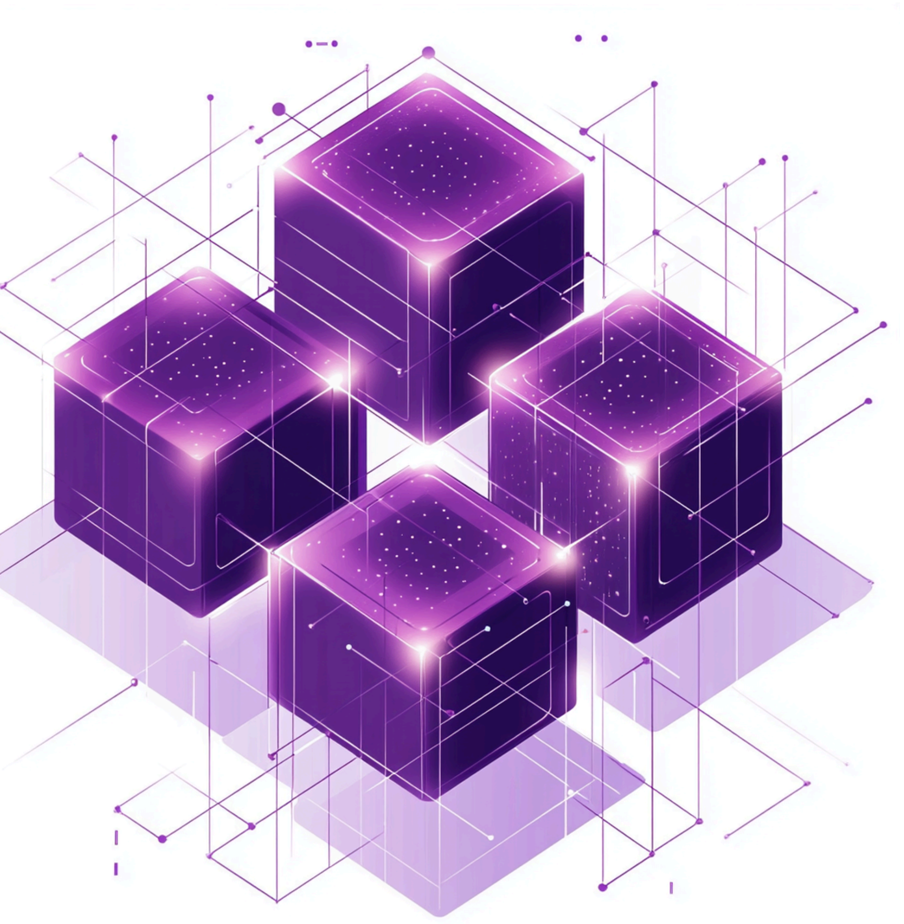
November 2024

Square Peg in a Round Hole:

Why the Bank Secrecy Act Should Not Apply to Blockchain Participants

Lizandro Pieper
Gavin Zavatone



DeFi
Education
Fund

defieducationfund.org

About the DeFi Education Fund

The DeFi Education Fund is a nonpartisan research and advocacy group working to explain the benefits of DeFi, achieve regulatory clarity for the future of the global digital economy, and help realize the transformative potential of DeFi for everyone.

We exist because DeFi has immense potential for human prosperity, but that can only be realized with buy-in from governments and appropriate policy. We work to help realize DeFi's promise by educating regulators and policymakers and advocating for smart approaches.

Acknowledgements

Thank you to our DeFi Education Fund colleagues, Miller Whitehouse-Levine, Amanda Tuminelli, Max Bernstein, and Nathan Hennigh, who were instrumental in the development of this paper. And to the DeFi community for supporting our efforts in advocating for sensible policy that will safeguard and nourish innovation for a better tomorrow.

Table of Contents

Introduction

Since the launch of Bitcoin in 2009, the cryptocurrency ecosystem has envisioned a model for conducting financial transactions in a manner never before seen: the ability to securely send value electronically and without an intermediary; people completely independent of one another, running software locally on their computers so they may share the labor of maintaining a network for communicating, validating, and recording data. These are known as blockchain networks, and with them came a revolution of software applications and protocols that evolved the manner in which humanity transacts in the digital age. There are no intermediaries to trust with handling one's assets in this era of finance, as a person maintains total control of their funds by simply leveraging cryptographic software and a decentralized communications network to send and receive value.

However, like the internet of the 1990s, this technology is novel and the regulatory landscape has not yet adapted to its existence. Financial regulations have thus far been designed with intermediaries in mind, and are not effective, nor sensible, in a world where intermediaries do not exist. Yet, there is a growing movement in support of applying such regulations to developers and operators of this software—regulations that will prove to be detrimental to maintaining this innovation in the United States and to protecting the privacy and security of the American people. Chief among them is the Bank Secrecy Act (BSA), an anti-money laundering framework that depends on the existence of a third-party in financial transactions to be effective. This framework is actively being applied to software developers who do not operate as financial intermediaries. Hence, this paper investigates the history and design of the BSA, and its application to activities involving cryptocurrency—or "convertible virtual currencies" (CVC), as defined by the Financial Crime Enforcement Network (FinCEN).[1]

First, we provide an overview of the BSA and the statutory authorities that have been granted in its wake, as well as money transmission laws that have been leveraged against the industry. Second, we outline FinCEN's Guidance related to CVCs. Third, we determine the application of FinCEN's Guidance to participants involved in CVC activities. This includes: blockchain miners and validators; wallet providers; smart contract and decentralized finance (DeFi) developers; front-end website developers; relayer operators; and remote-procedure call (RPC) nodes. Fourth, we provide policy considerations that analyze the practicality and Constitutional validity of applying the BSA to these participants, as well as the importance of financial privacy.

Finally, we conclude that software providers and operators across the technology stack are not subject to the BSA, and we ask Congress to implement this distinction into law. This distinction will provide clarity in an otherwise ambiguous regulatory landscape, and create a safe haven for innovation in this new frontier of financial technology. In doing so, it will also empower the

[1] U.S. Dep't of the Treasury, Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, at 1 (Mar. 18, 2013); (Substantially citing: Definition of Money Services Business, 76 Fed. Reg. 43,585 (July 21, 2011).

financial privacy and security of Americans who choose to leverage this technology to protect themselves and their dignity.

Bank Secrecy Act

a. *Overview*

In 1970, Congress passed the Currency and Foreign Transactions Reporting Act, legislation that forms the basis of the legal framework commonly referred to as the BSA. The BSA authorizes the Department of Treasury to impose registration,[2] disclosure, and compliance requirements for "financial institutions" to help detect and prevent financial crimes.[3] Under the BSA, financial institutions are required to identify and verify the identity of their customers,[4] keep records of cash purchases and negotiable financial instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and report suspicious activity that might signify money laundering, tax evasion, and other criminal activities.[5]

Since its passage, the BSA has become a central instrument in government oversight of American financial transactions, and it has expanded in scope over the years with the passage of several laws, *inter alia*, the Money Laundering Control Act (1986), Annunzio-Wylie Anti-Money Laundering Act (1992), Money Laundering Suppression Act (1994), American PATRIOT Act (2001),[6] and Anti-Money Laundering Act (2020).[7] Collectively, these laws establish government oversight over banks and other financial intermediaries that move or control money on behalf of their customers, and subject them to stringent reporting and disclosure requirements on customers and their transactions. Regulated entities generally comply with BSA obligations through the collection of customer identifying information, monitoring and disclosure of transactions, and the implementation of anti-money laundering procedures.[8]

Among its provisions, the BSA defines the term "financial institution" to include certain non-bank entities, including:[9]

[2] The statute uses the term ‘‘money transmitting business’’ to name those businesses subject to registration. See 31 U.S.C. 5330(a)(1) and (d)(1). However, FinCEN believes that the statute's use of this term to refer to all the types of businesses subject to registration and its later use of the nearly identical term ‘‘money transmitting service’’ to refer to a particular type of business subject to registration, compare 31 U.S.C. 5330(d)(1)(A) with 31 U.S.C. 5330(d)(2), may lead to confusion. Therefore, FinCEN has adopted the term ‘‘money services business’’ in place of the term ‘‘money transmitting business’’ throughout this document and under the final rule.

[3] 31 U.S.C. § 5318 (I).

[4] 31 CFR § 1020.220.

[5] Bank Secrecy Act, Fin. Crimes Enf't Network, https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act (last visited July 31, 2024).

[6] History of Anti-Money Laundering Laws, FinCEN, https://www.fincen.gov/history-anti-money-laundering-laws (last visited Aug. 23, 2024).

[7] U.S. Dep't of the Treasury, Fin. Crimes Enf't Network, Anti-Money Laundering Act of 2020, https://www.fincen.gov/anti-money-laundering-act-2020 (last visited Sept. 30, 2024).

[8] What is BSA Data?, Fin. Crimes Enf't Network, https://www.fincen.gov/what-bsa-data (last visited July 31, 2024).

[9] 31 U.S.C. 5312(a)(2)(A–Z).

> **(J) a currency exchange;...**
> **(K) an issuer, redeemer, or cashier of travelers’ checks, checks, money orders, or similar instruments;...**
> **(R) a licensed sender of money or any other 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 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;...**
> **(Y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or**
> **(Z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.”**

The BSA also provides the Secretary of Treasury with the authority to regulate and monitor financial institutions including banks and various non-bank financial services businesses. Under the Department of the Treasury Act of 1789, the Treasury was also granted authority to delegate responsibilities to offices within its department.[10] Pursuant to their authority, in 1990, Department of Treasury Order 105-08 established FinCEN, which is tasked with “provid[ing] a government wide, multisource intelligence and analytical network in support of the detection, investigation, and prosecution of domestic and international money laundering and other financial crimes by Federal, State, local, and foreign law enforcement agencies.”[11] The Director of FinCEN is responsible for “identify[ing] possible instances of non-compliance with the Bank Secrecy Act to Federal agencies with delegated responsibility for Bank Secrecy Act compliance.”[12] Thus, FinCEN became the primary regulatory authority for BSA-obligated entities.

FinCEN carries out this delegated authority through receiving and maintaining financial transaction data, issuing and interpreting regulations under the BSA, supporting law enforcement investigations and prosecutions, and providing government-wide access to financial transaction data and records.[13] In 1994, Congress passed the Money Laundering Suppression Act,[14] which amended the BSA by expanding FinCEN’s regulatory authority, creating stronger compliance and reporting requirements for BSA covered entities.[15] FinCEN’s

[10] 31 U.S.C. § 321(b).
[11] U.S. Dep’t of the Treasury, Treasury Order 105-08, Establishment of the Financial Crimes Enforcement Network (Apr. 25, 1990).
[12] U.S. Dep’t of the Treasury, Treasury Order 105-08, Establishment of the Financial Crimes Enforcement Network (Apr. 25, 1990).
[13] U.S. Dep’t of the Treasury, Fin. Crimes Enf’t Network, What We Do, https://www.fincen.gov/what-we-do#:~:text=FinCEN’s%20mission%20is%20to%20safeguard,strategic%20use%20of%20financial%20authorities (last visited Aug. 19, 2024).
[14] Money Laundering Suppression Act of 1994, H.R. 3235, 103d Cong. (1994) (enacted). Available at https://www.congress.gov/103/bills/hr3235/BILLS-103hr3235rfs.pdf.
[15] Registration of Money Services Businesses, 64 Fed. Reg. 45,438-53 (Aug. 20, 1999) (codified at 31 C.F.R. § 103 (5)).

regulatory and enforcement authority was later codified into statute with the passage of the PATRIOT Act of 2001, which established FinCEN as a Bureau of the Treasury Department.[16]

b. Statutory Authority Related to Money Transmission

The 1994 Money Laundering Suppression Act also defined a new category of financial institution under the BSA. The law added the term "money transmitting business" which was defined as any business other than the United States Postal Service which:[17]

> **(A) provides check cashing, currency exchange, or money transmitting or remittance services, or issues or redeems money orders, travelers' checks, and other similar instruments;**
> **(B) is required to file reports under section 5313; and**
> **(C) is not a depository institution (as defined in section 19(b)(1)(A) of the Federal Reserve Act.**

The Money Laundering Suppression Act also defined the term "money transmitting service" which includes:[18]

> **"accepting currency or funds denominated in the currency of any country and transmitting the currency or funds, or the value of the currency or funds, by any means through a financial agency or institution, a Federal reserve bank or other facility of the Board of Governors of the Federal Reserve System, or an electronic funds transfer network."**

The Act added a registration requirement for money transmitting businesses, stating that any person who owns or controls a money transmitting business must register the business with the Secretary of Treasury. The registration statement must include the name and location of the business, and the name and address of people involved in the business' affairs. The legislation added a harsh civil penalty of $5,000 per day in violation for those who failed to register.[19]

Importantly, the Act also amended the United States Criminal Code provision criminalizing the operation of an "illegal money transmitting business" to add severe criminal penalties for those persons convicted of owning, operating, or controlling an unlicensed money transmitting business under state and federal law.[20] With both civil and criminal liability, the legislation created harsh penalties for non-compliance, incentivizing parties to look to FinCEN in good faith to understand their obligations under the law.

[16] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 361, 115 Stat. 272, 329 (2001).
[17] Money Laundering Suppression Act of 1994, Pub. L. No. 103-325, § 8, 108 Stat. 2160, 2243 (codified as amended at 31 U.S.C. § 5330).
[18] Money Laundering Suppression Act of 1994, Pub. L. No. 103-325, § 8, 108 Stat. 2160, 2243 (codified as amended at 31 U.S.C. § 5330).
[19] 31 U.S.C. § 5330 (e)(1).
[20] 18 U.S.C. § 1960.

In 1999, following the mandate of Congress in the Money Laundering Suppression Act, FinCEN exercised their newfound regulatory authority under the BSA to define a new category of registrant called a "money services business" (MSB). Under FinCEN's regulations, the term ''money services business'' refers to five distinctive types of financial services providers: "currency dealers or exchangers"; "check cashers"; "issuers of traveler's checks, money orders, or stored value"; "sellers or redeemers of traveler's checks, money orders, or stored value"; and "money transmitters."[21] FinCEN defined an MSB as "a person wherever located in business, whether or not on a regular basis or as an organized or licensed business concern" that falls under one of the various categories listed under the BSA.[22]

Registered MSBs must maintain compliance operations with excessive data collection on customers and their transactions, which are then reported to FinCEN.[23] Importantly, unlike other regulated financial institutions, "MSBs become subject to FinCEN regulations not because of their license or charter, but rather based on the activities they conduct."[24] Therefore, FinCEN's regulatory definitions and subsequent interpretations of their regulations present the criteria for establishing whether a business is an MSB and must comply with BSA obligations. As one can imagine, numerous services and businesses used in everyday life qualify as a money transmitter and therefore as an MSB. Common examples of MSBs include Square, Paypal, and Venmo, businesses who transmit U.S. Dollars from one person to another.[25]

The term money transmitter was originally defined by FinCEN in a 1999 rulemaking[26] and revised in 2011 to include the acceptance of "value that substitutes for currency," subjecting CVC-denominated transactions to FinCEN jurisdiction.[27] FinCEN now defines a money transmitter under the Code of Federal Regulations as:[28]

> **(A) A person that provides money transmission services. The 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. "Any means" includes, but is not limited to, through a financial agency or institution; a Federal Reserve Bank or other facility of one or more**

[21] Registration of Money Services Businesses, 64 Fed. Reg. 45,438 (Aug. 20, 1999) (codified at 31 C.F.R. pt. 103).

[22] 31 C.F.R. § 1010.100(ff).

[23] 31 C.F.R. § 1022.320(a)(2).

[24] Enforcement Actions for Failure to Register as a Money Services Business, Fin. Crimes Enf't Network, https://www.fincen.gov/enforcement-actions-failure-register-money-services-business (last visited July 31, 2024).

[25] What is Money Transmission?, Modern Treasury, https://www.moderntreasury.com/learn/what-is-money-transmission (last visited July 31, 2024).

[26] Registration of Money Services Businesses, 64 Fed. Reg. 45,438 (Aug. 20, 1999) (codified at 31 C.F.R. pt. 103).

[27] Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses, 76 Fed. Reg. 43,585 (July 21, 2011) (codified at 31 C.F.R. pt. 1010, 1021, 1022).

[28] 31 C.F.R. § 1010.100(ff)(5).

> **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; or (B) Any other person engaged in the transfer of funds.**

In other words, a person must *accept* and *transmit* currency, funds, or other value as part of their business in order to be deemed a money transmitter—and simply providing "delivery, communication, or network access" does not constitute money transmission services. This definition was also included in subsequent FinCEN Guidance.

The Anti-Money Laundering Act (AMLA) of 2020, passed as part of the 2021 National Defense Authorization Act (NDAA), expanded the definition of the term "financial institution" to explicitly include businesses dealing in "value that substitutes for currency", such as CVCs.[29] The inclusion of this provision codified FinCEN's existing regulation and ensured that business entities engaged in the transfer, exchange, or custody of digital assets or CVCs are subject to FinCEN BSA oversight and must register with FinCEN. AMLA also redefined "monetary instruments" to include "value that substitutes for any monetary instrument" otherwise already defined in current law.[30] Both of these provisions solidified FinCEN jurisdiction and oversight over CVC money transmitting businesses. As a central element to the BSA framework money transmitting businesses must register with FinCEN.[31] Therefore, businesses that provide money transmission services denominated in CVCs must register with FinCEN as an MSB or face legal penalties.

Money transmitters have various surveillance, reporting, and compliance requirements which come along with their registration. Money transmitters are required to develop and implement a written anti-money laundering (AML) plan with internal policies and a compliance program.[32] Notably, Money transmitters must file Suspicious Activity Reports (SARs) when they detect a transaction or pattern of transactions that may involve illegal activity.[33] Money transmitters also are required to file Currency Transaction Reports (CTRs) when they have a cash-in or cash-out currency transaction, or multiple transactions, totaling more than $10,000 during one business day for any one person, or on behalf of any one person.[34]

[29] Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, § 6102(d), 134 Stat. 3388, 4547 (2021).

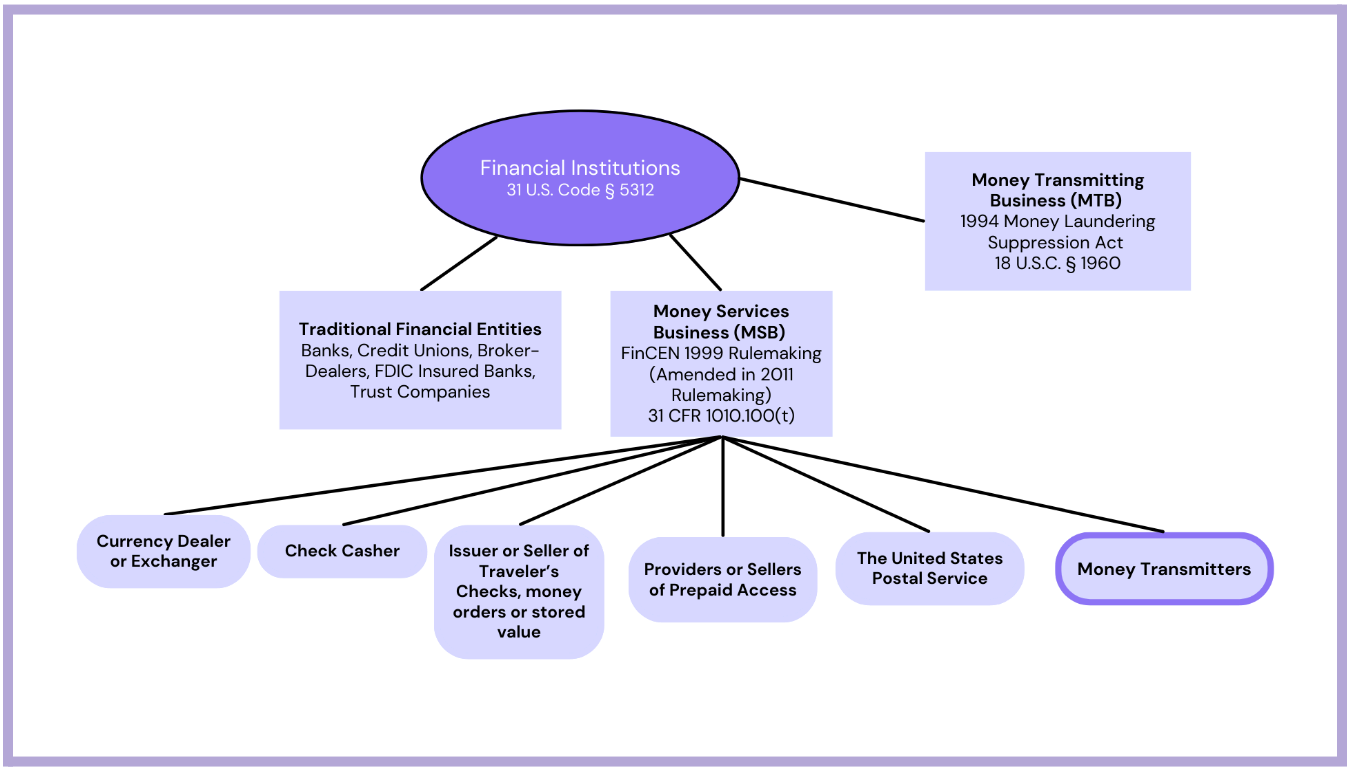
[30] Liana Rosen & Rena Miller, The Financial Crimes Enforcement Network (FinCEN): Anti-Money Laundering Act of 2020 Implementation and Beyond, CONG. RSCH. SERV. (Sept. 27, 2022), https://crsreports.congress.gov/product/pdf/R/R47255.

[31] 31 U.S.C. § 5330.

[32] Fact Sheet: MSB Registration Rule, FIN. CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/fact-sheet-msb-registration-rule (last visited Aug. 19, 2024).

[33] Money Services Business (MSB) Suspicious Activity Reporting, FinCEN, https://www.fincen.gov/money-services-business-msb-suspicious-activity-reporting (last visited Aug. 23, 2024).

[34] 31 C.F.R. § 1010.311.


Financial Institutions
31 U.S. Code § 5312
Money Transmitting Business (MTB)
1994 Money Laundering Suppression Act
18 U.S.C. § 1960
Traditional Financial Entities
Banks, Credit Unions, Broker-Dealers, FDIC Insured Banks, Trust Companies
Money Services Business (MSB)
FinCEN 1999 Rulemaking
(Amended in 2011 Rulemaking)
31 CFR 1010.100(t)
Currency Dealer or Exchanger
Check Casher
Issuer or Seller of Traveler's Checks, money orders or stored value
Providers or Sellers of Prepaid Access
The United States Postal Service
Money Transmitters

FinCEN Guidance Related to CVCs

In order to provide industry participants with greater clarity and consistency, FinCEN has issued guidance that serves as interpretations of the BSA and FinCEN's regulations. A guidance document is a statement of general applicability issued by an agency to inform the public of its policies or legal interpretations.[35] By definition, guidance documents "do not have the force and effect of law."[36] While agency guidance does not bind the public and is not considered legally binding by the courts, it can "'advise the public' of how the agency understands, and is likely to apply, its binding statutes and legislative rules."[37] Therefore, FinCEN guidance helps BSA-covered financial intermediaries to understand FinCEN's interpretation of its own regulations and the statute. This helps businesses and people to understand their compliance obligations, as well as their registration and reporting requirements.

With respect to CVC specifically, from its earliest days, FinCEN has responded to developments in the market by issuing guidance that helps people understand their obligations in the space. FinCEN first publicly stated its view that BSA MSB requirements included the transmission of

[35] U.S. Dep't of Justice, Limitation on Issuance of Guidance Documents, Just. Manual § 1-19.000 (2023), https://www.justice.gov/jm/1-19000-limitation-issuance-guidance-documents-1.
[36] *Perez v. Mortgage Bankers Ass'n,* 575 U.S. 92, 97 (2015) (quoting *Shalala v. Guernsey Mem'l Hosp*., 514 U.S. 87, 99 (1995)).
[37] *Kisor v. Wilkie*, *139 S. Ct. 2400* (2019) (quoting *Perez*, 575 U.S. at 97).

CVCs and digital assets in the publication of the 2013 FinCEN Guidance on Convertible Virtual Currencies. FinCEN defined CVCs as a "medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency," noting that CVCs did not have legal tender status in any jurisdiction."[38] Central to FinCEN's 2013 Guidance was the applicability of BSA definitions for MSBs and money transmitters to certain businesses using CVCs. The 2013 Guidance identifies three general CVC market participants: *users, administrators, and exchangers.*

FinCEN's general interpretation is that while administrators and exchangers are money transmitters, users are not. FinCEN found that a *user* of a CVC "is not an MSB under FinCEN's regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations."[39] FinCEN's rationale was that a user of a CVC does not fit into the BSA's definition of "money transmission services" due to the nature of a user's transaction activity because "such activity, in and of itself, does not fit within the definition of "money transmitting services" and therefore is not subject to FinCEN's registration, reporting, and recordkeeping regulations for MSBs."[40] This is because users merely employ CVC to affect the purchase of goods or services.

Alternatively, FinCEN concluded that *administrators* of centralized virtual currencies are money transmitters to the extent that it allows transfers of value between persons from one location to another.[41] However, FinCEN outlines "[decentralized] virtual currencies" which they define as a digital currency "(1) that has no central repository and no single administrator, and (2) that persons may obtain by their own computing or manufacturing effort."[42] In other words, decentralization plays a critical role in determining the extent of FinCEN's oversight of a CVC, which is explained in detail in the following section. Should a central issuer of a CVC exist—and should the issuer still maintain control of said CVC—they must adhere to BSA requirements. Also critical to the 2013 Guidance, FinCEN concluded that centralized exchanges, where users buy and sell CVC, qualify as MSBs. FinCEN wrote, an "*administrator* or *exchanger* is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption

[38] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, at 1, https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf (Mar. 18, 2013).
[39] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, at 2, https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf (Mar. 18, 2013).
[40] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, at 2, https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf (Mar. 18, 2013).
[41] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, at 3 (Mar. 18, 2013), https://www.fincen.gov/statutes_regs/Guidance/pdf/FIN-2013-G001.pdf.
[42] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, at 5 (Mar. 18, 2013), https://www.fincen.gov/statutes_regs/Guidance/pdf/FIN-2013-G001.pdf.

from the definition applies to the person."[43] They continue, "a person that creates units of [CVC] and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter."

In addition, a person is an *exchanger* (and therefore a money transmitter) "if the person accepts such [decentralized CVC] from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency."[44] In their 2013 Guidance, FinCEN recognizes that centralized exchanges custody users' assets and transmit them on their behalf. Thus, this guidance represented the first time that FinCEN explicitly prompted registration and reporting from CVC money transmitters, including centralized entities issuing crypto currencies and exchangers. In a subsequent administrative ruling, FinCEN determined that software developers are not money transmitters because "production and distribution of software, in and of itself, does not constitute acceptance and transmission of value, even if the purpose of the software is to facilitate the sale of virtual currency."[45]

FinCEN then further delineated their position in their 2019 Guidance. The 2019 Guidance explains how key concepts—such as hosted vs. unhosted services, and total independent control over the value in a transaction—relate to the determination of whether a particular entity is an MSB. The degree of control a CVC intermediary has over CVC is highly determinative of a CVC intermediary's legal status as a money transmitter and represents a continuation of FinCEN interpretation first set forth in 2013.

FinCEN states in their 2019 Guidance that the "regulatory interpretations of the BSA obligations of persons that act as intermediaries between the owner of the value and the value itself is not technology dependent."[46] Thus, a person that is not exempt from MSB status may be a money transmitter when the person engages in transactions covered under the definition of money transmission regardless of the technology employed for the transmission or the type of asset transmitted that substitutes for value. Therefore, the FinCEN analysis relies solely on the circumstances and facts around different business models in the CVC ecosystem such as wallets, exchanges, and different CVC services.

[43] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, at 3 (Mar. 18, 2013), https://www.fincen.gov/statutes_regs/Guidance/pdf/FIN-2013-G001.pdf.
[44] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, at 5 (Mar. 18, 2013), https://www.fincen.gov/statutes_regs/Guidance/pdf/FIN-2013-G001.pdf.
[45] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Virtual Currency Mining Operations, FIN-2014-R011, https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R011.pdf.
[46] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001, at 15, § 4.2, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (May 9, 2019).

The 2019 Guidance also clarifies that partial control over a user's CVC is insufficient to classify certain persons like wallet developers as money transmitters because money transmitters must exercise "total independent control" over the value.[47] The Guidance makes clear that software wallet providers, decentralized exchange developers, and other non-custodial software protocols are not regulated as money transmitters.

Application of FinCEN's Guidance on Activities Involving CVC

As previously discussed, FinCEN clarifies what it means to "accept and transmit" funds on behalf of another person multiple times in guidance. Specifically, in the 2019 Guidance, FinCEN develops four criteria for determining the regulatory treatment of persons involved in wallet applications: "(a) who owns the value; (b) where the value is stored; (c) whether the owner interacts directly with the payment system where the CVC runs; and (d) whether the person acting as intermediary has total independent control over the value."[48] While this criteria specifically applies to wallet applications, it serves as the appropriate criteria for any participant and software protocol or application across the CVC technology stack because, ultimately, if there is no "acceptance" of funds such that the provider has "total independent control" of them, then the nature of transactions flowing through the software protocol or application do not require customer or recipient identification in the same way that traditional financial intermediaries do.[49] Therefore, it is more accurate to deem software providers and operators as tool manufacturers and communication providers than intermediaries.

In determining the application of BSA requirements to the providers and operators of CVC technologies, it is critical to consider the nature of the technology and how its users interact with it. As explained in the next section, when CVC users custody their own assets to use decentralized networks directly, they have total independent control over their own assets and no one in the CVC technology stack accepts and transmits users' assets on their behalf, nor are they attempting to. Whether it's a wallet that provides storage; a front-end that allows access to a network; or a protocol that uses code to execute transactions upon users' instructions, full control remains with the user.

[47] Fin. Crimes Enf't Network, Guidance on Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001, at 16 (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[48] Fin. Crimes Enf't Network, Guidance on Convertible Virtual Currencies, FIN-2019-G001, at 15 § 4.2, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (May 9, 2019).

[49] Benjamin Gruenstein, Evan Norris & Daniel Barabander, *Secret Notes and Anonymous Coins: Examining FinCEN's 2019 Guidance on Money Transmitters in the Context of the Tornado Cash Indictment*, Int'l Acad. Fin. Crime Litigators, (Sept. 2023), https://www.cravath.com/a/web/qyCBWVBLEMsqxPHtd9ykoc/87ntut/the-international-academy-of-financial-crime-litigators.pdf.

c. Blockchain Protocols

At its foundation, the technology stack begins with a P2P protocol and network. A protocol is the set of rules and standards that govern communication between different peers in a network, whereas the network itself consists of independent people or businesses that operate the hardware and software needed to participate in the network. Specifically, in a P2P network there are two or more people or businesses who operate computers (nodes) and share authority and storage of the data via the internet. There is no need for a central server in a P2P network and, therefore, no single entity has control over it. This differs from the more popular client-server model, where users request and receive services from a centralized server that stores, manages, and protects the data; for example, a user's device interacts with Facebook by sending a request to Facebook's servers, which then retrieves requested data—posts, likes, etc.—and runs the application. Essentially, Facebook's parent company, Meta, has complete control over who can or cannot access their data and applications.

A mechanism for storing a P2P network's data and communicating information between nodes is known as a *public blockchain*, which is a type of distributed ledger technology. Essentially, each node in the P2P network runs a software application that enables it to communicate with other nodes in the network, validate new transactions and blocks according to the network's rules, maintain a copy of the blockchain, and have the option to participate in the creation of blocks.

Information stored in a block is encoded by a *hash value* and includes the hash value of the previous block to link two blocks together, creating a chain; hence, the term "blockchain." A hash value is a unique string of characters that is generated by a specific algorithm. This algorithm takes the transactions in the block, the hash of the previous block in the chain, and other relevant block data as input, and then outputs the hash value—i.e., a cryptographic signature. Each block is verified by a consensus mechanism, which is the process by which the network's nodes agree on the validity of transactions and the state of the blockchain.

Before a transaction reaches miners or validators (explained in the next section), it undergoes initial verification by the network's nodes for completion and correctness (e.g., signature validity, balance sufficiency, etc.). Once verified, the transaction is placed in a memory pool, or *mempool*—a pool of unconfirmed transactions—where it awaits inclusion in a block by a miner or validator. When a block is proposed, each node receives said block, independently validates its authenticity, and adds it to their copy of the blockchain. Through this process, the network reaches consensus on what is the correct chain of transactions—also known as *network synchronization*.

Network synchronization is an ongoing process by which all nodes in a network update their copies of the blockchain to ensure they all hold the same, most current version of the blockchain. When a new block is created or verified by a node, the node then broadcasts it to neighboring nodes in the network and the process continues as such. When a node receives a new block that is attached to a part of the blockchain that it doesn't have, it will compare this chain to its own. The node adopts the chain based on criteria for chain selection that varies depending on the consensus mechanism. The most popular forms of consensus mechanisms for blockchain networks are *Proof-of-Work (PoW)* and *Proof-of-Stake (PoS)*.

d. Consensus Mechanisms

PoW is most notably used in the Bitcoin network and requires nodes, known as *miners,* to compete to solve a cryptographic puzzle by finding a specific value known as a *nonce*. Miners combine this nonce with the block's data (e.g., previous block hash, timestamp, etc.) through a computing process known as a *hash function*, which then creates a unique string of characters called a *hash value.* The goal is to find a hash value that meets a specific criteria set by the network. Miners essentially input different nonces through the hash function until one succeeds. Then the network checks that the hash value and the block's transactions are correct. If everything is correct, the miner is rewarded with a newly minted network token such as a bitcoin.

Mining requires computing power and energy, which is used as an incentive system and security mechanism. A bad actor attempting to introduce a fraudulent block is disincentivized by the high energy cost required to solve for the hash value that would be lost when the network does not validate their block. Essentially, the actor would incur a significant energy cost for nothing in return. In order for a bad actor to successfully implement their desired block, they would need to control over 51% of the network's computational power to validate their block. This would take a tremendous amount of energy and would cost them more than they would profit, especially as networks like Bitcoin are rapidly expanding.

Nodes in a PoW network adopt the longest chain as a consensus for maintaining network synchronization. This is because the longest chain has accumulated the most proof of work, indicating that it has the highest level of computational effort and agreement among miners, and is therefore considered to contain the most valid and trusted blocks.

PoS, notably adopted in the Ethereum network, takes a different consensus approach where the blockchain protocol selects one node to validate and create a new block; as a result, the network uses less energy because nodes no longer need to expend computational power to compete to solve a cryptographic puzzle.

To prevent bad actors from manipulating the information stored on a network, *staking* requires providing collateral to the network in order to become a *validator*. While the selection process of validators is random, the probability of being selected increases with the amount staked. The validator node then validates the transactions, creates the block, and adds it to the blockchain. Successful validators are rewarded with a newly minted network token such as an ether on the Ethereum network. Staking also disincentivizes malicious behavior through punitive measures. If a validator acts dishonestly or negligently, their staked tokens are slashed, meaning the blockchain's underlying software automatically reduces the validator's staked tokens once the network detects the behavior and the nodes notify each other. Thus, the probability of being selected as the validator node is proportional to the amount of tokens staked as the validator has more to lose.

Unlike in a PoW network, where nodes adopt a chain based on the computational work done, nodes in a PoS network adopt a chain based on the amount of stake (tokens) backing it. When nodes stake their tokens, they do so to participate in the validation process. And even if they are not chosen as the validator for a specific block, their staked tokens remain active and could be used in future block validations. Therefore, the valid chain is the one backed by the most staked tokens because it reflects the consensus of the network—i.e., participants are willing to stake their assets on its validity, signaling their confidence in that chain.

e. Peer-to-Peer Transactions

A novel aspect of CVC transactions is that they are done in a P2P manner—i.e., without a third-party intermediary. This is securely done through a form of *asymmetric cryptography*—also known as *public key encryption*—so that a user is not required to trust an intermediary or another user to transact. Asymmetric cryptography is an encrypted method of communication—or in the case of CVC, a transaction—using a pair of keys: a public and a private key.

A user can generate a private key by using cryptographic algorithms that produce a random string of characters. The private key is then the basis for mathematically generating the corresponding public key. Importantly, while public key generation is easily computed, it is nearly impossible to reverse-engineer the private key from the public key—hence, making it a secure cryptographic process.

The public key, which can be shared openly, is used to verify digital signatures, while the private key is used to create these signatures for transactions. And because both keys are uniquely associated with each other and mathematically linked, only the private key can decrypt what the public key has encrypted. For example: Alice sends Bob a transaction using his public key to encrypt it so Bob can be the only one to decrypt (i.e., open or accept) the transaction using his private key.

Asymmetric cryptography is also used in authenticating the sender's identity and the transaction's information by producing a *digital signature*. This process begins with the automatic generation of a cryptographic hash of the transaction—much like the hash generated for a block, this hash serves as an identifier and consists of a long string of characters. The sender then encrypts the transaction's hash with their private key, serving as the digital equivalent of a signature. Upon receiving the transaction, the network uses the sender's public key to decrypt the digital signature, retrieving the original hash. Also upon receipt, a new hash is generated in the same manner as the original hash, and because it is generated using the same transaction data, the two hashes are identical. This allows the network to compare the hashes and verify that the transaction has not been altered in transit and confirm its authenticity. Overall, this process not only authenticates the sender's identity but also ensures the integrity of the transaction.

Lastly, to make sending CVC more user-friendly, a blockchain address is mathematically generated from a public key as a shorter string of characters. This serves as a more practical representation used for securely sending and receiving transactions. With a better understanding of asymmetric cryptography, it is evident that this mechanism provides a variety of benefits such as: securing transactions and user information without needing an intermediary, enabling non-repudiation, and eliminating the need to trust other users.

Blockchain Miners and Validators: Regulatory Treatment

First and foremost, miners and validators are all persons or businesses operating computers and applications. In other words, blockchains are dependent on people for their maintenance and security, and therefore, the conduct of those people require analysis of their regulatory treatment under FinCEN's money transmission laws. In their 2013 Guidance, FinCEN evaluates whether or not centralized "administrators" of CVCs—i.e., people putting CVCs into circulation and who have the authority to redeem them[50]—are money transmitters and determines that they are because of the nature of their business.[51] That is because centralized administrators control the asset and have authority over "transfers of value between persons or from one location to another" with regard to said asset.[52] In other words, centralized administrators have "total independent control" over the movement of funds.

FinCEN does not *per se* address the regulatory treatment of miners or validators in their guidances; however, they do exempt administrators of decentralized CVCs from being money transmitters. In this case, the CVC is deemed decentralized if it "has no central repository and no single administrator" and if it was obtained through the person's "own computing or manufacturing effort"[53]—i.e., mining and validating rewards. And while FinCEN does not explicitly state why this circumstance grants exemption, it's clear that those who create decentralized CVCs through their own computing and manufacturing efforts do not have total independent control over the CVC in the way that an administrator who has the authority to redeem them does. This is because an administrator who maintains a repository and has full discretion over a CVCs use has full control over the CVC. Miners and validators, on the other hand, create decentralized CVCs by participating in the consensus mechanism for a network

[50] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2012-G001, at 3, https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf (Mar. 18, 2013).

[51] Id..

[52] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2012-G001, at 4, https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf (Mar. 18, 2013).

[53] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2012-G001, at 5, https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf (Mar. 18, 2013).

and are rewarded by the network’s underlying software—they do not control its existence nor its use.

Considering transactions themselves, a blockchain is simply a tool for conducting P2P transactions, and those involved in the network maintain the software. Transactions are securely communicated from one user to another without an intermediary using asymmetric cryptography, and the blockchain serves as a ledger to record these transactions. Both miners and validators serve the same purpose of validating transactions and constructing blocks; meanwhile blockchain nodes verify the validity of these blocks and keep copies of the ledger to maintain the network’s existence. In other words, blockchain miners and validators in no way accept funds from a user and transmit them on a user’s behalf.

Wallet Providers: How It Works

Fundamental to CVC transactions on a decentralized network, is the concept of self-custody. Users employ *unhosted wallets* to control their own assets and to communicate with a blockchain network. Contrary to popular belief, assets are not actually stored in a wallet; rather, the wallet stores the cryptographic keys (public and private) that enable full control of assets. CVC should be thought of as data packets, as they represent pieces of information—specifically ownership of a certain value—that is transferred between users. And the blockchain simply records transactions and balances, but does not store or control any assets. Users have total control over said assets, because the cryptographic keys are the only mechanism for access and transmission of the assets.

A user connects their wallet to a blockchain through the internet and can rely on a related application to provide an interface for communicating with the network. The user interface displays the user’s public key or blockchain address for receiving assets, which can be displayed as a long string of characters. When sending assets, the sender specifies the recipient's blockchain address and the amount to be sent, then uses their private key to provide a digital signature. Under the direction of the user, wallet’s software communicates with the associated blockchain to update the user’s balance on the ledger as transactions are processed.

Unhosted wallets generally come in two forms: “hot” and “cold”. Keys kept in hot storage are connected to the internet. In contrast, users of cold storage wallets store keys offline, adding another layer of security to them as keys are not exposed to internet-based attacks. To perform transactions with cold storage, a user signs transactions offline with their private keys, and then the signed transaction is transferred to an online device (e.g., computer or mobile phone) to be broadcast to the blockchain network. For example, if a user had a hardware wallet—i.e., a physical device used for cold storage—and wanted to send a transaction, the user could connect the wallet to a computer and open an application compatible with the hardware wallet to input the transaction details.

In contrast, third-party custodians offer hosted wallets as a service for custodying users' assets on their behalf. For a hosted wallet, the custodian maintains the private key instead of the user. So, in this circumstance, the user can conduct a transaction the way they would in the traditional financial system: by notifying the custodian so they can conduct a transaction on the user's behalf. These custodians have total independent control of users' assets.

Wallet Providers: Regulatory Treatment

As previously discussed, FinCEN provides a rules-based rubric for defining whether a wallet provider or developer is a money transmitter. FinCEN's regulatory determination depends on four criteria: "(a) who owns the value; (b) where the value is stored; (c) whether the owner interacts directly with the payment system where the CVC runs; and, (d) whether the person acting as intermediary has total independent control over the value."[54] FinCEN assesses both hosted and unhosted wallet providers to determine their regulatory treatment, which effectively differentiates the activity conducted by both providers.

As expected, because hosted wallet providers "receive, store, and transmit CVCs on behalf of their accountholders," FinCEN maintains that these providers are money transmitters.[55] As FinCEN correctly points out, hosted wallet providers have "total independent control over the value" even if they are "contractually obligated to access the value only on instructions of the owner."[56]

On the other hand, FinCEN correctly defines an unhosted wallet as "software hosted on a person's computer, phone, or other device that allows the person to store and conduct transactions in CVC."[57] Importantly, FinCEN clarifies that unhosted wallets "do not require an additional third party to conduct transactions."[58] The user has total independent control over their assets, and the unhosted wallet itself is as FinCEN defines it: software hosted on a person's device.[59] Providers of the unhosted wallet software do not play a role greater than simply developing and providing a tool for users to store their assets and conduct their own transactions—i.e., they do not accept and transmit transactions on behalf of users.

Smart Contract and DeFi Protocol Developers: How It Works

a. *Smart Contracts*

Public blockchain technology serves as the foundational layer for CVC transactions, but its function is limited to the secure recording and broadcasting of data in a decentralized manner.

[54] Fin. Crimes Enf't Network, Guidance on Convertible Virtual Currencies, FIN-2019-G001, at 15, § 4.2, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (May 9, 2019).
[55] Id.
[56] Id.
[57] *Ibid.* at 16.
[58] Id.
[59] Id.

However, the introduction of the Ethereum blockchain in 2015 extended blockchains' capabilities by allowing anyone to develop applications and systems that leverage its core functions. Among these are DeFi protocols, which go beyond just P2P transactions to a wider range of financial services. DeFi consists of sets of a blockchain-based software program known as a *smart contract* to automatically execute certain actions when a user initiates the transaction and predefined conditions are met, eliminating the need for an intermediary. A simple analogy for a smart contract is that of a vending machine: the vending machine automatically releases a bag of chips on the condition that it receives $2. The consumer initiates the transaction then solely relies on code to execute it, not a third party vendor. And while the smart contract automatically executes transactions, the transactions are still initiated by the user and still verified by the blockchain network and recorded on the ledger—i.e., the fundamentals of a P2P blockchain transaction do not change. In other words, a smart contract is simply a software tool for users to conduct a variety of financial activities without an intermediary and employ the verifiability and security of a blockchain.

The deployment of a smart contract is no different than other blockchain transactions. Essentially, anyone can take software code and deploy it on a blockchain, and the blockchain's nodes will accept the code so long as the deployment transaction is a valid transaction. Here is how it works:

1) **Developer writes the code;**
2) **The developer, or another user wishing to deploy the code, creates a *deployment transaction* that includes the bytecode of the smart contract and its initialization parameters, and signs the transaction with their private key to authenticate and authorize it—the sender does not specify the recipient;**
3) **The deployment transaction is then sent to the sender's connected nodes within the blockchain network;**
4) **These nodes then relay the transaction to their own connected nodes and the transaction continues to propagate across the network;**
5) **Each receiving node verifies and validates the transaction's digital signature and sufficient gas, and ensures that it complies with the network's rules — they do not audit the smart contract's code;**
6) **Once the deployment transaction has reached consensus, miners or validators include it in their new block, which finalized the deployment;**
7) **Once it is added to the blockchain, the smart contract is activated and is assigned a unique address on the blockchain — its bytecode and initialization parameters are stored in the contract's storage.**
8) **Once it is deployed, the smart contract is autonomous and immutable, and anyone can use it.**

Using a smart contract to transact involves specifying details such as the sender address, recipient (i.e., smart contract) address, transaction value, and gas fees. This includes the data field which contains the instructions (i.e., the function) for the smart contract upon receiving the transaction. Specifically, the data field consists of two elements: a function identifier and a function argument.

The function identifier signals to the smart contract which function to execute (e.g., borrowing funds, token swapping, or voting on a governance proposal). The function argument for a transaction consists of the specific data or parameters that need to be provided to the smart contract function for it to execute it properly (e.g., amount of tokens or the voter's choice). The two elements ensure that a smart contract knows which operation to perform.

Constructing a transaction can be done manually by users with technical expertise; however, it is more commonly done by connecting the user's unhosted wallet to the DeFi protocol's front-end website (later discussed), as the process is much more intuitive and approachable. After constructing the transaction, the user then uses their private key, securely stored in their wallet, to sign the transaction and broadcasts it to the blockchain network. Once the transaction is included in a block and validated, it triggers the smart contract to automatically execute the logic defined in its code.

b. DeFi Protocols

DeFi protocols are a system of interrelated smart contracts and the governing arrangement designed to ensure distributed authority among a decentralized and disaggregated group of unrelated users. DeFi protocols offer communication, connectivity, or software services that parties can utilize to communicate trading interests, but they do not intermediate transactions. Hence, even when DeFi protocols originate from a single software developer or small group of developers, they maintain their decentralization.

It's important to recognize that while the term 'protocol' is used interchangeably between P2P networks and DeFi protocols, the two are distinct. As noted in the previous section, a P2P network is simply the governing model for communication method between two or more devices (nodes), and a blockchain is the mechanism used to store and communicate the data (transactions) between nodes; whereas, the term "protocol" in DeFi encompasses the rules, functions, and interactions defined by a collection of smart contracts that allow people to engage in specific activities.

As previously explained, a smart contract's code is immutable once deployed on a blockchain, which ensures security and trust, but also means that bugs and inefficiencies in the smart contract code are permanent unless mechanisms for upgradability are implemented. One approach is to deploy a new smart contract and migrate users over to the new one. This poses a challenge of upgrading a contract's code while preserving its existing state—i.e., data such as transaction history, user balances, etc. In this context, the migration from one smart contract to another involves transferring data which could lead to disruptions.

i. Upgradability

1. Data Separation Pattern

Fortunately, DeFi protocols can be designed to be upgradable through various architectural patterns. This has led to more innovative approaches to upgradability, such as a data separation pattern. In a general sense, a data separation pattern is a software design pattern that separates the state (i.e., data) from the business logic (i.e., code that dictates how the smart contract behaves). This is done by having one smart contract solely for data and one contract for logic. The data contract stores all the data and includes functions that allow for other contracts to access and modify the data. This contract remains persistent and is not typically the focus for upgrades. The logic contract maintains operational functions (e.g., transferring tokens, updating balances, etc.) and it refers to the data contract when it needs to read or modify data.

When upgrading a DeFi protocol that is designed with a data separation pattern, the logic contract is the smart contract that undergoes an upgrade and the data contract remains persistent. Due to the immutability of smart contracts, this means that the protocol's governance would choose a new logic contract to deploy on the blockchain and ensure that the new logic contract refers to the existing data contract.

The problem with the data separation method is that once a new logic contract is made, any smart contract connected to the original logic contract, or any front-end providing access to it, must be updated to reference the new logic contract. Furthermore, separating the data and logic into separate contracts can be expensive, as the logic contract has to make external calls to the data contract and requires more gas to do so than a smart contract that can read or modify the data stored within itself. Given these two factors, protocol developers have opted to a proxy pattern design which also separates the data but differs in how it handles the contract logic and data storage.

2. Proxy Pattern

In a proxy pattern, a placeholder or intermediary (i.e., the proxy) controls access to another object (i.e., the target). In the context of a DeFi protocol, there are two smart contracts: a proxy contract and an implementation contract. The proxy contract acts as a front-facing contract for users and other smart contracts, and delegates their calls to the implementation contract, which holds the main business logic. Importantly, the proxy contract typically stores all the contract's state.

An implementation contract contains the actual business logic and can be updated or replaced to upgrade the system. If there is an upgrade to the smart contract's logic, it is simply deployed as a new smart contract and the proxy contract is redirected to the new implementation contract. One way to understand the two contracts' relationship is to imagine the proxy contract as a universal remote and the implementation contract as a TV—the remote adds a layer of convenience and functionality to controlling what the TV does, but does not need to be changed when the TV's system is upgraded.

The proxy pattern approach allows for smart contract upgrades without changing the smart contract's address, preserving the contract's state, and ensuring continuity for the protocol's users. However, it's important to note that upgradability is typically left to smart contracts that are less foundational to the protocol's functionality such as those that handle auxiliary functions—i.e., features and operations that support the main functionality of the protocol, but are not central to the core mechanics. Smart contracts that are essential to the core mechanics of the protocol—e.g., privacy pools—are often made immutable to ensure a high level of security, as changes could threaten the integrity of the protocol.

Importantly, while a proxy pattern utilizes two smart contracts, just like a data separation pattern, it uses a specific function that allows it to execute the logic contracts code as if it were its own. In other words, users, front-ends, and other smart contracts use the proxy contract to directly execute code in the logic contract. Meanwhile, protocols that are designed with a data separation pattern require users, front-ends, and other smart contracts to interact with the logic contract that then executes external calls to the data contract, making the process more expensive and less convenient when there is an upgrade.

c. Decentralized Exchanges

Decentralized Exchanges (DEXs) are a subset of DeFi protocols where a variety of digital assets can be traded. As any DeFi protocol, DEXs are simply software programs that run "on top of" a blockchain, and users can employ them to conduct a variety of economic activities and financial transactions.

An important aspect to recognize is that unlike the traditional financial system that requires users to provide personal information for a third party to make transactions on their behalf, DEXs are public software that anyone can directly interact with and do not require them to share personal information to issue a transaction. Furthermore, because transactions are done via smart contracts, DEXs are non-custodial and users do not have to trust a third party with their assets.

There are two kinds of DEXs that are popularly used, the first uses an on-chain order book much like in a traditional stock exchange to match buyers and sellers. However, as the name implies, the matching process occurs on-chain—i.e., on the blockchain—through smart contracts. Essentially, when a buyer's order matches a seller's order, the smart contract automatically executes the transaction and it is then validated and recorded on the blockchain. These transactions are executed by software (smart contracts) and not a centralized entity overseeing the exchange, ensuring a trustless and P2P trading environment.

Another popular DEX is known as an automated market maker (AMM) and that uses the ratio of two assets in a special-purpose smart contract called a liquidity pool in which users (known as liquidity providers) deposit assets for others to trade and in return receive a portion of the trading fees. The AMM uses the ratio to determine the relative price of two assets. In this formula, x and y represent the assets and k represents the constant product value. The AMM calculates the prices of each asset based on their supply and demand: as x increases in supply, its price decreases to maintain a constant product value of k. As the exchanges are validated by the underlying blockchain, new prices are calculated in real-time. One benefit of this is that an exchange cannot manipulate asset pricing as it is mathematically formulated.

The price determination is the key difference between the two types of DEXs: while on-chain order books determine price based on what is set between buyers and sellers, AMMs determine their price based on the ratio formula above.

Smart Contract and DeFi Developers: Regulatory Treatment

Fundamentally, DeFi protocols offer communication, connectivity, or software services that parties can utilize to communicate trading interests, but they do not intermediate transactions.

In the 2019 Guidance, FinCEN differentiates two kinds of trading platforms and their regulatory treatment under the BSA. FinCEN applies the BSA exemption of providing the "delivery, communication, or network access services used by a money transmitter to support money transmission services" to trading platforms and DEXs.[60] FinCEN clarifies that a trading platform who "only provides a forum" for trading, regardless of its automation, is not deemed a money transmitter.[61] FinCEN distinguishes this activity from a trading platform that "purchases the CVC from a seller and sells it to the buyer," which is aligned with the act of accepting and transmitting funds.[62]

Furthermore, FinCEN distinguishes between anonymizing *service* providers and anonymizing *software* providers. In the 2019 Guidance, FinCEN applies the providing "delivery, communication, or network access" exemption to determine that software providers are not money transmitters.[63] In doing so, FinCEN recognizes and concludes that a user employing the software provided by a third-party to conduct transactions on their own behalf is quite different from an anonymizing service provider accepting and transmitting funds as a money transmitter or intermediary financial institution.[64]

[60] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001, at 24, § 5.1, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (May 9, 2019).

[61] Id.

[62] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001, at 24, § 5.1, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (May 9, 2019).

[63] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001, at 20, § 4.5.1(b), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (May 9, 2019).

[64] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, at 2, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf (Mar. 18, 2013).

In both instances, FinCEN illustrates a clear understanding of the nature of smart contracts and DeFi protocols. These are software applications deployed on a blockchain that serve as tools for users to conduct financial activities beyond just basic transactions. Users do not surrender their assets to an intermediary to transmit value on their behalf; instead, they employ software to transact on their own behalf. Providers of such software are not involved in these transactions besides providing the software employed. Therefore, they cannot possibly be deemed money transmitters under the law.

Front-end Developers: How It Works

Accessing a DeFi protocol for those with less technical expertise begins with obtaining a wallet. As previously explained, the wallet provides a front-end interface (i.e., a website or application) that facilitates communication between the user and the DeFi protocol over the internet. It displays the user's public key for receiving assets in a variety of ways, such as a long string of characters or a QR code.

When initiating the transaction, the wallet specifies the recipient's blockchain address, the amount to be sent, and uses the sender's private key to sign the transaction, ensuring its security and authenticity. As the transactions are validated, the amount of digital assets associated with a given public address is updated. To further simplify the process, front-end websites have been developed for users to easily connect their wallets and perform actions on a DeFi protocol.

For clarification, the front-end does not intermediate the transaction itself, it acts more as a "translator" from humans to blockchains, similar to the way email works. When sending an email, a person writes the email using the Roman alphabet to coherently write words and sentences. When that email is sent, the email protocol "translates" the message into a form that can be transmitted to the recipient in data packets that can be sent over the internet. Likewise, DeFi front-ends "translate" human-understandable activities into a data form that blockchains can understand.

Front End Developers: Regulatory Treatment

Developers and providers of front-ends are the most akin to a "person that only provides the delivery, communication, or network access services used by a money transmitter to support money transmission services." A front end is software that is generally hosted on the internet as a user-friendly access point to blockchains and DeFi protocols. It simply communicates data to a user that a protocol and blockchain can decipher and execute. Providing a front end to a DeFi protocol is providing "delivery, communication, or network access" for users to employ on their own behalf.

Relayer Operators: How It Works

Generally, relayers are a third party service—i.e., a software application typically run by an individual or group—that organizes transactions on behalf of users. Essentially, after a front-end generates the transaction data required to interact with the relevant smart contracts, it sends the data to a relayer. The relayer verifies that all the data is complete and correct before it optimizes the transaction. What this means is that the relayer determines the optimal gas fee for the transaction based on the current network conditions. While relayers recommend the optimized gas fees, users still have to approve the gas fee, as they have to approve the transaction overall. For complex transactions involving multiple steps, the relayer ensures that the steps are organized in the correct sequence to mitigate the risk of error. Overall, relayers are used for gas optimization and for organizing complex transactions. Importantly, relayers do not take custody of users' assets and those assets remain in the user's possession throughout an interaction with a relayer. Users still approve the transaction with their private key before it is broadcasted to the network. In other words, a relayer does not control the movement of funds.

Relayer Operators: Regulatory Treatment

As with each previous participant in the technology stack, relayer operators do not accept and transmit funds on behalf of users. They are simply running software applications for optimizing and organizing data that the user must then approve and broadcast from their wallet application.

RPC Nodes: How It Works

After a user approves a transaction with their private key, the wallet application broadcasts the transaction via a remote procedure call (RPC) node. An RPC node is a server or computer that receives the signed transaction data from the wallet and then propagates it across the blockchain network so it can be validated by other nodes and eventually included in a block. There are many RPC nodes run by individuals and groups around the world, contributing to the decentralized nature of blockchain networks. Importantly, the difference between an RPC node and a relayer is that a relayer organizes data for the RPC node to broadcast to the network. Even in the case of a privacy-enhancing relayer, the relayer still uses an RPC node to broadcast the transaction.

RPC Nodes: Regulatory Treatment

RPC nodes predate blockchain technology and are widely used in computer science and network communications between different software systems. They are not designed as intermediaries for financial transactions but for communicating data, and that is exactly their role in CVC transactions. Operators of RPC nodes do not accept and transmit value on behalf of users, they communicate transaction data to nodes in a decentralized network if and when a user approves a transaction with their private key. They're akin to a messenger between a user and a network. Therefore, to suggest they are accepting and transmitting funds on behalf of another person is technologically false—they do not have the total independent control required to move funds from one person to another.

Policy Considerations

Aside from the current regulatory analysis, it's equally imperative to analyze the practicality and prudence of imposing BSA obligations on participants across the technology stack. Participants across the technology stack can serve as software providers or operators that verify, communicate, and organize data. Data that consists of verifiable information, such as wallet address and digital signature, and does not require users' personal identifying information. For certain participants like those mentioned in this paper, requiring them to adhere to information collection and reporting requirements would completely alter the nature of the technology and their operations, as well as provoke constitutional concerns.

For example, miners and validators have no practical way of meeting BSA obligations should they be deemed money transmitters. This is because blockchain transactions involve wallet addresses, not personally identifiable information like individual's names and addresses, which would make it difficult or impossible to identify users in block creation. Also, because these networks consist of unrelated persons from around the globe, the ability to carry out compliance is highly constrained. Applying classic BSA requirements to miners and validators would result in criminalizing their conduct when they have no way to comply in the first place, unless blockchains were centralized, defeating the purpose of their existence.

In extrapolating this, it becomes clear that this is true across the technology stack. For example, unhosted wallet providers cannot functionally comply with BSA obligations for money transmitters either. Unhosted wallet providers do not collect identifying information of persons who choose to purchase their software products—much like a safe manufacturer does not identify persons who purchase their safes. So even with blockchains' transparency and traceability, unhosted wallet providers cannot track their customers' qualifying transactions (over $10,000) without connecting an identity to a wallet address. Imposing information collection requirements on unhosted wallet providers so they may comply with the BSA would be akin to imposing these requirements on safe manufacturers—it's nonsensical.

Furthermore, and equally problematic, such an expansion is not within the scope of the BSA, which is intended for financial institutions who accept and transmit funds on behalf of others. In fact, the BSA's information collection regime in general is predicated on the notion that customers voluntarily provide their personal information to traditional financial services businesses.[65] This is quite different from operating, providing, and using software tools, as doing so does not require users to share any information about themselves with anyone to use the technology. Should software providers and operators be required to comply with the BSA as money transmitters, users would no longer be voluntarily providing their identifying information and be forced to surrender their right to privacy. This is coercion in the strictest sense and should be met with scrutiny under the Fourth Amendment.

[65] *United States v. Miller,* 425 U.S. 435 (1976).

Financial privacy cannot be so easily dismissed, especially given the rise of technology and its surveillance capabilities. Public blockchains, for example, allow complete traceability of all transactions in a network. And while users are pseudonymous, advanced data analytics software has proven useful in tracking down and identifying the persons behind wallet addresses.[66] This is a positive development for law enforcement purposes, but the reality is that only a small group of users are leveraging blockchains for illicit activity,[67] and law-abiding users have legitimate reasons for maintaining financial privacy. A person's financial transactions can paint the most intimate picture of their beliefs, associations, and activities[68]—aspects of their lives which could lead to discrimination or harassment at the very least.[69] Exposing users' identities would provide the world with unprecedented access to all past and present transactions of users, as well as their balances, which could make users with large amounts of sums the targets for exploitation. Additionally, personal information collection has proven to be the target of large-scale hacks involving the sensitive information of millions of Americans, with a few happening in 2024 alone.[70] For these reasons developers have moved to make privacy-enhancing DeFi protocols, among other tools, for mitigating these risks. The United States should not only protect this development, but encourage it as it serves the interests of all Americans.

Conclusion

Given the nature of P2P CVC transactions and DeFi, it's evident that software providers and operators across the technology stack are not money transmitters. FinCEN recognizes this distinction through its guidances—guidances which are used to elaborate on the regulatory authority FinCEN has been granted.[71] Unfortunately, this has not stopped the Department of

[66] U.S. Dep't of Just., *Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency*, (Feb. 8, 2022), https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency?s=08.

[67] Chainalysis, *How to Use Blockchain Intelligence to Investigate Crypto Crime*, Chainalysis Blog (May 4, 2023), https://www.chainalysis.com/blog/investigate-crypto-crime-blockchain-intelligence/.

[68] Brief for Amicus Curiae DeFi Education Fund Supporting Appellant at 4, Harper v. IRS, No. 23-1565 (1st Cir. Oct. 20, 2023) (substantially citing Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018)).

[69] Jay Stanley, *We Need Digital Cash That is Actually Like Cash*, ACLU (Mar. 28, 2022), https://www.aclu.org/news/privacy-technology/we-need-digital-cash-that-is-actually-like-cash; Jay Stanley, *Say No to the "Cashless Future" — and to Cashless Stores*, ACLU (Aug. 12, 2019), https://www.aclu.org/news/privacy-technology/say-no-cashless-future-and-cashless-stores.

[70] Jon Healey, *Hacker Claims Theft of Every American's Social Security Number*, L.A. Times (Aug. 13, 2024), https://www.latimes.com/business/story/2024-08-13/hacker-claims-theft-of-every-american-social-security-number; Sarah Krouse, Dustin Volz, Aruna Viswanatha & Robert McMillan, *U.S. Wiretap Systems Targeted in China-Linked Hack*, Wall St. J. (Oct. 16, 2024), https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b.

[71] Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, No. FIN-2019-G001, § 4.5.1(b) (Anonymizing Software Provider), at 20 (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

Justice (DOJ) from indicting the developers of Tornado Cash in 2023.[72] The choice to impose criminal penalties on software developers is problematic in this context because participants in the space depend on FinCEN's authorized guidance to understand their regulatory treatment and obligations, and even if they act according to FinCEN in good faith, they may still be subject to enforcement from agencies like the DOJ. This is why it's imperative that Congress take action and pass sensible legislation meant to distinguish these participants from being money transmitters—legislation like the Blockchain Regulatory Certainty Act.[73] Otherwise, persons involved in P2P CVC transactions and DeFi would remain in an ambiguous regulatory environment that comes with significant punitive consequences.

[72] Indictment, *United States v. Roman Storm and Roman Semenov*, No. 1:23-cr-00430, ECF No. 1 (S.D.N.Y. Aug. 21, 2023).

[73] https://www.congress.gov/bill/118th-congress/house-bill/1747/text Blockchain Regulatory Certainty Act, H.R. 1747, 118th Cong. (2023) (sponsored by Rep. Tom Emmer (R-MN-6)) (The bill states, "No blockchain developer or provider of a blockchain service shall be treated as a money transmitter (as defined under State licensing laws), a financial institution (as defined under section 5312 of title 31, United States Code), or any other State or Federal legal designation requiring licensing or registration as a condition to acting as a blockchain developer or provider of a blockchain service, unless the developer or provider has, in the regular course of business, control over digital assets to which a user is entitled under the blockchain service or the software created, maintained, or disseminated by the blockchain developer.").