n.3 (2023), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf.

[59] This paper does not take on the herculean task of defining decentralization.

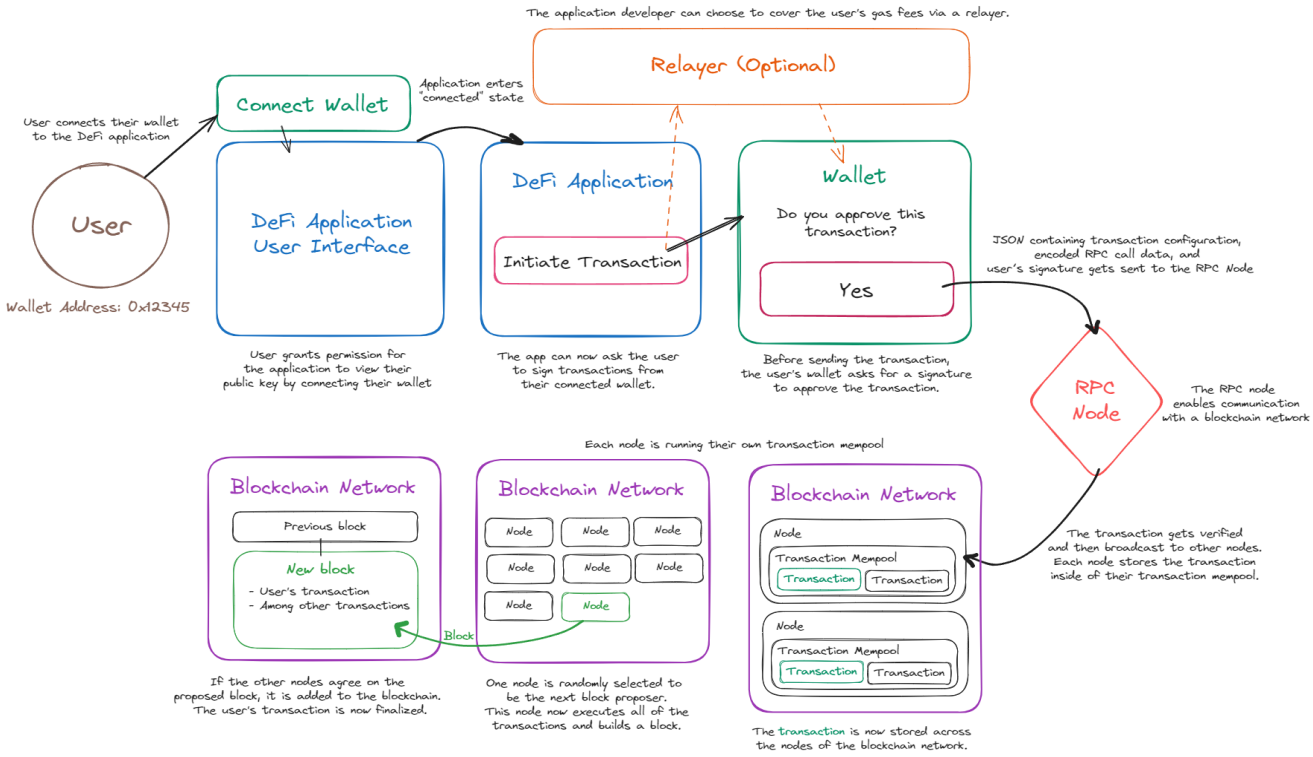
[60] On-Chain CeFi, *supra* note 7 at 8.

[61] *Id.* at 2.

[62] *See* DeFi Definitions, *supra* note 58 at 45 ("When reviewing the four definitions, we can find two areas that are common 1) DeFi is defined as a new financial system that operates in a decentralized manner, without the need for intermediaries, and 2) DeFi utilizes new technologies such as Distributed Ledger Technologies (DLT) and Smart Contracts to facilitate secure and transparent transactions."); *see also* Linda Jeng et al., *Key Elements of an Effective DeFi Framework*, Crypto Council for Innovation, 12 (2023), https://cryptoforinnovation.org/key-elements-of-an-effective-defi-framework/ [hereinafter Key Elements] ("The term 'DeFi' refers to the ecosystem of applications and protocols enabled by blockchain technology to provide digital and open access to financial services without a single intermediary or small group of intermediaries controlling the system offering the financial service.").

For purposes of this paper, we provide a visual of the flow of a typical DeFi transaction and, following the flow diagram, a brief discussion of the key software components involved in the flow.

DeFi Transaction Flow (see Appendix A for a larger version of this graphic)



As shown above, the way in which a user transmits a genuine DeFi System transaction for completion requires the user to communicate the desired transaction from their self-hosted wallet via a remote procedure call ("RPC") connection to a node (whether an individual node or through a node-as-a-service provider) and ultimately to a blockchain network.

The following are descriptions of the key software components involved in the DeFi Transaction Flow:

- **Wallets:** A "wallet" is software comprising two unique numbers, each called keys: one public key, which is an identifier that lets users receive cryptocurrencies (similar to an email address); and one private key, which allows the user to access and send the cryptocurrencies associated with the paired public key (similar to a password).[63] Together, these keys allow individuals to

[63] *See* Brief for DeFi Education Fund as Amici Curiae Supporting Respondents, Coinbase Inc. and Coinbase Global Inc.'s Motion for Judgment on the Pleadings, SEC v. Coinbase, Inc. et al., 23-cv-4738, ECF No. 60 (2023) at 4; *see also* 2019 FinCEN Guidance, *supra* note 35 at 16 ("Unhosted wallets are software hosted on a person's computer, phone, or other device that allow the person to store and conduct transactions in CVC. Unhosted wallets do not require an additional third party to conduct transactions. In the case of unhosted, single-

utilize their wallet to interact or communicate with a blockchain network. Wallets — also called "externally owned accounts" — can either be downloadable software stored locally on a user's computer or smart contract-based accounts stored directly on a blockchain network. In DeFi, wallets are typically "self-hosted" — that is, downloaded, owned and controlled by the user, without an external third party providing custody. The software developers of these wallets — who create and make them available for download — do not have any ongoing involvement with the wallet software's operation by users. When users engage in transactions with their self-hosted wallets, they maintain independent control over their cryptocurrency.

- **User Interfaces (or "Front Ends"):** User interfaces — or "front ends," as they have colloquially become known in the DeFi space — are websites, or user-facing applications, that run on a person's full service computer, phone, or other mobile device.

  All Internet interactive sites or applications require "front ends" and "back ends." The "front end" refers to the visual interface of a software system with which a user interacts. They are the part of a computer system or application that a user can see and with which a user interacts — usually, in order to more easily access information and services available on the Internet. "Back end" refers to the structure, system, data and logic underlying the user facing application — that is, the aspects of a system or software program that a user does not see or interact with directly.

  A user provides inputs through a front end, and the back end of the system processes the inputs. The back end may read, analyze and write data that it then provides as an output to the user, through the front-end user interface. For example, www.x.com is a "front end" that allows a user to access X's social media software algorithm and data, with the algorithm and data being the "back end."

  User interfaces relating to DeFi Systems can take a number of forms: (1) some only provide information about one or more DeFi protocols, such as potential transactions available through those protocols and related pricing and terms, without taking a fee; (2) others provide information and functionality to allow a user to connect their self-hosted wallet and then provide information about a transaction through their wallet directly to a protocol independent of the front end, with some of the providers of these interfaces taking a fee; and (3) a third type that provides some off-chain configuration (*e.g.*, a matching engine or order book hosted on a private server) where a user's transaction is reliant on the host of the off-chain server or service provider to match orders or otherwise to take steps towards completion of transactions,

signature wallets, (a) the value (by definition) is the property of the owner and is stored in a wallet, while (b) the owner interacts with the payment system directly and has total independent control over the value.").

regardless of whether they take a fee. Although many users employ user interfaces, they are *not a necessary prerequisite* for either initiation or completion of a genuine DeFi transaction; users are able to engage in transactions on genuine DeFi protocols by accessing the smart contracts directly on a blockchain network. User interfaces, however, make these interactions less technically demanding.

- **Protocol:** "Protocol" refers to a set of smart contracts that work together to allow users to communicate transaction instructions through a series of communications providers to a blockchain network for processing and execution. "Protocol" generally refers to a set of rules or procedures for a certain system; in DeFi protocols, the interaction among smart contracts sets the rules. These protocols may also be referred to as "dApps" — decentralized applications; this paper does not use that term, as it has been confusingly used to refer to user interfaces.

- **Relayers:** Relayers are software that sends a user's transaction instruction to a protocol[64] by accepting a user's communication from a DeFi protocol and sending it to the next step in the transaction flow, such as an RPC node or a blockchain network node. Relayers do not take custody of or exercise independent control over user assets at any time — they relay communications, often about transactions. Users or application developers may compensate parties who run relayers, or the developer of a software application may subsidize third party relayers' gas fees.[65] As shown in the DeFi Transaction Flow diagram, relayers are optional, at the discretion of each individual user for any transaction and for any protocol. Transactions can be fully accomplished and completed without relayers.

- **Nodes for Remote Procedure Calls:** RPC is a widely used software communication protocol that one software program can use to request a service from another software program that is running on a separate computer or network.[66] RPC is not specific to blockchains, but rather relates to technology network systems more generally and has been employed for decades. In the blockchain context, RPC nodes are computers that run blockchain client software (*e.g.*, an Ethereum node). RPC nodes receive communications from wallets about users' transactions

---

64 *See* Antier Solutions, *The Role of Blockchain Relayer in Transforming Financial Systems*, Medium (July 19, 2023), https://antiersolutions.medium.com/the-role-of-blockchain-relayer-in-transforming-financial-systems-ca2776dd761f [hereinafter Role of Relayers] ("Blockchain relayers are third-party services that facilitate the communication and transaction of data between different blockchain networks."); *see also* Benjamin Gruenstein, Evan Norris & Daniel Barabander, *Secret Notes And Anonymous Coins: Examining FinCEN's 2019 Guidance On Money Transmitters In The Context Of The Tornado Cash Indictment*, Int. Acad. Fin. Crime Litig., 10 (2023), https://edit.financialcrimelitigators.org/api/assets/b9fa10a1-5e91-4473-96f6-c240ff0761eb.pdf.

65 *See* Role of Relayers, *supra* note 64.

66 John Barkley, U.S. Dep't of Com., NISTIR 5277, Comparing Remote Procedure Calls, (1993), https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir5277.pdf ("The Remote Procedure Call (RPC) concept is a simple and useful technique for developing applications where communication between cooperating processes on networked systems is required").

and then transmit those communications to be included in a block that will ultimately be validated and finalized on a blockchain network.[67]

Individuals can maintain their own RPC node to communicate their own transactions. Some companies also provide RPC-node-as-a-service offerings (*e.g.*, Infura, Alchemy, Conduit), through which they host RPC nodes that individuals can use instead of running or hosting their own node. RPC-node-as-a-service providers generally charge fees for their services, usually paid by the developers of a DeFi application or by other third parties (*e.g.*, foundations), but typically *not* paid by users. Many RPC-node-as-a-service providers conduct some form of due diligence and/or sanctions screening on their direct customers (those that pay fees), akin to the type of due diligence and screening Amazon Web Services ("AWS") conducts when a customer seeks to open a new server. It is important to note that AWS does not conduct the same due diligence or screening on users of a website hosted on an AWS server.

DeFi protocols have proliferated in the last half decade to include exchanging or swapping through decentralized exchanges or "DEXs" (*e.g.*, Uniswap) or DEX aggregators (*e.g.*, Paraswap), liquidity provision and borrowing (*e.g.*, Compound, Aave), yield generation via liquid staking (*e.g.*, Lido), investing (*e.g.*, Enzyme Finance), insurance (*e.g.*, Nexus Mutual), among others. As shown above, the manner in which genuine DeFi Systems operate is fundamentally different from the way traditional financial institutions function. This is somewhat akin to the evolution of telephony: from telegraphs with operators who transcribed and transmitted; to telephone switchboard operators who connected calls to each other; to modern, automated cell packet switching with no intermediary operators.

B. Additional Relevant Considerations On DeFi Ecosystems

Considering how to combat illicit finance in on-chain CeFi and genuine DeFi requires acknowledging a few additional features of these ecosystems.

First, the DeFi Transaction Flow is the same as the flow for non-financial, blockchain-based applications, such as blockchain-based social media applications, gaming, consumer loyalty programs and the like. The user connects their self-hosted wallet to an application and the flow of the information about the database transaction or interaction in which the user wants to engage is communicated — also through RPC nodes and other parts of the software stack — until it is recorded on a blockchain network.

Second, the DeFi Transaction Flow does not show the ways in which a DeFi protocol can be changed or updated. Genuine DeFi protocols can be "static" — no one can upgrade, amend or otherwise change

[67] Relayers can also be — and frequently are — RPC node providers, whether as individuals or as RPC-node-as-a-service providers.

the smart contracts, as in the case of the Uniswap V1 and V2 smart contracts,[68] and the contracts run as intended absent an exploit or a bug;[69] or they can be "dynamic" — able to be changed or upgraded, typically through on-chain, transparent voting by a broader community of individuals. This decentralized, community voting frequently occurs through "governance tokens," another software protocol that allows for voting on the administration of certain features of a DeFi protocol.

In genuine DeFi, governance token holders vote and, if approved, a software protocol communicates the change to a DeFi protocol to implement autonomously, usually after a timelock — after a period of time for users to determine whether or not they wish to safely exit the system. By contrast, according to Schuler et al., in an on-chain CeFi System, governance token holders may still vote but a separate individual or entity is needed to implement the change or upgrade resulting from the vote.[70] Regulators have frequently cited the purported concentration of governance tokens by particular holders — coupled with lower voting participation — as an indicator of "centralization" in a DeFi protocol.[71] As discussed below, the ability to significantly influence the outcome of a governance vote does not bear the essential hallmarks of "independent control" — *i.e.*, absent certain circumstances, holding governance tokens, even a large amount, does not bestow the unilateral authority to immediately affect value or the user base of a particular DeFi System.

---

[68] *See, e.g.*, *The Uniswap Protocol: Introduction*, Uniswap Docs, https://docs.uniswap.org/concepts/uniswap-protocol (last visited Jan. 23, 2024) ("The protocol is implemented as a set of persistent, non-upgradable smart contracts; designed to prioritize censorship resistance, security, self-custody, and to function without any trusted intermediaries who may selectively restrict access."); *see also* Alex Wade, Michael Lewellen & Peter Van Valkenburgh, *How Does Tornado Cash Work?*, Coin Center (2022), https://www.coincenter.org/education/advanced-topics/how-does-tornado-cash-work/ ("As stated previously, for most readers, Tornado Cash is synonymous with a core subset of the Tornado Cash smart contracts: the Tornado Cash pools. The vast majority of these contracts are immutable. That is, they have no ability to be updated or removed by anyone.").

[69] In other words, the only method for new or upgraded versions of the same or similar protocol are through entirely new deployments.

[70] On-Chain CeFi, *supra* note 7 at 29 ("If a proposal is accepted, there will still be someone who writes the code and deploys the new logic contract. In this case, token-based governance is non-binding and the restricted function to upgrade the contract is actually governed by the deployer's admin key.").

[71] *See, e.g.*, DeFi Risk Assessment, *supra* note 3 at 13 ("Moreover, distribution and concentration of governance tokens and voting demonstrate control over decentralized applications. In some services, governance tokens or voting rights may be concentrated and held by a limited number of actors."); Olivier Fliche, Julien Uri & Mathieu Vileyn, ACPR, *"Decentralised" or "Disintermediated" Finance: What Regulatory Response?: Summary of Responses to the Public Consultation*, 9 (2023), https://acpr.banque-france.fr/sites/default/files/medias/documents/defi_synthese_consultation_en.pdf [hereinafter ACPR DeFi Consultation] ("Whether through the concentration of the majority of governance tokens in the hands of a few players, the retention of administrator keys, or the existence of other privileges that relativise voting mechanisms, the discussion paper showed that the governance of many protocols appeared to be falsely decentralised ('decentralised in name only')."); Fin. Stability Bd., *The Financial Stability Risks of Decentralised Finance*, 12 (2023), https://www.fsb.org/wp-content/uploads/P160223.pdf ("Voting power is typically proportional to the holdings of the relevant DAO's governance tokens, which are in principle open to be acquired by anyone. In practice, however, as seen in Table 1 below, voting control can be highly concentrated and opaque.").

C. Sources of Illicit Finance Risks in DeFi

In TradFi, failure to detect or disrupt illicit financial activity arises primarily from subjective errors in human judgment (*e.g.*, gaps in procedures or systems, missed risk factors in transaction analysis, etc.) or from concentration of data or information or fragmented, large volumes of data.[72] In fully decentralized software Systems such as genuine DeFi, however, technology takes the place of people in processing and reviewing transactions, and data is not centrally stored through opaque centralized entities. Genuine DeFi protocols execute transactions automatically via conditional code — *i.e.*, no human subjectivity — and transaction information is recorded and available on an immutable blockchain ledger, updated at a predictable interval and open for anyone to view and detect gaps or errors.

For this reason, illicit finance risk in DeFi Systems, emanates from different risks than in TradFi and typically from one of three sources: *first*, through cyber risks within the technology of the DeFi protocols themselves, stemming either from improper coding or from improper configuration of the system; *second*, from poor or compromising risk management practices that creates a vector for attack;[73] and *third*, from the use of a protocol for the laundering or concealment of ill-gotten or illicit funds.

1. *Cyber Risks*

Illicit actors can exploit or hack DeFi protocols and abscond with user funds due to "cyber risk," referring to vulnerabilities in the code itself — code errors, bugs or loopholes or flaws in code design. Regulators in the U.S. and abroad have issued policy papers discussing these risks,[74] and U.S. law enforcement acknowledges that these risks can lead to exploits and frequently assists in response to DeFi hacks.[75]

Typically sophisticated technical actors perpetrate exploits arising from cyber risks. A case study of one such exploit — the Wormhole Bridge hack — highlights this point, but also demonstrates that these cyber risks can be remediated to reduce the risk and any vulnerabilities in the code.

---

[72] U.S. Dep't of the Treas., National Money Laundering Risk Assessment, (2022), https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf.

[73] Eur. Sec. and Marks. Auth., Decentralised Finance in the EU: Developments and Risks, 9 (2023) https://www.esma.europa.eu/sites/default/files/2023-10/ESMA50-2085271018-3349_TRV_Article_Decentralised_Finance_in_the_EU_Developments_and_Risks.pdf ("Attacks on DeFi protocols essentially target code vulnerabilities (e.g. errors in the underlying smart contracts), and access control points (e.g. protocols' consensus mechanisms or governance frameworks), with a view to altering their functioning.").

[74] *See e.g.*, DeFi Risk Assessment, *supra* note 3; ACPR DeFi Consultation, *supra* note 71.

[75] *See, e.g.*, Public Service Announcement, Fed. Bureau of Investigation, Cyber Criminals Increasingly Exploit Vulnerabilities in Decentralized Finance Platforms to Obtain Cryptocurrency, Causing Investors to Lose Money, https://www.ic3.gov/Media/Y2022/PSA220829 (last visited Jan. 23, 2024).

Case Study #1: Wormhole Bridge Exploit[76]

In February 2022, an attacker found a bug in the smart contracts of the Wormhole bridge, which allowed the attacker to generate — and abscond with — $325 million worth of cryptocurrency that were locked in the bridge, resulting in one of the largest crypto exploits to date.[77]

Wormhole[78] is a generic message passing protocol that allows for communication among blockchains using Wormhole core smart contract software that are deployed on each supported blockchain. This core smart contract reads the information published by the source blockchain's smart contracts and emits this information to an off-chain Guardian network — a peer-to-peer network of validators that read messages emitted by the core contract and produce signed messages, similar to multi-signature wallet transactions, which are discussed separately — which then submits a transaction via a permissionless relayer[79] to the target blockchain once the designated number of Guardian signatures are obtained.[80]

One application of the Wormhole protocol functions as a bridge that connects the Solana blockchain to the Ethereum blockchain. A bridge is software code that allows users to, in effect, create a representation of a cryptocurrency relating to one blockchain and move that representation of value to another blockchain. Users supply cryptocurrencies on one blockchain and then cause the bridge, through its code, to send a message to smart contracts on the other blockchain to "mint" or create a representation of that cryptocurrency (sometimes referred to as a "wrapped asset") in the same amount on the other blockchain — resulting in a new cryptocurrency with its value pegged to the original asset.[81] The cryptocurrency on the original blockchain are supplied by the user to the bridge protocol where they remain, such that the "wrapped asset" is the only asset that can be moved on-chain.

During the Wormhole Bridge exploit, the attacker found a code vulnerability[82] that allowed them to bypass the Guardians and mint 120,000 wrapped Ethereum (equivalent of $325 million at the time)

---

[76] Thank you to the Wormhole Foundation and Asymmetric Research for their review and feedback on Case Study #1.

[77] *Rekt - Leaderboard*, rekt, https://www.rekt.news/ (last visited Jan. 23, 2024).

[78] This paragraph provides a brief overview of how Wormhole functions. For a more comprehensive description, *see Introduction*, Wormhole Docs, https://docs.wormhole.com/wormhole/ (last visited Jan. 23, 2024).

[79] For more on Wormhole relayers, *see Relayers*, Wormhole Docs, https://docs.wormhole.com/wormhole/explore-wormhole/relayer (last visited Jan. 23, 2024).

[80] Currently, there are 19 Guardians, made up of some of the largest and well-known validator companies in blockchain; transactions require 13 out of 19 Guardians.

[81] For more on bridges, *see What Is A Cross Chain Bridge?*, Chainlink, https://chain.link/education-hub/cross-chain-bridge (Jan. 12, 2024).

[82] For a technical explanation of what happened in the smart contract exploit, *see Wormhole - Rekt*, rekt, https://rekt.news/wormhole-rekt/ (last visited Jan. 23, 2024).

on the Solana blockchain without supplying the required amount of Ethereum on the Ethereum blockchain. Following the hack, the Wormhole Foundation — an organization that supports the Wormhole ecosystem — offered the attacker $10 million as a "whitehat agreement" in exchange for details about the exploit and the return of the minted assets. There was no response from the attacker. Less than 24 hours after the attack, Jump Crypto — the blockchain development and one of the investing arms of Jump Trading Group that was also involved in the development of the Wormhole protocol — supplied the necessary funds to replace the stolen Ethereum after the vulnerability was addressed.[83]

After the exploit, the Wormhole protocol implemented several defense-in-depth mechanisms to limit the potential for similar vulnerabilities. These included a mechanism called Governor, an optional capability which allows Wormhole Guardians to rate-limit the notional flow of value for any registered token bridge on a per-chain basis, as a means to guard against the existential risk of a smart contract or L1 compromise. Jump Crypto also launched a multi-million dollar bug bounty program to incentivize security researchers to help find and address vulnerabilities.[84]

2. *System Management Risks*

Illicit finance risks can also arise from the ways in which software developers manage or otherwise attend to issues of security and resilience in DeFi Systems. Centralization — and its concomitant introduction of subjective human judgment — presents additional vulnerabilities for potential exploitation, specifically through social engineering. This type of attack usually entails someone on X, Telegram or another social networking platform convincing a user or employee at a software company to provide their personal information or credentials to initiate or approve a scam transaction.

Case Study #2: Ronin Bridge Hack

One of the most notorious illicit finance exploits in crypto is the Ronin Bridge hack, in which the Lazarus Group — the cybercrime arm of the Democratic People's Republic of Korea's ("DPRK") — stole $625 million USD worth of cryptocurrency.[85] Although many refer to this as a "DeFi hack," it is anything but: Lazarus exploited a centralized vulnerability using a traditional cyber attack, known

[83] Jump Crypto (@jump_), Twitter (Feb. 3, 2022), https://twitter.com/jump_/status/1489301013408497666.
[84] *Wormhole Security Program — End-of-Year Update*, Wormhole (Dec. 21, 2022), https://wormhole.com/wormhole-security-program-end-of-year-update/.
[85] *Inside North Korea's Crypto Heists: $200M in Crypto Stolen in 2023; Over $2B in the Last Five Years*, TRM Labs (Aug. 18, 2023), https://www.trmlabs.com/post/inside-north-koreas-crypto-heists.

as social engineering, that allowed it to access the centralized servers that hosted the software for the Ronin bridge and steal the user funds.

The Ronin bridge connected the Ronin blockchain — an Ethereum side-chain developed for gaming and which hosted Axie Infinity, one of the then-most popular blockchain-based games — and Ethereum, which allowed users to initiate deposits or withdrawals of funds with a set of validator nodes to verify these transactions, similar to how blockchain networks function.

Transactions on the Ronin bridge required approval by the majority of nodes of the Ronin network — five of the nine. Out of the nine nodes, Sky Mavis — the software company that developed the Ronin bridge — controlled four. About a year before the hack, due to the high volume of transactions, the decentralized autonomous organization ("DAO") for Axie Infinity — another one of the nodes — gave its private key used for signing the transactions to Sky Mavis to facilitate faster authorization (*i.e.*, to increase speed of validating transactions). Although Sky Mavis stopped signing transactions on behalf of Axie DAO a month later, Axie DAO never revoked access to its private key stored on the Sky Mavis servers. Thus, Sky Mavis ran four of the nine nodes and unofficially controlled a fifth. This meant that Sky Mavis had centralized control over the network because it held the required majority for approval of transactions.

On March 23, 2022, Lazarus accessed the Sky Mavis servers through a backdoor facilitated by social engineering practices.[86] Specifically, Lazarus sent an infected PDF file to a single Sky Mavis employee that allowed it to gain control of the servers, obtained the private keys for the validators,[87] and used those keys to authorize two large withdrawals of users' cryptocurrencies — including stablecoins — from the Ronin bridge. Sky Mavis had no systems monitoring in place, which meant that it only discovered the breach when a user reported difficulty accessing funds, days later.

This risk is *not* inherent in all bridge smart contracts; if SkyMavis had used the proper security risk management, including the proper dispersion and decentralization of keys, it may have avoided the hack altogether. In addition, it is important to note that bridges are *not* DeFi per se and are not considered to be part of the definition of DeFi in this paper; they are separate software within the blockchain architecture.

[86] Adi Robertson, *Axie Infinity's Blockchain Was Reportedly Hacked via a Fake LinkedIn Job Offer*, The Verge (July 6, 2022), https://www.theverge.com/2022/7/6/23196713/axie-infinity-ronin-blockchain-hack-phishing-linkedin-job-offer.

[87] *Community Alert: Ronin Validators Compromised*, Ronin Network (Mar. 29, 2022) https://web.archive.org/web/20230528184521/https://blog.roninchain.com/p/community-alert-ronin-validators.

These system management risks are neither new nor unique to blockchain-based software systems; they are typical cyber attacks such as phishing that occur in the cyber-realm more broadly.[88]

3. *Usage Risks*

International regulators and policymakers also have focused on the ways illicit actors use DeFi protocols to launder stolen assets.[89]

Illicit actors employ many of the same unlawful tactics in DeFi that they do in TradFi: structuring — breaking up transactions into smaller amounts when placing them into the system; layering — creating an obscure network of transactions so the flow of funds are difficult to follow; and integration — moving funds out of DeFi to centralized exchanges or to the off-chain world.[90]

Structuring: In DeFi, structuring typically occurs by moving assets from the wallet holding illicit gains to numerous other wallets or DeFi protocols where assets are pooled together. This movement can be traced and tracked based on the inherently transparent nature of blockchains. Illicit actors engage in layering via privacy-preserving software, whether it be DeFi protocols, like "mixers," which are discussed below, or inherently shielded cryptocurrencies known as "privacy coins;" illicit actors integrate funds by transferring cryptocurrency from DeFi to centralized, custodial entities, such as exchanges, to exchange cryptocurrencies for fiat currency that can be used in the TradFi system for other illicit purposes such as purchasing weapons.[91]

Layering: Use of DeFi protocols in the layering stage has garnered the most attention from policymakers and regulators, who argue that autonomous, privacy preserving genuine DeFi protocols, such as certain mixers, carry a disproportionately high risk of illicit financial abuse.[92] Decentralized mixers work through smart contracts; these protocols allows users to supply cryptocurrencies from one wallet (Wallet A) to a "pool" comprised of smart contracts, where those inputs are joined in an anonymity set with inputs from multiple other persons, and then to withdraw the same amount of cryptocurrencies to a different wallet (Wallet B). In contrast, centralized mixing services are provided by

---

88 *See e.g.*, Guidance, Fin. Indus. Regul. Auth., Common Cybersecurity Threats, https://www.finra.org/rules-guidance/guidance/common-cybersecurity-threats (last visited Jan. 23, 2024).

89 But note the Treasury Department recognized in its DeFi Risk Assessment, "[M]oney laundering, proliferation financing, and terrorist financing most commonly occur using fiat currency or other traditional assets as opposed to virtual assets." *See* DeFi Risk Assessment, *supra* note 3 at 36.

90 DeFi Risk Assessment, *supra* note 3 at 16.

91 *Id.*

92 *See e.g.*, Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, 88 Fed. Reg. 72701-23 (proposed Oct. 23, 2023) (to be codified at 31 C.F.R. pt. 1010.662) [hereinafter Proposal of Special Measure].

an identifiable entity or person that receives, custodies, and exercises independent control over user funds sent from the user's wallet (Wallet 1), pools multiple users' funds together and then sends cryptocurrencies to a different wallet pre-specified by the user (Wallet 2) — all for a fee from the user.[93] These latter centralized mixers — decidedly *not* DeFi — do bear hallmarks of money transmission, with a clear person or entity providing a service that involves holding, custodying and independently controlling customer funds; whereas decentralized mixers run autonomously, without any human involvement, and users conduct transactions through their own wallets entirely at their direction. Both centralized and decentralized mixers allow users to diffuse the connection between the two wallets through which they transfer funds. Some regulators and policymakers argue that these mixers are intended to make it more difficult for law enforcement to trace ill-gotten assets. OFAC has imposed sanctions on both decentralized mixers, *e.g.,* Tornado Cash (discussed in Case Study #3 below) and centralized mixers, *e.g.*, Bitcoin Fog,[94] Helix,[95] and CoinNinja.[96]

Although mixers can be used to obscure illicit activities, mixers also can be used to enhance the privacy of legitimate transactions (*e.g.*, employers sending salaries to employees).[97] Privacy technologies and practices — whether Virtual Private Networks ("VPNs"), holding companies, mixers or encryption — are purpose-agnostic, allowing both legitimate/licit and illicit uses. Law-abiding individuals, corporations and even governments, such as the U.S. government, use privacy technology in furtherance of completely lawful, legitimate ends. Indeed, VPNs provide privacy for Internet data traffic that is critical to the security of online communications that most federal government agencies require employees to use this privacy technology to connect remotely to their servers,[98] even though these same VPNs often obscure the true Internet Protocol ("IP") address of users, including for users in comprehensively sanctioned jurisdictions. The U.S. federal government recognizes the importance of privacy preserving technology and, indeed, *requires* its employees to use it even if that same technology also can be used for illicit purposes.

---

93 Robert Stevens, *Bitcoin Mixers: How Bitcoin Mixers Work and Why People Use Bitcoin Mixers*, CoinDesk (May 11, 2023), https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used/.

94 Press Release, U.S. Dep't of Just., Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency "Mixer," (2021), https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer.

95 Press Release, U.S. Dep't of Just., Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin 'Mixer' That Laundered Over $300 Million, (2021), https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million.

96 Press Release, Fin. Crimes Enf't Network, First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws, (2020), https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws.

97 Proposal of Special Measure, *supra* note 92 at 72706 ("CVC mixing may be used for legitimate purposes, such as privacy enhancement for those who live under repressive regimes or wish to conduct licit transactions anonymously.").

98 *See e.g.*, Advisory, Cybersecurity & Infrastructure Security Agency, AA20-073A, Cybersecurity Advisory: Enterprise VPN Security, (2020), https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a ("Remote work options—or telework—require an enterprise virtual private network (VPN) solution to connect employees to an organization's information technology (IT) network.").

Integration: In practice, DeFi protocols actually pose obstacles for illicit actors at the integration stage. *First*, converting cryptocurrencies into fiat currencies requires the use of custodial cryptocurrency exchanges, which, in the United States, are BSA-obligated financial institutions required to implement AML programs.[99] As part of these programs, centralized exchanges block wallets that have been identified by law enforcement, their own risk indicators or blockchain analytics companies as belonging to illicit actors. *Second*, selling or converting sums of the size stolen in these exploits not only require high fees but also can cause the price of the relevant cryptocurrency to fall precipitously, given how illiquid some of these markets are.[100] *Third*, some U.S.-based centralized cryptocurrency exchanges have implemented pauses, stops or enhanced due diligence on transfers above a certain size or from an account based on certain patterns that raise suspicions.[101] For these reasons, blockchain analytics companies tracking the proceeds of illicit transactions that have been laundered through DeFi protocols recognize that a significant portion of these assets cannot be "integrated" — Lazarus and other bad actors face difficulty in moving the illicit funds out of their cryptocurrency wallets to exchanges for conversion to fiat currency.[102]

These challenges have not fully deterred bad actors from engaging with DeFi protocols as it relates to structuring or layering the proceeds of illicit activity, as discussed briefly in the case study below.

Case Study #3: Usage Risks — DPRK

After the Ronin bridge exploit discussed in Case Study #2 above, the Lazarus Group engaged in both structuring and layering to make it difficult for law enforcement to trace the funds.

O-chain tracing shows that immediately after exploiting the Ronin bridge, the Lazarus Group swapped certain stolen stablecoins — *e.g.*, USD Coin ("USDC") — for Ethereum on decentralized exchanges to avoid the funds being frozen by law enforcement. It then split the funds and either sent

99 *See* DeFi Risk Assessment, *supra* note 3 at 29 ("The 2022 NRAs identified that the most significant illicit financing risk associated with virtual assets stemmed from VASPs operating abroad with substantially deficient AML/CFT programs, particularly in jurisdictions where AML/CFT standards for virtual assets are nonexistent or not effectively implemented."); *see also* Fin. Action Task Force, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, 2 (2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf ("However, it is a serious concern that 75% of jurisdictions assessed against the revised standards are only partially or non-compliant with FATF's requirements.").

100 This frequently leads to hackers immediately converting low liquidity, vulnerable cryptoassets to stablecoins, as discussed further below.

101 The FBI recently published a list of wallets they have identified as belonging to the DPRK — which contain an estimated $40 million worth of bitcoin — meaning any compliant centralized exchange would not convert cryptocurrency from those wallets into fiat currencies and, moreover, would freeze those assets if they are stored on the exchange. *See* Press Release, Fed. Bureau of Investigation, FBI Identifies Cryptocurrency Funds Stolen by DPRK, (2023), https://www.fbi.gov/news/press-releases/fbi-identifies-cryptocurrency-funds-stolen-by-dprk.

102 *BBC Podcasts: The Lazarus Heist* (downloaded using Apple Podcasts).

them to centralized exchanges[103] for off-ramping or to mixers — both centralized and decentralized. Lazarus's attempted use of mixers has been well-documented elsewhere.[104]

Due to on-chain tracing, law enforcement has been able to determine that Lazarus — and other sanctioned actors — have sent proceeds of cryptocurrency exploits to decentralized mixers like Tornado Cash at a high rate, as well as to centralized mixers like Blender.io and Sinbad.io.[105] In fact, and infamously, DPRK deposited so much cryptocurrency to Tornado Cash that the deposits tested the capacity of the system.[106] As a result, in August 2022 (as amended in October 2022), OFAC sanctioned certain Ethereum addresses known to be the Tornado Cash[107] smart contracts, other mixers thereafter and, in November 2023, Bitcoin mixer, Sinbad.io,[108] likely a "rebrand" of the previously-sanctioned Blender.io Bitcoin mixer,[109] which OFAC sanctioned in May 2022.[110]

Despite the Lazarus Group's off-ramping efforts from mixers, U.S. law enforcement has been able to follow the funds to "cash out" points, freeze the assets and ultimately recover over $30 million.[111] A year later, the Norwegian government was able to recover another $6 million using similar methods. These recoveries "demonstrate that it is becoming more difficult for bad actors to successfully cash out their ill-gotten crypto gains."[112]

---

103 Changpeng Zhao (@cz_binance), Twitter (Apr. 22, 2022), https://twitter.com/cz_binance/status/1517385438469791749.

104 *See e.g.*, *North Korea's Lazarus Group Moves Funds Through Tornado Cash*, TRM Labs (Apr. 28, 2022), https://www.trmlabs.com/post/north-koreas-lazarus-group-moves-funds-through-tornado-cash; *North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High*, Chainalysis (Jan. 13, 2022), https://www.chainalysis.com/blog/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/; *Has a Sanctioned Bitcoin Mixer Been Resurrected to Aid North Korea's Lazarus Group?*, Elliptic (Feb. 13, 2023), https://www.elliptic.co/blog/analysis/has-a-sanctioned-bitcoin-mixer-been-resurrected-to-aid-north-korea-s-lazarus-group.

105 *North Korea's Lazarus Group Identified as Exploiters Behind $540 Million Ronin Bridge Heist*, Elliptic (Apr. 14, 2022), https://www.elliptic.co/blog/540-million-stolen-from-the-ronin-defi-bridge.

106 North Korea's Lazarus Group moves funds through Tornado Cash.

107 Press Release, U.S. Dep't of Just., Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency "Mixer," *supra* note 94.

108 Press Release, U.S. Dep't of the Treas., Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency, (2023), https://home.treasury.gov/news/press-releases/jy1933.

109 *Sinbad Crypto Mixer Flagged by Elliptic Sanctioned and Seized*, Elliptic (Nov. 29, 2023), https://www.elliptic.co/blog/sinbad-crypto-mixer-flagged-by-elliptic-sanctioned-and-seized.

110 Press Release, U.S. Dep't of the Treas., U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats, (2022), https://home.treasury.gov/news/press-releases/jy0768.

111 Erin Plante, *$30 Million Seized: How the Cryptocurrency Community Is Making It Difficult for North Korean Hackers To Profit*, Chainalysis (Sept. 8, 2022), https://www.chainalysis.com/blog/axie-infinity-ronin-bridge-dprk-hack-seizure/.

112 *Id*.

It has been reported that Hamas and Palestinian Islamic Jihad also purportedly used mixers; there is significantly less evidence on this point, though.[113]

4. *Data Accessibility as Illicit Finance Risk Mitigation*

Notwithstanding the risks set forth above, the public, accessible nature of blockchain data works in favor of law enforcement tracing, tracking and apprehending illicit actors. Although data transparency is not the only answer to combating illicit finance in DeFi Systems, a December 2023 report from the Government Accountability Office noted that despite risks posed by cryptocurrencies and blockchain-based systems, "advancements in capabilities to trace transactions and identify illicit actors could mitigate some sanctions evasion risks."[114] The DeFi Risk Assessment recognizes the same: "The ability to use data from the public blockchain in addition to the development of industry-driven compliance solutions for DeFi services can also help mitigate some illicit finance risks."[115]

Case Study #4 provides one example of how accessibility of blockchain data has proven to be beneficial to U.S. law enforcement on an international scale, with law enforcement agencies being able to share public blockchain information more easily than other, more sensitive, types of information.

Case Study #4: "Welcome to Video" Takedown

In 2019, the Department of Justice ("DOJ") announced the shutdown of Welcome to Video, one of the largest ever child pornography sites by amount of material stored, as well as the arrest of the site's owner and operator.[116] Law enforcement shut down the site and seized over eight terabytes[117] of child

[113] *See* Proposal of Special Measure, *supra* note 92. The reports of Hamas' illicit use of cryptocurrencies is the subject of debate. *See* Sam Lyman, *How Misinformation About Hamas And Crypto Fooled Nearly 20% of Congress*, Forbes (Nov. 8, 2023), https://www.forbes.com/sites/digital-assets/2023/11/08/how-misinformation-on-hamas-and-crypto-fooled-nearly-20-of-congress/?sh=5fd523168270.

[114] U.S. Gov't Accountability Off., GAO-24-106178, Economic Sanctions: Agency Efforts Help Mitigate Some of the Risks Posed by Digital Assets, 1 (2023).

[115] DeFi Risk Assessment, *supra* note 3 at 8; *see also id.* at 32-33 ("Public ledgers can support investigations by competent authorities in tracing the movement of illicit proceeds. While the ledgers do not contain names or traditional account identifiers associated with any particular address, regulators and law enforcement can in some cases take viewable pseudonymous user and transaction information and pair it with other pieces of information to identify transaction participants.").

[116] Press Release, U.S. Dep't of Just., South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin, (2019), https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child; For an additional case study on Welcome to Video, *see Chainalysis in Action: DOJ Announces Shutdown of Largest Child Pornography Website*, Chainalysis (Oct. 16, 2019), https://www.chainalysis.com/blog/chainalysis-doj-welcome-to-video-shutdown/.

[117] This is equivalent to 10,000 CDs, *see* Kelly Phillips Erb, *IRS Followed Bitcoin Transactions, Resulting In Takedown Of The Largest Child Exploitation Site On The Web*, Forbes (Oct. 16, 2019), https://www.forbes.com/sites/kellyphillipserb/2019/10/16/irs-followed-bitcoin-transactions-resulting-in-takedown-of-the-largest-child-exploitation-site-on-the-web/.

pornography, making it one of the largest — and most disturbing — seizures. In addition, law enforcement agencies identified and rescued 23 minors, while arresting over 300 users of the site.

The operation was made possible by tracking on-chain Bitcoin transactions. Welcome to Video used bitcoin for payments and funding its operation, which allowed governments around the world to use blockchain analytics to determine the location of the Welcome to Video's server and, ultimately, shut down its operation.

Welcome to Video had a global customer base, requiring cross-border collaboration among law enforcement agencies. Because of the open nature of blockchain, law enforcement agents could access blockchain data and use blockchain analytics software to trace transactions, map out contributors and users of the site and disseminate the public blockchain evidence to their global partners with minimal friction. They were able to view blockchain records regardless of where in the world they were created, without subpoenas or agreements with foreign jurisdictions. They were able to share this information across agencies and act quickly to take down the site and identify and rescue victimized children. The public blockchain ledger also disclosed which centralized exchanges had interacted with suspected wallets, so agents could go directly to the relevant exchanges and show them how the suspected perpetrator interacted with their platform.

The Welcome to Video investigation demonstrates how public blockchain records can assist law enforcement agencies to efficiently and effectively identify bad actors and prevent future harm. Rather than spending months or years finding the relevant financial institutions, subpoenaing them and using Mutual Legal Assistance Treaties to transfer information between jurisdictions, law enforcement officials instantly and simultaneously act based on public blockchain data. The permanence of blockchain records also means that law enforcement officials can continue analyzing the data for years to come. As Chris Janczewski, one of the lead investigators in the Welcome to Video case, stated "if a bank was robbed five years ago and you're still trying to chase down those leads, you have no idea potentially where that stolen cash could be at this point. With cryptocurrencies, like bitcoin, every transaction is on a public ledger. It's public and is there forever."[118]

III. A Conceptual Framework for Combating Illicit Finance Risks in DeFi

This section proposes a framework for combating illicit finance risks in DeFi built upon the realities of DeFi Systems as well as the sources of illicit finance risks therein. This framework addresses three main

[118] Michelle Cho & Ken Dilanian, *Cryptocurrency May Not Be so Crime-Friendly after All. Federal Law Enforcement Is Getting Good at Tracing It*, NBC News (May 13, 2022), https://www.nbcnews.com/news/crime-courts/cryptocurrency-may-not-crime-friendly-federal-law-enforcement-getting-rcna23844.

problems recognized by regulators, policymakers and industry: *first*, that not all DeFi Systems are actually "decentralized" — *i.e.*, they are not genuine DeFi Systems but instead have significant points of centralization such that existing regulations may apply;[119] *second*, existing, intermediary-based regulation does not lend itself to genuine DeFi systems — indeed, this type of regulation is both over- and under-inclusive and attempts to address risks that are not present or predominant in genuine DeFi Systems — but nonetheless require guardrails to combat illicit finance risks; and *third*, that sources of illicit finance risk in DeFi Systems significantly differ from those in TradFi and, thus, require new solutions.

To do so, the below framework proposes (a) defining what constitutes "independent control" over a software system, such that it could be classified as on-chain CeFi and, thus, likely subject to certain existing regulatory obligations, after examining the facts and circumstances of the person exercising independent control; (b) classifying genuine DeFi Systems as "critical infrastructure" in the financial sector overseen by the Treasury Department's OCCIP; and (c) creating a new category of "critical communications transmitters" that interact with and are integral to genuine DeFi Systems — but do not meet the definition of "independent control" — such that they would have to undertake certain tailored obligations to assist in protecting U.S. national and economic security, without becoming "financial institutions" subject to the BSA.

A. Identifying and Defining "Independent Control" in On-Chain Software Systems

Schuler et al. recognize that in on-chain CeFi Systems, certain identifiable actors have special privileges that allow them to place restrictions on user assets or otherwise have independent control over the System and, thus, over user funds.[120] These privileges, in some instances, may be similar to the control traditional financial intermediaries exercise over customer assets, systems or data, but may also work differently depending on the facts and circumstances of the specified activities. Schuler et al. further recognize that identifiable actors in on-chain CeFi Systems should be subject to appropriate regulation, depending on the activity being facilitated or the information being accessed and shared.[121] Where identifiable actors are performing the *exact same* functions as traditional financial intermediaries in on-chain CeFi Systems, regulations likely should not differ simply because of the type of software involved. This principle holds equally true where entities in blockchain-based, centralized Systems engage in the exact same conduct as "financial institutions" under the BSA; regulating these people or entities as BSA-

[119] *See, e.g.*, DeFi Risk Assessment, *supra* note 3 at 1-2.

[120] On-Chain CeFi, *supra* note 7 at 2.

[121] *Id.* at 37 ("Centralized financial services that run on a blockchain should not be referred to as DeFi. Instead, we propose the term on-chain CeFi and argue that these centralized service providers can and should be regulated in line with their non-blockchain-based counterparties.").

obligated financial institutions may fill some of the regulatory "gaps" cited by the DeFi Risk Assessment.[122]

Such regulation of on-chain CeFi intermediaries, however, does not require creating a "new cryptocurrency-related category" of "financial institution," as suggested by the Treasury Department's Deputy Secretary in late 2023.[123] The better approach is to define when persons, including natural persons or entities, are engaged in the *exact same* activity in blockchain-based software applications as BSA-enumerated "financial institutions." This definition should hinge on persons administering, managing or otherwise affecting users' assets or transactions in the DeFi context. To that end, as supported by the 2019 FinCEN Guidance, we proposed a definition of "independent control" that should capture on-chain CeFi intermediaries.

> "Independent control" means, for a blockchain-based software system that allows for financial transactions (the "System"), the unilateral ability to —
>
> 1. exercise operational authority over any third party's value in the System or otherwise immediately affect any value within the System, including by ceasing operation from within the System, or
> 2. admit, permit, restrict, deny or modify —
>   a. those who have had access to the System or
>   b. the ways in which anyone has used or accessed the System for any reason or at any time in a way that substantially affects any third party's value in the System.

A person[124] who exercises "independent control" over a System, as defined above, is referred to herein as a "System Control Person." Note that in a System where a user can counteract or otherwise avoid the impact of a change — *e.g.*, by exiting the system safely with all funds prior to any change — there is likely no person exercising independent control over user funds and, thus, no System Control Person. Using this broader definition of "independent control" — one that is not specific to upgrading code alone — will allow the definition to remain evergreen and grow as these technological, software-based systems evolve.

Applying this definition of "independent control" would produce results consistent with the 2019 FinCEN Guidance relating to "certain business models" involving cryptocurrency.[125] In the 2019

[122] DeFi Risk Assessment, *supra* note 3.

[123] *See* U.S. Dep't of the Treas., *Potential Options to Strengthen Counter-Terrorist Financing Authorities*, 2 (Nov. 28, 2023), https://www.coincenter.org/app/uploads/2023/12/11.28.2023-Counter-TF-Legislative-Proposals.pdf [hereinafter Potential Options].

[124] "Person," as used in this definition, has the same meaning as in the BSA. *See* 31 CFR §1010.100(mm).

[125] 2019 FinCEN Guidance, *supra* note 35 at 2.

FinCEN Guidance, FinCEN recognized that MSB obligations are the responsibility of those persons who are "acting as intermediaries [and] have total independent control over the value" owned by customers and provided to the software or business model.[126] FinCEN focused its analysis in the 2019 FinCEN Guidance on the facts and circumstances relating to a person's ability to affect value within a specific business model, not on technological details of how code operates or labels.[127] Although a System involving a System Control Person does not necessarily constitute one of the types of "financial institutions" subject to the BSA today, System Control Persons are more likely to bear some of the hallmarks of "financial institutions" in terms of their ability to intervene in protective ways, as recognized by Schuler et al.[128]

Attachment of BSA regulatory obligations to those persons that meet the definition of System Control Persons should not be automatic for at least two reasons. *First*, given the public accessibility of on-chain data, System Control Persons generally do not have the siloed, unique access to risk data that traditional "financial institutions" have, which is the impetus for the BSA's recordkeeping and reporting requirements. Law enforcement and other risk managers in the ecosystem already have access to the same information. This transparency contributes to the often fast responses and fixes to exploits in DeFi, compared to traditional finance where regulators impose specific requirements to obligate bank,[129] non-bank financial institutions[130] and their service providers to report cyber exploits, in addition to reporting indicators of siloed illicit finance activity. *Second*, illicit finance regulation and classification of persons as "financial institutions" requires analysis of the "facts and circumstances" of business models and certain types of activities. Failure to engage in this analysis would overlook a keystone of how FinCEN regulates "financial institutions."[131] Accordingly, after determining whether there is a person exercising "independent control" within a System, one must engage in examining the "facts and circumstances" of a particular System — the activities being conducted within the System and those conducted by any System Control Person — to determine whether the person merits any regulation or is subject to certain financial laws, including the BSA.[132] For example, a person who may qualify as a System Control Person

---

126 *Id*. at 15.

127 *See, e.g.*, *id.*

128 We note, however, that the Schuler et al. article does not posit a definition of "independent control" or "System Control Person." By using the term "on-chain CeFi" and coupling it with the definition of control and System Control Person, we do not intend to suggest that those authors subscribe to or endorse the definition of control proposed herein.

129 *Banker Resource Center: Information Technology (IT) and Cybersecurity*, Fed. Deposit Ins. Corp., https://www.fdic.gov/resources/bankers/information-technology/ (last visited Jan. 27, 2024); 12 C.F.R. § 304(c) (2021).

130 Press Release, Fed. Trade Comm'n, FTC Amends Safeguards Rule to Require Non-Banking Financial Institutions to Report Data Security Breaches, (2023) https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-amends-safeguards-rule-require-non-banking-financial-institutions-report-data-security-breaches.

131 *See* 2019 FinCEN Guidance, *supra* note 35 at 2 ("Within the context of this guidance, 'business model' refers to the subset of key facts and circumstances relevant to FinCEN's determination of (a) whether the specific person meets the definition of a particular type of financial institution and (b) what regulatory obligations are associated with the specific activities performed within the business model.").

132 *Id.* at 2.

but whose activities amount to no more than holding the key of an emergency multi-signature wallet that only has extremely limited powers in limited circumstances may not be subject to financial regulation. In contrast, a System Control Person holding an administrative key to an entire protocol and exercising independent control over the System consistently may be subject to laws and regulations.

By design, Systems Control Person does not include certain actors that regulators and policymakers have posited as having *some* form of "control" over DeFi Systems.

First, a person who holds significant portions of governance tokens associated with a particular DeFi protocol is not a System Control Person, notwithstanding claims by policymakers, regulators and industry to the contrary.[133] A person simply having an outsized influence in voting only allows that person to sway the potential outcome of a vote that may change how a DeFi protocol operates; it may affect funds within the System or affect who can access the System, depending on the change at issue — or it may not. The voting alone, however, does not allow a governance token holder to take such action *unilaterally*, unless the System is designed that way — *e.g.*, where the circumstances and a protocol's various voting thresholds, quorums and implementation timelines make it possible for a single holder with sufficient governance tokens to take action that unilaterally or immediately affects user funds, such as no timelock.

Second, on-chain governance systems, frequently referred to as DAOs, that can change how DeFi protocols function do not necessarily have "independent control" sufficient to be System Control Persons. The analysis here mirrors that for large governance token holders and depends on reviewing the specific characteristics of a DeFi System's design and the changes to it that an affiliated DAO can — or cannot — make. DAOs typically effect changes via votes by numerous governance token holders, and presently, most DAO-effected changes to DeFi Systems occur after a timelock (not "automatically" as the definition of "independent control" notes), which allows users to determine whether or not they wish to safely exit the system.

Third, the "System Control Person" definition does not capture third party, exogenous software integrated into a DeFi protocol — most notably, oracles, which are smart contracts that store information or data. DeFi software developers use these third party oracles to integrate information into a DeFi protocol regarding pricing, volume, or other data necessary to enable some types of financial transactions on the protocol.[134] The risk within these smart contract oracles may give rise to the need for

[133] *See, e.g.*, *supra* note 71.
[134] Eur. Sec. and Marks. Auth., *supra* note 73 at 5.

certain thoughtful policy solutions, but those remain outside the scope of this paper, although has been addressed in others.[135]

All of these caveats stem from the point above that where a user can counteract or otherwise avoid the impact of a change — *e.g.*, by exiting the system safely with all funds prior to any change — there is likely no person exercising independent control over user funds and, thus, no System Control Person.

Ultimately, any legislation, regulation or guidance imposing BSA-related obligations on System Control Persons must recognize both the two-part analysis set forth above — (1) is there a System Control Person? and if so, (2) what are the "facts and circumstances" of that System Control Person's activities? — as well as certain inherent differences in these on-chain CeFi Systems and appropriately scope the way in which the documentation, detection and deterrence features of financial integrity programs likely may have to be carried out differently.

B. Genuine DeFi as "Critical Infrastructure"

The question remains how to accomplish illicit finance policy objectives in genuine DeFi Systems — to create a risk management framework that both reasonably mitigates risks and allocates attention to priorities while allowing continued access to and innovation around this open technology.

As described above, genuine DeFi comprises neutral software that allows users to communicate certain cryptocurrency transactions. Traditionally, communication tools and communications providers (*e.g.*, telephone and internet infrastructure companies) — even when used to communicate one's intention to complete an economic transaction or, in fact, moving bits and bytes that represent actual value — are *not* classified as financial institutions subject to the BSA.[136] Regulators and policymakers applying a technology neutral approach[137] should (theoretically) apply the same rules to communication tools in genuine DeFi Systems.

---

[135] Regulation of oracles has been discussed in papers such as Tarik Roukny, European Commission, *Decentralized Finance: Information Frictions and Public Policies: Approaching the Regulation and Supervision of Decentralized Finance*, 44-45 (2022), https://data.europa.eu/doi/10.2874/444494.

[136] Although the definition of "financial institution" includes telegraph companies, the implemented regulations of the BSA also include an explicit exemption for telegraph companies "from the requirement in 31 U.S.C. § 5318(h)(1) concerning the establishment of anti-money laundering programs." The original inclusion likely reflects the fact that telegraph companies were some of the first businesses to provide services for customers to transmit value through signals transmission rather than physical delivery of fiat currency. *See* Western Union, *supra* note 33. However, what constitutes a "telegraph company" was never defined in subsequent regulations, and the ongoing exemption likely acknowledges that there is no reason to wholesale cover *all* elements of a telegraph company's data transmission. To the extent these communications systems operate today, many of them would be captured in the exemption for "delivery, communication, or network access services used by a money transmitter" codified in 31 CFR § 1010.100(ff)(5)(ii)(A). While the "money services" aspects of companies like Western Union would now fall under the separate "money services business" definition.

[137] *See The Framework for Global Electronic Commerce: Read the Framework*, President Clinton: The White House Archives (1997), https://clintonwhitehouse4.archives.gov/WH/New/Commerce/ (last visited Jan. 24, 2024) ("Rules should be technology-neutral (i.e.,

Although DeFi protocols continue to operate as neutral infrastructure and should be regulated (or not) accordingly, we recognize that these systems allow users to move value. Indeed, it is possible to create guardrails to combat illicit finance risks arising in these DeFi Systems. Regulators and policymakers should not, as some have suggested,[138] build these guardrails by forcibly importing intermediaries into genuine DeFi Systems[139] any more than it would make sense to require telephone companies to have switchboard operators again to affirmatively verify the identity of who is using any given phone. Rather, to align with the ways in which illicit finance risks in technology systems in the financial services sector are handled today, genuine DeFi should be classified as "critical infrastructure" subject to oversight by OCCIP.

1. *Background on Critical Infrastructure in the U.S.*

The concept of "critical infrastructure" dates back to 1998, when President William Clinton issued a presidential directive and whitepaper underscoring the need to strengthen national "critical infrastructure" to prevent attacks and avoid harm to the U.S.'s national and economic security ("Presidential Decision Directive 63").[140] This "critical infrastructure" included certain types of "interdependent and cyber-supported infrastructure" essential to the functioning of the U.S. economy, including in telecommunications, banking and finance and — as Presidential Decision Directive 63 recognized — "non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy."[141]

Over the last nearly three decades, various presidential directives and legislation have furthered the critical infrastructure oversight framework within the U.S. government. Today, the Cybersecurity and Infrastructure Security Agency ("CISA"),[142] a standalone federal agency that is part of the Department of Homeland Security ("DHS"), "lead[s] the national effort to understand, manage and reduce risk to our cyber and physical infrastructure."[143] According to CISA, "[c]ritical infrastructure are those

---

the rules should neither require nor assume a particular technology) and forward looking (i.e., the rules should not hinder the use or development of technologies in the future)").; *see also* Rajab Ali, *Technological Neutrality*, 14 Lex Electron., 5—10 (2009), https://www.lex-electronica.org/files/sites/103/14-2_ali.pdf.

138 The Bd. of the Int'l Org. of Sec. Comm'ns, Policy Recommendations for Decentralized Finance (DeFi) Consultation Report, 22 (2023), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf ("A regulator should aim to identify the natural persons and entities of a purported DeFi arrangement or activity that could be subject to its applicable regulatory framework (Responsible Person(s)).").

139 Carla Reyes, *Law's Detrimental Reliance on Intermediaries*, 92 Geo. Wash. L. Rev. (forthcoming 2025), SMU Dedman School of Law Legal Studies Research Paper No. 630 (2024), https://papers.ssrn.com/abstract=4692755.

140 The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, President Clinton: The White House Archives (1998), https://clintonwhitehouse5.archives.gov/WH/EOP/NSC/html/documents/NSCDoc3.html (last visited Jan. 24, 2024).

141 *Id.*

142 Pub. L. 115-278.

143 *About CISA*, Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/about (last visited Jan. 24, 2024).

infrastructure systems and assets that are so vital that their incapacitation or destruction would have a debilitating effect on security, the economy, public health, public safety, or any combination thereof."[144] Although CISA has not enumerated specific standards or thresholds for treating cyber and physical infrastructure as "critical," the "vital" and "debilitating effect" measurements are helpful touchpoints.

CISA focuses on 16 identified critical infrastructure sectors, which includes communications, financial services, information technology, among others.[145] It does not promulgate rules or regulations itself,[146] but does ensure that the regulators are able to bring about appropriate rules and regulations in compliance with best practices for the protection of cyber systems. Largely, CISA works across government agencies — including but not limited to the Treasury Department through OCCIP — and the private sector to analyze risk, coordinate responses and establish best practices related to cybersecurity and technological network architecture. It "connect[s] stakeholders in industry and government to each other and to resources, analyses and tools to help them build their own cyber, communications and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people."[147]

The concept of "critical infrastructure" is fundamentally different — and entirely separate — from the designation of certain persons or entities as "systemically important" by the Financial Stability Oversight Council ("FSOC"), and nothing in this paper is intended to conflate the two.[148] The Dodd-Frank Act authorized the FSOC "to designate certain nonbank financial companies for Federal Reserve supervision and prudential standards, and to designate systemically important financial market utilities and payment, clearing and settlement activities for additional risk-management requirements."[149]

---

144 *Critical Infrastructure Systems*, Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/resilience-services/infrastructure-dependency-primer/learn/critical-infrastructure-systems (last visited Jan. 24, 2024).

145 *Id*.

146 As recently as 2021, CISA and others resisted efforts from the executive and legislative branches to push it to be a regulatory agency, seeking instead to continue its collaborative — rather than "punitive" — efforts. *See* Rebecca Kern, *Cyber Agency Resists Regulator Role as Bills Aim to Expand Power*, Bloomberg Government (Nov. 10, 2021), https://about.bgov.com/news/cyber-agency-resists-regulator-role-as-bills-aim-to-expand-power/; David Uberti, *U.S. Cyber Agency Hopes to Avoid the 'Regulator' Label*, Wall Street Journal (Oct. 12, 2021), https://www.wsj.com/articles/u-s-cyber-agency-hopes-to-avoid-the-regulator-label-11634031001; Jen Easterly, *Looking Back to Chart Our Path Forward*, Cybersecurity & Infrastructure Security Agency (Jan. 12, 2023), https://www.cisa.gov/news-events/news/looking-back-chart-our-path-forward ("We're not a law enforcement agency, nor an intelligence agency, nor a military organization, nor a regulator in the traditional sense. We're largely a voluntary agency which relies on building trust with our partners across the globe . . .").

147 *About CISA*, *supra* note 143.

148 *See* Authority To Require Supervision and Regulation of Certain Nonbank Financial Companies, 88 Fed. Reg. 26234-44 (proposed Apr. 28, 2023) (to be codified at 12 C.F.R. pt.1310); *see also* Analytic Framework for Financial Stability Risk Identification, Assessment, and Response, 88 Fed. Reg. 78026-37 (proposed Nov. 14, 2023).

149 *Council Work*, U.S. Dep't of the Treas., https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/financial-stability-oversight-council/council-work (last visited Jan. 27, 2024).

Designation as a "systemically important" financial market utility ("FMU")[150] is based upon an assessment of whether "a failure or a disruption to the functioning of an FMU could . . . threaten the stability of the U.S. financial system."[151] That is, these FMUs are directly tied to — indeed entwined to an existential degree with — TradFi institutions in the United States, such that disruptions could fundamentally "threaten the stability of the U.S. financial system" as a whole.[152] As recognized below, global regulators agree that DeFi Systems are not integrated with the traditional financial markets today such that they could be a threat; thus, genuine DeFi does not even approximate the threshold for "systemic importance."

2. *Genuine DeFi as "Critical Infrastructure"*

Genuine DeFi Systems are technological infrastructure underpinning a new approach to conducting financial transactions and given the way in which they function, are most appropriately classified — for purposes of oversight, if any — as "critical infrastructure" under OCCIP's remit. In this way, OCCIP could make meaningful contributions to the safe operation of genuine DeFi Systems. Although OCCIP does not have regulatory authority, it does work — on behalf of the Treasury Department — with industry bodies in the financial services sector (*e.g.*, SIFMA) "to enhance the security and resilience of financial services sector critical infrastructure and reduce operational risk" and "to share information about cybersecurity and physical threats and vulnerabilities, encourage the use of baseline protections and best practices, and respond to and recover from significant incidents."[153] OCCIP's role in the development and rapid dissemination of information and standards on risk and resilience — across critical infrastructure sufficiently connected to the financial system, including some financial institutions — is exactly the type of collaborative work in an area of natural alignment between industry and government that could foster a safer — but more widely accessible — technologically-based financial system.

Whether genuine DeFi Systems rise to the level of being "so vital that their incapacitation or destruction would have a debilitating effect on security, the economy, public health, public safety, or any combination thereof" in the U.S. to be "critical infrastructure" remains subject to debate; on the one hand, numerous financial regulators and policymakers have recognized that DeFi is not yet integrated

---

[150] To date, only eight "systemically important" FMUs have been designated for increased risk-management requirements, which includes major companies such as The Clearing House Payments Company, L.L.C., the Chicago Mercantile Exchange, and The Depository Trust Company. *Designated Financial Market Utilities*, The Board of Gov.'s of the Fed. Res. Sys, https://www.federalreserve.gov/paymentsystems/designated_fmu_about.htm (last visited Jan. 27, 2024).

[151] *Id.*

[152] *Id.*

[153] *Financial Institutions*, U.S. Dep't of the Treas., https://home.treasury.gov/about/offices/domestic-finance/financial-institutions (last visited Jan. 24, 2024).

with — and therefore not a "threat" to — the TradFi system,[154] while on the other hand, U.S. policymakers and regulators have devoted significant resources and attention to DeFi as it relates to U.S. national security matters. Although integration with TradFi is *not* the hallmark of network architecture being classified as "critical" in the financial sector, any legislation, regulation or Presidential Directive classifying genuine DeFi as "critical infrastructure" should also impose thresholds as to when a DeFi protocol may rise to this level. Imposing qualifiers or gradients would have the policy benefits of ensuring certain genuine DeFi Systems remain subject to OCCIP's oversight and protecting innovation by allowing software developers to continue building, testing and launching new DeFi protocols that may (or may not) develop into something "critical" over time.

Specifying genuine Defi Systems as "critical infrastructure" under OCCIP's remit does not make a genuine DeFi System a "financial institution" subject to the BSA. To the contrary, OCCIP does not have regulatory authority under the BSA and is not confined to working only with or regarding "financial institutions," and its remit and cyber security-coordinating function does not implicate either. OCCIP supports the operating integrity of technological and cyber infrastructure that may underpin financial systems as network architecture, without implicating BSA requirements in that security-coordinating function. In this capacity, OCCIP conducts briefings "on existing and emerging cybersecurity threats" tied to financial systems;[155] releases alerts on ransomware typologies relevant to financial network security, coordinating across law enforcement and CISA to distill and disseminate information for taking effective mitigating measures for financial infrastructure;[156] and provides a conduit for ongoing, actionable information exchange in these areas through its seminal role in the Financial Services Information Sharing and Analysis Center ("FS-ISAC"), a private sector not-for-profit

---

[154] *See e.g.*, Sirio Aramonte, Wenqian Huang & Andreas Schrimpf, *DeFi Risks and the Decentralisation Illusion*, BIS Quarterly Review 21, 21 (2021), https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf ("Given this self-contained nature, the potential for DeFi-driven disruptions in the broader financial system and the real economy seems limited for now."); DeFi Risk Assessment, *supra* note 3 at 36 ("This report recognizes, however, that illicit activity is a subset of overall activity within the DeFi space and, at present, the DeFi space remains a minor portion of the overall virtual asset ecosystem. Moreover, money laundering, proliferation financing, and terrorist financing most commonly occur using fiat currency or other traditional assets as opposed to virtual assets"); Fin. Stability Bd., *supra* note 71 at 1 and 4 ("To date DeFi is mainly self-referential, meaning its products and services interact with other DeFi products and services rather than with the traditional financial system and the real economy" and "Crypto-asset markets are fast evolving and could reach a point where they represent a threat to global financial stability due to their scale, structural vulnerabilities and increasing interconnectedness with the traditional financial system"); *IMF-FSB Synthesis Paper*, *supra* note 4 at 9 ("Crypto-asset markets and the ecosystem are changing rapidly, and could, if they were to grow and become more interconnected with the traditional financial system, reach a point where they represent a threat to global financial stability.").

[155] 2023 Report on Cybersecurity and Resilience, Fed. Deposit Ins. Corp., 16 (2023), https://www.fdic.gov/regulations/resources/cybersecurity/2023-cybersecurity-financial-system-resilience-report.pdf.

[156] *OCCIP Issues Update on Ransomware Incident Targeting Financial Institutions*, America's Credit Unions (Nov. 15, 2023), https://news.cuna.org/articles/123316-occip-issues-update-on-ransomware-incident-targeting-financial-institution.

cybersecurity intelligence sharing organization that is governed by its roughly 4,600 members focused on the financial system.[157]

Treating genuine DeFi Systems as "critical infrastructure" would dovetail with the ways in which both industry and regulators have proposed creating regulatory guardrails for neutral software — namely, implementation of cybersecurity standards,[158] information sharing and analysis centers ("ISACs"), automation on risk indicators,[159] and similar risk mitigation tools. Much of this has been or is currently being built in the DeFi sector — notably, industry efforts for cyber-security frameworks[160] and an ISAC[161] — but the types of industry and regulatory coordination facilitated by OCCIP will further the robustness of this work.

C. Financial Integrity Risk Management Via "Critical Communication Transmitters"

OCCIP oversight is not the sole answer to combating illicit financial activity within genuine DeFi Systems. As with work to combat illicit finance in TradFi, this will require a multi-tiered approach consistent with the ways in which technology is used and continues to develop. As of today, people have developed business models around some of the integral technological communication functions in genuine DeFi Systems, which present an opportunity for additional illicit finance risk management. We propose that this be accomplished through a new type of regulated entity: "critical communications transmitters."

1. *CCTs As a Touchpoint for Tailored Financial Integrity Risk Management*

In the DeFi Transaction Flow, certain service providers operating as a business (*e.g.*, receiving compensation or charging fees for the service) have integrated technological services with genuine DeFi Systems and have become materially important for the transmission of user-initiated communications from a user to the software that allows the transaction to be finalized, most notably node-as-a-service for RPCs. Although these same communications transmitters can be hosted individually — anyone can own and operate a node to provide communications from their own wallet to the "bottom half" of the

---

157 *Information Sharing and Collaboration Issue Summary*, Bank Policy Institute (Aug. 18, 2021) https://bpi.com/information-sharing-collaboration-issue-summary/; *Multi-State Information Sharing and Analysis Center*, Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/resources-tools/services/multi-state-information-sharing-and-analysis-center (last visited Jan. 24, 2024); Crypto-ISAC, https://www.cryptoisac.org/ (last visited Jan. 24, 2024).

158 *See e.g.*, Key Elements, *supra* note 62 at 37-39; ACPR DeFi Consultation, *supra* note 71 at 2.

159 *Automated Indicator Sharing: Other Ways to Connect*, Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/news-events/news/automated-indicator-sharing-other-ways-connect (last visited Jan. 24, 2024).

160 *See e.g.*, *Can You Pass the Rekt Test?*, Trail of Bits Blog (Aug. 14, 2023), https://blog.trailofbits.com/2023/08/14/can-you-pass-the-rekt-test/; *see also* Sebastian Sinclair, *DeFi Gets a 'SEAL' Team as White Hat Hackers, Auditors Join Forces*, Blockworks (Aug. 8, 2023), https://blockworks.co/news/defi-seal-911-white-hat-hackers-auditors.

161 *See* CryptoISAC, https://www.cryptoisac.org/.

DeFi Transaction Flow (*e.g.*, block builders, validators and other parts of a blockchain network), today, certain of these communications flow primarily through service providers running businesses. This paper proposes defining these persons[162] as CCTs and requiring them to implement risk management practices and procedures reasonably designed to help mitigate illicit finance activity in ways tailored to their operations.

A Critical Communications Transmitter is a person providing a service —

a. necessary to the flow of communicating users' information about a financial transaction from a System to be settled on a blockchain network,
b. that transmits a material portion of such communications *and*
c. is offered for the person's profit or being run by the person as a business.

This definition is not intended to — and should not — capture persons who solely develop open source, downloadable software (*e.g.*, creators of self-hosted wallets).

Any risk management program for CCTs likely will be over-inclusive: blockchain-based technology is agnostic to the content of transactions — meaning that CCTs cannot determine whether the transaction processed relates to a consumer loyalty gaming program or for a DeFi System — and to the location of transactions — because all transactions are pseudonymous and do not collect or contain any personally identifying information ("PII") for users — which means that any CCT will be conducting illicit finance risk management for non-economic blockchain transactions and economic transactions alike.

CCTs are appropriate touchpoints for illicit finance risk controls because CCTs' positioning in the DeFi Transaction Flow — *i.e.*, as gatekeepers to moving communications about a transaction "down the flow" to a blockchain network — would allow them, with reasonable illicit finance risk mitigation controls in place, to detect, document and deter illicit actors from finalizing transactions on a blockchain network. A narrowly tailored CCT financial integrity program should include enhanced documentation and detection requirements that ultimately are aimed to reduce the amount of illicit activity completed through DeFi Systems.

An example underscores this point. Currently, many businesses that would be classified as CCTs today already implement geo-location blocking for sanctioned countries as well as wallet monitoring to screen and block sanctioned wallet addresses.[163] This only captures a narrow subset of illicit actors. A CCT

[162] *See* 31 CFR § 1010.100(mm).

[163] *See e.g.*, *Can I use MetaMask in My Country?* MetaMask Support, https://support.metamask.io/hc/en-us/articles/4783916052251-Can-I-use-MetaMask-in-my-country (last visited Jan. 25, 2024) ("Infura and all other US-based blockchain service providers are required

financial integrity program like the one contemplated herein could include a requirement that CCTs implement, among other things, wallet risk scoring and blocking, along with auto-report generation. Blockchain analytics companies have developed "wallet risk scoring" via a software risk engine that assigns each individual cryptocurrency wallet a "risk score" based on a variety of factors such as direct and indirect transactional proximity to illicit transactions or sanctioned wallet addresses; prior engagement in or proximity to suspicious financial activity on blockchain networks, including exploits; source of funds in the wallet; engagement with known child sexual abuse matters and the like. The CCT financial integrity program would then require a CCT to integrate a "wallet risk scoring" application programing interface ("API") that would screen for wallets with a risk score above a certain number — as determined by the CCT's risk landscape and tolerance — and potentially via factors set forth in legislation or regulation — and then block all such transactions involving "high score" wallet..

Given the extraordinary amount of transactions that flow through CCTs today, CCTs' blocking of these transactions would be extremely effective in preventing high risk wallets and their owners from communicating and, thus, completing transactions involving illicit funds, sanctioned actors or the proceeds of any illicit activity. CCTs could further implement technology — some of which has already been developed today — that automatically generates reports (akin to SARs) that identify the high risk wallet and, if known to the CCT, the details of the proposed transaction and then immediately sends the reports to FinCEN. Based upon the way in which CCTs operate today, any reports would contain certain limited information — date, time, transaction hash and wallet address. It would not, could not and *should* not provide the information typically found in SARs. As those involved in the provision of communications or network services, CCTs do not engage in — nor should they have to engage in — the collection of PII. Accordingly, any documentation requirements should not go above and beyond a set of reasonable, useful information relating to the actual communication of the transaction — wallet address, transaction hash and receiving address. The wallet risk scoring/blocking/auto-report program is one of a number of potential ways that illicit finance can be combatted through CCTs; continued sanctions screening is critical and already being implemented, as are other programs that will account for the practical realities of the way in which the industry operates.

With the high volume of DeFi transactions communicated to blockchain networks through CCTs, such a program — coupled with other risk mitigation tools — would detect high risk activity, document such activity through the reports and deter, and potentially prevent, it through the blocking function. Given the amount of publicly accessible and immutable data from blockchains — rather than the siloed data in traditional finance — the reporting can be meaningfully limited while still substantially helpful to law

to implement US sanctions. Infura closely monitors changes to US sanctions programs announced by the Office of Foreign Assets Control and narrowly tailors its internal controls to comply with the law. Currently, those regions are Iran, North Korea, Cuba, Syria, and the Crimea, Donetsk, and Luhansk regions of Ukraine.").

enforcement. Further, even if law enforcement is already tracking and tracing much of this information on transparent blockchain networks today, the auto-generation of reports relating to this activity and the fact that the majority of blockchain activity flows through CCTs today will enhance law enforcement's ability to detect, track and trace bad actors in a much more immediate and robust way. Instead of having to engage in monitoring the entirety of ecosystem activity, they will have near-real time reports helping focus resources on potential illicit activity or activity by illicit actors.

This new type of financial integrity program would achieve the traditional AML/CFT goals contemplated by FSB for "peer-to-peer" systems like DeFi, without imposing intermediary-based BSA obligations on entities that are not financial institutions. Indeed, CCTs should *not* be categorized as financial institutions under the BSA because they do not perform the same or even similar functions to BSA-defined "financial institutions." CCTs — as contemplated by the DeFi Transaction Flow and the definition set forth above — never have "independent control" over a user's cryptocurrency, never accept value and never transmit value, funds or cryptocurrency. CCTs provide tools and communication systems; they are not engaged in financial activity themselves but they are a necessary gateway to communicating information about users' transactions on a blockchain network.[164]

2. *FinCEN Likely Needs New Authority for CCT Regulation*

Existing regulations do not provide authority to the Treasury Department to create risk-based programs for non-financial institutions; they do contain the foundations, upon which new legislation and additional regulation (after rulemaking with notice and comment) may be built.

The AMLA mandates that FinCEN review various guidance to ensure the Treasury Department implements "appropriate safeguards" to protect U.S. national and economic security.[165] In addition, the BSA provides authority to the Secretary of the Treasury, which has been delegated to FinCEN, to require "any other participant" in a "transfer of United States coins or currency (or other monetary instruments the Secretary of the Treasury prescribes), in an amount, denomination, or amount and denomination, or under circumstances the Secretary prescribes by regulation" that involves a domestic financial institution to "file a report on the transaction at the time and in the way the Secretary prescribe."[166] The "monetary instruments" definition has already been updated by the AMLA to include "value that substitutes for any [such] monetary instrument," akin to the "value that substitutes for currency" framing used for certain types of cryptocurrency.[167] Although this is merely a reporting

[164] *See, e.g.*, 2019 FinCEN Guidance, *supra* note 35 at 20.

[165] 31 U.S.C. § 6216(a). Section 6216 of the AMLA mandates that FinCEN review various guidance to ensure the Treasury Department implements "appropriate safeguards" to protect U.S. national and economic security.

[166] 31 U.S.C. § 5313.

[167] Pub. L. 116-283 § 6102(d)(1)(C).

requirement, FinCEN's authority to implement "appropriate safeguards" may allow for Notice & Comment rulemaking and legal feedback to add certain levels of detection of risk in addition to the reporting of them.

The BSA's "domestic financial institution" limitation likely makes the statute an unlikely authority for FinCEN's regulation of CCTs under existing law — and we are unaware of other legislation that confers power on the Treasury Department to apply BSA-mandated AML/CFT programs on non-financial intermediaries. That existing laws do contemplate the need for risk-based programs for "other participants" in financial networks could be a starting place for a rulemaking that further develops this concept, without imposing overly broad and overly burdensome requirements or stifling innovation, but ultimately we believe that new, novel legislation may be required to create financial integrity programs narrowly tailored to this new, novel system.

After implementation of legislation conferring authority to FinCEN to regulate CCTs, and to more specifically address risk management expectations for CCTs through tailored and appropriate regulations as described in this paper, FinCEN, OCCIP and CISA could further explore their authorities to determine the viability, via public notice and comment rulemaking, of proposing expectations for persons critical to protecting U.S. economic and national security — particularly as it relates to critical financial infrastructure overseen by OCCIP. FinCEN, working with OCCIP, could develop standards for CCTs to create and maintain narrowly-tailored financial integrity risk management programs, at least with respect to supporting certain reporting requirements around risks under the existing authority, to start. As with any requirements for risk mitigation programs, regulation, after public notice and comment rulemaking, should set substantial thresholds for what constitutes a "material portion" of transactions or communications since the proposal seeks to address "critical" functions. Not every "communications provider" will be "critical" and, thus, may not need to assume the same risk-based programs contemplated herein, just as highways may have periodic weigh-stations for certain major tractor-trailers but do not checkpoint every city intersection to check vehicle weight and identification, even if doing so might prevent additional harm.

Any risk-based program must also recognize that technological infrastructure is inherently global and cross-functional — it is agnostic to the origin, destination, content or purpose of any transaction; it is not designed to be — nor is it — delivered in a jurisdiction-specific or sector-specific (*e.g.*, only financial) manner. Indeed, certain service providers in DeFi Systems also transmit communications relating to inherently non-financial blockchain-based protocols (*e.g.*, "web3 social" posts). Therefore, any regulation of CCTs should follow the well-worn "crawl, walk, run" approach, which prioritizes a principled and highly coordinated, global, consensus-driven foundation that will minimize divergences and asymmetries across jurisdictions and allow for continued innovation to keep open the opportunities

presented by various technologies. Given a natural alignment between the public and private sectors around wanting a safe operating environment for users in DeFi to prevent exploits of users by malign state actors like Lazarus, finding some core, non-controversial principles in common and collaboratively determining best practices to support them, via a meaningful Notice & Comment process, should be achievable.

* * *

This conceptual framework endeavors to acknowledge many realities to balance governmental and industry interests: it acknowledges the current limits of the Treasury Department's authorities as well as the potential opportunities under FinCEN's and OCCIP's remit to create guardrails for DeFi. FinCEN working with OCCIP — and CISA, as appropriate — would combine the best of the federal government's technical expertise and proprietary, including sensitive and uniquely insightful, information around financial integrity, critical infrastructure and cyber risk management, reflecting and supporting the resilience of the current evolution of communications systems that have important financial implications.

The proposed framework acknowledges the stark differences between on-chain CeFi and genuine DeFi Systems and the ways in which laws and regulation can apply; it acknowledges the businesses that have been built to increase efficiencies within DeFi Systems and contemplates how they may work to combat illicit financial activity. Ultimately it balances the government's near-term search for a solution to the question of illicit finance risks in DeFi with the industry's desire to develop new, useful technology and to protect users.

IV. Conclusion

The framework proposed in this paper seeks to address the FSB's and the Treasury Department's concerns that the type of illicit finance programs implemented by financial institutions simply cannot — and will not — "fit" wholesale on top of the peer-to-peer DeFi Systems that have developed in the blockchain space. The proposal herein overlays the realities of the technology on the policy goals underlying the financial integrity regime in the United States in an attempt to *begin* to answer questions posed by regulators and policymakers. Given the novelty of such proposal in an emerging space — where technology develops rapidly — we believe discussion, debate and further development through collaboration between government and industry is necessary and welcome input from technical experts across the industry as well as the government who may recognize collateral impacts or technical (rather than regulatory) solutions that may complement this proposal.

Blockchain and related technology hold promise to create new systems that open opportunities across sectors, economic lines and for individuals that previously were unable to participate in the financial system. For that reason, proposals to combat illicit activity in these new systems must balance the important task of ensuring that the technology cannot be co-opted by bad actors while still allowing innovation and accessible opportunity to flourish. In the urgency to stop illicit activity, we must not forget the important and fundamental goal to empower good activity that anchors the Treasury Department's explicit mandate as "the executive agency responsible for promoting economic prosperity and ensuring the financial security of the United States."[168]

[168] *Role of the Treasury*, U.S. Dep't of the Treas., https://home.treasury.gov/about/general-information/role-of-the-treasury (last visited Jan. 21, 2024).

Appendix A — DeFi Transaction Flow