

Regulating Cryptocurrency Non-Custodial Service Providers Through the Bank Secrecy Act

Kai Wang*

Bad actors launder dirty money through cryptocurrency non-custodial service providers, including cryptocurrency unhosted wallets, non-custodial mixers, and decentralized exchanges (DEXs). Unlike banks and other traditional financial intermediaries, these providers do not take custody of payment assets. Therefore, the Bank Secrecy Act (BSA) cannot require them to comply with its substantive obligations, such as monitoring and reporting of suspicious payment activities associated with money laundering. As a result, law enforcement agencies are unable to obtain useful reports and records to effectively investigate money laundering and prosecute bad actors.

To address this issue, this Article analyzes how cryptocurrency non-custodial service providers, despite not taking custody of payment assets, can retain a certain degree of controlling power over payment assets in three key dimensions: (1) clearing and settlement, (2) asset ownership, custody, and balance sheet recording, and (3) governance. This Article argues that the BSA should cover some of the cryptocurrency non-custodial service providers that can retain a certain degree of controlling power over payment assets. This Article argues that the BSA's definition of "money transmitting business," which merely considers the second dimension, is unable to accurately measure the collective degree of control a cryptocurrency service provider has over payment assets, namely cryptocurrencies. As such, this Article argues that the BSA should measure the collective degree of controlling power a service provider has over payment assets through all three dimensions. These three dimensions serve as variables within this framework: the more variables present, the greater the degree of collective control a provider has over cryptocurrency payments, and the more likely it is to fall within the scope of the regulatory perimeter of the BSA.

INTRODUCTION	343
I. THE FUNCTIONAL MECHANISM OF CRYPTOCURRENCY NON-CUSTODIAL SERVICE PROVIDERS FACILITATING CRYPTOCURRENCY PAYMENTS..	350
A. Cryptocurrency Payments in Distributed Ledger Technology (DLT): Collective Clearing and On-Chain Self-Settlement.	352

* Assistant Professor, Gonzaga University School of Law. J.S.D., Cornell Law School. I would like to thank Dan Awrey for his extremely helpful comments and suggestions. All errors remain my own.

B.	The Functional Mechanisms of Cryptocurrency Non-Custodial Service Providers	355
1.	Players for Accepting, Transmitting, and Storing Cryptocurrencies: Unhosted Wallets.....	355
2.	Players for Exchanging Different Categories of Cryptocurrencies: Decentralized Exchange	358
a.	Clearing and Settlement	360
b.	Asset Control.....	361
3.	Players for Obfuscating Cryptocurrency Payment Records: Non-Custodial Mixers	362
C.	How bad Actors Launder Dirty Money Through Cryptocurrency Non-Custodial Service Providers.....	363
II.	THE CURRENT ANTI-MONEY LAUNDERING LAW DOES NOT REGULATE CRYPTOCURRENCY NON-CUSTODIAL SERVICE PROVIDERS.....	365
A.	Background.....	366
B.	Money Transmission	367
1.	Instrument: Funds	369
2.	Instrument: Value that Substitutes for Currency.....	371
3.	Activity: Transmission	373
a.	Money Transmission.....	373
b.	Exemption	375
C.	Cryptocurrency Non-Custodial Service Providers do not fall Within the Scope of the Regulatory Perimeter of the BSA.	375
III.	NOT REGULATING CRYPTOCURRENCY NON-CUSTODIAL SERVICE PROVIDERS IS INCONSISTENT WITH THE BSA'S CONTROL-BASED PRINCIPLE AS THEIR CONTROLLING POWER OVER PAYMENT ASSET EXISTS ON A SPECTRUM RATHER THAN IN A BINARY	376
A.	Cryptocurrency Non-Custodial Service Providers' Three Dimensions of Controlling Power over Payment Assets	379
1.	The First Dimension: Clearing and Settlement	379
2.	The Second Dimension: Ownership, Control, and Balance Sheet	380
3.	The Third Dimension: Governance	380
a.	Introduction to Decentralized Autonomous Organizations (DAOs).....	381
b.	Cryptocurrency Non-Custodial Service Providers' Governance Through DAOs	383
B.	The BSA's Current Design is Unable to Adequately Measure the Degree of Control a Cryptocurrency Non-Custodial Service Provider has over Payment Assets.....	385
IV.	TOWARDS A NEW FRAMEWORK FOR REGULATING CRYPTOCURRENCY NON-CUSTODIAL SERVICE PROVIDERS	389
A.	Existing Regulatory Prescriptions Seeking to Expand the Scope of the Regulatory Perimeter of the BSA.....	390
1.	Direct Expansion: Adding Unhosted Wallets, Miners, and Validators into the list of Financial Institutions to Avoid	

the Discussion of Whether they Qualify as Money Transmitting Businesses	390
2. Direct Expansion: Arguing that Cryptocurrency Non-Custodial Service Providers Qualify as Money Transmitting Businesses	392
3. Indirect Expansion: FinCEN's two Attempts of Requiring some or all Players Already Within the Scope of the Regulatory Perimeter of the BSA to React on Transactions Between them and Unhosted Wallets and/or Mixers	395
B. Policy Prescription: Expanding the Scope of the Regulatory Perimeter of the BSA based on a Player's Degree of Controlling Power over Payment Assets.....	398
C. Potential Challenges and Objections	400
1. Potential Challenges	400
2. Potential Objections	402
CONCLUSION	403

INTRODUCTION

The modern payment systems¹ involve a sophisticated network of players facilitating cryptocurrency payments, including cryptocurrency custodial and non-custodial service providers.² However, in the eyes of the U.S. Department of the Treasury, cryptocurrencies have become a burgeoning method of payment for illegal goods and services.³ The annual volume of illicit payment flows in the conventional payment system is two to five percent of the global GDP, or \$800 billion to \$2 trillion.⁴ On the other hand, the annual total value of crypto payment flows in 2023 and 2022 has been \$76.70 billion and \$82.13 trillion, respectively.⁵ Figures show that illicit cryptocurrency addresses received approximately \$24.2 billion, \$39.6 billion, and \$23.2 billion of

¹ See FED. RES., FEDERAL RESERVE POLICY ON PAYMENT SYSTEM RISK 7 n.10 (2023), https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf.

² See OFFICE OF THE COMPTROLLER OF THE CURRENCY, COMPTROLLER'S HANDBOOK: PAYMENT SYSTEMS 2 (2021), <https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/payment-sys-funds-transfer-activities/pub-ch-payment-systems.pdf>.

³ See U.S. DEP'T OF THE TREASURY, NATIONAL MONEY LAUNDERING RISK ASSESSMENT 40–41 (2022) (citation omitted), <https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf>.

⁴ See *Money Laundering*, UNITED NATIONS OFF. ON DRUGS AND CRIME, <https://perma.cc/P6PK-T25Y>.

⁵ See *Crypto Trading Volume Tracker*, COINCODEX, <https://perma.cc/67E3-5KX5> (last visited July 1, 2024).

cryptocurrencies in 2023, 2022, and 2021, respectively.⁶ These funds may originate from criminal activities such as drug trafficking, bribery, fraud, and terrorism.⁷ While representing a relatively small portion of the global payment flows, including illicit flows, and the calculation method is still ambiguous, these figures do confirm the emergence of a new category of *dirty money*.⁸

Through a series of intricate money laundering techniques, money launderers deftly and clandestinely exploit this sophisticated cryptocurrency payment network to cast a veil of secrecy around the source and flows of money.⁹ To launder dirty money, bad actors could use the services of both cryptocurrency custodial and non-custodial service providers in the cryptocurrency payment network. Cryptocurrency custodial service providers take custody of customers' cryptocurrencies when facilitating payments on their behalf, whereas cryptocurrency non-custodial service providers do not. Both cryptocurrency custodial and non-custodial service providers fall into three major categories. First, hosted wallets (custodial) or unhosted wallets (non-custodial) serve as the starting point and/or destination for cryptocurrency payments.¹⁰ Second, centralized exchanges (CEXs) (custodial) or decentralized exchanges (DEXs) (custodial) enable customers to exchange one category of cryptocurrency for another.¹¹ Third, custodial or non-custodial mixers obscure cryptocurrency payment records that would otherwise be publicly accessible on blockchains. By exchanging various categories of cryptocurrencies through exchanges, making numerous small payments between different wallets, and obscuring payment records through mixers,

⁶ See Chainalysis Team, *2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Ransomware and Darknet Markets See Growth* (Jan. 18, 2024), <https://perma.cc/6X23-PV47> (last visited August 11, 2024).

⁷ See STEVEN MARK LEVY, *FEDERAL MONEY LAUNDERING REGULATION: BANKING, CORPORATE, AND SECURITIES COMPLIANCE* § 1.05 (2d Ed. Supp. I 2021).

⁸ See *History of Anti-Money Laundering Laws*, FINCEN, <https://perma.cc/FVW9-K9EK> (last visited Jan. 3, 2023); see also UNITED NATIONS OFF. ON DRUGS AND CRIME, *supra* note 4.

⁹ Money laundering typically involves three stages: placement, layering, and integration. See Sean Jettner, *Money Laundering*, 60 AM. CRIM. L. REV. 1071, 1071–72 (2023); see also generally U.S. DEP'T OF JUST., *THE REPORT OF THE ATTORNEY GENERAL PURSUANT TO SECTION 5(B)(III) OF EXECUTIVE ORDER 14067: THE ROLE OF LAW ENFORCEMENT IN DETECTING, INVESTIGATING, AND PROSECUTING CRIMINAL ACTIVITY RELATED TO DIGITAL ASSETS 4* (2022), <https://perma.cc/U54L-9MWE>.

¹⁰ See 85 Fed. Reg. 83840, 83841 n.4.

¹¹ See FinCEN, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, FIN-2021-A004, at 3 (Nov. 2021) (showing DEXs' role in the movement of cryptocurrency), https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf.

bad actors make it challenging for law enforcement to investigate the flow of dirty money and prosecute bad actors.

The Bank Secrecy Act (BSA) is the anti-money laundering law in the United States since 1970.¹² Through a bifurcated structure, the BSA¹³ only requires (1) a category of financial intermediary called money transmitting businesses,¹⁴ as well as (2) a list of financial institutions, such as banks,¹⁵ to register and comply with a series of carefully designed substantive obligations.¹⁶ These substantive obligations require money transmitting businesses and the listed financial institutions to collect customer identification information, monitor suspicious activities associated with money laundering, and generate reports and records that would be highly useful for law enforcement agencies to investigate the flow of dirty money and prosecute bad actors in financial crimes.¹⁷ Through these reports and records, law enforcement agencies, especially Financial Crimes Enforcement Network (FinCEN) under the U.S. Department of the Treasury,¹⁸ are able to investigate the flow of dirty money and prosecute bad actors.

Nevertheless, the BSA does not require cryptocurrency non-custodial service providers to comply with its substantive obligations due to the following two reasons. First, cryptocurrency non-custodial service providers are not within the BSA's list of financial institutions.¹⁹ Second, cryptocurrency non-custodial service providers do not qualify as money transmitting businesses. Here, to qualify as a money transmitting business, a business must first take custody of payment assets by accepting them and then

¹² See *infra* note 13; see also *BSA Timeline*, FinCEN, <https://perma.cc/4G7N-JFHU> (last visited Dec. 10, 2023).

¹³ See 86 Fed. Reg. 71201, 71202 (Dec. 15, 2021).

¹⁴ See *infra* note 144, § 5330(d)(1)(A) (2018); see also *infra* note 124, § 1010.100(ff)(5)(i)(A).

¹⁵ See *infra* note 144, § 5330(d)(1)(A) (2018); see also the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 6003, 134 Stat. 3388 (2021).

¹⁶ See, e.g., *infra* note 144, § 5313(a) (2018); see also *infra* note 124, §§ 1022.200, 1010.310, 1010.320.

¹⁷ See Currency and Foreign Transactions Reporting Act of 1970, Pub. L. No. 91-508, §§ 101, 102, 84 Stat. 1114, 1118 (1970); see also Jeremy Ciarabellini, *Cryptocurrencies' Revolt against the BSA: Why the Supreme Court Should Hold That the Bank Secrecy Act Violates the Fourth Amendment*, 10 SEATTLE J. TECH. ENVTL. & INNOVATION L. 135, 139–41 (2020).

¹⁸ See *What We Do*, FinCEN, <https://perma.cc/5DLT-ZL9N> (last visited Nov. 10, 2023). It should be noted that state laws and regulations also play important roles in anti-money laundering, yet they are not within the scope of this Article's research question.

¹⁹ See *infra* note 144, § 5330(d)(1)(A) (2018); see also § 6003, 134 Stat. 3388.

transmit them to another location or person.²⁰ As cryptocurrency non-custodial service providers do not take custody of payment assets,²¹ they do not qualify as money transmitting businesses.

The fact that the BSA does not regulate cryptocurrency non-custodial service providers is alarming. Due to the BSA's lack of coverage, the BSA does not require cryptocurrency non-custodial service providers to collect their customers' identification information. Nor does the BSA require them to monitor suspicious activities associated with money laundering. Additionally, the BSA does not require them to file reports and records with FinCEN, which, if filed, would have been highly useful for law enforcement agencies to investigate the flow of dirty money and prosecute bad actors. Therefore, through unhosted wallets, DEXs, and non-custodial mixers, bad actors can anonymously or pseudonymously launder dirty money without concern for regulatory detection and scrutiny. The consequence of excluding all cryptocurrency non-custodial service providers from the scope of the regulatory perimeter of the BSA is inconsistent with the BSA's legislative goals of eliminating dirty money and capturing bad actors.

There has been a series of legislative, judicial, and administrative actions seeking to directly and indirectly expand the scope of the regulatory perimeter of the BSA. While none of them have become effective law as of April 2025, it is useful to categorize their main approaches into three categories. First is the addition of cryptocurrency non-custodial service providers to the list of financial institutions. On July 27, 2023, Senators Elizabeth Warren, Roger Marshall, Lindsey Graham, and Joe Manchin, who was serving as a U.S. Senator at the time, introduced a bill that sought to add unhosted wallet service providers to the BSA's list of financial institutions.²² Second is requiring some or all players already within the scope of the regulatory perimeter of the BSA to react on payments from and/or to unhosted wallets and/or mixers. On December 23, 2020, FinCEN announced a Notice of Proposed Rulemaking (NPRM), seeking to require banks and money

²⁰ See *infra* note 124, §§ 1010.100(ff)(5)(i)(A), 1010.210, 1022.210(a); see also *infra* note 144, §§ 5318(a)(2), 5318(h) (2018).

²¹ See *infra* note 144, § 5330(d)(1)(A) (2018); see also *infra* note 124, § 1010.100(ff)(5)(i)(A).

²² See Digital Asset Anti-Money Laundering Act of 2023, S. 2669, 118th Cong. § 1 (2023). The bill's initial version, introduced on December 15, 2022, titled Digital Asset Anti-Money Laundering Act of 2022, did not seek to expand the scope of the regulatory perimeter of the BSA. See Digital Asset Anti-Money Laundering Act of 2022, S. 5267, 118th Cong. § 1 (2022), <https://perma.cc/9JMF-E44M>. Joe Manchin served as a U.S. Senator until January 2025.

transmitting businesses to verify the identification information of unhosted wallets holders, as well as to report and keep records of cryptocurrency transactions between them and unhosted wallets. According to the Federal Register published on August 16, 2024, FinCEN officially withdrew this NPRM on April 12, 2024. On October 14, 2023, FinCEN announced another NPRM, seeking to require financial institutions currently covered by the BSA to keep record of, and report to FinCEN, key information of transactions involving custodial and non-custodial mixers. Third is re-interpreting the definition of “money transmitting business” so that it covers cryptocurrency non-custodial service providers. On August 23, 2023, and April 24, 2024, the Department of Justice (DOJ) prosecuted the founders of Tornado Cash and Samourai Wallet, respectively, for charges including operating an unlicensed money transmitting business.²³ The DOJ’s language in its indictment shows that Samourai Wallet was a non-custodial service provider. An analysis of Tornado Cash’s source code confirmed that it was also a non-custodial service provider. Therefore, if a court determines that either Tornado Cash or Samourai Wallet qualifies as a money transmitting business, then such a decision would establish new case law confirming that cryptocurrency non-custodial service providers could qualify as money transmitting businesses. On May 9, 2024, in response to the DOJ’s indictment against the founders of Samourai Wallet, Senators Cynthia M. Lummis and Ron Wyden sent a letter to the United States Attorney General, arguing that such an expansion would be inconsistent with the BSA and the guidance established by FinCEN in 2019.²⁴

This is not to suggest that these approaches are perfect. Nevertheless, they collectively provide valuable insight allowing the BSA to function effectively not only as anti-*money* laundering law but also as anti-*cryptocurrency* laundering law in the United States. To address the issues arising from the BSA’s non-coverage of cryptocurrency non-custodial service providers, this Article argues that the BSA should cover some of the cryptocurrency non-custodial service providers that can retain a certain degree of controlling power over payment assets. This Article analyzes how

²³ See Indictment, *United States v. Keonne Rodriguez & William Lonergan Hill*, No. S2 24 Cr. 82 (S.D.N.Y. Apr. 24, 2024), <https://perma.cc/DP9X-3VHR>, at 1–3, 17–18; see also Indictment, *United States v. Roman Storm & Roman Semenov*, No. 23 Cr. 23 Crim 430 (S.D.N.Y. Aug. 23, 2023), <https://perma.cc/54UG-7F47>, at 15–20.

²⁴ See United States Senator Cynthia M. Lummis & United States Senator Ron Wyden, *Re: Money Transmitting Business Registration and Non-Custodial Crypto Asset Software*, UNITED STATES SENATE (May 9, 2024), <https://perma.cc/H2ES-2J69>.

cryptocurrency non-custodial service providers, despite not taking custody of payment assets, can retain a certain degree of controlling power over payment assets in three key dimensions: (1) payment clearing and settlement, (2) asset ownership, custody, and balance sheet recording, and (3) governance. Then, this Article argues that the BSA's definition of "money transmitting business," which merely considers the second dimension, is unable to accurately measure the collective degree of control a cryptocurrency service provider has over payment assets, namely cryptocurrencies. As such, this Article argues that the BSA should measure the collective degree of controlling power a service provider has over payment assets through all three dimensions. These three dimensions serve as variables within this framework: the more variables present, the greater the degree of collective control a provider has over cryptocurrency payments, and the more likely it is to fall within the scope of the regulatory perimeter of the BSA.

The Article proceeds as follows. Part I shows how cryptocurrency non-custodial service providers facilitate cryptocurrency payments. To do so, it describes what cryptocurrency non-custodial service providers are and how they interact with one another and the conventional payment system. These players include unhosted wallets, decentralized exchanges (DEXs), and mixers.

Part II explains why the current anti-money laundering law, namely the BSA, does not regulate cryptocurrency non-custodial service providers. To do so, it describes the scope of the regulatory perimeter of the BSA's registration requirements. Such a description shows that the BSA covers businesses that qualify as "money transmitting businesses," which refer to businesses that accept *and* transmit "currency, funds, or other value that substitutes for currency."²⁵ Part II finds that because cryptocurrency non-custodial service providers do not accept and transmit cryptocurrencies, they do not qualify as money transmitting businesses and, therefore, do not have to comply with the BSA.

Part III argues that the BSA's exclusion of cryptocurrency non-custodial service providers is not consistent with the BSA's control-based principle, as their controlling power over payment assets exists on a spectrum rather than in a binary. To do so, Part III first analyzes the BSA's control-based principle through FinCEN's Guidance in 2019, which serves as the basis for determining whether a business truly qualifies as a money transmitting

²⁵ *Infra* note 124, § 1010.100(ff)(5)(i)(A) (2023).

business. Part III then explains that cryptocurrency non-custodial service providers could maintain a certain degree of controlling power over payment assets in one or more of the three dimensions. First, the mechanism of payment clearing and settlement. Second, the mechanism of custody and ownership of payment assets, and the recording of payment assets into its balance sheet. Third, the governance mechanism. Accordingly, the controlling power each cryptocurrency non-custodial service provider has over payment assets differs depending on its business model, and such a controlling power would exist on a spectrum rather than in a binary. Part III concludes that because the BSA's current definition of money transmitting business merely focuses on the second dimension, namely asset custody, it is unable to adequately measure the degree of control a cryptocurrency non-custodial service provider has over payment assets.

Part IV offers a framework allowing the BSA to regulate some of the cryptocurrency non-custodial service providers that maintain a certain degree of controlling power over payment assets. To do so, Part IV first analyzes the existing legislative, judicial, and administrative actions seeking to directly and indirectly expand the scope of the regulatory perimeter of the BSA to cover cryptocurrency non-custodial service providers. Part IV explains the design and benefit of each approach, the potential issues that each of them needs to address, and the possible approach of addressing these potential issues. While analyzing the judicial actions, namely the indictments against the founders of Tornado Cash and Samurai Wallet, Part IV argues that the adequate manner of interpreting the concept of money transmitting businesses must follow the BSA's control-based principle. Therefore, the BSA should re-interpret the definition of money transmitting businesses, allowing the BSA to determine the businesses it may regulate based on the degree of control a business has over payment assets. Accordingly, Part IV proposes a framework, arguing that the BSA should measure the collective degree of controlling power a service provider has over payment assets through all the aforementioned three dimensions. These three dimensions serve as variables within this framework: the more variables present, the greater the degree of collective control a provider has over cryptocurrency payments, and the more likely it is to fall within the scope of the regulatory perimeter of the BSA. It also identifies and responds to potential challenges and objections.

I. THE FUNCTIONAL MECHANISM OF CRYPTOCURRENCY NON-CUSTODIAL SERVICE PROVIDERS FACILITATING CRYPTOCURRENCY PAYMENTS

The payment system is a vital part of the financial system of the United States.²⁶ Payment refers to the transmission of monetary value.²⁷ Payments could take place through various methods, including cash, checks, wire transfers, credit cards, and cryptocurrency transmissions from and/or to unhosted wallets.²⁸

Payments facilitated by financial intermediaries, such as banks, typically involve three stages. First, a payment across two financial intermediaries, such as banks, involves clearing and settlement.²⁹ Clearing refers to the transferring and recording of instructions by the payer's and payee's financial institutions by routing messages and other relevant information.³⁰ The purpose of clearing includes verifying the availability of payment assets, potentially netting down multiple orders between two financial intermediaries (which generally reduces the value for settlement),³¹ and establishing final positions for settlement.³² Settlement refers to the process in which financial intermediaries discharge their obligations to pay as a result of the clearing processes.³³ Second, prior to payment clearing and settlement, financial intermediaries can first accept money from their customers, namely payors, thereby gaining controlling powers over

²⁶ See Dan Awrey & Kristin van Zwieten, *The Shadow Payment System*, 43 J. CORP. L. 775, 776 (2018).

²⁷ For a discussion of why cryptocurrencies qualify as value that substitute for currency, see *infra* Part II; see also *infra* note 144, § 5330(d)(1) (2018); *infra* note 146, at 4; Morten Bech, Yuuki Shimizu & Paul Wong, *The Quest for Speed in Payments*, BIS Q. REV. 58 (2017); *supra* note 2 ("A payment is a transfer of value.").

²⁸ See *supra* note 2.

²⁹ See generally Bruce J. Summers, 3 *Clearing and Payment Systems: The Central Bank's Role* in PATRICK DOWNES & REZA VAEZ-ZADEH (EDS.), THE EVOLVING ROLE OF CENTRAL BANKS 30–45 (1991); see also *id.*

³⁰ See *Unpacking clearing and settlement*, FED. RES. BANK SERVICES, <https://perma.cc/Z837-7SCY> (last visited June 29, 2024).

³¹ See *id.*; see also VIRGINIA B. MORRIS, GUIDE TO CLEARANCE & SETTLEMENT: AN INTRODUCTION TO DTCC 9 (2021).

³² See *Glossary of Terms Related to Payment, Clearing and Settlement Systems*, EUR. CENT. BANK (Dec. 2009), <https://perma.cc/NKJ9-BYCS>; see also Summers, *supra* note 2929, at 33; Susan Herbst-Murphy, *Clearing and Settlement of Interbank Card Transactions: A MasterCard Tutorial for Federal Reserve Payments Analysts* 7 (Federal Reserve Bank of Philadelphia - Payment Cards Center, Discussion Paper No. 13-01); Craig Pirrong, *The Industrial Organization of Execution, Clearing and Settlement in Financial Markets* 6 (Center for Financial Studies, Working Paper No. 2008-43, 2007).

³³ See *supra* note 30; see also *Glossary of Terms Related to Payment, Clearing and Settlement Systems*, EUR. CENT. BANK (Dec. 2009), <https://perma.cc/NKJ9-BYCS>; Summers, *supra* note 29, at 33; Herbst-Murphy, *supra* note 32, at 9–10.

payors' money to clear payments on their behalf; subsequently, such controlling power allows financial intermediaries to transmit money to other financial intermediaries designated by payees, namely to settle payments.³⁴ For a smooth clearing and settlement process, a bank may work with clearinghouses, which aggregate, calculate, and confirm all the payments that each member bank owes to other banks and/or is entitled to receive from other banks, and then provide settlement services by completing these payments.³⁵ Third, before and/or after payments, payors or payees might exchange their money from one category to another based on exchange rates, such as from USD to GBP.³⁶ The key component of this process is financial intermediaries' gaining and exercising of controlling power over payment assets through acceptance and transmission. In other words, financial intermediaries gain custody over payment assets.

Yet, neither the clearing and settlement of cryptocurrency payments nor the exchange of different categories of cryptocurrencies necessitates financial intermediaries. A cryptocurrency payment can occur directly between the unhosted wallets of a payor and payee, meaning that intermediaries' acceptance and transmission of payment assets are not prerequisites for the payment to occur.³⁷ Additionally, decentralized exchanges (DEXs) can facilitate crypto-to-crypto exchanges without taking custody of payment assets.³⁸ By providing non-custodial payment

³⁴ See Awrey & van Zwieten, *The Shadow Payment System*, *supra* note 26, at 778; see also Dan Awrey & Kristin van Zwieten, *Mapping the Shadow Payment System* (SWIFT Institute, Working Paper No. 2019-001 & Cornell Legal Studies Research Paper No. 19-44 & Oxford Legal Studies Research Paper No. 55/2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3462351, at 3.

³⁵ See Dan Awrey & Joshua C. Macey, *Open Access, Interoperability, and DTCC's Unexpected Path to Monopoly*, 132 YALE L.J. 96, 123 (2022); see also Paolo Saguato, *The Unfinished Business of Regulating Clearinghouses*, 2020 COLUM. BUS. L. REV. 449, 463 (2020); Paolo Saguato, *Financial Regulation, Corporate Governance, and the Hidden Costs of Clearinghouses*, 82 OHIO ST. L. J. 1071, 1085 (2021).

³⁶ For example, a restaurant in London could possibly refuse to accept U.S. dollars, in which case U.S. visitors would have to convert/exchange U.S. dollars into British pounds before they could pay for their lunch.

³⁷ See TECH. ADVISORY COMM. (TAC) OF THE U.S. COMMODITY FUTURES TRADING COMM'N, *DECENTRALIZED FINANCE: REPORT OF THE SUBCOMMITTEE ON DIGITAL ASSETS AND BLOCKCHAIN TECHNOLOGY* 22 (2024).

³⁸ See *id.* at 28–33 (explaining the functional mechanisms of storing, trading, lending, payment, and RegTech in DeFi); see also Lioba Heimbach & Wenqian Huang, *DeFi Leverage* 5 (BIS Working Papers, No. 1171, 2024) (explaining the functional mechanism of lending in DeFi); Francesca Carapella, Edward Dumas, Jacob Gerszten, Nathan Swem, & Larry Wall, *Decentralized Finance (DeFi): Transformative Potential & Associated Risks*, FIN. AND ECON. DISCUSSION SERIES FED. RES. BOARD, WASH., D.C., June 2022, at 5–13

services, unhosted wallets, DEXs, and non-custodial mixers not only allow payments to happen in a peer-to-peer manner but also become subject to illicit finance threats, turning into vulnerable targets of wrongdoing, including money laundering.³⁹

The goal of Part I is to show how bad actors launder dirty money through cryptocurrency non-custodial service providers. To do so, this Part explains how distributed ledger technology (DLT)—specifically blockchain technology—supports the clearing and settlement of cryptocurrency payments. Then, it explains what cryptocurrency non-custodial service providers are and how they interact with one another and the conventional payment system. These players are unhosted wallets, decentralized exchanges (DEXs), and mixers. Third, it shows how bad actors launder dirty money through non-custodial service providers.

A. Cryptocurrency Payments in Distributed Ledger Technology (DLT): Collective Clearing and On-Chain Self-Settlement

The accounting term⁴⁰ “ledger” originally refers to a system of recordkeeping of financial activities, such as payments, and the underlying financial relationships stemming from these financial activities.⁴¹ A distributed ledger is a database shared or distributed⁴² across a network of various nodes.⁴³ Unlike a traditional ledger that exists in a single location, a distributed ledger is a category of ledger, the copy of which is distributed among various computers worldwide rather than existing in a single location.⁴⁴ There are generally five categories of distributed ledger,

(explaining the functional mechanisms of lending, trading, derivatives, payments, and asset management in DeFi).

³⁹ See U.S. DEPT OF THE TREASURY, ILLICIT FINANCE RISK ASSESSMENT OF DECENTRALIZED FINANCE 13 (2023), <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>.

⁴⁰ See A. C. Littleton, *Evolution of the Ledger Account*, 1 THE ACCT. REV. 12, 12–14 (1926).

⁴¹ See *Ledger Accounts*, KAPLAN FINANCIAL KNOWLEDGE BANK, <https://perma.cc/8Z8V-X7LF> (last visited Jan. 1, 2024).

⁴² See Raphael Auer, Cyril Monnet, & Hyun Song Shin, *Distributed Ledgers and the Governance of Money* 2 (BIS Working Papers No. 924, 2021) (revised Nov. 2021).

⁴³ The Bitcoin whitepaper uses the term “node.” See SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 3 (2008). However, “node” is commonly referred to as “miner.” See Sarah Jane Hughes & Stephen T. Middlebrook, *Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries*, 32 YALE J. ON REG. 495, 505 (2015).

⁴⁴ See Jamie Berryhill, Théo Bourgerie, & Angela Hanson, *Blockchains Unchained: Blockchain Technology and its Use in the Public Sector* 7 (OECD Working Papers on Public Governance No. 28, 2018).

depending on the specific technological mechanism.⁴⁵ Since the release of the Bitcoin whitepaper in 2008,⁴⁶ blockchain is by far the most well-known category of distributed ledger and has been playing key roles in cryptocurrency payments.⁴⁷

Distributed ledger technology (DLT) allows payors and payees to complete payments in a peer-to-peer manner, meaning that no single authority, such as banks, must exist to hold, clear, and settle their payments in blockchains.⁴⁸ As an example of DLT, each blockchain adds a new block through the *collective* agreement of all of its participants, or computer nodes. For example, to move a cryptocurrency from one address to another address within a blockchain, such as the Bitcoin and Ethereum blockchains, a payor must submit the payor's *cryptographic* digital signature,⁴⁹ as well as other information about this cryptocurrency payment to the entire blockchain network.⁵⁰ Subsequently, one of the nodes selected by the blockchain system, namely a miner or a

⁴⁵ These are Blockchain, Directed Acyclic Graph (DAG) or Tangle, Hashgraph, Sidechain, and Holochain. Each of the five DLT subcategories, including Blockchain, offers different promises and perils depending on their consensus mechanism for recordkeeping and ensuring data validity. These different consensus mechanisms manifest themselves in various dimensions, including scalability, validation, immutability, interoperability, security, fee, transparency, and energy consumption. See M.D. Khan et al., *A Review of Distributed Ledger Technologies in the Machine Economy: Challenges and Opportunities in Industry and Research* (55th CIRP Conf. on Manufacturing Sys.), 107 *PROCEDIA CIRP* 1168, 1169–72 (2022); see also Reza Soltani, Marzia Zaman, Rohit Joshi & Srinivas Sampalli, *Distributed Ledger Technologies and Their Applications: A Review*, *APPLIED SCI.* (Aug. 2022), at 4–16; Michael Anderson Schillig, *The Too-Big-to-Fail Problem and the Blockchain Solution*, 19 *BERKELEY BUS. L.J.* 126, 130 n.17 (2022); Shakila Zaman, *Thinking Out of the Blocks: Holochain for Distributed Security in IoT Healthcare*, 10 *IEEE ACCESS* 37064, 37065–66 (2022).

⁴⁶ The technological developments in computing power, distributed ledger technologies (DLT), cryptography, algorithms, and the Internet witnessed the release of Bitcoin whitepaper from a person or group of people under the pseudonym of Satoshi Nakamoto in 2008, who had started working on the Bitcoin whitepaper since 2007. See Nakamoto, *supra* note 43; see also Gautami Tripathi, *A Comprehensive Review of Blockchain Technology: Underlying Principles and Historical Background with Future Challenges*, 9 *DECISION ANALYTICS J.* (Oct. 2023), at 4; XUN YI ET AL., *BLOCKCHAIN FOUNDATIONS AND APPLICATIONS* (2022).

⁴⁷ See Dan Awrey, *Split Derivatives: Inside the World's Most Misunderstood Contract*, 36 *YALE J. ON REG.* 495, 564 (2019); see also Auer, Monnet & Shin, *supra* note 42, at 3.

⁴⁸ See *supra* note 42; see also 85 Fed. Reg. 83840, 83842 (Dec. 23, 2020). While centralized exchanges (CEXs), the counterpart of centralized financial institutions in cryptocurrency transactions, may still control users' funds, their presence is not a necessary condition for completing transactions.

⁴⁹ The manner of generating signature is discussed below in the wallet section.

⁵⁰ See ANDREAS M. ANTONOPOULOS & DAVID A. HARDING, *MASTERING BITCOIN: PROGRAMMING THE OPEN BLOCKCHAIN* 53–54 (3d ed. 2023); see also ANDREAS M. ANTONOPOULOS & GAVIN WOOD, *MASTERING ETHEREUM: BUILDING SMART CONTRACTS AND DAPPS* 62 (2018).

validator, would confirm the validity of the digital signature.⁵¹ A successful validation would move the cryptocurrency to another location, and the miner/validator would add a new block containing the aforementioned information and receive a new cryptocurrency and/or gas fee as a reward.⁵²

A consensus mechanism determines the manner in which a blockchain system selects the miner or validator qualified to validate a transaction and receive the corresponding reward.⁵³ Generally speaking, there are two categories of consensus mechanism, namely Proof-of-Work (PoW) that selects miners in blockchains, such as the Bitcoin blockchain,⁵⁴ as well as Proof-of-Stake (PoS) which selects validators in blockchains, such as the Ethereum blockchain.⁵⁵ The Bitcoin blockchain is the first widely known blockchain.⁵⁶ Figures show that the Ethereum blockchain's dominance is 64.4% based on trading volume.⁵⁷

For payment clearing, miners under PoW would verify whether a payor has sufficient payment assets to cover payment value in order to avoid double-spending problems before adding a new block, broadcasting it to the entire network, and receiving newly mined coins as a reward.⁵⁸ For PoS-based blockchains that do not generate new coins as remuneration for validators, payers would directly pay validators a fee called "gas fee"—a condition to clear and settle a payment—as remuneration for the validation work that costs computational resources.⁵⁹ An essential component of payment clearing is the miners' and validators' verification of sufficient payment assets to avoid double-spending. The

⁵¹ See Antonopoulos & Harding, *supra* note 50, at 183; see also Antonopoulos & Wood, *supra* note 50, at 321.

⁵² See Antonopoulos & Harding, *supra* note 50, at 23; see Antonopoulos & Wood, *supra* note 50, at 62.

⁵³ See Paul Wackerow et al., *PROOF-OF-STAKE (POS)*, ETHEREUM (Mar. 29, 2024), <https://perma.cc/J9GF-YB9T>.

⁵⁴ See PHIL CHAMPAGNE, *THE BOOK OF SATOSHI: THE COLLECTED WRITINGS OF BITCOIN CREATOR SATOSHI NAKAMOTO* 69 (2014); see also Nakamoto, *supra* note 43, at 3; Hughes & Middlebrook, *supra* note 43, at 505.

⁵⁵ See VITALIK BUTERIN, *ETHEREUM: A NEXT-GENERATION SMART CONTRACT AND DECENTRALIZED APPLICATION PLATFORM* 10, 19 (2014).

⁵⁶ See Nakamoto, *supra* note 43.

⁵⁷ See *Top Blockchains by Total Value Locked (TVL)*, COINGECKO, <https://www.coingecko.com/en/chains> (last visited July 1, 2024) (confirming that the Ethereum blockchain's dominance is 64.40% with \$1,398,456,271 24 hour trading volume and \$59,588,708,973 total value locked as of 16:48 PM EST, July 1, 2024).

⁵⁸ See Nakamoto, *supra* note 43, at 3; see also Hughes & Middlebrook, *supra* note 43, at 505; Yonatan Sompolinsky & Aviv Zohar, *Bitcoin's Underlying Incentives*, 61 COMM. OF THE ACM 46, 48 (2018).

⁵⁹ See, e.g., *GAS AND FEES*, ETHEREUM, <https://perma.cc/Y7EM-TL8P> (last visited June 1, 2024).

collective process of selecting miners/validators in and of itself demonstrates the collective nature of clearing in blockchains.

For payment settlement, for example, the addition of a new block in the Bitcoin blockchain in and of itself signals the validation of a particular Bitcoin payment, namely payment settlement.⁶⁰ The completion of such a validation would simultaneously change cryptocurrencies' legal ownership, meaning that settlement would happen as soon as such a validation is completed.⁶¹ Therefore, the peer-to-peer manner of adding new data, coupled with the immutability of existing data, would enable payors to directly and safely pay payees through blockchains without relying on banks for settlement.

The collective clearing and on-chain self-settlement of payments result in a shift of customers' trust concerning the safety of their assets from a single authority, such as banks, to a distributed ledger and its underlying technology, namely DLT.⁶²

B. The Functional Mechanisms of Cryptocurrency Non-Custodial Service Providers

To explain the functional mechanism of non-custodial service providers that allows cryptocurrency payment to happen, this Article describes how unhosted wallets, DEXs, and non-custodial wallets interact with one another and the conventional financial system.

1. Players for Accepting, Transmitting, and Storing Cryptocurrencies: Unhosted Wallets

A cryptocurrency wallet, a software user interface (UI), not only enables its owner to accept and transmit cryptocurrency but also displays the number and category of cryptocurrency it controls in a layman-friendly manner. Therefore, for most individuals, a major part of their interaction with cryptocurrencies, other than cryptocurrency exchanges explained below, is highly likely to begin with cryptocurrency wallets.

A cryptocurrency wallet does *not* store any cryptocurrency; it is a blockchain that stores all the cryptocurrencies mined/minted

⁶⁰ See Nakamoto, *supra* note 43, at 3; see also Hughes & Middlebrook, *supra* note 43, at 505.

⁶¹ See Austin Adams, Mary-Catherine Lader, Gordon Liao, David Puth, & Xin Wan, On-Chain Foreign Exchange and Cross-border Payments 5 (last revised on Apr. 14, 2023) (unpublished manuscript); see also Auer, Monnet, & Shin, *supra* note 42, at 2.

⁶² See Soltani, *supra* note 45, at 4; see also Khan, *supra* note 45, at 1169; Awrey, *supra* note 47, at 564.

therefrom at various blockchain addresses therein.⁶³ A wallet generates and stores multiple private keys that allow its owner to transmit cryptocurrencies.⁶⁴ A private key is typically a 256-bit hexadecimal number randomly generated by a wallet service provider.⁶⁵ It is supposed to be visible only to the wallet owner since the knowledge of a private key is equal to the power to control all the cryptocurrencies stored in the associated blockchain address.⁶⁶ Based on each private key, a wallet would then generate and store a corresponding public key.⁶⁷

To send a cryptocurrency from a blockchain address, the underlying blockchain that was mined/minted and stores the cryptocurrency would require a payor to verify, through a cryptographic digital signature, the knowledge of the private key associated with the blockchain address without disclosing the private key to any external party.⁶⁸ Through a wallet, the owner of a cryptocurrency could submit this cryptographic digital signature to the blockchain, thereby requesting a selected miner/validator to validate this cryptocurrency payment.⁶⁹

Controlling a wallet's private keys would control all the corresponding cryptocurrencies the wallet controls, making a wallet an attractive target for hackers.⁷⁰ There are two approaches to enhance a wallet's security. First, a cryptocurrency owner could keep the private keys of the associated wallet offline, such as storing it on a mobile device offline, or handwriting it on paper and keeping it locked in a safe place.⁷¹ Second, a wallet service

⁶³ See Antonopoulos & Harding, *supra* note 50, at 89; see also Antonopoulos & Wood, *supra* note 50, at 80.

⁶⁴ See Antonopoulos & Harding, *supra* note 50, at 53, 112; see also Antonopoulos & Wood, *supra* note 50, at 62–63.

⁶⁵ See Antonopoulos & Harding, *supra* note 50, at 55; see also Antonopoulos & Wood, *supra* note 50, at 63.

⁶⁶ See Antonopoulos & Harding, *supra* note 50, at 7, 53; see also Antonopoulos & Wood, *supra* note 50, at 62–63.

⁶⁷ See Antonopoulos & Harding, *supra* note 50, at 59; see also Antonopoulos & Wood, *supra* note 50, at 64.

⁶⁸ See Antonopoulos & Harding, *supra* note 50, at 184–85; see also Antonopoulos & Wood, *supra* note 50, at 115–16.

⁶⁹ See Antonopoulos & Harding, *supra* note 50, at 3, 53–54; see also Antonopoulos & Wood, *supra* note 50, at 60.

⁷⁰ See Mordechai Guri, *BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets*, IEEE/ACM INT'L CONF. ON & INT'L CONF. ON CYBER, PHYSICAL AND SOC. COMPUTING (CPSCom) GREEN COMPUTING AND COMM. (GREENCOM), 2018, at 1308; see also Nabil Alkeilani Alkadri, *Deterministic Wallets in a Quantum World*, CCS'20: PROCEEDINGS OF THE 2020 ACM SIGSAC CONF. ON COMPUTER AND COMM. SECURITY, Oct. 2020, at 2.

⁷¹ See, e.g., *How to Export an Account's Private Key*, METAMASK (Apr. 26, 2024), <https://perma.cc/3WTS-WEKB>; see also *How to Export Private Key*, ELLIPAL (Feb. 3, 2021),

provider could incorporate a mechanism that requires multiple private keys to sign a payment, and a wallet incorporating such a mechanism is called a multiple signature wallet, or a multisig wallet.⁷² A multisig wallet could, but does not necessarily have to, allow its owner to maintain one private key, and the wallet's service provider would maintain the other private key.⁷³ A wallet owner would use one private key the owner maintains to first *request* the wallet service provider to submit a payment signature and other information to the entire blockchain.⁷⁴ After receiving and verifying the payment signature request, the wallet service provider would use the other private key it maintains to sign and submit the payment signature and other information to the entire blockchain network.⁷⁵

In addition to classifying wallets into multisig wallets and single signature (singlesig) wallets depending on the requirements for generating signatures, wallets can be classified into unhosted and hosted wallets, depending on whether wallet owners have independent control over private keys.

Unhosted or non-custodial wallets allow wallet owners to independently control the private keys, thereby enjoying exclusive control over their cryptocurrencies at all stages of both (1) crypto-to-crypto exchanges through decentralized exchanges (DEXs) and (2) cryptocurrency payments, which includes unhosted wallets' acceptance and/or transmission of cryptocurrencies from external hosted or unhosted wallets.⁷⁶

Depending on whether their private keys are kept online or offline, unhosted wallets can be either (1) cold wallets, such as a

<https://perma.cc/8PMZ-H8PX>; *What is a Private Key?*, DYDX (Apr. 28, 2024), <https://perma.cc/C3Q2-TH5J>; *infra* note 145, at 15.

⁷² See *infra* note 145, at 17; see also *infra* note 73.

⁷³ See Alex, *What is a Multisignature (Multisig) or Shared Wallet?*, BITPAY (Mar. 2024), <https://perma.cc/JVD2-WKV9>.

⁷⁴ See *infra* note 145, at 17; see also, e.g., *Buy, Store, Swap and Spend Your Crypto*, BITPAY, <https://perma.cc/P7GW-DW9W>; (last visited June 20, 2024); see also *How to Set Up Bitcoin Multisig Wallet with Ledger and Unchained*, LEDGER (Mar. 12, 2024), <https://perma.cc/9JUQ-2XD8>.

⁷⁵ See *infra* note 145, at 17.

⁷⁶ See Shlomit Azgad-Tromer, Joey Garcia, & Eran Tromer, *The Case for On-Chain Privacy and Compliance*, 6 STAN. J. BLOCKCHAIN L. & POL'Y 265, 278–80 (2023); see also Aniruddh Vadlamani & Sarthak Sharma, *Bridging the Divide Between Defi and Regulators: Showcasing Decentralized Autonomous Governance as the Future for Self-Custody Wallet Regulation*, 2023 U. ILL. J.L. TECH. & POL'Y 373, 377 (2023).

variety of wallets offered by Ellipal⁷⁷ and Ledger,⁷⁸ or (2) hot wallets, such as MetaMask.⁷⁹ Cold wallets are usually on air-gapped computers, while hot wallets are usually on smartphone applications or computer programs.⁸⁰ Unlike cold wallets, hot wallets are consistently online, meaning that they are technically more vulnerable to attacks compared to cold wallets.⁸¹ If an unhosted wallet is insufficiently funded to cover both payment value and gas fees, then miners/validators would not clear and settle payments.⁸²

2. Players for Exchanging Different Categories of Cryptocurrencies: Decentralized Exchange

In the conventional payment system, banks' currency exchange services allow the exchange of different categories of money, such as exchanging USD for GBP, in addition to their domestic and international wire transfer services that allow the transmission of money from one location or person to another. These would not be possible without the existing domestic and international agreements, as well as entities such as the Society for Worldwide Interbank Financial Telecommunications (SWIFT). For example, an inter-bank international wire transfer would necessitate an exchange of a set of messages to determine the specific details of such a payment through SWIFT, and banks would then clear and settle payments on behalf of their customers as explained earlier.⁸³

While cryptocurrency wallets alone can facilitate cryptocurrency payments, they cannot perform the exchange functions since a wallet simply stores a pair of private and public keys.

⁷⁷ See *ELLIPAL, Leader of Air-Gapped Cold Wallet*, ELLIPAL, <https://perma.cc/57A2-549C> (last visited Apr. 28, 2024).

⁷⁸ See *Compare Ledger Hardware Wallets*, LEDGER, <https://perma.cc/57A2-549C> (last visited Apr. 28, 2024).

⁷⁹ See, e.g., *MetaMask is a self-custodial wallet*, METAMASK (May 7, 2025), <https://support.metamask.io/getting-started/metamask-is-a-self-custodial-wallet> ("MetaMask includes a self-custodial (also commonly referred to as non-custodial) cryptocurrency and token wallet. It gives you complete control of your access keys and therefore your assets.").

⁸⁰ See Jean-Philippe Aumasson & Omer Shlomovits, *Attacking Threshold Wallets*, IACR CRYPTOLOGY EPRINT (Paper No. 1052, 2020), at 2–3; see also Sabine Houy, Philipp Schmid, & Alexandre Bartel, *Security Aspects of Cryptocurrency Wallets—A Systematic Literature Review*, 56 ACM COMPUTING SURVEYS, No. 1, at 4 (2023).

⁸¹ See Aumasson & Shlomovits, *supra* note 80, at 2–3; see also Houy, Schmid, & Bartel, *supra* note 80, at 4.

⁸² See, e.g., Joel Willmore, *How to Fix 'Insufficient Funds' Error or Greyed-Out Confirm Button*, METAMASK (June 13, 2024), <https://perma.cc/MU7J-4TB9>.

⁸³ See *Discover Swift*, SWIFT, <https://perma.cc/9Z8G-W9XS> (last visited July 4, 2024).

Cryptocurrency exchanges facilitate crypto-to-crypto and/or crypto-to-fiat/fiat-to-crypto exchanges.⁸⁴ Cryptocurrency exchanges are blockchain-based user interfaces (UIs) that utilize permissionless blockchains to exchange cryptocurrencies.⁸⁵ Similar to a cryptocurrency wallet allowing its owner to accept and transmit cryptocurrencies in a layman-friendly manner, a cryptocurrency exchange allows its customers to exchange cryptocurrencies also in a layman-friendly manner.⁸⁶ Therefore, for most individuals, another major part of their interaction with cryptocurrencies, other than cryptocurrency wallets, is highly likely to begin with cryptocurrency exchanges, either CEXs or DEXs.⁸⁷

Only CEXs offer crypto-to-fiat/fiat-to-crypto exchange services, such as exchanging USD for USDT (also called on-ramp), and vice versa, such as exchanging USDT for USD (also called off-ramp).⁸⁸ On the contrary, both CEXs and DEXs offer crypto-to-crypto exchange services, such as exchanging USDT for USDC.⁸⁹ Intuitively, this would seem to limit the relevant anti-money laundering and countering the financing of terrorism (AML/CTF) risks stemming from DEXs.

The total trading volume of all DEXs in March, April, and May 2024 was \$267.397 billion, \$196.658 billion, and \$176.443 billion, respectively.⁹⁰ As of July 2, 2024, the market capitalization of DEXs is approximately \$18 billion to \$19 billion,⁹¹ with a

⁸⁴ See *supra* note 26; see also Elizabeth Boison & Leo Tsao, *Money Moves: Following the Money beyond the Banking System*, 67 DEP'T OF JUST. J. FED. L. & PRAC. 95, 119 (2019).

⁸⁵ See Brett Hemenway Falk & Sarah Hammer, *A Comprehensive Approach to Crypto Regulation*, 25 U. PA. J. BUS. L. 415, 433 (2023); see also Zhixuan Zhou & Bohui Shen, *Toward Understanding the Use of Centralized Exchanges for Decentralized Cryptocurrency*, ARXIV:2204.08664, June 2022, at 5.

⁸⁶ See, e.g., *How to Swap Tokens*, UNISWAP HELP CTR. (Oct. 2023), <https://perma.cc/8LFB-W777>.

⁸⁷ See Carapella, Dumas, Gerszten, Swem, & Wall, *supra* note 38, at 10; Kristin N. Johnson, *Decentralized Finance: Regulating Cryptocurrency Exchanges*, 62 WM. & MARY L. REV. 1911, 1953 (2021).

⁸⁸ See, e.g., *Crypto Calculator and Converter*, OKX, <https://perma.cc/LjV7-L3A4> (last visited Jan. 10, 2024); see also *Cash Out Your Balance*, COINBASE, <https://perma.cc/CVL3-FJUJ> (last visited Jan. 10, 2024); Daniel Dupuis & Kimberly Gleason, *Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic*, 28 J. FIN. CRIME 60, 69–70 (2021). For discussions of on- and off-ramp, see Adam J. Levitin, *Not Your Keys, Not Your Coins: Unpriced Credit Risk in Cryptocurrency*, 101 TEX. L. REV. 877, 892 (2023).

⁸⁹ See, e.g., *Supported Assets and Networks*, COINBASE, <https://perma.cc/45ZJ-CAZY> (last visited Jan. 15, 2024); see also *Tokens*, UNISWAP, <https://perma.cc/3UL5-YSMP> (last visited Jan. 15, 2024).

⁹⁰ See *DEXs Volume*, DEFI LLAMA, <https://defillama.com/dexs>. (last visited June 16, 2024).

⁹¹ See, e.g., *Top Decentralized Exchange (DEX) Coins by Market Cap*, COINGECKO, <https://www.coingecko.com/en/categories/decentralized-exchange> (last visited Jan. 4, 2024) (confirming that the market cap of decentralized exchange (DEX) coins is

24-hour trading volume of approximately \$0.9 billion to \$1.17 billion.⁹² There are two categories of DEXs, namely automated market makers (AMMs)⁹³ and order book DEXs,⁹⁴ depending on the manner of maintaining liquidity.⁹⁵ Liquidity refers to the tradability of assets in a market without loss of value, which could manifest itself through a combined list of various bids, namely the highest price of each buy order, and asks, namely the lowest price of each sell order.⁹⁶ To facilitate crypto-to-crypto exchanges, DEXs adopt the following mechanisms for clearing and settlement, as well as asset custody.

a. Clearing and Settlement

DEXs are essentially automated software protocols based on permissionless blockchains supported by smart contracts.⁹⁷ Smart contracts are code-based programs that may automatically carry out a function when one or more of an agreement's predetermined conditions are met, such as the exchange rate for crypto-to-crypto exchanges.⁹⁸ The programmability of smart contracts allows the enforcement of the requirement that successful settlements must be premised on the strict fulfillment of all the

\$18,066,411,662 as of 6:54 PM EST, July 2, 2024); *see also Top Decentralized Exchange (DEX) Token by Market Capitalization*, COINMARKETCAP, <https://perma.cc/5MGU-6DH4> (last visited July 2, 2024).

⁹² *See, e.g., Top Decentralized Exchange (DEX) Coins by Market Cap*, COINGECKO, <https://www.coingecko.com/en/categories/decentralized-exchange> (last visited Jan. 4, 2024) (confirming that the 24h trading volume of decentralized exchange (DEX) coins is \$1,171,664,964 as of 6:54 PM EST, July 2, 2024); *see also Top Decentralized Exchange (DEX) Token by Market Capitalization*, COINMARKETCAP, <https://perma.cc/5MGU-6DH4> (last visited July 2, 2024).

⁹³ *See, e.g., The Uniswap V1 Smart Contracts*, UNISWAP DOCS, <https://perma.cc/5AJB-5SNH> (last visited Jan. 12, 2024).

⁹⁴ *See, e.g., Everett Hu, Where Does Liquidity Come From?*, DYDX (Apr. 2024), <https://perma.cc/9EJZ-V36H>.

⁹⁵ *See Samantha Altschuler, Should Centralized Exchange Regulations Apply to Cryptocurrency Protocols?*, 5 STAN. J. BLOCKCHAIN L. & POL'Y 92, 96 (2022).

⁹⁶ *See M. Konrad Borowicz, Law, Liquidity, and Monetary Policy*, 83 U. PITT. L. REV. 779, 797–98 (2022).

⁹⁷ *See Lindsay X. Lin, Deconstructing Decentralized Exchanges*, 2 STAN. J. BLOCKCHAIN L. & POL'Y 58, 58 (2019); *see also id.*

⁹⁸ *See Nick Szabo, The Idea of Smart Contracts*, PHONETIC SCI., AMSTERDAM, 1997, <https://perma.cc/RQ94-CETH> (last visited Feb. 7, 2023); *see also* Stuart D. Levi & Alex B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, HARV. L. SCH. F. ON CORP. GOVERNANCE (May 26, 2018), <https://perma.cc/GV73-48EF>; Françoise Birnholz & Kelsey Barthold, *Back to the Future: Sorting Old Law from New Technology in Blockchain Smart Contract Applications & Assessing the Need for Regulation*, 89 GEO. WASH. L. REV. ARGUENDO 96 (2021).

conditions set out by the smart contracts, namely atomic settlement.⁹⁹ For DEXs' underlying smart contracts, the conditions are typically twofold. First, the successful settlement of a swap order is conditioned on the simultaneous delivery of the transaction value in the form of two categories of cryptocurrencies to both sides.¹⁰⁰ Second, the successful settlement of a swap order is conditioned on the successful delivery of a gas fee.¹⁰¹ Therefore, a violation of even a tiny part of a smart contract's rule would stop the smart contract from interacting with miners or validators for settlement.

The collective clearing and on-chain self-settlement model of blockchains also characterizes DEXs' functional mechanism in the following two manners. First, if a smart contract determines that a party's unhosted wallet is insufficiently funded to cover both the gas fees and the payment value, then it would not submit the swapping order to the corresponding blockchains.¹⁰² This means that the clearing process would not begin. Second, if the smart contract submits an order to the corresponding blockchains, then DEXs' customers must directly interact with miners and validators to clear and settle their swapping/exchange orders on-chain through DEXs' underlying smart contracts and their unhosted wallets.¹⁰³

b. Asset Control

Customers maintain exclusive control over their cryptocurrencies at all stages of crypto-to-crypto exchanges throughout clearing and settlement. While CEXs control customers' assets, DEXs neither require disclosure of private keys of customers' unhosted wallets nor require customers to transmit their

⁹⁹ See Hossein Nabilou, *Probabilistic Settlement Finality in Proof-of-Work Blockchains: Legal Considerations*, 7 BUS. & FIN. L. REV. 139, 155 (2024); see also Michael Lee, Antoine Martin, & Benjamin Müller, *What Is Atomic Settlement?*, FED. RES. BANK OF N.Y. (Nov. 7, 2022), <https://perma.cc/W9E8-HJBA>; Holger Neuhaus & Mirjam Plooi, *Central Bank Money Settlement of Wholesale Transactions in the Face of Technological Innovation*, ECB ECON. BULL. (Aug. 2023), <https://perma.cc/49FS-B8S8>.

¹⁰⁰ See *The Financial Stability Risks of Decentralised Finance*, FIN. STABILITY BD. 41 (Feb. 16, 2023).

¹⁰¹ See, e.g., Sourajyoti Gupta, *What Does the "Insufficient Funds for Gas * Price + Value" Error Mean When Using the Estimate Gas Function?*, POLYGON SUPPORT (Nov. 30, 2023), <https://perma.cc/J2Z3-LS7U>; see also *What Does 'Insufficient Funds for Gas Price' Mean?*, ALPHAWALLET, <https://perma.cc/U8DE-K94X> (last visited June 1, 2024).

¹⁰² See Morten Bech, Jenny Hancock, Tara Rice, & Amber Wadsworth, *On the Future of Securities Settlement*, BIS Q. REV. 76 (Mar. 2020).

¹⁰³ See Carapella, Dumas, Gerszten, Swem & Wall, *supra* note 3838, at 10; see also Chris Brummer, *Disclosure, Dapps and DeFi*, 5 STANFORD J. BLOCKCHAIN L. & POL'Y 137, 141 (2022); *infra* note 145, at 24.

cryptocurrencies to any omnibus wallets.¹⁰⁴ Therefore, DEXs do not control their customers' cryptocurrencies as custodians, meaning that the use of omnibus wallets and/or segregated wallets is not within DEXs' businesses.

3. Players for Obfuscating Cryptocurrency Payment Records: Non-Custodial Mixers

A research showed that the total amount of payment mixers processed reached \$7.8 billion in 2022, and 24% of them originated from illicit addresses.¹⁰⁵ Moreover, mixers helped to launder nearly 10% of cryptocurrencies held by illicit entities in 2022.¹⁰⁶ Each block of a blockchain stores the data of various historical payments, including the wallet addresses of payors and payees, as well as a timestamp.¹⁰⁷ If a blockchain is permissionless, then these data are accessible to the public.¹⁰⁸ This enables the tracking of each cryptocurrency's historical movements. Mixers break the chain of historical payments. In practice, mixers not only help to protect personal privacy but also illegally facilitate the laundering of a large amount of dirty money.

There are two major categories of mixers, which are custodial mixers and non-custodial mixers.¹⁰⁹ Non-custodial mixers can further be classified into coinjoins and smart contract mixers depending on whether they combine users' cryptocurrencies in a single transaction or not.¹¹⁰ A custodial mixer has access to both the private and public keys of customers' wallets, meaning that it

¹⁰⁴ See, e.g., *How to Connect a Wallet to Uniswap*, UNISWAP (Feb. 2024), <https://perma.cc/NM89-9W4U>; see also Antonio Juliano, *How Do I Create an Account or Sign Up?*, dYdX (Apr. 2024), <https://perma.cc/A6TZ-BLQ7>.

¹⁰⁵ See Chainalysis Team, *Crypto Money Laundering: Four Exchange Deposit Addresses Received Over \$1 Billion in Illicit Funds in 2022*, CHAINALYSIS (Jan. 26, 2023), <https://perma.cc/7MUV-G6MP>.

¹⁰⁶ See Chainalysis Team, *Crypto Mixers and AML Compliance* (Aug. 23, 2022), <https://perma.cc/6U78-Q29P>.

¹⁰⁷ See Fran Casino et al., *A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues*, 36 *TELEMATICS AND INFORMATICS* 55, 55–56 (2019); see also MIT Technology Review Editors, *Explainer: What Is a Blockchain?*, MIT TECH. REV. (Apr. 2018).

¹⁰⁸ See George Tian, *Blockchain, RegTech, and Their Application to Transfer Pricing Activities in the Cloud*, 21 *HOUS. BUS. & TAX L.J.* 142, 162, 172 (2020).

¹⁰⁹ See Neeraj Agrawal, *Non-Custodial Cryptocurrency Mixer Developers Are Not Subject to U.S. Regulation* (May 23, 2019), <https://perma.cc/C5GW-4Z9V>; see also *Crypto Mixers and AML Compliance*, *supra* note 106.

¹¹⁰ See Alexandra D. Comolli & Michele R. Korver, *Surfing the First Wave of Cryptocurrency Money Laundering*, 69 *DEP'T OF JUST. J. FED. L. & PRAC.* 183, 216 (2021); see also Stan Sater, *Do We Need KYC/AML: The Bank Secrecy Act and Virtual Currency Exchanges*, 73 *ARK. L. REV.* 397, 419 (2020); *Crypto Mixers and AML Compliance*, *supra* note 106.

fully controls users' funds.¹¹¹ Nevertheless, non-custodial mixers are merely blockchain protocols allowing the exchange of information between users; it is their users who have exclusive custody of their cryptocurrencies throughout the mixing processes.¹¹²

C. How bad Actors Launder Dirty Money Through Cryptocurrency Non-Custodial Service Providers

Payment appears in all three stages of money laundering as bad actors must transmit dirty money from one location or person to another,¹¹³ particularly in the following two scenarios. First, bad actors could repeatedly transmit small amounts of dirty money into legitimate financial systems without necessarily triggering regulatory scrutiny and/or detections. To do so, bad actors would break down large transactions into multiple smaller transactions and pay them separately, the amount of each transaction is lower than the threshold at which banks must report to the government,¹¹⁴ a money laundering technique called structuring or smurfing.¹¹⁵ Second, bad actors could lower the traceability of dirty money through crypto-to-crypto exchanges, crypto-to-fiat/fiat-to-crypto exchanges, and mixers.¹¹⁶ In these processes, non-custodial service providers interact with one another, custodial service providers, and the traditional payment system to pay and exchange cryptocurrency and/or fiat currency in the following manner.

If a bad actor's unhosted wallet holds the adequate category and sufficient amount of cryptocurrency for payment, then the bad actor could transmit cryptocurrency to another hosted or unhosted wallet after paying gas fees. Such a transmission directly

¹¹¹ See, e.g., *United States v. Harmon*, No. 19-cr-395 (BAH), 2021 WL 1518344, at *8 (D.D.C. Apr. 16, 2021); see also Colin Harper, *The Bitcoin Mixing Case at the Center of the Fight for Transaction Privacy*, BITCOIN MAGAZINE (Mar. 17, 2020), <https://perma.cc/FQK9-MU4E>.

¹¹² See Agrawal *supra* note 109; see also *Crypto Mixers and AML Compliance*, *supra* note 106.

¹¹³ Money laundering typically involves three stages: placement, layering, and integration. See Jettner, *supra* note 9; see also generally THE REPORT OF THE ATTORNEY GENERAL PURSUANT TO SECTION 5(B)(III) OF EXECUTIVE ORDER 14067, *supra* note 9.

¹¹⁴ For the reporting obligations under the Bank Secrecy Act (BSA), see *infra* Part II.

¹¹⁵ See Maame Nyakoa Boateng, *Global Partnership Should Be the Way Forward to Combat Money Laundering*, 126 DICKINSON L. REV. 837, 841 (2022); see also Christopher J. Wilkes, *A Case for Reforming the Anti-Money Laundering Regulatory Regime: How Financial Institutions' Criminal Reporting Duties Have Created an Unfunded Private Police Force*, 95 IND. L.J. 649, 654 (2020).

¹¹⁶ See Jettner, *supra* note 9; see also generally THE REPORT OF THE ATTORNEY GENERAL PURSUANT TO SECTION 5(B)(III) OF EXECUTIVE ORDER 14067, *supra* note 9.

to another wallet stands for the first category of payment in this Article. Yet, if a bad actor's unhosted wallet does not hold the adequate category and sufficient amount of cryptocurrency for payment, then either of the following approaches would allow the bad actor to obtain the adequate category and sufficient amount of cryptocurrency for subsequent payment.

First, a bad actor could accept cryptocurrency directly from another wallet, which could be a hosted wallet controlled by a CEX or an unhosted wallet. Such an acceptance directly from another wallet also stands for the first category of payment in this Article discussed above.

Second, a bad actor could exchange cryptocurrencies through DEXs. This not only allows the bad actor to acquire the adequate category and sufficient amount of cryptocurrency but also lowers the traceability of payment history. As explained earlier, DEXs allow bad actors to swap their coins from one category to another, such as swapping DAI for USDT, USDT for USDC, USDC for WBTC, and eventually from WBTC back to DAI. Eventually, it is highly possible that the DAI coins that the bad actor received differ from the ones the bad actor initially owned, even though their value remained unchanged except for the gas fees. Since a DEX does not control its customers' cryptocurrencies, it must receive approval from the payor to transmit cryptocurrencies from the payor's unhosted wallet to an external address as the condition to initiate a swap order, which could be a DEX's router address.¹¹⁷ Transmitting cryptocurrency from a bad actor's unhosted wallet to an address provided by a DEX, as well as accepting the swapped cryptocurrency from a DEX, would stand for the second category of payment in this Article.

Third, a bad actor could receive newly minted/mined cryptocurrency in either of the following two manners. First, some cryptocurrency issuers only issue new cryptocurrencies to customers who have followed strict know-your-customer (KYC) procedures,¹¹⁸ namely the provision of identification information. As discussed in Part II, because the BSA does not require unhosted wallet service providers to comply with its substantive obligations, including the collection of personal identification information, unhosted wallets may not be able to receive these newly minted/mined cryptocurrencies. Second, because mining new

¹¹⁷ See, e.g., *Router02*, UNISWAP, <https://perma.cc/QT4L-URCM> (last visited May 9, 2024); see also *Router v2*, PANCAKESWAP, <https://perma.cc/5ZKH-ZN5G>.

¹¹⁸ See, e.g., *What Are Tether Tokens and How Do They Work?*, TETHER, <https://perma.cc/Z5HD-LC5W> (last visited May 9, 2024).

cryptocurrencies, such as Bitcoin, does not necessitate any KYC procedures, miners can store mined cryptocurrencies in their unhosted wallets.¹¹⁹

In any of the aforementioned situations, a bad actor could send cryptocurrencies from an unhosted wallet to a mixer to anonymize payment histories. Moreover, the governance of these key players, such as DEXs, cross-chain bridges, and mixers, could involve the voting carried out by DAOs' members holding governance tokens, which could be exchanged in both CEXs and DEXs.¹²⁰ By sending cryptocurrencies from unhosted wallets to hosted wallets, the off-ramp function of CEXs would allow a customer to convert cryptocurrencies to fiat currencies.

II. THE CURRENT ANTI-MONEY LAUNDERING LAW DOES NOT REGULATE CRYPTOCURRENCY NON-CUSTODIAL SERVICE PROVIDERS

Since 1970, the United States has sought to eliminate dirty money and capture bad actors through the carefully designed, highly sophisticated regulatory frameworks based on the BSA, which governs the modern payment system. These regulatory frameworks require centralized players of the payment system to register and follow a set of substantive obligations. The substantive obligations include four key components: the anti-money laundering program requirements,¹²¹ monitoring and reporting requirements,¹²² recordkeeping requirements,¹²³ and the travel rule.¹²⁴ Together, they serve to generate reports and records that would be highly useful for law enforcement in its efforts to investigate the flow of dirty money and prosecute bad actors in financial crimes.¹²⁵ More importantly, federal courts held that cryptocurrencies qualify as either funds or value that substitutes for currency as analyzed below. As such, the regulatory perimeter of

¹¹⁹ See, e.g., *Receive Mining Proceeds*, LEDGER (July 7, 2024), <https://perma.cc/9EMJ-SY6U>.

¹²⁰ See, e.g., *Buy Uniswap*, KRAKEN, <https://www.kraken.com/learn/buy-uniswap-uni> (last visited May 9, 2024); see also *Swap Anytime, Anywhere.*, UNISWAP, <https://perma.cc/G6LH-XRPA> (last visited May 9, 2024).

¹²¹ See *infra* note 124, §§ 1010.210, 1022.210(a) (2023); see also *infra* note 144, §§ 5318(a)(2), 5318(h) (2018).

¹²² See *infra* note 124, §§ 1010.310, 1010.320, 1022.310, 1022.320; see also *infra* note 144, § 5318(a)(2) (2018).

¹²³ See *infra* note 124, §§ 1010.400, 1022.400; see also *infra* note 144, § 5318(a)(2) (2018).

¹²⁴ See 31 C.F.R. §§ 1022.400, 1022.410, 1022.420 (2023).

¹²⁵ See Currency and Foreign Transactions Reporting Act of 1970, *supra* note 17; see also Ciarabellini, *supra* note 17, at 139-41.

the registration requirements of the BSA would cover intermediaries that accept and transmit cryptocurrencies. However, since non-custodial service providers do not accept and transmit, they are not within the scope of the BSA. As such, the BSA still leaves a gap through which bad actors could launder their dirty cryptocurrencies.

Part II explains why the current anti-money laundering law, namely the BSA, does not regulate cryptocurrency non-custodial service providers. To do so, Part II starts with the historical and policy background around the existing anti-money laundering (AML) regulatory framework's creation, rationale, and the specific harms it seeks to address. Then, Part II describes the scope of the regulatory perimeter of the BSA's registration requirements. The description shows that the BSA covers businesses that qualify as money transmitting businesses, which refer to businesses that accept *and* transmit "currency, funds, or other value that substitutes for currency."¹²⁶ Part II finds that because cryptocurrency non-custodial service providers do not accept and transmit cryptocurrencies, they do not qualify as money transmitting businesses and, therefore, do not have to comply with the BSA.

A. Background

The BSA's registration requirements were designed in a bifurcated structure to determine the businesses to which it is applicable.¹²⁷ The first part provides a list of *financial institutions* whose existing registration status under other regulatory frameworks brings them within the perimeter of the BSA's registration requirements, such as banks, securities brokers or dealers, currency exchanges, and insurance companies.¹²⁸ Recent legislation added two additional entities under the concept of financial institutions: electronic fund transfer networks and clearing and settlement systems.¹²⁹ This means that these businesses must file reports and keep records for regulators, thereby helping regulators against dirty money and bad actors. Therefore, the first part of the bifurcated structure can be straightforwardly applied, requiring only confirmation that the firms in question fall within one of the listed categories of financial institutions.

¹²⁶ *Supra* note 124, § 1010.100(ff)(5)(i)(A) (2023).

¹²⁷ *See infra* note 144, §§ 5312(a)(2), 5333(a) (2021).

¹²⁸ *See id.* § 5312(a)(2) (2021).

¹²⁹ *See* The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, *supra* note 15.

The second part of the registration requirements offers a description of *activities* that, if undertaken by a business, require the business to register and renew its registration.¹³⁰ Its application therefore requires a deeper analysis of the nature of individual businesses, which creates a set of relevant definitions and case law interpreting the scope of the registration requirements, namely the definition of money transmitting business explained below.¹³¹

B. Money Transmission

There are two sets of definitions relating to money transmission. The first is “money,” namely the *instruments* being transmitted, including currency, funds, and value that substitutes for currency. The latter is “transmission,” namely the *activities* that covered businesses undertake.

The BSA requires anyone who owns or controls a money transmitting business to register with FinCEN¹³² as a money services business (MSB).¹³³ The BSA defines a money transmitting business as “any . . . person who engages as a business in the transmission of currency, funds, or value that substitutes for currency, including any person who engages as a business in an informal money transfer system,”¹³⁴ or “any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system.”¹³⁵ These two categories of activities serve as examples of a “person who engages as a business in the transmission of currency, funds, or value that substitutes for currency,”¹³⁶ thereby helping to create a single definition of money transmitting business.¹³⁷ Then, the BSA’s implementing regulations

¹³⁰ See *infra* note 144, § 5330(a)(1) (2021); see also *supra* note 124, §§ 1022.380(a)(1), (b)(1)(i), (b)(2) (2016); *supra* note 124, § 1022.380(b)(2) (2016) (“Each two-calendar-year period following the initial registration period is a renewal period”).

¹³¹ See *infra* note 144, § 5330(d)(1) (2018).

¹³² See *What We Do*, *supra* note 18.

¹³³ According to 31 U.S.C. § 5330(a)(1), “[a]ny person who owns or controls a money transmitting business shall register the business . . . with the Secretary of the Treasury.” In *United States v. Harmon*, the court clarified that “[r]egulations promulgated under [31 U.S.C. § 5330] require ‘money services businesses’ (MSBs) to register with FinCEN. 31 C.F.R. § 1022.380(a)(1).” *United States v. Harmon*, 474 F. Supp. 3d 76, 102 (D.D.C. 2020).

¹³⁴ *Infra* note 144, § 5330(d)(1) (2018) (This is the result of the BSA’s amendment, which is § 6102(2)(A) of the AML Act).

¹³⁵ *Id.*

¹³⁶ *Id.*

¹³⁷ See *id.*

identify a category of MSB called money transmitter,¹³⁸ which refers to either “[a] person that provides money transmission services”¹³⁹ or “[a]ny other person engaged in the transfer of funds.”¹⁴⁰ Specifically, “[t]he term ‘money transmission services’ means the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.”¹⁴¹ Here, the term “by any means” shows that the means for acceptance and transmission “includes, but is not limited to, through a financial agency or institution; a Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System, or both; an electronic funds transfer network; or an informal value transfer system.”¹⁴² Moreover, “currency” refers to “[t]he coin and paper money of the United States or of any other country that is designated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance.”¹⁴³

Yet, the BSA and its implementing regulations alone can hardly clarify the scope of the regulatory perimeter. This is because the BSA and its implementing regulations are silent about the meaning of the following three terms, which are “currency, funds, . . . [and] value that substitutes for currency.”¹⁴⁴ The analysis below clarifies how case law and FinCEN’s administrative guidance have interpreted them. While FinCEN clarified in 2019 that its guidance “does not establish any new regulatory expectations or requirements,”¹⁴⁵ it helps to understand FinCEN’s interpretation of the BSA and its implementing regulations.¹⁴⁶

¹³⁸ See *supra* note 124, § 1010.100(ff).

¹³⁹ *Id.* § 1010.100(ff)(5)(i)(A) (2023).

¹⁴⁰ *Id.* § 1010.100(ff)(5)(i)(B) (2023).

¹⁴¹ *Id.* § 1010.100(ff)(5)(i)(A) (2023).

¹⁴² *Id.*

¹⁴³ *Id.* § 1010.100(m) (2018).

¹⁴⁴ 31 U.S.C. § 5330(d)(1) (2018).

¹⁴⁵ U.S. DEPT OF THE TREASURY, *Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001, at 1 (May 9, 2019).

¹⁴⁶ See 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*, THE INT’L ACAD. OF FIN. CRIME LITIGATORS (Sept. 2023), at 5, 16.

1. Instrument: Funds

The analysis of the definition of funds has primarily been explored in the context of criminal prosecutions, specifically the applicability of 18 U.S.C. § 1960 and 18 U.S.C. § 1956 to Bitcoin, based on the following three reasons. First, 18 U.S.C. § 1960(b)(1)(B) punishes a regulatory offense¹⁴⁷ analogously to violations of the BSA's registration requirements.¹⁴⁸ Second, both 18 U.S.C. § 1956 and 18 U.S.C. § 1960 are under the same federal criminal statute against money laundering, and the term "fund" appears in both sections and the case law interpreting them. Third, the majority of case law pertaining to cryptocurrencies is about Bitcoin, and the reasoning of these cases supports the view that these decisions can be extended from Bitcoin to other categories of cryptocurrencies.

A number of lower court decisions have discussed the definition of "funds." In *United States v. Ulbricht*, the court held that Bitcoins constituted "funds" under 18 U.S.C. § 1956¹⁴⁹ through the reasoning that "'funds' can be used to pay for things in the colloquial sense"¹⁵⁰ and that "Bitcoins can be either used directly to pay for certain things or can act as a medium of exchange and be converted into a currency which can pay for things."¹⁵¹ In *United States v. Faiella*, the court held that "Bitcoin clearly qualifies as . . . 'funds'"¹⁵² under 18 U.S.C. § 1960 through the reasoning that "Bitcoin can be easily purchased in exchange for ordinary currency, acts as a denominator of value, and is used to conduct financial transactions."¹⁵³ In *United States v. Murgio*, the court held that Bitcoins are funds under 18 U.S.C. § 1960¹⁵⁴ through the reasoning that "Bitcoins can be accepted 'as a payment for goods and services' or bought 'directly from an exchange with [a] bank account'"¹⁵⁵ and therefore "function as 'pecuniary resources' and are 'used as a medium of exchange' and 'a means of payment.'"¹⁵⁶

¹⁴⁷ See 18 U.S.C. § 1960(b)(1)(B) (2006).

¹⁴⁸ See Courtney J. Linn, *One-Hour Money Laundering: Prosecuting Unlicensed Money Transmitting Businesses under 18 U.S.C. 1960*, 8 U.C. DAVIS BUS. L.J. 137, 139 (2007).

¹⁴⁹ See *United States v. Ulbricht*, 31 F.Supp.3d 540, 570 (S.D.N.Y. 2014).

¹⁵⁰ *Id.*

¹⁵¹ *Id.*

¹⁵² *United States v. Faiella*, 39 F.Supp.3d 544, 545 (S.D.N.Y. 2014).

¹⁵³ *Id.*

¹⁵⁴ See *United States v. Murgio*, 209 F. Supp. 3d 698, 707 (S.D.N.Y. 2016).

¹⁵⁵ *Id.* (quoting *Getting Started with Bitcoin*, Bitcoin, <https://perma.cc/62XD-D4H7> (last visited Sept. 16, 2016)).

¹⁵⁶ *Id.*

In *United States v. Mansy*, the court held that Bitcoin qualified as “money” or “funds” through the reasoning in *Murgio*,¹⁵⁷ *Faiella*,¹⁵⁸ *Ulbricht*,¹⁵⁹ and *United States v. E-Gold, Ltd.*¹⁶⁰ explained below.¹⁶¹ In *United States v. Stetkiw*, the court held that “Bitcoin qualifies as ‘money’ and ‘funds’ under § 1960”¹⁶² based on “the reasoning in *Murgio* and *Faiella*.”¹⁶³ Clearly, courts think that the term “funds” describes a medium of exchange.¹⁶⁴ Therefore, if Bitcoins can act as a medium of exchange,¹⁶⁵ then they would qualify as funds.¹⁶⁶

The first federal appellate court to substantively explore the issue of whether Bitcoin qualifies as “funds” was the Sixth Circuit, even though the Eleventh Circuit had already explained in *United States v. Decker* that by the time of 2020 “no court has adopted” the argument that 18 U.S.C. § 1956 “does not encompass financial transactions in cryptocurrency.”¹⁶⁷ In 2022, in *United States v. Iossifov*, the Sixth Circuit explained that “[t]he ordinary meaning of ‘funds[]’ . . . is ‘available pecuniary resources,’ which essentially means, ‘something generally accepted as a medium of exchange, a measure of value, or a means of payment.’”¹⁶⁸ The court further explained that “the term ‘funds’ encompasses any currency that can be used to pay for things”¹⁶⁹ and held that “Bitcoin qualifies as ‘funds’ because it ‘is often used [to] pay for things, and it may sometimes be used as a medium of exchange that is subsequently converted to currency to pay for things.’”¹⁷⁰ Incidentally, the fact that the price of Bitcoin in “2021 . . .

¹⁵⁷ See *supra* note 154.

¹⁵⁸ See *supra* note 152.

¹⁵⁹ See *supra* note 149.

¹⁶⁰ See *United States v. E-Gold, Ltd.*, 550 F.Supp.2d 82 (D.D.C. 2008).

¹⁶¹ See *United States v. Mansy*, No. 2:15-cr-198, 2017 WL 9672554, at *1 (D. Me. May 11, 2017).

¹⁶² *United States v. Stetkiw*, No. 18-20579, 2019 WL 417404, at *2 (E.D. Mich. Feb. 1, 2019).

¹⁶³ *Id.*; see also *supra* note 154 (quoting *United States v. Faiella*, 39 F. Supp. 3d 544, 545 (S.D.N.Y. 2014)); *supra* note 161.

¹⁶⁴ See *infra* note 168, at 913–14; see also *supra* note 149.

¹⁶⁵ See *infra* note 168, at 914; see also *supra* note 149; *supra* note 152; *supra* note 154 (quoting *Getting Started With Bitcoin*, <https://perma.cc/62XD-D4H7> (last visited Sept. 16, 2016)); *supra* note 161; see also *supra* note 162.

¹⁶⁶ See *infra* note 168, at 914; see also *supra* note 149; *supra* note 152; *supra* note 154 (quoting *Getting Started With Bitcoin*, <https://perma.cc/62XD-D4H7> (last visited Sept. 16, 2016)); *supra* note 161; *supra* note 162.

¹⁶⁷ *United States v. Decker*, 832 Fed. Appx. 639, 650 n.7 (11th Cir. 2020).

¹⁶⁸ *United States v. Iossifov*, 45 F.4th 899, 913 (6th Cir. 2022) (quoting *United States v. Stetkiw*, No. 18-20579, 2019 WL 417404, at *2 (E.D. Mich. Feb. 1, 2019)).

¹⁶⁹ *Id.* at 913–14.

¹⁷⁰ *Id.* at 914.

climb[ed] as high as \$68,990 . . . [b]ut . . . bounced stubbornly around \$20,000”¹⁷¹ in 2022 shows its high volatility. This is consistent with the fact that the Sixth Circuit held that Bitcoin qualifies as funds because it qualified as a means of payment and a medium of exchange while remaining silent about whether Bitcoin qualifies as a measure of value.¹⁷²

It is worth noting that the Sixth Circuit also acknowledged in its reasoning that “while the terms ‘monetary instrument’ and ‘funds’ are not defined within the money laundering statute, courts that have addressed this question have unanimously determined that Bitcoin falls under those terms.”¹⁷³

Furthermore, it is reasonable to infer from this summary that other categories of cryptocurrencies may also qualify as funds as long as they qualify as either a means of payment or a medium of exchange,¹⁷⁴ consistent with the outcome in the following two cases in which the court held that cryptocurrencies other than Bitcoin qualified as funds. In *United States v. Budovsky*, the court held that the virtual currency called LR qualifies as funds by citing its own reasoning in *United States v. Faiella*.¹⁷⁵ In *United States v. E-Gold, Ltd.*, the court held that the defendant, an issuer of a type of digital currency known as “e-gold,” violated 18 U.S.C. § 1960¹⁷⁶ because the transmission of funds can be made by any means, which may include but are not limited to cash, currency, check, or wire;¹⁷⁷ therefore, “a ‘money transmitting service’ includes not only a transmission of actual currency, but also a transmission of the value of that currency through some other medium of exchange.”¹⁷⁸

2. Instrument: Value that Substitutes for Currency

Even if the *instruments* being transmitted qualify neither as currency nor funds, the registration requirements may still apply if the instruments being transmitted have “value that substitutes

¹⁷¹ Ryan Browne & Arjun Kharpal, *Bitcoin’s Trading Has Become ‘Boring’ — But That’s Not Necessarily a Bad Thing*, CNBC (Oct. 30, 2022), <https://perma.cc/RPT4-AHFB>.

¹⁷² See *supra* note 168, at 914.

¹⁷³ See *id.* at 913.

¹⁷⁴ See *supra* note 168, at 913–14; see also *supra* note 149.

¹⁷⁵ See *United States v. Budovsky*, No. 13-cr-368 DLC, 2015 WL 5602853, at *14 (S.D.N.Y. Sept. 23, 2015) (citing *United States v. Faiella*, 39 F.Supp.3d 544, 545 (S.D.N.Y. 2014)).

¹⁷⁶ See *supra* note 160, at 89–97 (D.D.C. 2008).

¹⁷⁷ See *id.* at 94.

¹⁷⁸ *Id.*

for currency.”¹⁷⁹ An analysis of FinCEN’s Guidance in 2019 helps to understand the definition of such value.¹⁸⁰ While FinCEN’s Guidance is not legally binding, it does illustrate FinCEN’s attitude toward activities involving cryptocurrencies based on its regulations.¹⁸¹

In 2019, FinCEN released a Guidance in which it explained that “value that substitutes for currency”¹⁸² could be created “either (a) specifically for the purpose of being used as a currency substitute or (b) originally for another purpose but then repurposed to be used as a currency substitute by an administrator (in centralized payment systems) or an unincorporated organization, such as a software agency (in decentralized payment systems).”¹⁸³ The Guidance also mentioned that “[i]n either case, the persons involved in the creation and subsequent distribution of the value (either for the original purpose or for another purpose) may be subject to additional regulatory frameworks (other than the BSA).”¹⁸⁴ Moreover, “the person may be exempted from MSB status but be covered as a different type of financial institution under FinCEN regulations.”¹⁸⁵ Furthermore, the Guidance specified that “convertible virtual currency (CVC),”¹⁸⁶ which includes digital currency, cryptocurrency, cryptoasset, digital asset, etc.,¹⁸⁷ was “a type of virtual currency that either ha[d] an equivalent value as currency, or act[ed] as a substitute for currency, and [wa]s therefore a type of ‘value that substitutes for currency.’”¹⁸⁸

Based on FinCEN’s interpretation of the BSA’s statutory language, “funds” and “value that substitutes for currency” are interchangeable in determining the nature of Bitcoin and cryptocurrencies at large. FinCEN has been silent about the implication of this interchangeability. Certainly, it offers FinCEN flexibility in broadening the scope of the regulatory perimeter of the BSA and its implementing regulations instead of limiting it to specific instruments.

¹⁷⁹ *Supra* note 144, § 5330(d)(1) (2018).

¹⁸⁰ *See id.*

¹⁸¹ *See supra* note 146, at 5.

¹⁸² *Supra* note 144, § 5330(d)(1) (2018).

¹⁸³ *Supra* note 145, at 4.

¹⁸⁴ *Id.*

¹⁸⁵ *Id.*

¹⁸⁶ *Id.* at 7.

¹⁸⁷ *See id.*

¹⁸⁸ *Id.*

3. Activity: Transmission

Transmission is the key to understanding the definition of money transmitting business and MSB and, therefore, the accurate scope of the regulatory perimeter of the BSA's registration requirements. Unlike the relationship between cryptocurrency and money, the bewildering variety and complexity of cryptocurrency products created a less obvious question of whether and how the services they offer could fit into the definition of transmission. Therefore, the definition of transmission is another key to drawing a line for distinguishing whether a service provider must register with FinCEN.

a. Money Transmission

The term 'money transmission services' includes both "the *acceptance* of currency, funds, or other value that substitutes for currency from one person *and* the *transmission* of currency, funds, or other value that substitutes for currency to another location or person by any means,"¹⁸⁹ unless there are applicable limitations or exemptions.¹⁹⁰ Therefore, acceptance and transmission must both occur.¹⁹¹ If one of them, or both of them, cannot be identified, then a business is not a money transmitter and, therefore, does not fall within the scope of the regulatory perimeter of the BSA's registration requirements. Additionally, there must be an intermediary that accepts "currency, funds, or other value that substitutes for currency"¹⁹² and transmits "currency, funds, or other value that substitutes for currency to another location or person by any means."¹⁹³ It is such an intermediary that qualifies as a money transmitter.

Prior to releasing its Guidance in 2019, FinCEN had already released its first Guidance regarding cryptocurrencies in 2013.¹⁹⁴ Regarding the definition of "transmission," the 2013 Guidance explained the definition of money transmission in detail through two major parts.¹⁹⁵ The first part discussed the transmission of

¹⁸⁹ *Supra* note 124, § 1010.100(ff)(5)(i)(A) (2023).

¹⁹⁰ It is worth noting that the BSA's implementing regulations enumerated six circumstances in which a person is not a money transmitter. *See id.*, § 1010.100(ff)(5)(ii) (2023).

¹⁹¹ *See supra* note 124, § 1010.100(ff)(5)(i)(A) (2023).

¹⁹² *Id.*

¹⁹³ *Id.*

¹⁹⁴ *See* U.S. DEP'T OF THE TREASURY, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001, at 1 (Mar. 18, 2013).

¹⁹⁵ *See id.* at 4–5.

centralized virtual currency,¹⁹⁶ and the second part discussed the transmission of decentralized virtual currency.¹⁹⁷ In the first part, the Guidance explained that transmission through a money transmitter “that has a centralized repository . . . may take one of two forms.”¹⁹⁸

The first form of transmission refers to “transmission to another *location*, namely from the user’s account at one location (e.g., a user’s real currency account at a bank) to the user’s convertible virtual currency account with the administrator.”¹⁹⁹ Here, “FinCEN interpret[ed] the term ‘another location’ broadly.”²⁰⁰ According to FinCEN, in this process, “an exchanger (acting as a ‘seller’ of the convertible virtual currency) . . . accepts real currency or its equivalent from a user (the ‘purchaser’) and transmits the value of that real currency to fund the user’s convertible virtual currency account with the administrator.”²⁰¹

The second form of transmission refers to “transmission to another *person*, namely each third party to which transmissions are made at the user’s direction.”²⁰² In this process, an “*exchanger* accepts currency or its equivalent from a user and privately credits the user with an appropriate portion of the exchanger’s own convertible virtual currency held with the administrator of the repository. The *exchanger* then transmits that internally credited value to third parties at the user’s direction.”²⁰³ In the second part, the Guidance discussed two forms of transmission, which are (1) creating “units of convertible virtual currency and sell[ing] those units to another person for real currency or its equivalent”²⁰⁴ and (2) “accept[ing] . . . de-centralized convertible virtual currency from one person and transmit[ing] it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency.”²⁰⁵ FinCEN’s Guidance in 2019 confirmed the clarification in FinCEN’s Guidance in 2013.²⁰⁶

Case law is consistent with FinCEN’s view in its Guidance. In *United States v. Stetkiw*, the court held that the defendant’s

¹⁹⁶ See *id.* at 4.

¹⁹⁷ See *id.* at 5.

¹⁹⁸ *Id.* at 4.

¹⁹⁹ *Id.*

²⁰⁰ *Id.* at 13.

²⁰¹ *Id.* at 4.

²⁰² *Id.* at 5.

²⁰³ *Id.* at 4–5.

²⁰⁴ *Id.* at 5.

²⁰⁵ *Id.*

²⁰⁶ See *supra* note 145, at 13–14.

“transfer of Bitcoin to . . . [other] virtual accounts . . . constitutes money transmitting”²⁰⁷ because the transfers were transmissions of funds to another location.²⁰⁸ In *United States v. Harmon*, the court held that the defendant, who operated “Helix, an underground tumbler for bitcoin,”²⁰⁹ had “satisfie[d] the definition of ‘unlicensed money transmitting business’ at § 1960(b)(1)(B) because Helix’s core business was receiving bitcoin and transmitting that bitcoin to another location or person.”²¹⁰ It is worth noting that the court in *Harmon* also held that the Bitcoin blockchain was not a single location and, therefore, transfer between addresses on the blockchain was transmission between different locations.²¹¹

b. Exemption

There are six categories of statutory exemption in the BSA’s implementing regulations regardless of whether or not a business qualifies as a money transmitting business,²¹² including those that merely “[p]rovide[] the delivery, communication, or network access services used by a money transmitter to support money transmission services.”²¹³

Consistent with its 2013 Guidance,²¹⁴ in one of its Administrative Rulings in 2014, FinCEN established that cryptocurrency miners are not money transmitters as long as they use cryptocurrencies “solely for . . . [their] own purposes and not for the benefit of another . . . because these activities involve neither ‘acceptance’ nor ‘transmission’ of the convertible virtual currency.”²¹⁵

C. Cryptocurrency Non-Custodial Service Providers do not fall Within the Scope of the Regulatory Perimeter of the BSA

So far, Part II has described how the scope of the regulatory perimeter of the BSA’s registration requirements has sought to cover some components of the highly sophisticated network of cryptocurrency payments. Cryptocurrency non-custodial service providers do not fall within the scope of the regulatory perimeter

²⁰⁷ *Supra* note 162.

²⁰⁸ *See id.*

²⁰⁹ *Supra* note 134, at 80.

²¹⁰ *Id.* at 109.

²¹¹ *See id.*

²¹² *See supra* note 124, § 1010.100(ff)(5)(ii).

²¹³ *Supra* note 124, § 1010.100(ff)(5)(ii)(A).

²¹⁴ *See supra* note 194, at 5.

²¹⁵ *See* U.S. DEP’T OF THE TREASURY, *Application of FinCEN’s Regulations to Virtual Currency Mining Operations*, FIN-2014-R001, at 3 (Jan. 30, 2014).

of the BSA due to the following two reasons. First, they are not within the BSA's list of financial institutions. Second, they do not accept and transmit cryptocurrencies and, therefore, are not money transmitting businesses.

Specifically, DEXs and non-custodial mixers fall outside of the scope since they do not accept and transmit cryptocurrency simultaneously. FinCEN's Guidance in 2019 confirmed that if a DEX "only provides a forum where buyers and sellers of CVC post their bids and offers (with or without automatic matching of counterparties), and the parties themselves settle any matched transactions through an outside venue (either through individual wallets or other wallets not hosted by the trading platform)," ²¹⁶ then it would fall within one of the statutory exemptions of the BSA's implementing regulations and, ²¹⁷ therefore, are not money transmitters. ²¹⁸ The same reason would be applicable to non-custodial mixers due to their business model explained in Part I. Additionally, FinCEN's 2019 Guidance confirmed that service providers of both singlesig and multisig unhosted wallets do not qualify as money transmitting businesses since they do not accept and transmit cryptocurrency. ²¹⁹

III. NOT REGULATING CRYPTOCURRENCY NON-CUSTODIAL SERVICE PROVIDERS IS INCONSISTENT WITH THE BSA'S CONTROL-BASED PRINCIPLE AS THEIR CONTROLLING POWER OVER PAYMENT ASSET EXISTS ON A SPECTRUM RATHER THAN IN A BINARY

While Part II concluded that cryptocurrency non-custodial service providers do not fall within the scope of the regulatory perimeter of the BSA, Part III argues that this should not be the case. This argument is based on a careful analysis of FinCEN's language in its 2019 Guidance. In the section explaining whether singlesig and multisig wallets would qualify as money transmitting businesses, the Guidance offered four criteria to determine whether a player truly accepts and transmits cryptocurrencies. According to the Guidance:

[t]he regulatory treatment of such intermediaries depends on four criteria: (a) who owns the value; (b) where the value is stored; (c) whether the owner interacts directly with the

²¹⁶ *Supra* note 145, at 24.

²¹⁷ *See supra* note 124, § 1010.100(ff)(5)(ii)(A).

²¹⁸ *See supra* note 145, at 24.

²¹⁹ *See supra* note 145, at 16–17.

payment system where the CVC runs; and, (d) whether the person acting as intermediary has total independent control over the value.²²⁰

The Guidance explicitly confirmed that the four criteria are applicable to “persons that act as intermediaries between the owner of the value and the value itself [in a manner that] is not technology-dependent,”²²¹ “*regardless of the label the person applies to itself or its activities.*”²²² Therefore, the four criteria are applicable to unhosted wallets, DEXs, non-custodial mixers, and any other technological and institutional players of cryptocurrency payments.²²³ The Guidance’s four criteria fall into the following three dimensions,²²⁴ namely (1) clearing and settlement,²²⁵ (2) asset ownership, custody, and balance sheet recording,²²⁶ and (3) governance mechanism that influences a provider’s controlling power over customers’ payment assets.²²⁷ Based on these four criteria, the Guidance seeks to determine whether a player truly accepts and transmits cryptocurrencies. In fact, the BSA, its implementing regulations, case law, and FinCEN’s other materials all remain silent about the definition of acceptance and transmission, which appears to be clear but is actually ambiguous. Therefore, these four criteria remain the only available source to interpret the definition of acceptance and transmission.

Yet, the Guidance lacks a guiding principle explaining the manner of applying the four criteria. It only clarified that these four criteria would be applicable to all categories of players and offered examples of how it applies these four criteria to determine whether singlesig and multisig wallets qualify as money transmitting businesses. Without a guiding principle from FinCEN concerning the manner of applying the four criteria, the manner of their application remains ambiguous.

²²⁰ *Supra* note 145, at 15.

²²¹ *Id.*

²²² *Id.*, at 17.

²²³ *See id.*

²²⁴ *See id.* at 15.

²²⁵ *See, e.g.*, Francesca Carapella, Edward Dumas, Jacob Gerszten, Nathan Swem, & Larry Wall, *Decentralized Finance (DeFi): Transformative Potential & Associated Risks*, FIN. AND ECON. DISCUSSION SERIES FED. RES. BOARD, WASH., D.C. (June 2022), at 4; *see also id.*

²²⁶ *See, e.g., infra* note 235, at 22.

²²⁷ *See, e.g., id.; see also, e.g.*, Sirio Aramonte, Wenqian Huang, & Andreas Schrimpf, *DeFi Risks and the Decentralisation Illusion*, BIS Q. REV. 21 (Dec. 2021); Ashish Rajendra Sai et al., *Taxonomy of Centralization in Public Blockchain Systems: A Systematic Literature Review*, 58 INFO. PROCESSING & MGMT., at 25 (2021); Arthur Gervais et al., *Is Bitcoin a Decentralized Currency?*, 12 IEEE SEC. & PRIV. 54, 60 (2014).

In response to the ambiguity, Part III argues that measuring their collective degree of control entails consideration of the various dimensions of cryptocurrency non-custodial service providers' controlling power over payment assets. Based on the Guidance's regulatory treatment of singlesig and multisig wallets, Part III argues that each of the four criteria does not always exist in the binary. Based on the non-binary nature of controlling power, Part III also argues that the more dimensions to which a player's control extends, the more likely it would qualify as a money transmitting business, and the more suitable the BSA's substantive obligations will be. As a number of empirical studies have already shown that the degree of power concentration in DAOs' governance is high,²²⁸ these findings could potentially challenge FinCEN's conclusion that DEXs, non-custodial wallets, and unhosted wallets are outside of the scope of the regulatory perimeter of the BSA.

To do so, Part III first analyzes the BSA's control-based principle through FinCEN's 2019 Guidance, which serves as the basis for determining whether a business truly qualifies as a money transmitting business. Part III then explains that cryptocurrency non-custodial service providers could maintain a certain degree of controlling power over payment assets in one or more of the three dimensions. First, the mechanism of payment clearing and settlement. Second, the mechanism of custody and ownership of payment assets, and the recording of payment assets into its balance sheet. Third, the governance mechanism. Accordingly, the controlling power each cryptocurrency non-custodial service provider has over payment assets differs depending on its business model, and such a controlling power would exist on a spectrum rather than in a binary. Part III concludes that because the BSA's current definition of money transmitting business merely focuses

²²⁸ See, e.g., Stefan Kitzler, Stefano Ballestti, Pietro Saggese, Bernhard Haslhofer, & Markus Strohmaier, *The Governance of Decentralized Autonomous Organizations: A Study of Contributors' Influence, Networks, and Shifts in Voting Power*, ARXIV:2309.14232 (CS.SI) (Sept. 2023), <https://perma.cc/KT85-Z9C2>; see also Xiaotong Sun, Charalampos Stasinakis & Georgios Sermpinis, *Decentralization Illusion in Decentralized Finance: Evidence from Tokenized Voting in MakerDAO polls*, ARXIV:2203.16612 (CS) (Mar. 2023), <https://perma.cc/D6NJ-ADLK>; Xuan Liu, *The Illusion of Democracy? An Empirical Study of DAO Governance and Voting Behavior* (June 2024), <https://perma.cc/59E6-U2BN>; Maury Shenk, Sven Van Kerckhoven, & Jonas Weinberger, *The Crown, the Market and the DAO*, 6 STAN. J. BLOCKCHAIN L. & POL'Y 244, 258 (June 2023); Robin Fritsch, Marino Müller, & Roger Wattenhofer, *Analyzing Voting Power in Decentralized Governance: Who Controls DAOs?*, ARXIV:2204.01176 (Apr. 2022), <https://perma.cc/2R85-HVX7>; Sirio Aramonte, Wenqian Huang, & Andreas Schrimpf, *DeFi Risks and the Decentralisation Illusion*, BIS Q. REV., Dec. 2021; *infra* note 236, at 22.

on the second dimension, namely asset custody, it is unable to adequately measure the degree of control a cryptocurrency non-custodial service provider has over payment assets.

A. Cryptocurrency Non-Custodial Service Providers' Three Dimensions of Controlling Power over Payment Assets

1. The First Dimension: Clearing and Settlement

One of the important dimensions of such a controlling power, about which the BSA did not specifically mention, is the ability to *clear and settle* payments due to the following two reasons. This is the third criterion in FinCEN's Guidance in 2019.²²⁹ First, control manifests itself largely in payment settlement since only settlement involves the actual transfer of value. Second, clearing manifests identical significance since it is the process of verifying the sufficiency of payment assets and gas fees.

Under the collective clearing and self-settlement model based on atomic settlement,²³⁰ customers clear and settle payments by directly interacting with blockchains' miners/validators through their unhosted wallets. Such an interaction could refer to a customer's submission of a full and valid cryptographic digital signature to a blockchain so that in each payment a selected miner or validator therein would clear and settle it.²³¹ DEXs, singlesig unhosted wallets, and non-custodial mixers themselves do not interact with miners and validators to initiate payment clearing and settlement. It should be noted that unhosted wallets' and DEXs' underlying smart contracts would not allow their customers to interact with miners/validators if their customers' unhosted wallets are insufficiently funded for payment assets and gas fees.²³² Although it seems that these smart contracts took part in the clearing process by verifying that customers' unhosted wallets are sufficiently funded, that is incorrect. As such a process happens

²²⁹ See *supra* note 145, at 15.

²³⁰ See Hossein Nabilou, *Probabilistic Settlement Finality in Proof-of-Work Blockchains: Legal Considerations*, 7 BUS. & FIN. L. REV. 139, 155 (2022); see also Michael Lee, Antoine Martin, & Benjamin Müller, *What Is Atomic Settlement?*, FED. RES. BANK OF N.Y. (Nov. 7, 2022), <https://perma.cc/M5AY-FMV2>; see also Holger Neuhaus & Mirjam Plooi, *Central Bank Money Settlement of Wholesale Transactions in the Face of Technological Innovation*, ECB ECON. BULL. (Aug. 2023), <https://perma.cc/Q3MC-AW6U>.

²³¹ See ANDREAS M. ANTONOPOULOS & DAVID A. HARDING, *MASTERING BITCOIN: PROGRAMMING THE OPEN BLOCKCHAIN* 184–85 (3d ed. 2023); see also ANDREAS M. ANTONOPOULOS & DR. GAVIN WOOD, *MASTERING ETHEREUM: BUILDING SMART CONTRACTS AND DAPPS* 1115–16 (2018).

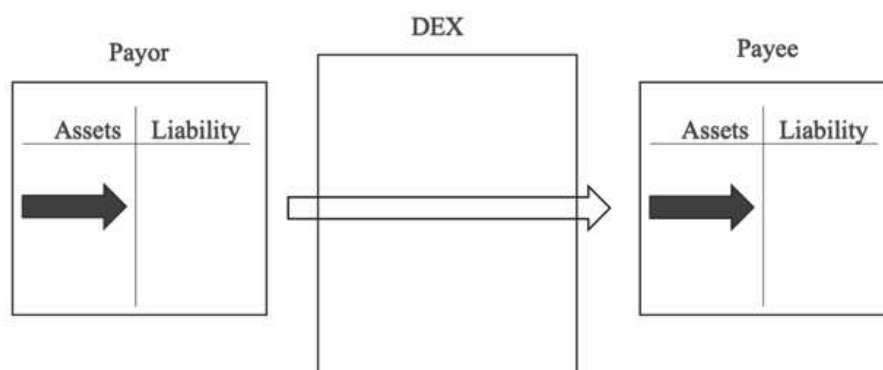
²³² See *supra* note 102.

before the order is submitted to the blockchain, it happens off-chain, namely within the unhosted wallet or DEX application and, therefore, will not leave any record in the blockchain. Only after these smart contracts have verified that these unhosted wallets are sufficiently funded will they submit the payment or swap orders to the blockchains where miners/validators would complete the clearing and settlement processes.

2. The Second Dimension: Ownership, Control, and Balance Sheet

The second criterion requires an analysis of the custody status of payment assets, specifically the design of private key management mechanisms and the status of these private keys.²³³ As explained in Parts I and II, DEXs allow their customers to maintain full control over the cryptocurrency they own.²³⁴ Therefore, DEXs' balance sheets do not incorporate customers' accounts, and swapping cryptocurrencies through DEXs would only change the balance sheets of payors and payees.²³⁵

Figure 1: Payor's and Payee's Balance Sheets



3. The Third Dimension: Governance

To comply with the BSA's substantive obligations, the boards or equivalent senior management committees of covered businesses, such as CEXs, must constantly exercise residual controls

²³³ See *supra* note 145, at 15.

²³⁴ See, e.g., *How to Connect a Wallet to Uniswap*, UNISWAP (Feb. 2024), <https://perma.cc/8ATU-VNCL>; see also Antonio Juliano, *How Do I Create an Account or Sign Up?*, DYDX (Oct. 2024), <https://perma.cc/8ZM4-ANP3>.

²³⁵ See Tech. Advisory Comm. (TAC) of the U.S. Commodity Futures Trading Comm'n, *Decentralized Finance: Report of the Subcommittee on Digital AI Assets and Blockchain Technology* 22 (2024).

over business decisions, a top-down approach to governance. In this capacity, governance refers to the exercise of human residual controls over business decisions. The specific approach that each intermediary undertakes to comply with the BSA's substantive obligations may uniquely differ from one another depending on the governance decisions. Yet, those with controlling power must exercise their governance power to comply with the BSA.

Nevertheless, cryptocurrency non-custodial service providers do not necessarily incorporate any boards or equivalent senior management committees. These players include DEXs and mixers, which are software protocols based on permissionless blockchains supported by smart contracts, meaning that no human personnel, including compliance officers, may exist to support their business operations.²³⁶ Smart contracts are code-based programs that may automatically carry out a function when one or more of an agreement's predetermined conditions are met, such as the exchange rate for crypto-to-crypto exchanges.²³⁷ The design and operation of these smart contracts could potentially be subject to the governance of decentralized autonomous organizations (DAOs).

a. Introduction to Decentralized Autonomous Organizations (DAOs)

A decentralized autonomous organization (DAO) is essentially a smart contract-based computer program running on top of blockchains.²³⁸ DEXs' and mixers' protocols are subject to their underlying DAOs' residual controls over business decisions. A DAO's smart contract is the ultimate authority that determines

²³⁶ See Lindsay X. Lin, *Deconstructing Decentralized Exchanges*, 2 STAN. J. BLOCKCHAIN L. & POL'Y 58, 58 (2019); see also *supra* note 95.

²³⁷ For discussions of smart contract, see Nick Szabo, *The Idea of Smart Contracts*, PHONETIC SCI., AMSTERDAM (1997), <https://perma.cc/9BKQ-QVGL>; see also Stuart D. Levi & Alex B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, HARV. L. SCH. F. ON CORP. GOVERNANCE (May 26, 2018), <https://perma.cc/6S42-3W2A>; Françoise Birnholz & Kelsey Barthold, *Back to the Future: Sorting Old Law from New Technology in Blockchain Smart Contract Applications & Assessing the Need for Regulation*, 89 GEO. WASH. L. REV. ARGUENDO 96 (2021); *What Is A Smart Contract?*, ETHEREUM (Apr. 22, 2024), <https://perma.cc/W727-PQKV>; Paul Wackerrow et al., *Introduction to Smart Contracts*, ETHEREUM (Apr. 22, 2024), <https://perma.cc/Y58A-AFZT>.

²³⁸ See Maury Shenk, Sven Van Kerckhoven, & Jonas Weinberger, *The Crown, the Market and the DAO*, 6 STAN. J. BLOCKCHAIN L. & POL'Y 244, 244–45 (2023); see also Pierluigi Matera, *Delaware's Dominance, Wyoming's Dare: New Challenge, Same Outcome?*, 27 FORDHAM J. CORP. & FIN. L. 73, 130 (2022).

its operation.²³⁹ Based on the smart contract, members of a DAO are entitled to propose new proposals regarding the operation of DEXs or mixers and to vote in a binary scheme to approve or disapprove them,²⁴⁰ such as the implementation of protocol fees.²⁴¹

The smart contract of a DAO typically determines each member's voting power based on one of the following two mechanisms: governance token-based or share-based voting. Share-based voting mechanism remains less well-known, and it restricts access to members only.²⁴²

Governance-token DAOs, such as MakerDAO, determine each member's voting power based on each member's account balance of governance token.²⁴³ Governance tokens, a category of cryptocurrency, allow their holders to propose and vote for or against changes to protocols, thereby potentially influencing a project's governance mechanism.²⁴⁴ The manner of distributing governance tokens varies, which may include initial coin offerings (ICOs) for fundraising, rewards for staking, and exchanging at DEXs.²⁴⁵ For example, at early stages, their developing teams may transfer governance power to DAOs by burning their admin keys.²⁴⁶ In this capacity, DAOs are the functional equivalents of

²³⁹ See Aaron Wright, *The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges*, STAN. J. BLOCKCHAIN L. & POL'Y 152, 155 (2021).

²⁴⁰ See FINANCIAL ACTION TASK FORCE (FATF), GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS 27 (2019), <https://perma.cc/PZ2P-GJBU>.

²⁴¹ See GFX Labs, *Making Protocol Fees Operational*, UNISWAP, (May 10, 2023), <https://perma.cc/VCE7-82EQ>.

²⁴² See, e.g., Ameen Soleimani et al., *The Moloch DAO: Beating the Tragedy of the Commons using Decentralized Autonomous Organizations DRAFT v1.0*, MOLOCH DAO 4, <https://perma.cc/9MJL-ESEW>.

²⁴³ See *Maker Governance Voting Portal*, MAKERDAO, <https://perma.cc/V4S8-4LUP>.

²⁴⁴ See, e.g., Sirio Aramonte, Wenqian Huang, & Andreas Schrimpf, *DeFi Risks and the Decentralisation Illusion*, BIS Q. REV. (Dec. 2021); see also *infra* note 236, at 22; Xiaotong Sun, Charalampos Stasinakis, & Georgios Sermpinis, *Decentralization Illusion in Decentralized Finance: Evidence from Tokenized Voting in MakerDAO polls*, ARXIV:2203.16612 (CS) (Mar. 2023), <https://perma.cc/D6NJ-ADLK>; Xuan Liu, *The Illusion of Democracy? An Empirical Study of DAO Governance and Voting Behavior* (June 2024), <https://perma.cc/59E6-U2BN>; THE MAKER PROTOCOL: MAKERDAO'S MULTI-COLLATERAL DAI (MCD) SYSTEM, MAKERDAO 1 (2014); Chris Brummer, *Disclosure, Dapps and DeFi*, 5 STAN. J. BLOCKCHAIN L. & POL'Y 137, 143 (2022); Matthias Nadler & Fabian Schär, *Decentralized Finance, Centralized Ownership? An Iterative Mapping Process to Measure Protocol Token Distribution*, ARXIV PREPRINT ARXIV:2012.09306 1 (Dec. 2020).

²⁴⁵ See Jonathan Rohr & Aaron Wright, *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, 70 HASTINGS L.J. 463, 475 (2019); see also Chris Brummer, *Disclosure, Dapps and DeFi*, 5 STAN. J. BLOCKCHAIN L. & POL'Y 137, 156 (2022).

²⁴⁶ See Max Parasol, *Enforcing Persistent "Smart Contracts": Admin Keys and the Myth of Decentralized Finance?*, 24 N.C. J.L. & TECH. 67, 106 (2023); see generally Denise Garcia Ocampo, Nicola Branzoli & Luca Cusmanol, *FSI Insights on Policy Implementation*

the boards or senior management committees of financial institutions or money transmitting businesses.

In theory, DAOs are supposedly operating with a low degree of power concentration. This means that no centralized decision-making body would govern DEXs and/or mixers as the functional equivalent of covered businesses' boards or equivalent senior management committees, showing a bottom-up approach to governance through DAOs. Yet, in practice, the governance of DAOs is not free from human interventions due to voting power concentration. Moreover, a project's developing team could also surpass its DAO and exercise human intervention through admin key, bug fixing, kill switch, and/or backdoor.

b. Cryptocurrency Non-Custodial Service Providers' Governance Through DAOs

Based on ownership, custody, the ability to interact with blockchains to initiate payment clearing and settlement, and even the ability to directly clear and settle payment off of blockchains, a player would have a high degree of control over payment assets. Yet, a cryptocurrency non-custodial service provider's governance mechanism, in addition to the first, second, and third criterion, is crucial to determine whether a player has total independent control over payment assets. For example, by maintaining private keys, customers of singlesig hosted wallets could retain the ownership, custody, and ability to submit cryptographic digital signatures to blockchains. However, in theory, a DAO could propose to update the smart contract that controls the wallets. Some wallet users might not be able to vote on such a proposal because they have no government tokens or because they are disinterested. If a DAO successfully passed a proposal through voting, aiming to convert a singlesig wallet service provider into a multisig wallet service provider, then customers of these multisig wallets, which were previously singlesig, would lose control over the payment assets.

(1) Human Intervention Through Voting Power Concentration

Members of DAOs could exercise their voting power to collectively make governance decisions. DAOs make governance decisions through share-based voting or governance token-based voting. Studies and data concerning share-based DAOs are

extremely limited. Nevertheless, existing studies and data have shown that governance token-based voting is not free from the problems of voting power concentration and voter apathy.

(2) Human Intervention by the Developing Team

A project's developing team could also surpass its DAO and exercise human intervention in the following three scenarios.

In the first scenario, at least during the early stage of a project, its developing team could maintain an admin key that allows them to surpass the DAO and unilaterally make governance decisions.²⁴⁷ This seems to indicate that the project could turn into a completely self-executing program free from human intervention when the developing team burns the admin key, a claim the developers of Tornado Cash have made.²⁴⁸ Yet, the two additional scenarios below show that human intervention would still exist after the developing team burns admin keys, namely a kill switch and a backdoor.

The second scenario focuses on the possible malfunctioning of the blockchain's algorithm or the embedded smart contract. Computer code, such as Blockchain protocols and smart contracts, is hardly free from bugs, which may result in system malfunction. The programmer(s) of a DAO's developing team could either fix the bugs or, under extreme circumstances, utilize a kill switch, a part of a specific smart contract that enables self-destruction of a specific part of, or the entirety of, the smart contract, to stop the smart contract from running.²⁴⁹ Depending on the design of each smart contract, invoking a kill switch could transfer all funds associated with the smart contract to the owner of the smart contract, prevent users from interacting with the smart contract in

²⁴⁷ See THE FINANCIAL STABILITY BOARD, ASSESSMENT OF RISKS TO FINANCIAL STABILITY FROM CRYPTO-ASSETS 17 (2022), <https://perma.cc/U2XM-UK6W>; see also Tomonori Yuyama, Ken Katayama, & Paul Brigner, *Proposal of Principles of DeFi Disclosure and Regulation*, in ALEKSANDER ESSEX ET AL. (EDS.), FINANCIAL CRYPTOGRAPHY AND DATA SECURITY FC 2023 INTERNATIONAL WORKSHOPS 141, 145 (2024).

²⁴⁸ See Max Parasol, *Enforcing Persistent "Smart Contracts": Admin Keys and the Myth of Decentralized Finance?*, 24 N.C. J.L. & TECH. 67, 106 (2023); see generally Denise Garcia Ocampo, Nicola Branzoli, & Luca Cusmanol, *FSI Insights on Policy Implementation No. 49 Crypto, Tokens and DeFi: Navigating the Regulatory Landscape*, BIS, at 32 n.101 (May 2023), <https://perma.cc/XPM4-5FGV>.

²⁴⁹ See SHAUN AGHILI, THE AUDITOR'S GUIDE TO BLOCKCHAIN TECHNOLOGY 31 (2022); see also Max Parasol, *Enforcing Persistent "Smart Contracts": Admin Keys and the Myth of Decentralized Finance?*, 24 N.C. J.L. & TECH. 67, 100 n.142 (2023); Alberto Maria Gambino & Andrea Stazi, *Contract Automation from Telematic Agreements to Smart Contracts*, 7 ITALIAN L.J. 97, 108 n.53 (2022).

the future, and keep the computer code in the blockchain.²⁵⁰ In either situation, human intervention regarding the operation of a DAO's smart contract would be possible.

In the third scenario, the development team may need to decide when and how to update the algorithm to account for changes in real-world legal requirements when coding the smart contract, namely a backdoor.²⁵¹ For example, a blockchain that facilitates money transmission may be programmed to collect user identification information to comply with the substantive obligations of the BSA, as well as other related regulatory requirements, such as the Treasury's Office of Foreign Assets Control's (OFAC) primary and secondary sanctions programs through the Specially Designated Nationals and Blocked Persons List (SDN List).²⁵² A crucial concern is whether a blockchain of such kind might remain current in the face of legislative changes. If not, human intervention would be necessary for the MSB behind it to stay in compliance with the BSA and the sanctions programs under OFAC.

B. The BSA's Current Design is Unable to Adequately Measure the Degree of Control a Cryptocurrency Non-Custodial Service Provider has over Payment Assets

Despite the four criteria's wide *applicability*, the Guidance did not provide any central rule illustrating the manner of applying each of these four criteria,²⁵³ such as a rule identifying which of the four is most important to determine whether a platform accepts and transmits cryptocurrency.²⁵⁴ The Guidance only provided four examples that show "[t]he regulatory treatment of each type of CVC wallet based on these factors,"²⁵⁵ which are hosted

²⁵⁰ See Nikos Fotiou & George C. Polyzos, *Smart Contracts for the Internet of Things: Opportunities and Challenges*, ARXIV:1901.10582 5 (Jan. 2019); see also SHAUN AGHILI, THE AUDITOR'S GUIDE TO BLOCKCHAIN TECHNOLOGY 31(2023).

²⁵¹ See Thibault Schrepel, *Collusion by Blockchain and Smart Contracts*, 33 HARV. J. L. & TECH. 117, 162 (2020); see also Jessica Bookout, Lauren Cimbol, Shannon Leigh Collins, & Devin L. Newman, *A Brief Introduction to Digital Art & Blockchain*, 37 CARDOZO ARTS & ENT. L.J. 553, 556 (2019); PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 184 (2018).

²⁵² See *Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists*, OFAC (Nov. 7, 2023), <https://perma.cc/ME7D-2B9P>.

²⁵³ See *supra* note 145, at 1-30.

²⁵⁴ But see *supra* note 146, at 8.

²⁵⁵ *Supra* note 145, at 15.

wallet,²⁵⁶ unhosted wallet,²⁵⁷ multisig unhosted wallet,²⁵⁸ and multisig hosted wallet.²⁵⁹

It is important to clarify that neither multisig unhosted wallet service providers nor owners alone could maintain complete control over payment assets and the process to initiate payment clearing and settlements. Both of them merely maintain some degree of control over payment assets and the process to initiate payment clearing and settlements due to the following two reasons.

First, the third criterion focuses on whether “the owner interacts with the wallet software and/or payment system to initiate a transaction, supplying part of the credentials required to access the value,”²⁶⁰ namely the first dimension of controlling power: clearing and settlement. As explained in Part I, neither an unhosted multiple-signature wallet service provider nor a wallet owner *alone* is able to initiate a payment.²⁶¹ In other words, neither on its own is able to submit a valid encrypted digital signature to blockchains so that a selected miner or validator could initiate payment clearing and settlement. An unhosted multiple-signature wallet service provider and a wallet owner must both exist to submit a full cryptographic digital signature to blockchains so that a selected miner or validator therein would clear and settle a payment. Therefore, they both retain some degree of control over the process to initiate payment clearing and settlements; not total control, but more than none at all.

Second, the fourth criterion focuses on whether “the person participating in the transaction to provide additional validation at the request of the owner does not have total independent control over the value,”²⁶² namely the second dimension of controlling power: asset custody. Here, what the Guidance did not say, but is of significant importance, is that the wallet owner’s control over the cryptocurrencies is not total and independent. As explained in the previous paragraph, if a wallet service provider refuses to sign its part, then merely one signature from the wallet owner is not able to convince miners/validators to clear and settle a payment, which requires signatures by all the key holders. In such a situation, nobody alone can move the cryptocurrency controlled

²⁵⁶ See *id.* at 15–16.

²⁵⁷ See *id.* at 16.

²⁵⁸ See *id.* at 17.

²⁵⁹ See *id.*

²⁶⁰ *Id.*

²⁶¹ See *supra* note 146, at 8.

²⁶² *Supra* note 145, at 17.

by the wallet, which would continue to stay in the same blockchain address and go nowhere without full signatures from all private key holders. This means that both the wallet owner and the unhosted multisig wallet service provider are merely necessary rather than sufficient for the payment to occur.²⁶³ Accordingly, neither the unhosted multiple-signature wallet service provider nor the wallet owner *alone* maintains total and independent control over *payment assets*.

The highly sophisticated networks of cryptocurrency payment suggest that not only multisig wallets but also cryptocurrency non-custodial service providers could maintain some degree of controlling power over payment assets in some of the three dimensions. In the governance dimension, such a higher degree of controlling power could exist when DAOs' voting powers are within the hands of a small group of people rather than a larger community, which could be made obvious when most governance token holders are apathetic about voting. Furthermore, admin keys, backdoors, and/or kill switches could allow a small number of people to fundamentally change and/or pause the operation of a player's underlying smart contract, thereby indirectly controlling customers' payment assets.

These dimensions of control show that each player's degree of controlling power over payment assets may differ. Some of them have a high degree of control, yet some of them that currently fall outside of the scope of the regulatory perimeter of the BSA still preserve a minor degree of control over the entire payment process. For those that govern their protocols through DAOs, the uncertainty of voting outcomes and their founders' and/or operating teams' potential exercise of human residual decision-making power explained below could result in their non-binary control over payment assets.

For example, a DEX and non-custodial mixer could adopt a decentralized approach of clearing, settlement, ownership, control, and balance sheet, while potentially maintaining a high degree of controlling power over payment assets through governance. While they adopt completely different approaches for (1) clearing and settlement and (4) acceptance and transmission, their approaches for (2) ownership/balance sheet and (3) governance could share certain similarities. For example, neither of them owns their customers' cryptocurrencies, and it is possible that a concentration of voting powers would exist both in the

²⁶³ See *supra* note 146, at 8.

boards of CEX and the DAOs of DEXs. Given the similarity that CEXs and DEXs share regarding governance and asset ownership, it is reasonable to conclude that some DEXs could still preserve certain degrees of control over swapped cryptocurrencies. As a number of empirical studies have already shown that the degree of power concentration in DAOs' governance is high,²⁶⁴ the findings below potentially challenge FinCEN's conclusion that DEXs, non-custodial wallets, and unhosted wallets are outside of the scope of the regulatory perimeter of the BSA.

Table 1: Comparison Between CEXs and AMMs

	Dimension 1	Dimension 2			Dimension 3
	Clearing & Settlement	Ownership	Control	Balance Sheet	Centralized Governance
DEXs	No	No	No	No	Potentially Yes (via DAO, Admin Key, Backdoor, and/or Kill Switch)
Non-custodial Mixers					
Singlesig Unhosted Wallets					
Multisig Unhosted Wallets			Yes (Some Degree of Control)		

²⁶⁴ See, e.g., Stefan Kitzler, Stefano Ballestti, Pietro Saggese, Bernhard Haslhofer, & Markus Strohmaier, *The Governance of Decentralized Autonomous Organizations: A Study of Contributors' Influence, Networks, and Shifts in Voting Power*, ARXIV:2309.14232 (CS.SI) (Sept. 2023), <https://perma.cc/KT85-Z9C2>; see also Xiaotong Sun, Charalampos Stasinakis, & Georgios Sermpinis, *Decentralization Illusion in Decentralized Finance: Evidence from Tokenized Voting in MakerDAO polls*, ARXIV:2203.16612 (CS) (Mar. 2023), <https://perma.cc/D6NJ-ADLK>; Xuan Liu, *The Illusion of Democracy? An Empirical Study of DAO Governance and Voting Behavior* (June 2024), <https://perma.cc/59E6-U2BN>; Maury Shenk, Sven Van Kerckhoven, & Jonas Weinberger, *The Crown, the Market and the DAO*, 6 STAN. J. BLOCKCHAIN L. & POL'Y 244, 258 (2023); Robin Fritsch, Marino Müller, & Roger Wattenhofer, *Analyzing Voting Power in Decentralized Governance: Who Controls DAOs?*, ARXIV:2204.01176 (Apr. 2022), <https://perma.cc/2R85-HVX7>; Sirio Aramonte, Wenqian Huang, & Andreas Schrimpf, *DeFi Risks and the Decentralisation Illusion*, BIS Q. REV. (Jan. 2014); *supra* note 236, at 22.

The controlling power each cryptocurrency non-custodial service provider has over payment assets differs depending on its business model, and such a controlling power exists on a spectrum rather than in a binary. Because the BSA's current definition of money transmitting business merely focuses on the second dimension, namely asset custody, it is unable to adequately measure the degree of control a cryptocurrency non-custodial service provider has over payment assets. In light of the three dimensions of control, this Article argues that whether a player currently falling outside of the BSA's scope should fall inside depends on their degree of controlling power based on the aforementioned three dimensions. The more dimensions over which a player has control, the higher the degree of controlling power over payment assets is, the more likely it would qualify as a money transmitting business, and the more suitable the BSA's substantive obligations are for covered businesses.

IV. TOWARDS A NEW FRAMEWORK FOR REGULATING CRYPTOCURRENCY NON-CUSTODIAL SERVICE PROVIDERS

Part IV offers a framework allowing the BSA to regulate some of the cryptocurrency non-custodial service providers that maintain a certain degree of controlling power over payment assets. To do so, Part IV first analyzes the existing legislative, judicial, and administrative actions seeking to directly and indirectly expand the scope of the regulatory perimeter of the BSA to cover cryptocurrency non-custodial service providers. Part IV explains the design and benefit of each approach, the potential issues that each of them needs to address, and the possible approach to addressing these potential issues. While analyzing the judicial actions, namely the indictments against the founders of Tornado Cash and Samurai Wallet, Part IV argues that the adequate manner of interpreting the concept of money transmitting businesses must follow the BSA's control-based principle. Therefore, Part IV argues that the BSA should re-interpret the definition of money transmitting businesses, allowing the BSA to determine businesses it should regulate based on the degree of control a business has over payment assets. Accordingly, Part IV proposes a framework, arguing that the BSA should measure the collective degree of controlling power a service provider has over payment assets through all the aforementioned three dimensions. These three dimensions serve as variables within this framework: the more variables present, the greater the degree of collective control a provider has over cryptocurrency payments, and the more likely

it is to fall within the scope of the regulatory perimeter of the BSA. It also identifies and responds to potential challenges and objections.

A. Existing Regulatory Prescriptions Seeking to Expand the Scope of the Regulatory Perimeter of the BSA

Lawmakers and policymakers are aware of the challenges stemming from the existing scope of the regulatory perimeter of the BSA and have taken steps to directly and indirectly expand it. As of April 2025, there has been a proposed bill, two proposed regulations, and two indictments that have sought to directly or indirectly bring unhosted wallets, DEXs, non-custodial mixers, miners, and validators into the scope of the regulatory perimeter of the BSA. While none of them have become effective law as of April 2025, they all offered a valuable experience that would help to update the BSA to regulate unhosted wallets, DEXs, and non-custodial mixers.

1. Direct Expansion: Adding Unhosted Wallets, Miners, and Validators into the list of Financial Institutions to Avoid the Discussion of Whether they Qualify as Money Transmitting Businesses

As Part II explained, the BSA, through a bifurcated structure, only requires money transmitting businesses and a list of financial institutions to register and comply with a series of carefully designed substantive obligations.²⁶⁵

The benefit of adding unhosted wallets and miners/validators into the list of financial institutions, rather than seeking to classify them as a part of money transmitting businesses, is twofold. First, it avoids potential conflict between the bill and FinCEN's decision in its 2019 Guidance that exempted unhosted wallets and miners/validators from MSBs. Second, it avoids discussions and even critiques regarding whether a financial institution's operation is centralized or decentralized. Specifically, the key question is whether the BSA should have covered businesses that, on the one hand, do not qualify as MSBs but, on the other hand, still operate with a low degree of controlling power over payment assets.²⁶⁶

²⁶⁵ See *supra* note 144, § 5313(a) (2018); see also *supra* note 124, §§ 1022.200, 1010.310, 1010.320.

²⁶⁶ See *supra* note 124, § 1010.100(ff)(5)(i)(A).

Yet, there are two potential issues that need addressing. First, the list of financial institutions within the BSA covers those whose existing registration status under other regulatory frameworks brought them within the perimeter of the BSA's registration requirements.²⁶⁷ As such, it could potentially be necessary for Congress to either enact new laws or amend the BSA to establish the registration requirements of unhosted wallets and miners/validators as new categories of financial institutions, which might result in additional discussions. Second, if no registration requirement exists for unhosted wallets and miners/validators as new categories of financial institutions, such as due to exemptions, then a reasonable justification for such an exemption could be necessary. While these two issues are under the assumption that registration requirements must either exist or be exempted for financial institutions, the BSA could indeed offer special treatment by intentionally remaining silent about whether unhosted wallets and miners/validators must register. Yet, since registration requirements provide regulators with essential information about their operation, such as the activities in which they engage and the structure of their business operations, which could significantly help regulators to ensure that they comply with the BSA's substantive obligations, the cost of such silence is significant.²⁶⁸

A proposed bill, which is yet to become law as of July 2024, sought to adopt this approach. On July 27, 2023, Senators Elizabeth Warren, Roger Marshall, Lindsey Graham, and Joe Manchin, who was serving as a U.S. Senator at the time, introduced a bill titled Digital Asset Anti-Money Laundering Act of 2023. The bill sought to expand the scope of the BSA's regulatory perimeter to cover a list of players of DeFi payments, including unhosted wallets and miners/validators.²⁶⁹ The uniqueness of this bill is that it avoids the potential complex discussions of whether unhosted wallets and miners/validators would qualify as money transmitting businesses that accept and transmit value that substitutes for currency.²⁷⁰ Instead, the bill sought to directly add the following players, including (1) unhosted wallet service providers

²⁶⁷ See *supra* note 144, § 5312(a)(2) (2018).

²⁶⁸ See, e.g., *MSB Registration Website*, FINCEN (Jan. 27, 2012), <https://perma.cc/E8XS-BYXJ>.

²⁶⁹ The bill's initial version, introduced on December 15, 2022, titled Digital Asset Anti-Money Laundering Act of 2022, did not seek to expand the scope of the regulatory perimeter of the BSA. See Digital Asset Anti-Money Laundering Act of 2022, S. 5267, 117th Cong. § 1 (2022), <https://perma.cc/96FT-CCKX>.

²⁷⁰ See *supra* note 144, § 5330(d)(1) (2018).

and (2) validators, to the list of financial institutions.²⁷¹ The bill's definitions of digital assets, unhosted wallets, and validators would cover both hot and cold unhosted wallets, as well as both miners and validators in a variety of blockchains that clear and settle cryptocurrency payments.²⁷² As of May 2025, the bill has yet to go through subsequent legislative processes following its last hearing on the Senate Committee on Banking, Housing, and Urban Affairs on February 1, 2024.²⁷³

2. Direct Expansion: Arguing that Cryptocurrency Non-Custodial Service Providers Qualify as Money Transmitting Businesses

In addition to adding new players to the existing list of financial institutions in the BSA, the other way of expanding the scope of the regulatory perimeter of the BSA is to interpret the concept of money transmitting business so that it covers additional new players. The DOJ's two indictments against the founders of two mixers, Tornado Cash and Samourai Wallet, sought to expand the scope of the regulatory perimeter of the BSA through this approach. While the court has yet to rule on the DOJ's attempt at expansion, the DOJ's indictments have resulted in discussions as explained below.

The first indictment was against the founders of Tornado Cash for various charges, including conspiracy to operate an unlicensed money transmitting business.²⁷⁴ The DOJ sought to establish that Tornado Cash, by controlling customers' cryptocurrencies, qualified as a custodial mixer and, therefore, fell within the scope of the regulatory perimeter of the BSA.²⁷⁵ To do so, the DOJ argued that Tornado Cash's:

UI . . . would provide a unique “secret note” to the Tornado Cash customer for each deposit, and the customer would be the only person with access to the secret note. To make withdrawal from the Tornado Cash service, the customer would go to the ‘Withdraw’ tab on the UI and enter the secret note that the customer had received when making the deposit,

²⁷¹ See *id.* § 5312(a)(2) (2018); see also *infra* note 272.

²⁷² See Digital Asset Anti-Money Laundering Act of 2023, S. 2669, 118th Cong. §§ 2, 3 (2023), <https://perma.cc/8RM5-MD9L>.

²⁷³ See *All Actions: S.2669 — 118th Congress*, CONGRESS (2023–2024).

²⁷⁴ See *infra* note 275, at 32–34; see also *supra* note 147; *supra* note 144, § 1960(b)(1)(C) (2018).

²⁷⁵ See Indictment, *U.S. v. Roman Storm & Roman Semenov*, No. 23 Cr. 23 Crim 430 at 15–20 (S.D.N.Y. Aug. 23, 2023), <https://perma.cc/F8FW-JLH9>.

along with the recipient address where the withdrawal should be transmitted When a customer later submitted a secret note to the Tornado Cash UI for the purpose of making a withdrawal to an Ethereum blockchain address designated by the customer, the UI sent the secret note to a smart contract created by the Tornado Cash founders to initiate a withdrawal.²⁷⁶

Alternatively, customers seeking to withdraw their cryptocurrencies could “have a Tornado Cash relay transmit the[ir] secret note[s] to the Tornado Cash smart contract,”²⁷⁷ a public smart contract.²⁷⁸

The DOJ’s language in the indictment seemed to confirm that while customers originally maintained exclusive control over their cryptocurrency through these secret notes that were exclusively accessible to them, they would subsequently share these secret notes with the public through the public smart contract, thereby granting Tornado Cash control over their cryptocurrencies. However, an analysis of Tornado Cash 10 ETH Pool’s source code confirmed that the indictment’s language did not fully explain the complete spectrum of Tornado Cash’s functional mechanism.²⁷⁹ According to the code, each secret note itself never goes to the smart contract, and a customer only shares a hashed value generated through a cryptographic hashing algorithm, which serves as the proof of each secret note.²⁸⁰ Therefore, contrary to the DOJ’s indictment, Tornado Cash’s customers did not share their control over their cryptocurrencies with Tornado Cash. This means that rather than being a *custodial* mixer, Tornado Cash was a *non-custodial* mixer, thereby falling outside of the existing scope of the regulatory perimeter of the BSA. As such, the real question the court now faces is whether it should reinterpret the definition of money transmitting business, currently established under the acceptance-and-transmission standards so that a reinterpreted definition would cover non-custodial mixers and other players that do take custody of customers’ funds.

The second indictment was against the founders of Samourai Wallet for conspiracy to commit money laundering and conspiracy

²⁷⁶ *Id.*, at 7–8; see also *supra* note 146, at 11.

²⁷⁷ *Supra* note 275, at 7–8; see also *supra* note 146, at 11.

²⁷⁸ See *supra* note 146, at 12.

²⁷⁹ See *id.* at 16.

²⁸⁰ See *supra* note 146, at 12–15, 14 n.22; see also *Tornado Cash’s Contract Source Code*, BLOCKSCAN, <https://perma.cc/4HP4-WS7U>.

to operate an unlicensed money transmitting business.²⁸¹ On April 24, 2024, the DOJ sought to establish that Samurai Wallet, an unhosted wallet,²⁸² by engaging “in the business of transferring funds on behalf of the public,”²⁸³ also qualified as a custodial mixer and, therefore, would fall within the scope of the regulatory perimeter of the BSA.²⁸⁴ Yet, according to the indictment, “Samurai [Wallet] automatically generates the new address that are used as inputs and outputs throughout the process on behalf of the users, although the private keys for these cryptocurrency addresses are stored in each user’s individual cellphone and not shared with Samurai’s employees.”²⁸⁵ The plain language of the indictment shows that Samurai Wallet was a non-custodial mixer since its customers maintained exclusive control over the private keys throughout the mixing process.²⁸⁶

The key question of fact now presented is whether Samurai Wallet, an unhosted wallet service provider that simultaneously provides non-custodial mixing services, actually controlled customers’ funds. If the answer is no, which is what the language of the DOJ’s indictment alleges,²⁸⁷ then the key question of law now presented is whether an intermediary that does not accept nor transmit money would qualify as a money transmitter. The DOJ’s self-contradictory manner of interpreting the BSA has brought before the court a key question of policy. The key question of policy now presented before the court is whether the BSA’s definition of money transmitter should cover entities that do not simultaneously accept and transmit money, such as service providers of unhosted wallets and non-custodial mixers.

As explained in Part III, this Article argues that, if the court decides to embark on this task, then it should conduct a complex assessment of the degree of controlling power of a player’s operation. In this process, the key question of policy would be whether having total and independent control over cryptocurrencies would be the prerequisite for a player to accept and transmit them.

The court is yet to make its rulings. Yet, on May 9, 2024, in a letter sent to the United States Attorney General, two senators argued against expanding the scope of the regulatory perimeter

²⁸¹ See Indictment, *U.S. v. Keonne Rodriguez & William Lonergan Hill*, No. S2 24 Cr. 82 at 1–3, 17–18 (S.D.N.Y. Apr. 24, 2024), <https://perma.cc/YQ95-PBE9>.

²⁸² See *id.* at 3.

²⁸³ *Id.* at 13.

²⁸⁴ See *id.* at 12–14, 17–18.

²⁸⁵ *Id.* at 5–6.

²⁸⁶ See *id.*

²⁸⁷ See *id.*

of the BSA because such an expansion is inconsistent with the BSA and FinCEN's Guidance established in 2019.²⁸⁸

3. Indirect Expansion: FinCEN's two Attempts of Requiring some or all Players Already Within the Scope of the Regulatory Perimeter of the BSA to React on Transactions Between them and Unhosted Wallets and/or Mixers

FinCEN sought to indirectly expand the scope of the regulatory perimeter of the BSA to cover unhosted wallets and non-custodial mixers. The essence of FinCEN's strategies remained identical, namely to require players already within the scope of the BSA's regulatory perimeter to take specific actions regarding transactions involving actors outside of the scope of the regulatory perimeter of the BSA.

(1) Unhosted Wallet

On December 23, 2020, FinCEN announced a Notice of Proposed Rulemaking (NPRM) seeking to indirectly expand the scope of the regulatory perimeter of the BSA through the following two manners.²⁸⁹ First, the NPRM would require banks and MSBs to keep records of, and file reports similar to CTRs to FinCEN, cryptocurrency transactions between them and unhosted wallets that exceeded a certain amount, individually or in aggregation.²⁹⁰ Second, the NPRM would require banks and MSBs to verify the identification information of unhosted wallets when accepting or transmitting cryptocurrency from or to unhosted wallets, respectively.²⁹¹ As such, if enacted, this rule would essentially create a new obligation of Know Your Customer's Customer (KYCC) in addition to the Know Your Customer (KYC) obligation.

From December 2020 to March 2021,²⁹² FinCEN requested comments on proposed requirements regarding unhosted wallets. During its commenting period, the rule sparked more than 8,270 comments in total,²⁹³ including intense criticism.

²⁸⁸ See Sen. Cynthia M. Lummis & Sen. Ron Wyden, *Re: Money Transmitting Business Registration and Non-Custodial Crypto Asset Software*, U.S. SENATE (May 9, 2024), <https://perma.cc/7SLM-R9KE>.

²⁸⁹ See 85 Fed. Reg. 83840, 83848–62.

²⁹⁰ See *id.* at 83848–49.

²⁹¹ See *id.* at 83849.

²⁹² See 86 Fed. Reg. 7352, 7352 (Jan. 28, 2021).

²⁹³ See *All Comments on Docket: Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*, ERULEMAKING INITIATIVE, <https://perma.cc/39YQ-GNSU> (last visited June 1, 2024).

Here, some comments challenged the constitutionality of this rule in light of the limit of FinCEN's administrative power due to the following two reasons.²⁹⁴ First, the objective of the proposed rule was more comparable to that of lawmaking by Congress and/or courts than law implementation by FinCEN through its regulatory actions. The NPRM sought to indirectly expand the scope of the BSA's regulatory perimeter to cover those unhosted wallets seeking to accept cryptocurrency from or transmit cryptocurrency to banks and/or MSBs. Accordingly, such a decision to change the BSA, a legislation passed by Congress, merely through a FinCEN-proposed rule was more comparable to lawmaking. Secondly, the BSA does not authorize FinCEN to write new rules in a way that is more comparable to lawmaking. Pursuant to Treasury Order 180-01, FinCEN, as an administrative agency whose responsibility primarily lies in law enforcement, has the authorities delegated by the Department of Treasury to issue regulations to implement and administer the BSA.²⁹⁵ As such, while the BSA's language was silent about the limit of the Secretary's authority for prescribing the situations for new reporting requirements, some comments argued that such a silence in and of itself does not necessarily stand for a clear legal basis for creating additional legal requirements, showing the limit of FinCEN's authority to write new rules.²⁹⁶ Therefore, a challenge to the legitimacy of such an attempt in light of the U.S. Constitution would inevitably arise in the absence of a clear legal basis provided by the BSA or other laws.

According to the Federal Register published on August 16, 2024, FinCEN officially withdrew this NPRM on April 12, 2024.²⁹⁷

(2) Mixers

²⁹⁴ See, e.g., Coin Center, *Further Supplemental Comments to the Financial Crimes Enforcement Network on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*, ERULEMAKING INITIATIVE 3–4 (Mar. 15, 2021), <https://perma.cc/CD3L-BHPZ>; see also New Civil Liberties Alliance, *Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*, Docket Number FINCEN-2020-0020-0001, ERULEMAKING INITIATIVE 10–11 (Apr. 7, 2021), <https://perma.cc/3FS5-KDWC>.

²⁹⁵ See Treas. Order 180-01 (July 1, 2014).

²⁹⁶ See, e.g., Coin Center, *Further Supplemental Comments to the Financial Crimes Enforcement Network on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*, ERULEMAKING INITIATIVE at 4 (Mar. 15, 2021), <https://perma.cc/CD3L-BHPZ>; see also New Civil Liberties Alliance, *Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*, Docket Number FINCEN-2020-0020-0001, ERULEMAKING INITIATIVE at 10 (Apr. 7, 2021), <https://perma.cc/3FS5-KDWC>.

²⁹⁷ See 89 Fed. Reg. 66858, 66861 (Aug. 16, 2024).

Pursuant to Section 311 of the USA PATRIOT Act,²⁹⁸ the Secretary of the Treasury implements special measures for one “or more classes of transactions within, or involving, a jurisdiction outside of the United States . . . to be of primary money laundering concern.”²⁹⁹ The design of the special measures is fivefold, including recordkeeping and reporting of certain financial transactions.³⁰⁰ Under this legal basis, on October 19, 2023, FinCEN announced an NPRM, “finding that transactions involving CVC mixing within or involving jurisdictions outside the United States are a class of transactions that are of primary money laundering concern.”³⁰¹ By adopting a broad definition of CVC mixer, CVC mixing, and covered transaction,³⁰² the NPRM proposed to require that financial institutions currently covered by the BSA must keep records of, and report to FinCEN, key information of transactions involving all categories of mixers, including non-custodial mixers that are not within the scope of the regulatory perimeter of the BSA.³⁰³ Therefore, it is no longer within covered businesses’ discretion to determine the reportable information concerning transactions involving mixers. Accordingly, the NPRM, in effect, indirectly expanded the scope of the regulatory perimeter of the BSA to cover non-custodial mixers.

From October 2023 to January 2024,³⁰⁴ FinCEN requested comments on this NPRM. During its commenting period, the rule sparked more than 2,160 comments in total,³⁰⁵ less than the approximately 8,270 comments for the NPRM for unhosted wallets,³⁰⁶ including criticism mainly based on the following two reasons. Following the commenting period, the NPRM has yet to become effective law as of July 2024.

First, some comments emphasized the potential legitimate use of mixers, thereby questioning the expansive scope of the regulatory perimeter of this NPRM that would cover all categories of

²⁹⁸ See *infra* note 301, at 72701–23; see also generally Public Law 107–56, 115 Stat. 272 (Oct. 26, 2001).

²⁹⁹ *Supra* note 144, § 5318A (2018).

³⁰⁰ *Id.* § 5318A(b) (2018).

³⁰¹ 88 Fed. Reg. 72701, 72702 (Oct. 19, 2023).

³⁰² See *id.* at 72709.

³⁰³ See *id.* at 72709–11.

³⁰⁴ See *id.* at 72701.

³⁰⁵ See *All Comments on Docket: Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern*, ERULEMAKING INITIATIVE (Oct. 22, 2023), <https://perma.cc/FVP8-LV75>.

³⁰⁶ See *All Comments on Docket: Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*, ERULEMAKING INITIATIVE, <https://perma.cc/39YQ-GNSU> (last visited June 1, 2024).

mixers.³⁰⁷ Second, some comments questioned the insufficient statutory authority of the NPRM.³⁰⁸ While Section 311 of the USA PATRIOT Act is the basis for implementing special measures, the targeted class(es) of transactions must be “within, or involving, a jurisdiction outside of the United States.”³⁰⁹ Yet, the broad definition of “CVC mixing” would allow the NPRM to cover transactions within or involving the United States and non-U.S. jurisdictions without explaining how to limit the coverage to foreign jurisdictions.³¹⁰

B. Policy Prescription: Expanding the Scope of the Regulatory Perimeter of the BSA based on a Player’s Degree of Controlling Power over Payment Assets

This prescription argues for an amendment to the scope of the regulatory perimeter of the registration requirements of the BSA so that it covers both the existing list of financial institutions and a new category of business, what we might call a payment controlling business, with broader coverage compared to the current standard of money transmitting business. Here, a payment controlling business maintains a high degree of controlling power over the payment of currency, funds, and value that substitutes for currency.³¹¹ The degree of control necessary to qualify as a payment controlling firm is the minimum degree that would stop a

³⁰⁷ See, e.g., Coinbase, *Re: Ensuring Responsible Development of Digital Assets; Request for Comment*, ERULEMAKING INITIATIVE at 3–5, 15–19 (Jan. 22, 2024), <https://perma.cc/XAD7-3L7V>; Chainalysis, *Re: Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern*, ERULEMAKING INITIATIVE 88 Fed. Reg. 72,701, 9–10 (Oct. 23, 2024), <https://perma.cc/9CEP-J75D>; Paradigm, *RE: Paradigm Operations LP Comment Regarding Notice of Proposed Rule Making (FINCEN-2023-0016)*, ERULEMAKING INITIATIVE 2–7 (Jan. 22, 2024), <https://perma.cc/LQM5-NN3K>; Polygon Labs & DELV, *Response to FinCEN’s Notice of Proposed Rulemaking on CVC Mixing as a Class of Transactions of Primary Money Laundering Concern (Docket No. FINCEN-2023-0016) By Polygon Labs and DELV*, ERULEMAKING INITIATIVE 13–18 (Jan. 22, 2024), <https://perma.cc/84FQ-843Q>.

³⁰⁸ See, e.g., Coin Center, *Comments to the Financial Crimes Enforcement Network on “Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern”*, ERULEMAKING INITIATIVE 4–7 (Jan. 22, 2024), <https://perma.cc/H8AW-XVXQ>.

³⁰⁹ *Supra* note 144, § 5318A (2018).

³¹⁰ See, e.g., Coin Center, *Comments to the Financial Crimes Enforcement Network on “Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern”*, ERULEMAKING INITIATIVE 4–7 (Jan. 22, 2024), <https://perma.cc/H8AW-XVXQ>; see also, e.g., Chainalysis, *Re: Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern*, ERULEMAKING INITIATIVE 88 Fed. Reg. 72,701, 10–11 (Oct. 23, 2024), <https://perma.cc/9CEP-J75D>.

³¹¹ See *supra* note 144, § 5330(d)(1) (2018).

payment from happening. It is based on the collective measurement in terms of (1) clearing and settlement, (2) asset ownership, control, and the recording of assets in balance sheets, and (3) governance. The higher a player's degree of controlling power is, the more likely it qualifies as a payment controlling business. Therefore, the real focus is the degree of control that a player has over its customers' payment assets, regardless of whether the player *claims* that its service is custodial or non-custodial.

A payment controlling business must register with FinCEN. The BSA's current substantive obligations would be applicable to a payment controlling business, including the anti-money laundering program requirements,³¹² monitoring and reporting requirements,³¹³ recordkeeping requirements,³¹⁴ and the travel rule.³¹⁵

While the current standard of money transmitting business is based on the action a player takes, namely simultaneously accepting and transmitting monetary instruments, such a standard does not necessarily adequately evaluate the degree of control a player has over payment assets, particularly for cryptocurrency non-custodial service providers that are highly centralized. The ability to accept and transmit cryptocurrency merely focuses on the asset custody dimension of controlling power, and such a dimension exists in parallel to the governance dimension of control as discussed in Part III. Therefore, a payment controlling business would include, but is not limited to, a money transmitting business that accepts and transmits cryptocurrency.

A payment controlling business could potentially cover cryptocurrency non-custodial service providers. A cryptocurrency non-custodial service provider could retain a high degree of control in terms of governance, which could be within the control of a small number of governance token holders with concentrated voting power and/or founders with admin keys, back doors, and/or kill switches. These people could amend the smart contract, which could potentially, for example, (1) turn a non-custodial service provider into a service provider that is neither completely custodial nor completely non-custodial, such as converting a singlesig wallet into a multisig wallet, (2) make it harder for customers to

³¹² See *supra* note 124, §§ 1010.210, 1022.210(a); see also *supra* note 144, §§ 5318(a)(2), 5318(h) (2018).

³¹³ See *supra* note 124, §§ 1010.310, 1010.320, 1022.310, 1022.320; see also *supra* note 144, § 5318(a)(2) (2018).

³¹⁴ See *supra* note 124, §§ 1010.400, 1022.400; see also *supra* note 144, § 5318(a)(2) (2018).

³¹⁵ See *supra* note 124, §§ 1022.400, 1022.410, 1022.420 (2018).

withdraw their assets from DEXs,³¹⁶ or (3) not provide customers of mixer services with proof of withdrawing their mixed assets.

A payment controlling business could potentially cover miners and validators. While miners and validators do not have control over the governance of service providers, such as wallets, exchanges, and mixers, they have exclusive control over the clearing and settlement of cryptocurrency payments, without which payments are unable to happen.

The possibility that a non-custodial service provider, a miner, and a validator could fall within the scope of the regulatory perimeter indicates that the AML/CFT law of the U.S. does not necessarily rely on intermediation. While such a no-intermediation rule could seem extreme, such proposals also exist in other areas of financial regulation.³¹⁷

C. Potential Challenges and Objections

1. Potential Challenges

Like any prescription addressing policy questions, the prescription above would inevitably result in a potential challenge and a number of potential objections. The challenge is the possibility of variances between the proposed updates for the BSA and the current state-level equivalents, such as state-level MSB and cryptocurrency-specific laws.³¹⁸ In the United States, money transmitting businesses are subject to the regulatory frameworks both at the federal, namely the BSA, and state levels.³¹⁹ The specific definitions of money transmitter or money transmitting business may differ state by state.³²⁰ Yet, this could result in different but potentially overlapping coverage between the proposed

³¹⁶ A summary of payment categories, which explains that payments are crucial components of cryptocurrency exchanges, concludes Part I.

³¹⁷ See Dan Awrey, *Unbundling Banking, Money, and Payments*, 110 GEO. L.J. 715, 775 (2022).

³¹⁸ See, e.g., N.Y. COMP CODES R. & REGS. tit. 23, § 200.1 (2021); see also Dan Awrey, *Unbundling Banking, Money, and Payments*, 110 GEO. L.J. 715, 770, 770 n.344 (2022) (explaining the state-level MSB laws and New York's new "BitLicense" regime).

³¹⁹ See Dan Awrey, *Bad Money*, 106 CORNELL L. REV. 1, 46–47 (2020).

³²⁰ See Carol R. Goforth, *The Case for Preempting State Money Transmission Laws for Crypto-Based Businesses*, 73 ARK. L. REV. 301, 315–18, 322–36 (2020). For example, nine states, as well as the District of Columbia, the U.S. Virgin Islands, and Puerto Rico follow the definition based on the Uniform Money Service Act (UMSA) drafted by the Uniform Law Commission (ULC). See *Money Services Act*, UNIFORM L. COMM. (Feb. 4, 2022), <https://perma.cc/M6G8-HQKR>. Massachusetts money transmission law only regulate cross-border money transmission. See MASS. GEN. LAWS ch. 169, §§ 1–16 (2023); see also *supra* note 319.

updates for the BSA and the state-level MSB laws due to the following two reasons. First, generally speaking,³²¹ the definition of money transmission in the majority of state-level MSB laws only requires *either* acceptance *or* transmission to exist, rather than the simultaneous existence of both, and exempt platforms merely deliver communications from the money transmitting business status.³²² Such a standard could potentially cover miners and validators that issue or transmit cryptocurrency without receiving or accepting them and exempt cryptocurrency non-custodial service providers that merely match bids and asks from the status of money transmitting businesses. Second, state-level MSB laws' definition of money transmitting business typically does not adopt the proposed definition based on the degree of controlling power.³²³

Accordingly, a business could find itself in a situation where it is subject to the regulatory perimeter of the federal BSA and certain state MSB laws but is exempted from money transmitting business status under other state MSB laws. In practice, a business could, but does not necessarily have to, obtain an MSB license from FinCEN and all state-level regulators to avoid potential violations.³²⁴ Yet, the proposed BSA updates, which are highly likely with broader coverage compared to the majority of its state-level counterparts, could signal the importance of regulating

³²¹ *But see* Md. Code Ann., Fin. Inst. § 12-401(p)(1) (“Money transmission” means engaging in the business of . . . receiving currency, funds, or other value that substitutes for currency and transferring currency, funds, or other value that substitutes for currency to another person or a location within or outside the United States by any means”).

³²² *See, e.g.*, UNIF. MONEY SERV. ACT, § 102(14) (“‘Money transmission’ means selling or issuing payment instruments, stored value, or receiving money or monetary value for transmission. The term does not include the provision solely of delivery, online or telecommunications services, or network access”); *see also, e.g.*, GA. CODE ANN. § 7-1-680(14) (“‘Money transmission,’ ‘transmit money,’ or ‘transmission of money’ means engaging in the business of: (A) Receiving money or monetary value for transmission or transmitting money or monetary value within the United States or to locations abroad by any and all means . . . ; (B) Selling or issuing payment instruments, including the creation, issuance, or sale of a payment instrument that is redeemable in cash or monetary value . . .”).

³²³ For details regarding the design of the state-level MSBs, *see supra* note 319. While the article explained that no money transmission law exists in Minnesota at the time of writing in 2020, “[o]n May 24, 2023, Governor Tim Walz signed Minnesota Session Law 2023, Chapter 57, Senate File 2744 into law, which included the Minnesota Money Transmission Modernization Act (MTMA).” *Money Transmitters and Currency Exchangers*, COM. DEP’T LICENSING, <https://perma.cc/H669-V5ZM> (last visited July 4, 2024). *See also* Joseph Jasperse, *50-State Review of Cryptocurrency and Blockchain Regulation*, STEVENS CTR. FOR INNOVATION IN FIN. (June 23, 2022), <https://perma.cc/Y4G4-RL84>.

³²⁴ *See, e.g.*, *Coinbase, Inc. Is Licensed in the Following US Jurisdictions*, COINBASE, <https://perma.cc/4YAG-YCQD> (last visited July 4, 2024); *see also, e.g.*, *State Licenses*, PAYPAL, <https://perma.cc/Z5HL-C7HC> (last visited July 4, 2024).

players of DeFi payments that maintain certain degrees of controlling power and offer an example of regulatory design, however awkwardly.

2. Potential Objections

The prescription would also attract several potential objections. The first objection is that the regulatory framework should not regulate technology as FinCEN has traditionally taken the technology-neutral and activity-based standpoint to interpret and enforce the BSA.³²⁵ This objection is not compelling for the following reasons. First, such an objection is flawed as a matter of basic logic since allowing cryptocurrency non-custodial service providers to operate outside of the BSA based on the argument of technological neutrality would give all technology supporting cryptocurrency payments a clear advantage, which is inconsistent with the principle of technological neutrality. Second, the prescription does not seek to regulate technologies supporting cryptocurrency non-custodial service providers. It is the manner of using these technologies that is the focus of the prescription, namely the controlling power a service provider has over payment assets.

The second objection is that regulations could limit technological and financial innovations. This objection is not compelling for the following reasons. First, limiting regulatory arbitrage in the guise of technological and/or financial innovations would not only prevent undesirable regulatory outcomes,³²⁶ such as innovations that facilitate money laundering, but also benefit the goal of lawmaking and technological ethics.³²⁷ Second, limiting technological innovations in areas vulnerable to money launderers' misuse would not limit technological innovations in areas with no or relatively lower threats from money launderers. For example, innovations in encryption technology would hardly cease to happen when the regulatory framework requires non-custodial mixers to register with FinCEN.

³²⁵ See 76 Fed. Reg. 45403, 45411; see also Alexandra D. Comolli & Michele R. Korver, *Surfing the First Wave of Cryptocurrency Money Laundering*, 69 DEP'T OF JUST. J. FED. L. & PRAC. 183, 240 (2021).

³²⁶ See, e.g., Dan Awrey, *Complexity, Innovation, and the Regulation of Modern Financial Markets*, 2 HARV. BUS. L. REV. 235, 275–76 (2012).

³²⁷ See, e.g., Haochen Sun, *Regulating Algorithmic Disinformation*, 46 COLUM. J.L. & ARTS 367, 396 (2022); see also, e.g., Hilary J. Allen, *DeFi: Shadow Banking 2.0?*, 64 WM. & MARY L. REV. 919, 924 (2023).

CONCLUSION

Dirty money and bad actors have been a key issue since the birth of the monetary system. The law and regulation have played indispensable roles in regulating such a key issue. This Article elaborates on such a challenge as the result of the intermediation-based regulatory approach taken by the BSA's money transmitting business rule allowing cryptocurrency non-custodial service providers to operate without complying with the BSA's substantive obligations. As a result, bad actors launder dirty money through cryptocurrency non-custodial service providers, including unhosted wallets, DEXs, and non-custodial mixers, without worrying about regulatory detection and scrutiny.

This Article argues that the BSA should cover some of the cryptocurrency non-custodial service providers that can retain a certain degree of controlling power over payment assets. To do so, this Article offers a prescription, arguing for the creation of payment controlling businesses that must register with FinCEN and comply with the BSA's substantive obligations. By measuring the collective degree of controlling power a service provider has over payment assets through three dimensions, cryptocurrency non-custodial service providers with a high degree of controlling power over payment assets could qualify as payment controlling businesses and, therefore, comply with the BSA's substantive obligations. The three dimensions serve as variables within this framework: the more variables present, the greater the degree of collective control a provider has over cryptocurrency payments, and the more likely it is to fall within the scope of the regulatory perimeter of the BSA.

