February 2025

Prosecuting Privacy

Examining Samourai Wallet, Money Transmitters, and the Criminalization of Innovation

Spencer Peek

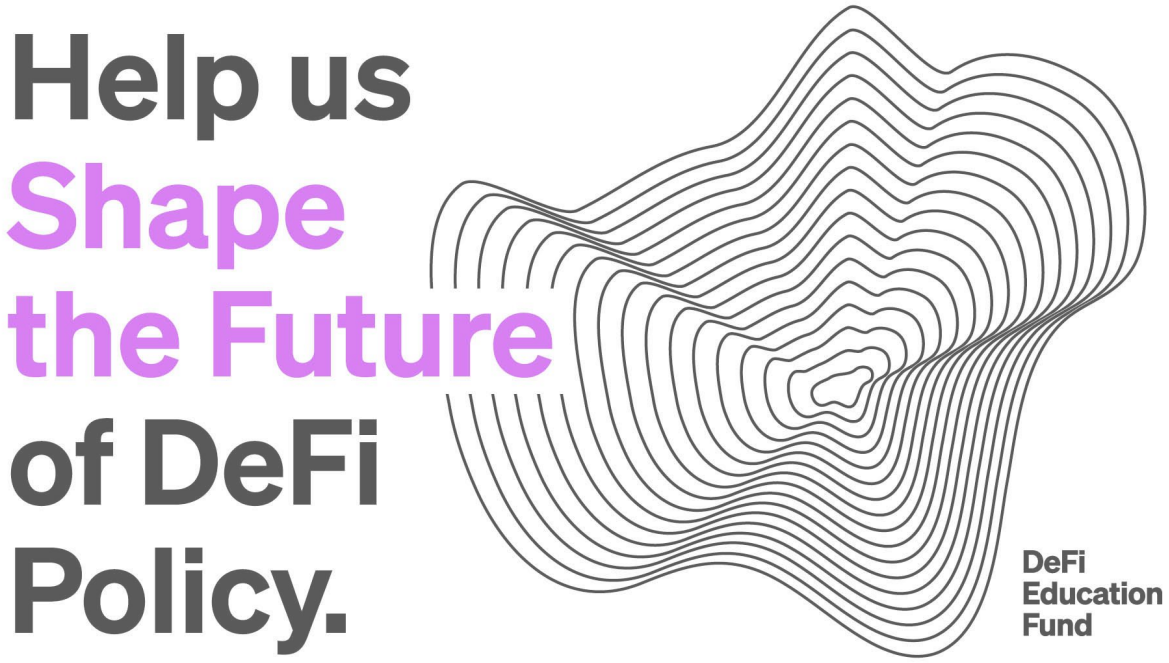
DeFi Education Fund

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 my DeFi Education Fund colleagues, 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

Executive Summary

Part I of this paper presents a factual summary of Samourai Wallet's Whirlpool and Ricochet features, as alleged by the Department of Justice (DOJ) in the Indictment[1] against Keonne Rodriguez and William Hill, the founders of Samourai Wallet. Whirlpool and Ricochet are the principal technologies at issue with respect to the allegation that Samourai Wallet's founders operated an unlicensed money transmitting business.

Part II examines the statutory and administrative basis for the DOJ's allegations that the Samourai Wallet founders operated an unlicensed money transmitting business, focusing on the definition of "money transmitter" under criminal statute 18 U.S.C. 1960, the Bank Secrecy Act (BSA), and the BSA's implementing regulations.

Finally, Part III argues that the DOJ's allegations are insufficient to prove that the founders of Samourai Wallet operated an unlicensed money transmitting business through Whirlpool and Ricochet.

Introduction

In *The Federalist No. 62*, James Madison warned of the consequences attendant to mutable and unstable government policy, explaining that such instability "poisons the blessing of liberty itself."[2] He knew that clear and stable policy was critical for society to function, cautioning that "[i]t will be of little avail to the people, that the laws are made by men of their own choice, if the laws be so voluminous that they cannot be read, or so incoherent that they cannot be understood; if they be repealed or revised before they are promulgated, or undergo such incessant changes that no man, who knows what the law is today, can guess what it will be tomorrow."[3]

Madison's fear that unclear and mutable policy would undermine liberty has been realized at various times in American history. For nearly a decade, it has manifested itself in the federal government's approach to digital assets, which has caused tremendous uncertainty, particularly as it relates to the legal classification of non-custodial software and privacy-enhancing technology.[4] The uncertainty carries profound consequences, deterring

[1] *United States v. Rodriguez*, No. 1:24-cr-00082-RMB (S.D.N.Y Superseding Indictment filed February 14, 2024).
[2] THE FEDERALIST NO. 62, JAMES MADISON (1788).
[3] *Id.*
[4] Peter Van Valkenburgh, *Broad, Ambiguous, or Delegated: Constitutional Infirmities of the Bank Secrecy Act*, CoinCenter, 8 (November 2023), https://www.coincenter.org/app/uploads/2023/11/BroadAmbiguousDelegated.pdf ("[W]e will set aside our "best reading" of the [Bank Secrecy Act] and the attendant conclusion that it is absurdly broad, and, in the alternative, we will proceed to a discussion of ambiguity. . . . We discuss why this invented ambiguity is a convenient article of faith, or *ipse dixit*, that enables courts and regulators to save the statute from

innovation by causing software developers to fear potential criminal prosecution under ambiguous or inconsistently applied law and eroding the fundamental principle that criminal law must be grounded in clear and predictable normative frameworks.[5]

The DOJ's Indictment[6] against Keonne Rodriguez and William Hill, the founders of Samourai Wallet, exemplifies the harsh consequences that can result from mutable interpretations of laws governing novel technology.[7] Samourai Wallet developed and operated Whirlpool and Ricochet, non-custodial, privacy-enhancing software tools for users on the Bitcoin[8] network.[9] One of the issues presented by the Indictment, and the only issue on which this paper takes a position, is whether the government has sufficiently alleged that the founders of Samourai Wallet operated an "unlicensed money transmitting business" pursuant to 18 U.S.C. Section 1960 by offering Whirlpool and Ricochet via the Samourai Wallet mobile application.[10] This issue is particularly troubling given that the DOJ's application of the money transmitter laws to the development and operation of non-custodial software products is novel. The Indictment signals a significant and unexpected shift in the DOJ's interpretation of the law governing money transmission.[11]

This paper explores the scope of liability for operating an unlicensed money transmitting business in the context of non-custodial software development, and argues that Whirlpool and Ricochet do not fall within the relevant criminal statute's definition of "money transmitting" — even according to the facts alleged by the DOJ. This paper further contends that Samourai Wallet's operation of Whirlpool and Ricochet do not oblige them to register as a "money transmitter" with the U.S. Department of the Treasury, as they fall outside of the definition provided in the BSA, as well as the rules and interpretive guidance issued by Financial Crimes Enforcement Network (FinCEN).[12]

---

probable unconstitutionality. . . . Furthermore, we find that any attempt to narrow the statute's application by use of these substantive canons would fail to adequately inform persons of their obligations under the law.").

[5] Nat. Archives, Thomas Jefferson Letter to William Johnson (June 12, 1823) ("Laws are made for men of ordinary understanding, and should therefore be construed by the ordinary rules of common sense. Their meaning is not to be sought for in metaphysical subtleties, which may make any thing mean every thing, or nothing, at pleasure."), https://founders.archives.gov/documents/Jefferson/03-19-02-0518.

[6] *United States v. Rodriguez*, No. 1:24-cr-00082-RMB (S.D.N.Y Superseding Indictment filed February 14, 2024) [Hereinafter "the Indictment."].

[7] *Id.*

[8] Throughout this paper, references to uppercase B "Bitcoin," refer to the decentralized blockchain network, while references to lowercase b "bitcoin," refer to the native currency for transacting on the Bitcoin network.

[9] *Rodriguez*, No. 1:24-cr-00082-RMB at 1.

[10] *Id.* at 17; 18 U.S.C. § 1960(b)(1)(b) and (b)(1)(C); *see also* 31 U.S.C. § 5330.

[11] Fin. Crimes Enf't. Net., *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currency*, FIN-2019-G001, 16 § 4.2.1, 20 § 4.5.1 (May 9, 2019) [Hereinafter the *2019 Guidance*]; 18 U.S.C. § 1960(b)(2); 31 U.S.C. § 5330; 31 C.F.R. § 1010.100(ff)(5)(ii)(A).

[12] 31 C.F.R. § 1010.100(ff)(5)(ii)(A).

Samourai Wallet

Samourai Wallet[13] operated a mobile application that, along with functioning like a traditional non-custodial wallet, offered non-custodial, privacy-enhancing tools for users on the Bitcoin network. Specifically, Samourai Wallet created two software tools called Whirlpool and Ricochet.[14] Below is a summary of the technologies *as alleged by the DOJ*. Unfortunately, the lack of technical specificity and nuance in the DOJ's allegations about Samourai Wallet's technology creates confusion about the reality of how Whirlpool and Ricochet transactions actually work.[15]

However, as the DOJ makes clear in the Indictment, Samourai Wallet users "store[d] their private keys for any bitcoin address they *control* inside of the Samourai program" on their local device.[16] Private keys are necessary to sign and authorize any Bitcoin transaction. "These private keys [we]re not shared with Samourai employees[.]"[17] Once a user stored their private key in the Samourai Wallet software on their local device, they were able to access Whirlpool and Ricochet.

Critically, the DOJ's characterization of Samourai Wallet's server as "facilitating transactions between Samourai users," with respect to both Whirlpool and Ricochet, is misleading because the control over the private keys—and therefore control over the funds involved in transactions—remains exclusively with the users at all times.[18] While Samourai

---

[13] Throughout this paper, references to "Samourai Wallet" or "Samourai" refer to the entity that developed the non-custodial wallet, the Whirlpool and Ricochet software tools, and operated the server used for coordinating communication between users of their non-custodial tools.

[14] *United States v. Rodriguez*, No. 1:24-cr-00082-RMB, 3 (S.D.N.Y Superseding Indictment filed February 14, 2024)

[15] For example, drawing on resources from outside of the Indictment, it is clear that Samourai's server mathematically derived wallet addresses from the user's extended public key (xPub) without accessing or gaining control of the user's private key. Alternatively, many users chose to run their own "Dojo" node which enabled them to derive their own addresses without sharing their xPub. xPubs allow the centralized server to derive addresses for the various stages of the Whirlpool process while the user maintains control over their private keys. The signed transactions are broadcast to the Bitcoin network, either directly by the wallet, which only uses the Samourai servers to deliver the transaction data to the blockchain without giving up custody, or through the user's own Dojo node if configured. Data from the company providing the "Dojo" nodes for Samourai users, suggests that 85% of Whirlpool users ran their own Dojo. Curiously, the DOJ does not mention Dojo nodes or attempt to elaborate on the address generation or transaction broadcasting nuances employed by Whirlpool. *See What is a public key (XPUB)?*, Trezor, https://trezor.io/learn/a/what-is-a-public-key-xpub; *see also* L0la L33tz, *Samourai Wallet: Breaking Down Dangerous Precedents*, Nasdaq (originally published in Bitcoin Magazine), Apr. 29, 2024, https://www.nasdaq.com/articles/samourai-wallet:-breaking-down-dangerous-precedents; Econoalchemist, Samourai Wallet+Ronin Dojo, an article on privacy, anonymity, & options, Sept. 16, 2020, https://www.econoalchemist.com/post/samourai-wallet-ronin-dojo-an-article-on-privacy-anonymity-options

[16] *United States v. Rodriguez*, No. 1:24-cr-00082-RMB, 3 (S.D.N.Y Superseding Indictment filed February 14, 2024)

[17] *Id.* at 3.

[18] *Id.* ("To authorize a transfer of [b]itcoins from an address, a user must use his or her "private key," or password, to conduct the Bitcoin transaction. . . After users download Samourai, they can store their

Wallet's server may coordinate communication between users or assist with transaction setup, it does not have the authority or ability to execute transactions, as only the user holding the private key can do so.[19] Accordingly, this paper takes the position that the DOJ's use of the term "facilitates" fundamentally mischaracterizes the role that Samourai Wallet plays in transactions through both Whirlpool and Ricochet, which are merely privacy enhancing tools for the user-controlled peer-to-peer transactions on the Bitcoin network.

A. Whirlpool

Whirlpool is a non-custodial software tool for organizing peer-to-peer, on-chain transactions for privacy-enhancing purposes.[20] Whirlpool coordinates communication between users who contribute bitcoin to predefined, non-custodial pools and transact directly with one another on the Bitcoin blockchain.[21] The server run by Samourai Wallet acts solely as a coordinator, identifying and grouping participants who have selected the same pool.[22] Once grouped, the participants' local software prepares and broadcasts the transaction directly to the Bitcoin blockchain.[23] Whirlpool is merely a privacy-enhancing tunnel through which users *access the Bitcoin network directly* for peer-to-peer transactions.

Samourai Wallet collects a fee from the user for using Whirlpool. The broadcast transaction includes sending a fee paid by the user to an address designated by the Samourai Wallet software."[24] This one-time fee reflects the cost to use Whirlpool, and, importantly, is unrelated to the transmission of bitcoin. As the DOJ points out in the Indictment, the transaction fees ("mining fees" in the words of the DOJ) required for broadcasting Whirlpool transactions to the Bitcoin blockchain are paid by the user, not Samourai Wallet on behalf of the user.[25]

The 'key' point to note, which is discussed throughout this paper, is that even according to the DOJ's Indictment, Whirlpool users retain control over their private keys, and therefore

---

private keys for any bitcoin address they control inside of the program. These private keys are not shared with any Samourai employees[.]").

[19] *Id.* at 3, 5-6, 8.

[20] *Id.* at 5-6, 8 (discussing how all private keys associated with addresses in Whirlpool and Ricochet transactions are maintained by the user and never accessed by Samourai or its employees); *Harmon*, 474 F. Supp. 3d at 82 ("The [Bitcoin] Network then verifies the transaction by confirming that (1) the public key is associated with the address of the sender and (2) the digital signature was produced for this transaction using the sender's private key . . . Ownership of bitcoin is thus based on a user's possession or knowledge of the private key associated with a public key address.").

[21] *Rodriguez*, No. 1:24-cr-00082-RMB at 5 ("the Samourai *application on each user's cellphone then broadcasts a transaction to the Blockchain*[.]") (emphasis added).

[22] *Id.* at 5-6.

[23] *Id.* at 5.

[24] *Id.*

[25] *Id.* at 5-6 ("[T]he Samourai software on the user's cellphone will broadcast a transaction to the blockchain transferring 1 bitcoin into 19 addresses, each containing approximately 0.05 bitcoin (plus the mining fees necessary for broadcasting the subsequent transactions to the blockchain) . . . Mining fees for the broadcasting of these [subsequent Whirlpool] transactions are covered by new bitcoin entering the pool.").

their funds, throughout the entire transaction process.[26] Notably, the DOJ does not allege that Samourai Wallet, nor any third party accepts or transmits funds on the behalf of users during the Whirlpool process.

a. The User Chooses a Pool

When using Whirlpool, a user begins by selecting the amount of bitcoin they wish to place in a pool. The software offers predefined pools tailored to specific denominations of bitcoin—0.001, 0.01, 0.05, and 0.5 bitcoin.[27] The user selects a pool that matches their needs and pays an up-front, one-time fee, which is typically between 3.5% and 5% of the amount of bitcoin the user is entering into the pool.[28]

b. The User's bitcoin is "Cut Down"

Once the user chooses their pool, the local software on their device "cuts down" the bitcoin "into the correct size for the chosen pool."[29] This involves splitting the bitcoin into smaller, standardized chunks that correspond to the selected pool.[30] As alleged by the DOJ, "if a user wishes to contribute 1 bitcoin into the 0.05 bitcoin pool, *the Samourai software on the user's cellphone will broadcast a transaction to the blockchain transferring 1 bitcoin into 19 addresses*, each containing approximately 0.05 bitcoin (plus the mining fees necessary for broadcasting the subsequent transactions to the blockchain)."[31] Then, each address matching the pool's predefined denomination of bitcoin becomes an eligible input for the Whirlpool process.[32]

It is important to note that users selecting a pool do not "send" Bitcoin to a centralized pool in any sense. The division of a user's bitcoin into the pool's predefined denomination, as noted by the DOJ, is conducted through the software on the user's device, with the transaction being broadcast to the Bitcoin blockchain by "the Samourai application on the user's cellphone."[33] Critically, throughout the Whirlpool process, the private keys associated with each of the user's addresses remain on their device, and are not accessible by Samourai Wallet nor its employees.[34]

---

[26] *Id.*; *see also* Fin. Crimes. Enf't. Net., *2019 Guidance* at 20, § 4.5.1(b).
[27] *Rodriguez*, No. 1:24-cr-00082-RMB at 4.
[28] *Id.* at 4-5.
[29] *Id.* at 5 ("First, once a user has contributed cryptocurrency from their Samourai wallet to be sent into the Whirlpool, the cryptocurrency is "cut down" into the correct sizes for a chosen pool. Samourai also collects its fee and the mining fees from the transaction, and then the funds wait to join a mix.").
[30] *Id.*
[31] *Id.* (emphasis added).
[32] *Id.* at 5-6.
[33] *Id.* at 5.
[34] *Id.* at 5-6.

The DOJ also alleges that any amount of bitcoin that is too small for the selected pool—*i.e.*, .03 bitcoin leftover after cutting .53 bitcoin down for the .05 bitcoin pool—is "placed in a separate address and provided back to the Samourai user."[35]

c. User's Local Software Communicates with Other Participants in the Pool Through Samourai Wallet's Coordinator Server

Once the bitcoin is "cut down," a coordinator server operated by Samourai Wallet organizes the Whirlpool process by randomly selecting four other users who have independently selected the same pool. These five participants, including the initiating user, form "a batch."[36]

The coordinator server "communicates with other Samourai users," and Samourai Wallet "automatically generates the new addresses that are used as inputs and outputs;" again, Samourai Wallet never takes custody of the user's bitcoin when coordinating the transaction, and the private keys controlling the user's addresses stay on the user's device.[37]

d. User's Software Broadcasts Transaction

Once the batch is formed, the DOJ alleges that the newest user entering the pool initiates the transaction and broadcasts it to the Bitcoin blockchain, which kicks off the previously-signed transactions from the other users' local devices.[38] Each participant's input is then transferred to a new address that is unique to the user, which continues to be controlled by the user via the private key stored on their local device.

The transaction involves five inputs—one from each participant—and five outputs – one address per participant.[39] As explained by the DOJ, Samourai Wallet's server is only involved in the creation of the addresses used as inputs and outputs in the Whirlpool process, while the user broadcasts the transaction to the Bitcoin blockchain from their device using their private key.[40]

e. Subsequent Whirlpool Transactions

After the initial Whirlpool transaction, the newly created outputs—the five new addresses—are eligible for continuous transactions with future batches.[41] As the DOJ explains in the Indictment, ongoing Whirlpool transactions do not involve additional cost to the user (again, users just pay the up-front fee when they enter the first batch). The fees for broadcasting

---

[35] *Id.* at 5.
[36] *Id.*
[37] *Id.*
[38] *Id.* ("Samourai automatically generates the new addresses 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 Samourai's employees*.").
[39] *Id.*
[40] *Id.* at 5-6.
[41] *Id.* at 6-7.

the subsequent transactions are covered by new bitcoin entering the pool, which means the fees are paid by new users.[42]

In other words, as new users enter a specific pool, users that were already using the pool are matched with them automatically, and then the new user pays the necessary transaction fees. The transaction fees required for broadcasting a transaction to the Bitcoin network are separate and entirely unrelated to the one-time fee paid to Samourai Wallet for the provision of the tool that is Whirlpool and its attendant communication services.[43]

B. Ricochet

Ricochet, as alleged by the DOJ, is a separate non-custodial software tool available to users of the Samourai Wallet mobile application. Ricochet allows users to further enhance their privacy on a public blockchain by adding intermediate transactions when sending bitcoin, helping to ensure that the sender's identity stays private.[44] According to the Indictment, users specify the amount of bitcoin they wish to send, the destination address, and whether the transaction should occur instantly or over a designated period of time.[45]

Using the local Samourai Wallet software, Ricochet creates a series of intermediate transactions between the sender and the destination address, also known as "hops."[46] Each hop generates new bitcoin addresses on the user's device, which the local software transmits to Samourai Wallet's centralized server.[47] The bitcoin sent by the user will flow through these addresses, which are generated by the application on the user's cellphone, before arriving at the address originally designated by the user as the destination, with each new address constituting a "hop."[48] As acknowledged in the Indictment, the private keys for these addresses, as with Whirlpool, are stored locally on the user's device and are never accessed by Samourai Wallet's employees or infrastructure.[49] Before the Ricochet transaction is executed, the user pays Samourai Wallet a fee by sending Bitcoin to an address designated by the Ricochet server.[50]

The server coordinates the transaction sequence but does not take control of the user's funds.[51] This is because, as alleged by the DOJ, the user sends bitcoin from addresses

---

[42] *Id.* at 7.
[43] *Id.* ("Mining fees for broadcasting of these cryptocurrency transactions are covered by new bitcoin inputs entering the pool.").
[44] *Id.*
[45] *Id.*
[46] *Id.* at 8 ("The Samourai application then creates the series of bitcoin transactions for each Ricochet, including the creation of new addresses, which are transmitted to a server run by Samourai.").
[47] *Id.*
[48] *Id.* at 7-8.
[49] *Id.* at 8.
[50] *Id.* ("A server run by the Samourai developers . . . provides an address where Samourai's fees are received prior to the execution of the series of Ricochet transactions.") (emphasis added).
[51] The Indictment alleges that the Samourai server broadcasts the series of Ricochet transactions to the Bitcoin blockchain. It fails, however, to indicate whether Samourai or the user is paying the transaction

controlled by their private key to other addresses controlled by the same private key until it reaches the destination specified by the user.[52] And if the user opts for a time-based delay, the software automatically schedules the intermediate hops to occur over the chosen time period.[53]

* * *

Understanding Whirlpool and Ricochet, *as the DOJ alleges they operated*, provides vital context for evaluating whether the Indictment is sufficient to support the unlicensed money transmission charges brought against Samourai Wallet's founders.

The next section examines the legal framework for unlicensed money transmission, focusing on how the criminal statute, BSA, FinCEN regulations, relevant case law, and administrative rulings apply to software tools like Whirlpool and Ricochet.

Law Related to Unlicensed Money Transmitting

Originally enacted in 1970, the Bank Secrecy Act (BSA) is the cornerstone of the United States' anti-money laundering (AML) framework. It authorizes the Treasury to promulgate regulations requiring "financial institutions" to register and implement recordkeeping and reporting measures to detect and prevent illicit financial activity.[54] Among the financial institutions subject to the BSA's provisions are "money transmitters," a subset of the broader Money Services Business (MSB) category, defined as entities that "accept" and "transmit" currency, funds, or other value.[55]

Compliance with the BSA is enforced through both civil and criminal statutes, with FinCEN issuing final rules to codify definitions, operational requirements, and exemptions.[56] The criminal statute related to unlicensed money transmitting, 18 U.S.C. § 1960 (hereinafter,

---

fees associated with broadcasting the Ricochet transaction to the blockchain In the case of Whirlpool, however, the user includes the transaction fees with their inputs to the pool. Given the fact that the bitcoin is moving from a user-controlled address to another user-controlled address for each "hop" in Ricochet transactions, it would be natural to assume that the address initiating the original transaction was also responsible for paying the transaction fee. Without more information in the Indictment, however, it is unclear. *United States v. Rodriguez*, No. 1:24-cr-00082-RMB, 6-7 (S.D.N.Y Superseding Indictment filed February 14, 2024).

[52] *Id.*

[53] *Id.*

[54] 31 U.S.C. § 5311 ("It is the purpose of this subchapter to . . . establish appropriate frameworks for information sharing among financial institutions . . . the Department of the Treasury, and law enforcement authorities to identify, stop, and apprehend money launderers and those who finance terrorists."); *see also* Lizandro Pieper and Gavin Zavatone, *Square Peg in a Round Hole: Why the Bank Secrecy Act Should Not Apply to Blockchain Participants*, DeFi Education Fund, at 6, (November 2024), https://www.defieducationfund.org/_files/ugd/84ba66_a568e222f78048e2a8625abb76d3b0fc.pdf.

[55] 31 C.F.R. § 1010.100(ff)(5)(A) ("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"); 31 U.S.C. § 5330.

[56] 31 U.S.C. § 5318(a)(2).

Section 1960), operates alongside state law and the BSA to enforce compliance with registration requirements and criminally penalize "unlicensed money transmitting businesses."[57]

In the case against Samourai Wallet, the DOJ alleges that Rodriguez and Hill conspired to operate an unlicensed money transmitting business in violation of Sections 1960(b)(1)(B) and (b)(1)(C).[58] The next section breaks down the definition of "money transmitting" set forth in Section 1960(b)(2) and the elements of an "unlicensed money transmitting business" in Sections 1960(b)(1)(B) and (b)(1)(C).

A. 18 U.S.C. Section 1960 - Criminal Provision related to Count II: Conspiracy to Operate an Unlicensed Money Transmitting Business

To meet their burden and prove a defendant is guilty of violating Section 1960, the DOJ must show that a person operated a "money transmitting business" as defined in Section 1960(b)(2), and also prove the business was "unlicensed" according to one of the three provisions set forth in Section 1960(b)(1)(A)-(C).[59]

Section 1960(b)(1)(B) criminalizes a person's failure to register as a money transmitting business with the U.S. Department of Treasury as required under Title 31 U.S.C. Section 5330, a key provision of the BSA, and its implementing regulations.[60] Section 1960(b)(1)(B) and its connection to Section 5330 are discussed *infra* § II.C.

Under Section 1960(b)(1)(C), criminal liability arises when a person engages in the "transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity."[61] Section 1960(b)(1)(C) is discussed *infra* § II.D.

B. 18 U.S.C. Section 1960(b)(2)

Section 1960(b)(2), the threshold element the DOJ must prove to support conviction under Section 1960(b)(1)(B) or (b)(1)(C), defines "money transmitting" as "transferring funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier[.]"[62] From the plain meaning of that provision, it is clear that "[a] party can only "transfer[] funds on behalf" of another if it

[57] 18 U.S.C. § 1960; 31 U.S.C. § 5330.
[58] *United States v. Rodriguez*, No. 1:24-cr-00082-RMB at 17 (S.D.N.Y Superseding Indictment filed February 14, 2024); 18 U.S.C. § 1960(b)(1)(B) and (b)(1)(C).
[59] *U.S. v. E-Gold, Ltd.*, 550 F. Supp. 2d 82, 90 (D.D.C. May 8, 2008).
[60] Section 1960(b)(1)(A) relates to the operation of a money transmitting business without proper state licensure and is not relevant to this analysis, as it was not included as a charge in the indictment; *see also* 18 U.S.C. § 1960(b)(1)(B) ("'Unlicensed money transmitting business' means a money transmitting business that . . . fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section.")
[61] 18 U.S.C. § 1960(b)(1)(C).
[62] 18 U.S.C. § 1960(b)(2)

receives funds by obtaining control over those funds, and transmits funds by relinquishing that control."[63]

Courts have recognized that there is "virtually no substantive difference" between the term "money transmitting," as used in Section 1960, and the term "money transmitting business," as defined in Section 5330.[64] Other highly qualified authors have engaged in an in depth review of Section 5330's "money transmitter" definition and the relevant case law, and concluded it is nearly identical to Section 1960(b)(2)'s definition.[65]

In general, this paper takes the position that the two terms should be understood as being "'substantively coextensive[,]' [] acknowledging the reality that Congress's choice to use the same term in two different statutes was not a coincidence and it is, therefore, helpful to look to see how the term [money transmitting] is used and interpreted under Section 5330 and related provisions."[66]

C. 18 U.S.C. Section 1960(b)(1)(B) & 31 U.S.C. Section 5330

Section 1960(b)(1)(B) expressly makes it unlawful to "fail[] to comply with the money transmitting business registration requirements under [Section 5330], or regulations prescribed under such section."[67] Accordingly, criminal liability under Section 1960(b)(1)(B) hinges in part on whether one has an obligation to register under Section 5330, which requires "[a]ny person who owns or controls a money transmitting business" to register with FinCEN.[68]

A "money transmitting business" is in turn defined in Section 5330 as "any business other than the United States Postal Service" that:

> provides check cashing, currency exchange, or *money transmitting or remittance services*, or issues or redeems money orders, travelers' checks, and other similar instruments 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

---

[63] Amanda Tuminelli, Daniel Barbender, & Jake Chervinsky, *Through the Looking Glass: Conceptualizing Control and Analyzing Criminal Liability For Unlicensed Money Transmitting Businesses Under Section 1960*, Int'l. Acad. of Fin. Crime. Litigators, 13 (Dec. 2024).
[64] *United States v. Harmon*, 474 F. Supp. 3d 76, 101 (D.D.C. Jul. 24, 2020) (quoting *E-Gold*, F. Supp. 2d at 92 n.10); *cf. United States v. Budovsky*, No. 13-cr-368 (DLC), 2015 WL 5602853, at *8 (S.D.N.Y. Sept. 23, 2015) (""Against this backdrop, an indictment need only allege a violation of § 5330's implementing regulations to sufficiently allege a violation of 18 U.S.C. § 1960(b)(1)(B).").
[65] Amanda Tuminelli, Daniel Barbender, & Jake Chervinsky, *Through the Looking Glass: Conceptualizing Control and Analyzing Criminal Liability For Unlicensed Money Transmitting Businesses Under Section 1960*, Int'l. Acad. of Fin. Crime. Litigators, 24 n.86 (Dec. 2024).
[66] *Id.* at 24 n.86.
[67] 18 U.S.C. § 1960(b)(1)(B).
[68] 31 U.S.C. § 5330; *see also U.S. v. E-Gold, Ltd.*, 550 F. Supp. 2d 82, 95 (D.D.C. May 8, 2008)(outlining that the relevant question under § 1960(b)(1)(B) is whether the "[d]efendants' conduct, as alleged, require[s] them to comply with the registration requirements under Section 5330[.]").

> of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system[.][69]

Section 5330 then defines "money transmitting service" as "*accepting* currency, funds, or value that substitutes for currency *and transmitting* the currency, funds, or value that substitutes for currency by any means[.]"[70]

Looking "to the plain language of [Section 5330] . . . [those who] *engage in the transmission of funds*, must be registered . . . with the Department of Treasury."[71] And through the authority delegated to it by Section 5330, the Department of Treasury established FinCEN to oversee BSA obligated entities, which was later expanded by the Money Laundering Suppression Act, making FinCEN the primary regulatory authority for BSA obligated entities.[72]

Accordingly, to fully grasp the scope of what constitutes "the transmission of funds"—and, by extension, the scope of criminal liability under Section 1960(b)(1)(B)—FinCEN's implementing rules and interpretive guidance issued under the authority granted to it by the Treasury via Section 5330 must be examined.

a. Money Transmitters Under the FinCEN Rules

Building on the statutory framework in Section 5330, FinCEN defines a broad category of entities called "money services businesses" (MSBs), which includes money transmitters as one of its key subsets,[73] and "each money services business . . . must register with the Department of Treasury."[74] 31 C.F.R. Section 1010.100(ff)(5)(A) broadly defines a money transmitter as "a person that provides money transmission services" or "any other person engaged in the transfer of funds."[75] "Money transmission services" is in turn defined as "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."[76]

In line with the definition of "money transmitting service" in Section 5330, FinCEN regulations require both the *acceptance* and *transmission* of currency, funds, or other value for

---

[69] 31 U.S.C. § 5330(d)(1)(A)
[70] 31 U.S.C. § 5330(d)(2).
[71] *E-Gold*, 550 F. Supp. 2d, at 94 (emphasis added).
[72] *See* Pieper & Zavatone, *supra* note 54, at 7.
[73] 31 U.S.C. § 5330(d)(1)(A); 31 C.F.R. § 1010.100(ff)(5)(A).
[74] *E-Gold* 550 F. Supp 2d, at 96; *see also* Pieper and Zavatone, *supra* note 54, at 6 n.2 ("FinCEN believes that [Section 5330's] use of [money transmitting business] 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, may lead to confusion. Therefore, FinCEN has adopted the term 'money services business' in place of the term 'money transmitting business' . . . ") (internal citations ommitted).
[75] 31 C.F.R. § 1010.100(ff)(5)(A).
[76] *Id.*

given conduct to fall within the scope of money transmission.[77] Further, FinCEN regulations specifically exempt persons that only provide "*delivery, communication, or network access services* used by a money transmitter to support money transmission services" from the obligation to register.[78]

Despite what feels like an exhaustive list of definitions and cross references across the US Code and Code of Federal Regulations, examining FinCEN's interpretive guidance is necessary to determine the scope of the obligation to register under Section 5330 and by extension, the scope of criminal liability under Section 1960 (b)(1)(B). To provide clarity and ensure that the law is applied consistently, FinCEN issues interpretive guidance which, while it does not have the binding force of law, "'advises' the public of how the agency understands, and is likely to apply, its binding statutes and legislative rules."[79]

b. 2019 Guidance

FinCEN's 2019 Guidance, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (CVCs), provides critical insight into how the agency interprets the definitions and obligations of money services businesses (MSBs) as applied to digital asset companies like Samourai Wallet.[80] The 2019 Guidance makes it clear that FinCEN does not view non-custodial software providers as money transmitters, because they lack any actual control over the user's value.[81] Accordingly, FinCEN's 2019 Guidance should play a significant role in analyzing whether Samourai Wallet's operation of Whirlpool and Ricochet obligated them to register as a "money transmitting business" under federal law.

The 2019 Guidance builds on FinCEN's prior rules and interpretations, including its 2013 guidance, to clarify how the BSA's regulatory framework applies to entities operating in the digital asset space. In determining whether an individual or entity qualifies as an MSB generally, FinCEN's focus is "on the person's *activities* and not its formal business status."[82] The 2019 Guidance reiterates that the principal activities giving rise to money transmitter status are "*receiving* one form of value . . . and *transmitting* either the same or a different form of value to another person or location, by any means."[83] As with FinCEN rules, this is in line with Section

---

[77] *Id.*; 31 U.S.C. § 5330(d)(2).
[78] 31 C.F.R. § 1010.100(ff)(5)(ii)(A); *see also* Fin. Crimes Enf't. Net., *2019 Guidance* at 20, (Despite the language "used by a money transmitter to support money transmission services[,]" the exemption does not seem to be limited to providers actually servicing money transmitters to support money transmission. In the 2019 Guidance, FinCEN explains that it is a fact-based determination and a non-money transmitter-user would "employ the software when paying for goods and services on its own behalf, while a money transmitter would use it to engage as a business in the acceptance or transmission of value [].").
[79] *See* Pieper & Zavatone, *supra* note 54, at 11 (quoting *Kisor v. Wilkie*, 139 S. Ct. 2400 (2019)) (citations omitted).
[80] Fin. Crimes Enf't. Net., *2019 Guidance* at 1; *See* Pieper & Zavatone, *supra* note 54, at 13.
[81] *See* Pieper & Zavatone, *supra* note 54, at 14.
[82] *Id.* at 7 § 2 ("Under the BSA, the term 'person' means 'an individual, a corporation, a partnership . . . and all entities cognizable as legal personalities.").
[83] *Id.* at 7-8, § 2.

5330's requirement for both the *acceptance* and *transmission* of currency, funds, or other value for given conduct to fall within the scope of money transmission.[84]

The 2019 Guidance provides a framework for evaluating various types of crypto-related businesses, clarifying whether their activities qualify them as money transmitters under the BSA by examining factors, such as: their role in the flow of funds, the services they provide, and their level of control over customer transactions.[85] Importantly, the Guidance also reiterates how exemptions apply to certain activities, such as providing anonymizing software or infrastructure, emphasizing that these entities are engaged in trade rather than money transmission.[86] For our purposes the two most relevant business models contemplated by the 2019 Guidance are Unhosted Wallet Providers and Providers of Anonymizing Services for CVCs.[87]

i. Unhosted Wallet Providers

FinCEN describes unhosted wallets as "software hosted on a person's computer, phone, or other device that allow the person to store and conduct transactions in CVC."[88] These wallets enable users to maintain full control over their private keys, which are stored locally on their device, rather than relying on a third party for custody or transaction facilitation. The Guidance provides a four prong test to evaluate the nature of an unhosted wallet, that is: (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."[89] The Guidance finds that unhosted wallets meet this criteria because "(a) the value (by definition) is the property of the owner and is stored in a wallet, while (b) the owner interacts with the payment system directly and has total independent control over the value."[90] *These are often known as "non-custodial" wallets due to the fact that the provider never takes custody of the user's private key.*

As a result, unhosted wallet providers do not accept or transmit currency, funds, or value on behalf of others, and therefore, they are not classified as money transmitters under FinCEN's regulations.[91] This distinction highlights their role as non-custodial tools, which empower users to transact directly on blockchain networks without the involvement of intermediaries.

---

[84] *Id.*; 31 C.F.R. § 1010.100(ff)(5)(A); 31 U.S.C. § 5330(d)(1).
[85] Fin. Crimes Enf't. Net., *2019 Guidance*, at 1.
[86] Fin. Crimes. Enf't. Net., *2019 Guidance* at 20, § 4.5.1(b); *see also* Fin. Crimes. Enf't. Net., *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001, at 1 (Mar. 18, 2013), https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.
[87] *Id.* at 15-16, 20, §§ 4.2.1., 4.5.1; *see also* Pieper & Zavatone, *supra* note 54, at 13 ("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.").
[88] *Id.* at 16, § 4.2.1.
[89] *Id.* at 15, § 4.2.1.
[90] *Id.* at 16, § 4.2.1.
[91] *Id.*

Further and hypothetically, even if there was partial control resulting from an unhosted wallet developer's activities, FinCEN explains that a money transmitter must exercise "total independent control" over the user's funds, so it would also be insufficient to constitute this hypothetical scenario as a money transmission.[92]

ii. Providers of Anonymizing Services for 'Convertible Virtual Currencies' (CVCs)

The 2019 Guidance delineates two categories of providers of anonymizing services for CVCs: (1) anonymizing *services* providers; and (2) anonymizing *software* providers, emphasizing key differences based on their involvement in the flow of funds.[93]

1. Anonymizing Services Providers

FinCEN describes an anonymizing *service* provider as a person that *accepts* CVC from customers and *retransmits* it in a manner designed to obfuscate the source or destination of the funds.[94] These entities are generally considered money transmitters because they provide a custodial service, first accepting a user's crypto in wallets they control, and then transmitting an equivalent amount of "clean" crypto back to the user.[95] Of note, the service provider accepts and transmits value as an intermediary through wallets controlled via private key.[96]

2. Anonymizing Software Providers

In contrast, an anonymizing *software* provider supplies tools—such as communication platforms or software applications—that allow users to anonymize their transactions, but does not itself accept or transmit value, and are therefore not classified as money transmitters under FinCEN regulations.[97] The guidance specifically exempts entities that only provide "delivery, communication, or network access services" used by money transmitters to facilitate money transmission services.[98] FinCEN has explained that these providers are exempt "because

---

[92] *See* Pieper & Zavatone, *supra* note 54, at 14 ("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."); *see also* 2019 Guidance, at 16.
[93] 2019 Guidance, at 19-20, § 4.5.1(a)-(b).
[94] *Id.* at 19, § 4.5.1(a).
[95] *Id.*
[96] Fin. Crimes. Enf't. Net., *2019 Guidance* at 20, § 4.5.1(a) ("[A] person . . . who provides anonymizing services by accepting value from a customer and transmitting the same or another type of value to the recipient, in a way designed to mask the identity of the transmittor, is a money transmitter under FinCEN regulations.").
[97] *Id.* at 20, § 4.5.1(b).
[98] *Id.*

suppliers of tools that may be utilized in money transmission, like anonymizing software, *are engaged in trade and not money transmission*."[99]

***

FinCEN's 2019 guidance clearly distinguishes between entities that directly engage in money transmission—such as anonymizing *services* providers—and those that merely provide non-custodial tools for user-controlled transactions, such as anonymizing *software* providers.[100] The key determinant is whether the entity accepts and transmits value on behalf of others or simply provides the means for users to control their own transactions.[101]

c. ***Judicial and Administrative Application of 18 U.S.C. Section 1960(b)(1)(B) & BSA Regulations***

While the regulatory framework provides guidance on what entities are excluded from money transmitter status due to their role in delivering communication or network access services, courts have rarely addressed the scope of the exemption in detail as it relates to non-custodial technologies like Whirlpool and Ricochet. However, Courts have dealt with analogous, yet distinct, technology in the context of a Section 1960(b)(1)(B) prosecution, which can guide us in part here.

a. United States v. Harmon

In *United States v. Harmon*, the court held that the defendant's operation of Helix, a bitcoin 'tumbler,' qualified as the operation of an unlicensed money transmitting business under Section 1960(b)(1)(B).[102] Helix customers would "send bitcoin to *addresses controlled by Helix*. Helix would then remit cleaned bitcoin—that is, bitcoin 'that have never been on the darknet before—to an address designated by the customer.'"[103]

Describing the nature of bitcoin, the court explained that "[o]wnership of bitcoin is thus based on a user's possession or knowledge of the private key associated with a public key and address."[104] In other words, whoever controls the private key to the address in which bitcoin is stored owns the bitcoin and "controls" the address.[105] The court further noted that bitcoin users "store their private keys in a digital wallet, which 'can take the form of software or hardware[.]"[106]

The main issue considered by the court was whether Helix "move[d] funds from one person or place to another," as required to be a money transmitting business under Section

---

[99] *Id.*
[100] *Id.* at 19-20, § 4.5.1(a)-(b).
[101] *Id.*
[102] *United States v. Harmon*, 474 F. Supp. 3d 76 (D.D.C. July 24, 2020).
[103] *Id.* at 103-104.
[104] *Id.* at 82.
[105] *Id.*
[106] *Id.*

5330 and its implementing regulations.[107] The court ultimately held that Helix did operate as an unlicensed money transmitting business because it "transfer[ed] bitcoin from one location to another."

The principal conduct giving rise to the court's conclusion that Helix was a money transmitter—and the primary distinction from the role that Samourai Wallet plays in Whirlpool and Ricochet transactions—was Helix's role as an intermediary: "Accept[ing] bitcoins from the address where they were stored . . . and transmit[ing] those bitcoins to a designated address or addresses . . . for the benefit of the same person."[108] As noted above, Helix would "accept" the bitcoin at addresses that were themselves controlled by Helix (i.e., Helix held the private key).[109]

b. FinCEN Ruling on MSB Regulations for Renting Computer Systems for Cryptocurrency Mining

In 2014, FinCEN issued an Administrative Ruling on the *Application of Money Services Business regulations to the rental of computer systems for mining virtual currency*, holding that the "delivery, communication, and network access services" exception applied to a company that rented computer systems for cryptocurrency mining.[110]

The company had developed a computer system that enabled third parties to perform cryptocurrency mining using the company's infrastructure. FinCEN, however, determined that the company was not a money transmitter because it did not accept, transmit, or control the crypto; it simply offered the infrastructure for users to conduct mining independently.[111] The company's role was limited to providing delivery, communication, and network access services, not handling or transmitting the funds themselves.[112]

Third parties would "furnish the Company with limited information about its mining pool, which the Company will enter into the system so the third party benefits directly and exclusively from the mining work. *All virtual currency mined by the third party remains the third party's property, and the Company has no access to the third party wallet*, nor receives or pays virtual currency on the third party's behalf."[113]

FinCEN determined that "even if the Company rents a computer system to third parties that will use it to obtain virtual currency to fund their activities as exchangers, such rental activity, in and of itself, would not make the Company a money transmitter subject to BSA

---

[107] *Id.* 103.
[108] *Id.* at 107.
[109] *Id.* at 82, 103-04.
[110] Fin. Crimes Enf't. Net., Administrative Ruling, *Application of Money Services Business regulations to the rental of computer systems for mining virtual currency*, FIN-2014-R007 (Apr. 29, 2014), https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/application-money-services-business-0.
[111] *Id.*
[112] *Id.*
[113] *Id.*

regulation."[114] FinCEN concluded that because the Company was not engaged in money transmission, it was exempt from registration requirements under the delivery, communication, or network access services exception.[115]

D. 18 U.S.C. Section 1960(b)(1)(C)

In addition to the Section 1960(b)(1)(B) charge, the DOJ has also charged the Samourai Wallet founders under Section 1960(b)(1)(C), which makes it a crime to engage in the "transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity."[116]

As noted above, Section 1960(b)(1)(C) does not operate independently. As with all subsections of Section 1960, it requires that the government first prove that the defendant's conduct meets the definition of "money transmitting" as set forth in Section 1960(b)(2): "transferring funds on behalf of the public by any and all means, including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier."[117] The nature of Section 1960(b)(2) ensures that liability under Section 1960(b)(1)(C) applies only to activities that qualify as money transmitting under Section 1960 in the first place,[118] as does the language of Section 1960(b)(1)(C), which requires "*transportation or transmission*" of funds. This means that the defendant must have engaged in the acceptance and subsequent transfer of funds on behalf of others, acting as an intermediary in the movement of funds from one party or location to another.

In *United States v. Murgio*, the Southern District of New York held that evidence demonstrating that the defendant "transmitted bitcoins to another location or person for its customers" would be sufficient to find that they operated a money transmitting business under Section 1960.[119]

Samourai Wallet Did Not Operate as an Unlicensed Money Transmitting Business

As discussed below, Samourai Wallet's operation of Whirlpool and Ricochet did not constitute a money transmitting business under Section 1960(b)(2), nor did it qualify as a money transmitter under Section 5330 and its implementing regulations. While the DOJ's failure to allege that Samourai Wallet operated a money transmitting business under Section 1960(b)(2) should, in itself, be fatal to any charge under Section 1960(b)(1)(B), we analyze whether it was required to register pursuant to Section 5330 nonetheless.

---

[114] *Id.*
[115] *Id.*
[116] 18 U.S.C. § 1960(b)(1)(C).
[117] 18 U.S.C. § 1960(b)(2).
[118] *E-Gold*, F. Supp. 2d at 92.
[119] United States v. Murgio, 209 F. Supp. 3d 698, 711 (S.D.N.Y. Sept. 19, 2016).

A. Samourai Wallet & 18 U.S.C. Section 1960(b)(1)(B)

Looking at both Whirlpool and Ricochet specifically, as the DOJ alleges they functioned, it is clear that neither involves the receipt or subsequent transmission of any value on behalf of users. Accordingly, the DOJ's Indictment fails to sufficiently allege that Whirlpool and Ricochet operate as an unlicensed money transmitting business under section 1960(b)(2). Additionally, both features fit within the exemption for delivery, communications, or network access services, further supporting the position that neither Whirlpool nor Ricochet should not be understood to create an obligation to register with FinCEN on behalf of Samourai Wallet.

a. Whirlpool Was Not a Money Transmitting Business Under Section 1960(b)(1)(B)

Akin to how all 'virtual currency' mined by the third party users of the Company's systems remained the property of the third party users in FinCEN's 2014 ruling, all bitcoin involved in Whirlpool transactions remains the sole property of the users, controlled by their private key.[120] Samourai Wallet, like the mining company, had no access to users' wallets, nor did it receive, hold, or transmit bitcoin on their behalf.[121] The mining company was deemed to not be a money transmitter because it provided infrastructure and tools, not custodial or transmission services, despite needing to deploy user information to ensure the user was the exclusive beneficiary of the Company's mining system.[122]

Examining the individual steps of the Whirlpool process below, as alleged by the DOJ, it is clear that none involve "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."[123] Therefore, Whirlpool should instead be classified as within the exemption for "delivery, communication, or network access services" for purposes of determining their obligation to register under Section 5330.[124]

i. The User Chooses a Pool

When a user selects their preferred pool, Samourai Wallet is acting as an interface, allowing users to dictate the parameters of their transaction (i.e., the amount of bitcoin and their desired pool).[125] Samourai Wallet provides software tools that allow users to initiate their own

---

[120] Fin. Crimes Enf't. Net., Administrative Ruling, *Application of Money Services Business regulations to the rental of computer systems for mining virtual currency*, FIN-2014-R007 (Apr. 29, 2014); *Rodriguez*, No. 1:24-cr-00082-RMB at 5-6.
[121] Fin. Crimes Enf't. Net., *supra* note 110; *Rodriguez*, No. 1:24-cr-00082-RMB at 5-6; *see also Harmon*, 474 F. Supp. 3d at 82 ("Ownershup of bitcoin is thus based on a user's possession or knowledge of the private key associated with a public key and address.").
[122] Fin. Crimes Enf't. Net., *supra* note 110; *see also 2019 Guidance*, at 20 ("This is because suppliers of tools (communications, hardware, and software) that may be utilized in money
[123] *Id.*
[124] 31 C.F.R. § 1010.100(ff)(5)(ii)(A).
[125] *Rodriguez*, No. 1:24-cr-00082-RMB at 5.

transactions on the Bitcoin blockchain in accordance with the parameters of Whirlpool, similar to how the computer system in FinCEN's 2014 Administrative ruling allowed users to mine their own crypto within the parameters of the system.[126]

The Whirlpool selection process functions like a user configuration tool, akin to how a Virtual Private Network (VPN) allows users to select a server or region for their connection without managing the content of their internet traffic. In both cases, the service provides the infrastructure and options for users to enhance their privacy, but the users retain full control over their activities and data—ultimately underscoring that Samourai Wallet's role is limited to organizing user-directed, peer-to-peer transactions with no engagement in the transmission or custody of funds.

ii. The User's bitcoin is "Cut Down"

The "cutting down" of the user's bitcoin is performed by the software locally hosted on the user's device, broadcasting the appropriate number of transactions to break the bitcoin into the denomination of the selected pool.[127] This transaction is broadcast to the Bitcoin blockchain by the user, who as noted throughout this paper (and the Indictment), retains complete control over their private key.[128] At no point does Samourai accept or transmit the funds; the software merely coordinates the pool's users and includes the users' independently broadcast transactions as "inputs" for the Whirlpool transaction, which are similarly user-controlled transactions.[129]

Unlike in *Harmon*, where bitcoin was *sent to addresses controlled by Helix via private keys*, the bitcoin in Whirlpool transactions remain in the exclusive control of the user.[130] The Samourai software instead is a local tool for users to independently "cut" their bitcoin down to fit within the parameters of their desired pool; to reiterate, at no point do the users relinquish control or custody of their bitcoin.[131]

Further, the Indictment alleges that any bitcoin leftover that is too small of a denomination for the selected pool is "placed in a separate address and provided back to the Samourai user."[132] In reality, because the user retains control over their private keys at all times, the bitcoin being "returned" to the sender is really just bitcoin that doesn't fit the parameters for the particular pool and is therefore ineligible for Whirlpool transactions in that denomination, it never left the user's custody. In other words, because the bitcoin was never "sent" to any third-party, it is incapable of being "provided back" to the user who had control the whole time via their private key.[133]

---

[126] *Id.*; *see also* Fin. Crimes Enf't. Net., *supra* note 110.
[127] *Rodriguez*, No. 1:24-cr-00082-RMB at 5.
[128] *Id.* at 5-6.
[129] *Id.*
[130] *Harmon*, 474 F. Supp. 3d at 103-04; *see also Rodriguez*, No. 1:24-cr-00082-RMB at 5-6.
[131] *Harmon*, 474 F. Supp. 3d at 103-04; *see also Rodriguez*, No. 1:24-cr-00082-RMB at 5-6.
[132] *Rodriguez*, No. 1:24-cr-00082-RMB at 5.
[133] *Id.* at 5-6 ("[T]he private keys for these cryptocurrency addresses are stored in each user's individual cellphone and not shared with Samourai's employees.); see also United States v. Harmon, 474 F. Supp.

Finally, the fee collected at this point in the Whirlpool process compensates Samourai for providing the technical infrastructure, software, and communication services that enable users to transact directly with one another through the Whirlpool.[134] This one-time fee reflects the cost of providing privacy-enhancing tools for user-directed on-chain transactions through Whirlpool, such as the communication services needed to coordinate participants in a pool before they broadcast their own transactions, and maintenance of the frontend mobile application.[135]

iii. User's Local Software Communicates with Other Participants in the Pool Through Samourai Wallet's Coordinator Server

In coordinating the Whirlpool transaction, Samourai Wallet's function is limited to coordinating communication among participants in the pool.[136] The server randomly selects participants and automatically generates the new addresses used in the mixing process, and, critically, the private keys associated with the generated addresses remain exclusively on the users' devices, ensuring users retain custody and control over their bitcoin throughout the process.[137]

iv. The User's Software Broadcasts the Transaction

The Whirlpool transaction is broadcast from the user's local device.[138] Each participant retains full control over their private keys corresponding to the unique addresses for each input and output.[139] As the court noted in *Harmon,* "FinCEN has long considered transfers of funds from one unique account to another for the benefit of the same person, *when the two accounts are subject to control or hosted by separate entities,* to amount to a change of the funds'

3d 76, 82 (D.D.C. July 24, 2020). ("Ownership of bitcoin is thus based on a user's possession or knowledge of the private key associated with a public key and address.").

[134] *2019 Guidance*, at 20, § 4.5.1(b) ("[S]uppliers of tools . . . that may be utilized in money transmission, like anonymizing software, are engaged in trade and not money transmission."); *Rodriguez*, No. 1:24-cr-00082-RMB at 6.

[135] *Rodriguez*, No. 1:24-cr-00082-RMB at 5-6; *2019 Guidance*, at 20, § 4.5.1(b)

[136] *Id.* at 5 ("Second, through a centralized coordinator server that Samourai operates, the *Samourai application on a user's cellphone communicates with other Samourai users, and Samourai' s coordinator server randomly selects four other inputs* already in the selected pool to be mixed with the new incoming input and communicates that information to each user. *The Samourai application on each user's cellphone then broadcasts a transaction to the Blockchain* in which all five inputs (each a separate address) are then transferred to five outputs (each a separate address).") (emphasis added).

[137] *Harmon*, 474 F. Supp. 3d at 82 ("Ownership of bitcoin is thus based on a user's possession or knowledge of the private key associated with a public key and address."); *Rodriguez*, No. 1:24-cr-00082-RMB at 5-6; *2019 Guidance*, at 20, § 4.5.1(b).

[138] *Rodriguez*, No. 1:24-cr-00082-RMB at 6 (DOJ describing the Whirlpool transactions, which they have already admitted occur on addresses controlled by the users' private keys: "If, for example, as set forth above, 1 bitcoin enter the 0.05 bitcoin pool, each new unit of 0.05 bitcoin contributed by the user into the 0.05 bitcoin pool will combine with four other units of 0.05 bitcoin already in the pool from up to four other users to engage in a five-input-five-output transaction." In other words, Samourai is nowhere involved in the transfer between the inputs and outputs of any given Whirlpool transaction, Samourai only receives any value in the form of a fee paid prior to the Whirlpool transaction for coordinating the participants in the pool.).

[139] *Rodriguez*, No. 1:24-cr-00082-RMB at 5-6.

location."[140] Unlike the Helix addresses in *Harmon*, which received bitcoin 'cleaned' on behalf of the user and sent to new designated addresses, the addresses generated for Whirlpool inputs and outputs are controlled exclusively by the user through a private key, without any control by Samourai or a third party at any point during the transaction.[141]

Rather than receiving value from the users and transmitting it to another location on their behalf, Samourai provides the users with the necessary tools to enhance their privacy when sending bitcoin between addresses exclusively controlled by the user with no interruption in the user's custody of the bitcoin being sent.[142] In other words, the bitcoin in Whirlpool transactions is moving between addresses, subject to the exclusive control of the user, without moving through any wallets owned or controlled by Samourai or any other third-party.

For these reasons, the DOJ's bare allegations in the Indictment are substantially insufficient in establishing a claim that Samourai Wallet was engaged in money transmission. The DOJ's concession that the user's private keys are never accessed by Samourai is fatal to its allegations. The condition precedent to having custody or control over digital assets like bitcoin is control over the private keys, and similarly, the condition precedent to money transmission is the *acceptance* and subsequent *transmission* of funds or other value.[143]

v. Subsequent Whirlpool Transactions

As noted above, the fee paid to Samourai is a one-time payment that allows users to engage in continuous Whirlpool transactions. In these subsequent transactions, users themselves cover the separate and distinct transaction fees required by the Bitcoin network, Samourai bears no cost for the actual transmission of funds, only the provision of the privacy-enhancing software.[144] Furthermore, subsequent Whirlpool transactions never involve Samourai Wallet's acceptance and subsequent transmission of funds. All Whirlpool transactions are prepared and broadcast directly by the users' local software, which clearly exemplifies that Samourai's involvement is purely technical—and non-custodial—consistent with FinCEN's exemption for communication, delivery, and network access services.[145]

***

In summary, Whirlpool should not be classified as a money transmitter because it does not engage in the acceptance or transmission of funds. Whirlpool falls squarely within the

---

[140] *Harmon*, 474 F. Supp. at 106.
[141] *Rodriguez*, No. 1:24-cr-00082-RMB at 5-6 ("Samourai automatically generates the new addresses 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 Samourai's employees.").
[142] *Id.* at 5-6.
[143] 31 U.S.C. § 5330; 18 U.S.C. § 1960; *see also United States v. Harmon*, 474 F. Supp. 3d 76, 82 (D.D.C. July 24, 2020).
[144] *Id.* at 6-7.
[145] *Id.* at 5.

network access services exemption, as its role in providing software tools is confined to facilitating the organization of pool inputs without ever assuming custody or control over users' funds.

b. Ricochet Was Not a Money Transmitting Business Under Section 1960(b)(1)(B)

Ricochet, like Whirlpool, fits within the network access services exemption to FinCEN registration requirements because it operates solely as a tool that enables user-directed, privacy-enhancing transactions, while ensuring that users maintain exclusive control over their bitcoin.[146] Ricochet's process involves users selecting the number of "hops" to add between the sending and receiving addresses to enhance privacy, with all private keys stored locally on the user's device.[147] The transactions are prepared and signed by the user's software, and the resulting Bitcoin transfers occur between multiple addresses that are controlled entirely by the user, ensuring no custodial relationship exists between the user and Samourai Wallet.[148]

The coordinator server employed by Samourai Wallet plays a limited role in providing communication and coordination between the user's device and the Bitcoin network.[149] This is analogous to the mining pool coordination discussed in FinCEN's 2014 ruling, where the infrastructure supported the user's independent control of their funds without any acceptance or transmission by the mining system's provider.[150] Further, under Section 5330, FinCEN regulations, the 2019 guidance and *Harmon*, money transmission requires the acceptance and transmission of funds between separate entities or locations. In Ricochet, bitcoin transactions involve transfers between addresses controlled exclusively by the user.[151] Ricochet's limited functionality should not be interpreted as the acceptance and subsequent transmission of user funds, because Ricochet clearly aligns with the BSA's express exemption for communication, delivery, and network access services, as its role is restricted to providing privacy-enhancing functions without taking custody of user funds at any point.[152]

B. Samourai Wallet & 18 U.S.C. Section 1960(b)(1)(C)

In addition to proving that the defendant's conduct meets the definition in Section 1960(b)(2), conviction under Section 1960(b)(1)(C) cannot be sustained unless the government can separately prove that the defendant transmitted funds they knew to be derived from or in furtherance of criminal activity.[153]

---

[146] *Id.* at 7-8.
[147] *Id.* at 8.
[148] *Id.* at 7-8.
[149] *Id.*
[150] *Id.*; Fin. Crimes Enf't Net., *supra* note 110.
[151] *Id.* at 5-6; *Harmon*, 474 F. Supp. 3d 76, at 103 ("Thus, both the statutory and regulatory language of § 5330 seemingly require a money transmitting business to move funds from one person or place to another.").
[152] 31 U.S.C. § 5330; *see also Rodriguez*, No. 1:24-cr-00082-RMB at 7-8.
[153] 18 U.S.C. § 1960.

The threshold question for analyzing the Section 1960(b)(1)(C) charge is whether or not Samourai Wallet engaged in money transmission as defined by Section 1960(b)(2). If the DOJ is unable to prove that Whirlpool and Ricochet are engaged in money transmission under Section 1960(b)(2), then Hill and Rodriquez' knowledge of the nature and purpose of the funds involved in user's transactions is irrelevant.

In *United States v. Singh*, the Ninth Circuit explained that under Section 1960(b)(2), "[a] money transmitting business receives money from a customer and then, for a fee paid by the customer, transmits that money to a recipient in a place that the customer designates."[154] In *United States v. E-Gold, Ltd.*, the Court noted that "there is virtually no substantive difference, nor did Congress intend there to be a substantive difference, between the terms "money transmitting" in Section 1960 and "money transmitting business" in Section 5330."[155]

Without engaging in an analysis of whether the terms of Section 5330 and its implementing regulations are coextensive with Section 1960's definition of "money transmitter," the principal question here is whether Samourai Wallet, through Whirlpool and Ricochet, "transmitted bitcoins to another location or person for its customers."[156] We believe the answer is very clearly no. Under the framework applied in *Singh* and *Murgio*, it is clear that at no point does Samourai Wallet "receive" bitcoin and "transmit" that bitcoin to another place for a fee.[157] The bitcoin involved in Whirlpool and Ricochet transactions, as explained throughout this paper and the Indictment, remains in wallets controlled by the user via their private key throughout both processes.[158]

Further, engaging in a purely textual analysis of the term "transmit" demonstrates that transmission inherently requires control over the thing being transmitted, which again, as explained above, Samourai Wallet lacks with respect to both Whirlpool and Ricochet transactions. According to Black's Law Dictionary, "transmit" means "to send or transfer from one person or place to another."[159] Implicit in this definition is the necessity of control or possession—an entity cannot send or transfer something unless it has the authority or ability to direct its movement. Merriam-Webster defines "transmit" as "to send or convey from one person or place to another."[160] These definitions further reinforce the idea that transmitting involves an active role in the movement of the item, which necessitates possession or authority over it. Without control, an entity cannot meaningfully send, transfer, or convey anything.

---

[154] *United States v. Singh*, 995 F.3d 1069, 1077 (9th Cir. 2021) (quoting *United States v. Velastegui*, 199 F.3d 590, 592 (2d Cir. 1999); *see also United States v. Han*, 637 F. Supp. 3d 527, 545 (N.D. Ill. Oct. 26, 2022) (finding that there was sufficient evidence to support conviction under Section 1960 when the defendant "picked up large quantities of cash in Chicago and then transferred that cash to bank accounts in China.").
[155] *E-Gold*, 550 F.Supp 2d at 92, n.10.
[156] *United States v. Murgio*, 209 F. Supp. 3d 698, 711 (S.D.N.Y. Sept. 19, 2016).
[157] *United States v. Singh*, 995 F.3d 1069, 1077 (9th Cir. 2021); *Murgio*, 209 F. Supp. 3d at 711.
[158] *Rodriguez*, No. 1:24-cr-00082-RMB at 3, 5-6, and 8.
[159] *Transmit*, Black's Law Dictionary (12th Ed. 2024).
[160] *Transmit*, Merriam-Webster Online (2024).

Historically, the act of transmitting has always required intermediary control or possession. For example, a courier transmits a letter by taking custody of it and physically delivering it to the recipient. Similarly, a financial institution transmits funds by taking possession of the funds either physically or digitally and transferring them to another account or location. In both cases, the transmitting entity plays an active role in the transfer, with custody or control over the item being transmitted.

Applied to Samourai Wallet, this analysis shows that it does not "transmit" bitcoin on behalf of its users through Whirlpool or Ricochet. Samourai Wallet users retain exclusive control of their private keys, which are essential for authorizing any Bitcoin transaction.[161] Without the private key, no bitcoin can be transferred, making it clear that the users, not Samourai Wallet, control and direct the movement of their bitcoin.

The DOJ admits as much in the Indictment, pointing out that "[t]o authorize a transfer of [b]itcoins from an address, a user must use his or her "private key" [] to conduct the Bitcoin transaction."[162] Samourai Wallet's role is limited to providing software tools that organize user-directed transactions. Since Samourai Wallet never takes custody of or controls users' bitcoin, it does not meet the plain meaning of "transmit" under any of these definitions, and should not be deemed to be operating a money transmitting business under Section 1960(b)(2). Accordingly, regardless of Hill or Rodriguez's knowledge of the nature or purpose of their user's funds, they cannot be held criminally liable under Section 1960(b)(1)(C).

Conclusion

The DOJ's approach in this case reflects an unsettling trend of regulation by criminal enforcement, where ambiguous or evolving laws are applied inconsistently to prosecute innovative technologies. By pursuing charges that seemingly contradict or confuse existing law, FinCEN regulations, and guidance, the DOJ creates significant uncertainty for software developers who might otherwise innovate using decentralized technologies.

This inconsistency not only undermines the predictability and clarity foundational to the rule of law, but also can result in a chilling effect on technological progress; software developers may refrain from creating privacy-enhancing tools or other novel innovations out of fear of criminal prosecution. Such enforcement strategies risk stifling innovation and depriving the market of valuable tools that could benefit users, while remaining compliant with regulatory requirements.

To cite a question from James Madison in *The Federalist No. 62*: "What prudent merchant will hazard his fortunes in any new branch of commerce when he knows not but that his plans may be rendered unlawful before they can be executed?"[163]

---

[161] *Rodriguez*, No. 1:24-cr-00082-RMB at 3, 5-6, and 8.
[162] *Id.* at 2.
[163] THE FEDERALIST NO. 62, JAMES MADISON (1788).

Privacy-enhancing tools like Whirlpool and Ricochet are essential for law-abiding users[164] of public blockchains because they provide protection against transaction surveillance, safeguard financial confidentiality, and reduce risks of targeted exploitation, such as hacking, scams, or physical attack, by obscuring personal financial data, among other things.[165] Imagine if we banned cell phones because they made it easier to deal drugs. While all tech tools are at risk of being used for criminal activities, intentionally undermining their development in an attempt to prevent select illicit activities only serves to disproportionately harm law-abiding individuals and stifles U.S. innovation—which could result in chilling effects on financial autonomy in an increasingly transparent digital economy.[166]

Technology will invariably evolve, and it is incumbent upon governments to regulate in a manner that ensures that citizens can fully access and benefit from the advancements that technology offers. A failure to recognize and account for the unique technical capabilities that decentralized network structures offer—while forcing developers to conform to outdated or ill-fitting legal frameworks—stifles innovation, discourages experimentation, and ultimately risks pushing technological progress toward jurisdictions with more adaptive regulatory approaches. By neglecting to create forward-looking regulatory frameworks that align with the realities of emerging technologies, governments risk not only harming their own economies, but also depriving society of the transformative potential these technologies can deliver.

---

[164] *Robert Huang, Samourai Indictment & FBI Notice Are An Assault On Bitcoin And Privacy, Forbes, (Apr. 26, 2024).*

[165] *See id.; see also Krisztian Sandor, Ledger Co-Founder's Kidnapping Highlights Threat of Crypto Robberies, CoinDesk, (Jan. 24, 2025), https://www.coindesk.com/policy/2025/01/24/ledger-co-founder-s-kidnapping-sheds-light-on-soaring-crypto-robberies.*

[166] *See Huang, supra,* note 164 *("What was alarming is that access to Whirlpool isn't a good criminal tool. The action was set in motion even though only ~5% of activity in [Whirlpool] could be attributed to criminal activity. The rest of the 95% was treated as suspect just for trying to enforce more privacy over one's transactions, for a tool that wasn't designed for large-scale criminal inflows but rather as a privacy-enhancing layer."*).