DeFi
Education
Fund

January 22, 2024

*Submitted via the Federal eRulemaking Portal at www.regulations.gov*

Financial Crimes Enforcement Network
U.S. Department of the Treasury
www.regulations.gov

**Re: Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, Docket No. FINCEN-2023-0016**

The DeFi Education Fund (DEF) respectfully submits these comments in response to the Financial Crimes Enforcement Network’s (FinCEN) Notice of Proposed Rulemaking titled “Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern,” FINCEN-2023-0016 (NPRM, Proposed Rule, or Proposal).[1]

DEF supports FinCEN’s goal of creating policy that will prevent illicit activity and support maintaining a safe and secure ecosystem. However, the Proposed Rule will, at best, only minimally achieve its stated goals and come at a high cost. There are existing regulatory requirements under the Bank Secrecy Act (BSA) that provide for the collection, retention, and reporting of nearly the same information as described in this NPRM. FinCEN and its government partners need only clarify, examine for compliance with, enforce, and potentially update these existing requirements to accomplish the Proposal’s goals.

By way of background, DEF is a non-partisan research and advocacy group. Our mission is to educate lawmakers about the technical workings and benefits of DeFi, achieve regulatory clarity for the future of the global digital economy, and advocate for individual users and developers in the DeFi space. Decentralized finance has immense potential to advance innovation in the world economy, and we believe that potential can best be realized in conjunction with smart policy.

[1] FINCEN-2023-0016, Prop. Treas. Reg. § 1010.662, 88 Fed. Reg. 72701 (Oct. 23, 2023), is cited as “NPRM at __.”

Part I of this comment letter provides a discussion of DeFi, the benefits DeFi brings to the world economy, and an overview of how DeFi relates to captured entities. Part II argues that, rather than implement new rules, FinCEN should enforce existing regulatory requirements that provide FinCEN, law enforcement, and others the highly useful information that FinCEN itself believes regulated financial institutions currently possess but do not report. Part III illustrates the ways in which the Proposed Rule is vague, overbroad, and unworkable—and, as a result, renders the Proposed Rule arbitrary and capricious. Part IV explains the gross underestimation of the Proposed Rule's compliance burden. Part V explains why the Proposed Rule violates the Fourth Amendment. Part VI argues that FinCEN should not finalize this rule and should instead allow for the development of privacy-preserving technological solutions. Appendix I includes examples of real blockchain transactions, referenced throughout the letter, and Appendix II describes a potential technological solution—proof of innocence models—that would allow privacy-enhancing technology to coexist with regulatory requirements.

## I. Overview of DeFi

DeFi is an umbrella term used to describe decentralized software protocols that can be used to conduct economic activities on blockchain networks. Users of DeFi protocols have open, transparent access to systems that allow them to conduct various types of financial activities without requiring centralized intermediaries or institutions. Instead of relying on centralized intermediaries to establish trust between counterparties in financial transactions, DeFi systems establish trust via rules-based, encoded protocols that allow individuals to transact via blockchain networks.

### a. Blockchain Technology Basics

In a blockchain network, users are connected through a *peer-to-peer* (P2P) computer network, which is composed of two or more nodes who share authority over the validation and storage of data. There is no need for a central server in a P2P network and, therefore, no single entity has control over a blockchain network — hence, they are referred to as "public blockchains."

Public blockchains are permissionless, decentralized, and immutable ledgers that enable all computers (nodes) participating in a network to (1) hold a record of the history of transactions on the network and (2) reach consensus as to the validity of those transactions. No single entity participating in the network has control over, or can alter, the ledger of transactions.

Users interact with a blockchain using a "wallet." A wallet is a pair of two numbers—a private key and a public key—that are necessary to interact with a blockchain.[2] A "private key" is nothing more than a randomly selected number in a range that is astronomically large and known only to the user. A "public key" is a cryptographically-generated string of letters and numbers associated with a private key, but is public-facing. People colloquially refer to a shorter, user-friendly derivative of the public key as the wallet's "address." While there are software programs that assist a user in creating a wallet and executing transactions associated with a wallet, no third party is needed to create or use a wallet.

Self-hosted wallets empower users with complete control over their digital assets by allowing users to store their public and private keys locally (e.g., on the user's device or even written down on a piece of paper). Contrary to popular belief, assets are not actually stored "in" a wallet because digital assets are simply digital representations of ownership on a ledger. In reality, only the user's keys that grant access to their assets make up a wallet.

Wallets allow users to interact with "smart contracts," which are software programs that run on a blockchain and automatically execute a function when certain conditions are met. Smart contracts are analogous to a vending machine that automatically releases a bag of chips on the condition that it receives $2: the user solely relies on the machine to operate according to the "code" in place. Smart contracts deployed on a blockchain are transparent, secure, and immutable.[3]

### b. The Benefits of DeFi

DeFi protocols are software systems consisting of smart contracts that allow users to engage in various economic activities on blockchains, such as exchanging assets through decentralized exchanges (or "DEXs") or liquidity provisions and borrowing. These protocols aim

[2] Asymmetric cryptography is an encrypted method of communication using two keys: a public and a private key. The public key is used to encrypt messages (transactions), while the private key is used to decrypt them; both of which belong to the user receiving the message and are mathematically related to each other. For example: Alice sends Bob a message using his public key to encrypt it so Bob can be the only one to open the message. Bob then uses his private key to decrypt the message. Asymmetric cryptography is also used in authenticating the sender's information by producing a digital signature with the sender's private key, which is then verified by the recipient using the sender's public key, as well as the network when validating the transaction. A private key mathematically generates a public key, which then mathematically generates a blockchain address; a public key is used to encrypt and a blockchain address is an identifier for sending and receiving.

[3] While smart contracts are immutable once they are deployed, users may create intermediary or proxy contracts that redirect calls and transactions to a modified contract as a way of updating an earlier contract.

to address challenges and risks inherent in the structure of intermediated financial services—including limited access, slow settlement cycles, inefficient price discovery, liquidity challenges, a lack of assurance around underlying assets, opaqueness, broker risk, and uptime issues. DeFi protocols can be distinguished from traditional and centralized exchanges and other market infrastructures in several ways, but most importantly, these protocols are unique in that users exercise total independent control over their assets. Assets are held by users in self-hosted wallets or through smart-contract-based escrow.[4]

By allowing market participants to transact directly utilizing open-source software, DeFi protocols provide the following benefits to consumers:

- Increased transparency: DeFi protocols increase operational transparency about the mechanics of market infrastructures and associated fees by using open-source software, which makes transactions more transparent and auditable by using blockchain-based records.

- Equitable market access: DeFi protocols are open and available to anyone in the world with an internet connection, giving them the potential to significantly expand access to financial services.[5] That access empowers more people to use financial services without having to go through intermediaries who may prevent sectors of the market from participation through unavailability, absolute prohibitions, excessive pricing, or unfair or discriminatory treatment. This includes rural communities in the United States that have limited access to banking options.

- 24/7/365 liquidity: Users can access and use markets at all times of the day without the need for closing markets at the end of each day. Among other things, this eliminates the risk of capital dislocations due to illiquid aftermarket trading in traditional systems.

[4] Before making a transaction, tokens are transferred to a smart contract called escrow. The escrow holds the deposited tokens until the payment conditions are satisfied. The escrow is not controlled by any designated third party.

[5] *See, e.g.*, Bitange Ndemo, *The role of cryptocurrencies in sub-Saharan Africa*, Brookings Institution (Mar. 16, 2022), https://www.brookings.edu/blog/africa-in-focus/2022/03/16/the-role-of-cryptocurrencies-in-sub-saharan-africa (describing how cryptocurrency platforms can "help level the economic playing field and expand finance options to underserved customer markets")

- Lower costs and faster settlement: DeFi protocols reduce friction and transaction costs for the creation, distribution, trading, and settlement of financial assets with faster settlement times for users.[6]

- Improved security: Transactions using DeFi protocols are recorded on blockchains, the records of which cannot be manipulated or amended, offering greater security to users.

- Greater control: The absence of intermediaries in DeFi protocols provides stakeholders greater control and certainty. Additionally, in some instances, market participants can directly develop community governance standards.

- Greater Uptime: Permissionless blockchains are operationally resilient (the Ethereum blockchain has never gone down), whereas traditional exchanges have had major technology failures resulting in downtime for securities markets. Additionally, the use of certain DeFi protocols referred to as automated market makers eliminates trading halts that occur at times as a result of buy and sell order imbalances.

- Eliminate broker risk: DeFi protocols have no employees to supervise, no financial risk for users from broker activity or custody, and no interaction between a broker and customers that could result in unlawful sales practices or other unfair and discriminatory dealing.

- Eliminate anti-competitiveness: Users can easily move their cryptocurrencies from one protocol to another at any time without significant friction, unlike the experience on traditional exchanges where sharing liquidity across exchanges is near-impossible, resulting in a lack of competition.

DeFi protocols are already making substantial contributions to financial innovation generally and in the U.S. specifically. The Official Monetary and Financial Institutions Forum observed that DeFi is being harnessed for the public good and has spurred innovation in the

[6] To be sure, users of DeFi protocols may pay certain fees, such as gas fees, to facilitate use of the protocol. But any comparison of costs should also account for the fact that DeFi users do not additionally need to compensate other intermediaries such as executing brokers, prime brokers, clearing brokers, or custodians. On balance, this typically leads DeFi protocols to be available to users at lower costs than centralized exchanges and traditional banking institutions. As additional blockchains are created and new technology, such as scaling solutions, are developed, costs for transacting using DeFi protocols likely will continue to decrease.

banking system.[7] Academic scholarship has discussed how DeFi protocols (1) benefit efficiency by "significantly decreas[ing] counterparty credit risk"; (2) benefit transparency by offering more publicly available data during a crisis than the data "scattered across a large number of proprietary databases or not available at all" in traditional financial systems; (3) benefit accessibility as "the risk of discrimination is almost inexistent due to the lack of identities"; and (4) benefit composability by creating "an ever-expanding range of possibilities and unprecedented interest in open financial engineering."[8]

### c. DeFi and Captured Entities

To the extent DeFi protocols are included in the Proposed Rule's definition of "CVC mixers," DeFi users' transactions with financial institutions could be subject to the proposed enhanced reporting requirements. Users who conduct on-chain transactions using DeFi protocols regularly conduct transactions from their wallets to financial institutions or from financial institutions to their wallets. Indeed, U.S. financial institutions serve as the primary "on-ramps" and "off-ramps" for users seeking to engage in peer-to-peer and DeFi transactions, and those financial institutions are already subject to U.S. anti-money laundering (AML) compliance obligations.

For example, in order to conduct transactions using DeFi protocols, a user needs to have cryptocurrency in the wallet they intend to use for the transactions. Because there is no ability to store fiat currency on-chain, in order to obtain cryptocurrency, most users purchase cryptocurrency with fiat currency through the services of U.S. financial institutions. Selling cryptocurrency for fiat currency likewise requires the services of a financial institution. Whether it be for these reasons or others, DeFi users regularly engage in transactions with U.S. financial institutions. Thus, should a DeFi transaction be included in the proposal's conception of "CVC mixing," a DeFi user's related transaction with a U.S. financial institution would be subject to the Proposed Rule's reporting obligations.

[7] *See* Kenneth Bok, *Harnessing decentralized finance innovation for the public good*, OFFICIAL MONETARY AND FIN. INST. FORUM (July 20, 2021), https://www.omfif.org/2021/07/harnessing-decentralised-finance-innovation-for-the-public-good/.

[8] *See, e.g.,* Fabian Schär, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*, FED. RESERVE BANK OF ST. LOUIS REVIEW, Second Quarter 2021 at 153, 169; *see also* Fabian Schär, *DeFi's Promise and PitFalls*, INT'L MONETARY FUND, September 2022 at 33, 34 ("DeFi can mitigate counterparty risk and replicate numerous financial services without the need for intermediaries and centralized platform operators. This can reduce costs and the potential for errors. Lending markets, exchange protocols, financial derivatives, and asset management protocols are just a few examples.").

## II. Existing Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) Regulatory Requirements Already Meet FinCEN's Goals.

FinCEN is the administrator and primary regulator of the BSA, and existing regulatory requirements are available to FinCEN now that would "guard against international money laundering and other financial crimes"[9] and provide highly useful information to law enforcement regarding potentially illicit activity of the kind described in the NPRM. The NPRM confirms our view: "[t]he existing risk-based approach to AML/CFT compliance used by covered financial institutions *already largely encompasses the information FinCEN is requesting*. While the information is available to covered financial institutions, at present it is not universally reported to FinCEN."[10] In other words, FinCEN has acknowledged that it already has the regulatory tools it needs to accomplish the goals stated in the NPRM and does not need to implement new requirements to do so. Instead, FinCEN should focus on enforcing compliance with existing tools.

FinCEN should examine covered financial institutions for compliance with risk-based reporting requirements and enforce non-compliance where appropriate and warranted. But this Proposed Rule instead imposes a 311 special measure to create a zero-dollar suspicious activity report (SAR) for an enormous class of cryptocurrency transactions, including the vast majority of cryptocurrency-only and DeFi transactions. An overbroad, blanket reporting requirement is not an appropriate or effective substitute for risk-based BSA compliance and enforcement.

### a. Rather Than Issuing a New Rule, FinCEN Should Leverage and Enforce Existing Risk-Based Regulatory Obligations.

As FinCEN knows, the BSA requires that financial institutions implement risk-based AML programs. Risk-based AML programs must take into account the risks associated with a financial institution's products, services, customers, and geographic locations, as appropriate.[11] Suspicious activity identification, evaluation, and reporting is a fundamental component of a risk-based AML program. A regulated financial institution is *required* to file a SAR under certain circumstances and *can* file a SAR on any suspicious transaction that it believes is relevant to the possible violation of any law or regulation.[12] A money services business (MSB), for example, is

[9] NPRM at 72707.

[10] *Id.* at 72708 (emphasis added).

[11] *See, e.g.*, BSA/AML Manual: BSA/AML Risk Assessment, FFIEC BSA/AML INFOBASE, https://bsaaml.ffiec.gov/manual/BSAAMLRiskAssessment/01 (last visited Jan. 19, 2024).

[12] 31 C.F.R. § 1022.320(a)(1).

required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the MSB involves or aggregates to $2,000 or more in funds or other assets and (1) involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; (2) is designed to evade regulations promulgated under the BSA; (3) lacks a business or apparent lawful purpose; or (4) involves the use of the financial institution to facilitate criminal activity.[13]

Financial institutions have been aware of potential AML/CFT risks related to the obfuscation of cryptocurrency transaction histories for years. As the NPRM notes in significant detail, FinCEN, the U.S. Department of the Treasury (Treasury), and other domestic and foreign government agencies have repeatedly flagged the use of privacy enhancing technologies or obfuscation methods by bad actors to facilitate illegal activity. Indeed, FinCEN's June 2021 AML/CFT National Priorities note the use of "CVC mixers" as one of several techniques used by illicit actors to obscure the source of illicit funds.[14] FinCEN has issued advisories and a financial trend analysis that highlight the abuse of privacy-enhancing technologies by bad actors to facilitate illicit activity, such as ransomware and other crimes.[15] And the NPRM lists in detail the civil and criminal enforcement actions taken in the United States and abroad against certain "CVC mixers" and individuals who use "CVC mixing" to facilitate their illegal activity. There is no shortage of information to assist financial institutions with adjusting their risk-based AML programs, as appropriate, to identify and detect suspicious activity associated with the use of privacy-enhancing technology. There are also a multitude of blockchain analytics tools that financial institutions can and do currently use as part of their risk-based programs to identify and report suspicious cryptocurrency transactions.

To the extent there is a shortage of compliance, the Proposed Rule will not fill that gap and will instead result in a huge torrent of information reporting that will not be useful to

[13] 31 C.F.R. § 1022.320(a)(2).

[14] FinCEN, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities*, 5 n.25 (June 30, 2021), https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf ("Mixing or tumbling involves the use of mechanisms to break the connection between an address sending CVC and the addresses receiving CVC.")

[15] *See, e.g.,* FinCEN, *FIN-2021-A004: Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments* (Nov. 8, 2021), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2021-a004; FinCEN, *Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021*, https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf; FinCEN, *FIN-2019-A003: Advisory on Illicit Activity Involving Convertible Virtual Currency* (May 9, 2019), https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf

FinCEN and will infringe on U.S. citizens' rights, as explained below. Instead, covered financial institutions should be directed to comply with their existing obligations, calibrate their risk-based AML programs with due consideration of FinCEN's priorities, and, as appropriate, report the suspicious activity information that they already have to FinCEN.

The fact that the fields of information a financial institution must currently provide on a SAR largely duplicate those required by the Proposed Rule underscores that existing obligations already meet the Proposal's objectives. These fields include the amount of the transaction, date of the transaction, customer information, photo identification, IP addresses, and a narrative description of the transaction. The SAR form does not explicitly include the cryptocurrency type, type of "CVC mixer," wallet addresses, and transaction hashes, but FinCEN has repeatedly encouraged financial institutions through advisories, public-private partnerships, and other publications to include as much information as possible in the SAR narrative, including these specific data points.[16] And even the NPRM explicitly states that "the proposed regulation only requires a covered financial institution to report information in its possession, and thus does not require a covered institution to reach out to the transactional counterparty to collect additional information on the CVC mixing transaction."[17] To the extent that FinCEN wants to invariably collect these fields on a SAR, FinCEN can and should instead publish a proposed revised SAR form for notice and comment in the Federal Register.

### b. FinCEN Should Continue to Regulate Financial Institutions and Police Bad Actors Rather Than Target a Class of Transactions.

Rather than impose a rule that targets a class of transactions, FinCEN should focus on examining financial institutions and alleged bad actors for compliance with existing regulatory requirements and impose penalties against any non-compliant institutions. Indeed, the government has been able to enforce against individual mixers in the past, as cited extensively in the NPRM.[18]

[16] *See, e.g.*, FinCEN, *FIN-2021-A004: Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, 9 (Nov. 8, 2021), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2021-a004 ("When filing a SAR . . . financial institutions should provide all pertinent available information on the event and associated with the suspicious activity, including cyber-related information and technical indicators, in the SAR form and narrative.")

[17] NPRM at 72711.

[18] *Id.* at 72704-72705.

It seems unlikely that FinCEN would designate a class of traditional financial transactions even though bad actors use traditional financial tools more frequently than cryptocurrency.[19] To illustrate, one would be surprised to see FinCEN use Section 311 of the Patriot Act to bring a similar special measure against a class of automated clearing house transactions, even with a demonstrated high percentage of usage by criminals to facilitate illegal activity. Rather, the government has traditionally used the expectations of compliance and the stick of enforcement against bad actors and non-compliant companies to address illicit finance risks associated with other categories of transactions, such as those involving cash, wire transfers, and credit cards. Similarly, FinCEN and its government partners should continue to use existing resources to direct compliance and bring appropriate enforcement actions against individual actors and companies, rather than designate an entire class of transactions involving cryptocurrency.

### c. Enforcing Compliance With the Risk-Based Approach Will Ultimately Result in More Useful Information for Law Enforcement Purposes Than the Blanket Reporting Proposed in the NPRM.

Focusing FinCEN's and financial institutions' AML resources on risk-based reporting requirements is also more likely to produce useful information for law enforcement purposes over the long term. Granted, this approach would necessitate dedicating resources to better identify potentially illegitimate activity that involves obfuscation techniques. But the Proposed Rule would instead allocate financial institutions' compliance resources to the reporting of information about a vast number of transactions, regardless of whether the transactions evidence some illegitimate activity or not. Inevitably, such a reporting requirement will produce reports about perfectly legitimate transactions, "noise" that is not useful for law enforcement purposes and implicates the Fourth Amendment rights of U.S. users. On the other hand, directing compliance resources to the production of information about transactions potentially related to illicit activity, based on a financial institution's risk-based assessment, will produce higher-value information for law enforcement purposes. Indeed, the prudence of a risk-based approach to transaction reporting across the entire BSA framework is a major theme of the AML Act of 2020 for these same reasons—that is, to provide useful information to law enforcement.[20]

[19] *See* U.S. Dep't. of the Treasury, *National Money Laundering Risk Assessment*, 41 (February 2022), https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf ("the use of virtual assets for money laundering remains far below that of fiat currency and more traditional methods").

[20] *See* Anti-Money Laundering Act of 2020, Pub. L. No.: 116-283, §§ 6001-6511.

## III. The Proposed Rule is Vague, Overbroad, and Unworkable, and Consequently, It Is Arbitrary and Capricious.

As described in more detail below, the definitions FinCEN proposes are inapposite, vague, overbroad, and unworkable. The definitions have the cumulative effect of sweeping in the broadest possible range of non-obfuscatory cryptocurrency transactions and counterparties, including those that have no connection to potentially illicit financial activity. The Proposal admits as much: FinCEN acknowledges that the Proposed Rule "could affect more than 300 million users of unhosted CVC wallets"[21] and repeatedly asks for comments that would help it progress towards a narrower Final Rule. As written, the Proposed Rule is arbitrary and capricious under the APA and cannot be finalized. We take each definition in turn.

### a. The Definition of a "CVC Mixer" in Proposed §1010.662(a)(2) Is Overly Broad and Inconsistent With Prior FinCEN Guidance.

The Proposed Rule defines a "CVC mixer" as "any person, group, service, code, tool, or function that facilitates CVC mixing" and concludes, without elaboration, that the breadth of this definition is "necessary" because of the "nature of CVC mixing."[22] This definition is unduly broad, its justification is unclear, and its impact is unprecedented. Nowhere else in the BSA is any "code, tool, or function" singled out in such a way—and for good reason. To do so would sweep in an entire trade industry and business activity that has nothing to do with the transmission of funds or value or the understood and defined activities of a regulated financial institution.

Indeed, FinCEN has made it clear in other contexts—such as defining a money transmitter—that it is not seeking to regulate code, tools, or functions, and it should do so here as well. For example, the "money transmitter" definition explicitly excludes those persons that only "[p]rovide[] the delivery, communication, or network access services used by a money transmitter to support money transmission services."[23] FinCEN also issued 2019 guidance that re-emphasized this point in the cryptocurrency context, stating that "[a]n anonymizing software provider is not a money transmitter . . . This is because suppliers of tools (communications, hardware, or software) that may be utilized in money transmission, like anonymizing software,

[21] NPRM at 72716. (emphasis added).

[22] *Id.* at 72709.

[23] 31 C.F.R. 1010.100(ff)(5)(ii)(A).

are engaged in trade and not money transmission."[24] These previous exclusions recognize that software developers and those writing code for applications should not be swept into regulations intended to capture money services businesses. However, by extending the definition of a "CVC mixer" to a "code, tool, or function," FinCEN fails to import that nuance here, in express conflict with existing regulation and guidance.

### b. The Definition of "CVC Mixing" in Proposed §1010.662(a)(3) Is Unjustifiably Vague and Overbroad.

In contrast to prior FinCEN guidance defining "mixing,"[25] the Proposed Rule defines "CVC mixing" as "the facilitation of CVC transactions in a manner that *obfuscates* the source, destination, or amount involved in one or more transactions, regardless of the type of protocol or service used"[26] yet goes on to list various methods explicitly included within that definition that do not "obfuscate[] the source, destination, or amount [of CVC] involved in one or more transactions." Although the NPRM provides more specific context for each method,[27] that context is entirely discarded in the proposed regulatory text. Stripping the context away from each listed method results in vague and overbroad definitions foreign to the NPRM's intent and justification, as broken down below.

FinCEN's focus on transactions conducted in a manner intended to obfuscate transactional information is at odds with its proposed regulatory definitions. Its reasoning in finding transactions involving "CVC mixing" to be a primary money laundering concern is founded on "CVC mixing's" ability to "make CVC transactions untraceable and anonymous," "obscur[e] the connection between the CVC wallet addresses used to receive illicit CVC proceeds" and other wallets, and provide "anonymity that allows [illicit actors] to launder their illicit proceeds."[28] However, the proposed definitions would include transactions that do not obfuscate anything. As a result, the Proposed Rule fails to establish what it initially requires covered financial institutions to ascertain and what the NPRM identifies as the true money laundering concern: the facilitation of cryptocurrency transactions "in a manner that obfuscates."

[24] FinCEN, *FIN-2019-G001: Application of FinCEN Regulations to Certain Business Models Involving Convertible Virtual Currencies*, 20 (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[25] *Supra*, Section III(a).

[26] NPRM at 72709 (emphasis added).

[27] *See id.* at 72703.

[28] *Id.* at 72702.

### i. “Pooling or aggregating CVC from multiple persons, wallets, addresses, or accounts”

The Proposed Rule includes in the definition of “CVC mixing” “[p]ooling or aggregating CVC from multiple persons, wallets, addresses, or accounts.”[29] Such a definition encompasses numerous benign activities that do not “obfuscate” transaction information and are instead used commonly to foster economic activity. For example, the following businesses and protocols would be included, even though there is no allegation that they are connected to illicit activity or and do not obscure transaction history: many centralized exchanges with a multinational user base pool funds and therefore, fall within this definition (and do not appear to be otherwise exempted pursuant to proposed §1010.662(a)(3)(ii)); liquidity pools that pool assets through which users can swap tokens also fall within this definition (*see* Appendix I); borrowing protocols to which users contribute their assets to a pool and from which users can borrow assets will also qualify (*see* Appendix I); and staking pools that allow multiple users to combine their assets on a proof-of-stake network would also meet this definition. None of these activities “obfuscate[] the source, destination, or amount [of CVC] involved in one or more transactions,”[30] nor has FinCEN demonstrated that they do in this NPRM.

### ii. “Using programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction”

The Proposed Rule includes “[u]sing programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction” as an example of “mixing.”[31] This definition is so vague as to be unworkable. It likewise reaches beyond obfuscation and captures nearly all cryptocurrency transactions, which themselves are lines of code that automatically execute transactions when predefined conditions are met.

“Using… code to coordinate” the structure of a transaction has the potential to include all cryptocurrency transactions, including the transactions described in the previous section and in Appendix I.

“Managing” the structure of a transaction, similar to “coordinating,” has the potential to include decentralized exchange and automated market maker activity, such as when a user wants to trade one token for another and the smart contract returns an “exchange rate” based

[29] NPRM at 72709.

[30] *See* Appendix I (providing common transactions and demonstrating how transaction history is evident and transparent).

[31] NPRM at 72709.

on the pool balance. It may also include borrowing protocol activity, where a smart contract prompts the liquidation of collateral if the value falls below a certain threshold.

"Manipulating" the structure of a transaction is even more vague, and it is entirely unclear what examples might meet any intended definition. Does changing the price of an asset based on a liquidity pool's ratio constitute "manipulation" because it changes the price of a transaction? Again, none of these activities are inherently associated with illicit finance or methods of obfuscation, nor has FinCEN demonstrated such in this NPRM.

### iii. "Splitting CVC for transmittal and transmitting the CVC through a series of independent transactions"

The Proposed Rule includes "[s]plitting CVC for transmittal and transmitting the CVC through a series of independent transactions."[32] Because the Bitcoin network uses an unspent transaction output (UTXO) model, this definition could be interpreted to include every transaction using bitcoin (BTC) or other tokens on blockchains using UTXO models.[33]

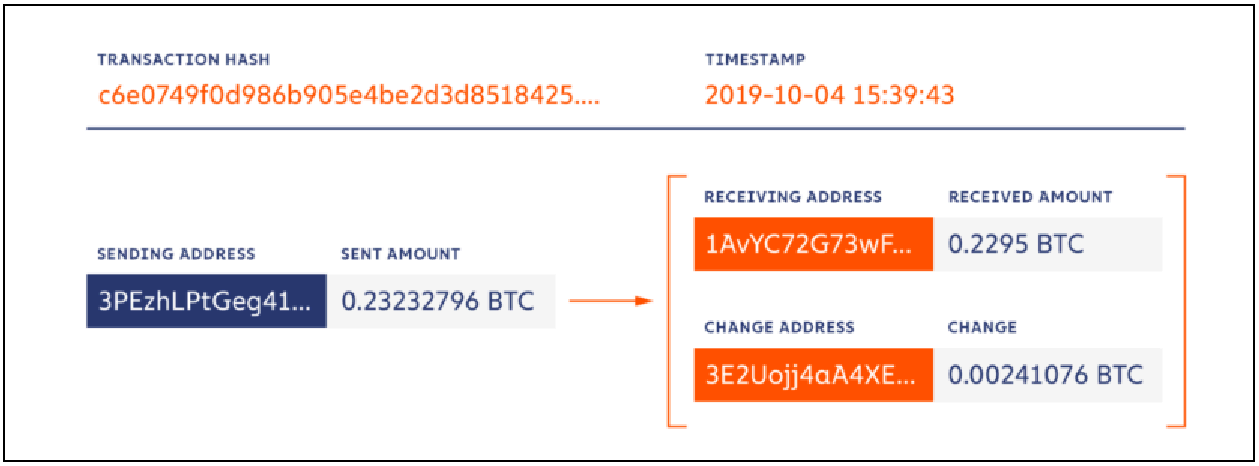
A UTXO model is easiest to understand by analogy: if one wants to buy a $14 sandwich from the store, but one only has a $20 bill, one must hand over the $20 bill and receive back $6 in change. Bitcoin works in a similar way so as to avoid double-spending. When a Bitcoin user writes a transaction for which their wallet contains more than the exact amount of the transaction, the user empties their entire wallet and two outputs are created: (1) the exact amount the user intended to spend is sent to the recipient and (2) the excess BTC is sent back to the original user's change address.[34] As shown in the diagram below, for a transaction in which the user intended to send 0.2295 BTC to the recipient but had 0.2323 BTC in their wallet, the blockchain reflects that a total 0.2323 BTC was sent from the user wallet. In reality, however, (1) 0.2295 BTC was sent to the recipient and (2) 0.00241 BTC of the leftover "change" was sent back to the original user's change address.[35]

[32] NPRM at 72709.

[33] Litecoin, Cardano and Dogecoin also use a UTXO model.

[34] *See also* Chainalysis Team, *Understanding 460 Million Bitcoin Addresses and Economic Activit*y, CHAINALYSIS (Dec. 19, 2018), https://www.chainalysis.com/blog/bitcoin-addresses/ ("To understand change, consider a person who has ten bitcoins and wants to sell one. Because of the way blockchain technology works, the seller has to empty his or her address of all ten bitcoins before receiving nine back in change. So even though he or she only sold one bitcoin, the blockchain records a transaction value of ten BTC.")

[35] This diagram is taken from Chainalysis. *See* Chainalysis Team, *Is Bitcoin Traceable?*, CHAINALYSIS (Apr. 11, 2022), https://www.chainalysis.com/blog/is-bitcoin-traceable/.



TRANSACTION HASH
c6e0749f0d986b905e4be2d3d8518425....

TIMESTAMP
2019-10-04 15:39:43

SENDING ADDRESS
3PEzhLPtGeg41...

SENT AMOUNT
0.23232796 BTC

RECEIVING ADDRESS
1AvYC72G73wF...

RECEIVED AMOUNT
0.2295 BTC

CHANGE ADDRESS
3E2Uojj4aA4XE...

CHANGE
0.00241076 BTC

While we would not interpret FinCEN's definition to include these transactions, nor do we believe that that FinCEN intended to capture these transactions, the breadth of this definition means that one could argue that this basic bitcoin transaction meets the definitional example in the NPRM as "mixing" because it splits the user's bitcoin and creates two independent outputs with two different wallet addresses. As above, none of these activities are inherently associated with illicit finance or are methods of obfuscation, nor has FinCEN demonstrated such in this NPRM.

### iv. "Creating and using single-use wallets, addresses, or accounts, and sending CVC through such wallets, addresses, or accounts through a series of independent transactions"

The Proposed Rule includes "[c]reating and using single-use wallets, addresses, or accounts, and sending CVC through such wallets, addresses, or accounts through a series of independent transactions."[36] As explained above, this definitional example also has the potential to capture the entirety of transactions on the Bitcoin network every time a new change address is created with every transaction. Moreover, many users often try different wallets or utilize different blockchains as they search for what works best for them—it is not uncommon for individuals to abandon old wallets. This definition would capture such legitimate activity that does not "obscur[e] the connection between the CVC wallet addresses" and is not inherently associated with potentially illicit activity (*see* Appendix I). None of these activities are inherently associated with illicit finance, nor has FinCEN demonstrated that they are in this NPRM.

[36] NPRM at 72709.

#### v. "Exchanging between types of CVC or other digital assets"

The Proposed Rule includes "[e]xchanging between types of CVC or other digital assets."[37] This definition is plainly untenable. Similar to the other example definitions above, this definition encompasses transactions that do not "break" on-chain transaction histories and are instead used in everyday economic activity (*see* Appendix I). It captures all swaps, liquidity pool interactions, and borrowing protocol interactions. Indeed, it captures all cryptocurrency trading that does not include a swap for fiat currency. None of these activities are inherently associated with illicit finance nor obfuscation, nor has FinCEN demonstrated that they are in this NPRM.

#### vi. "Facilitating user-initiated delays in transactional activity"

The Proposed Rule includes "[f]acilitating user-initiated delays in transactional activity."[38] This definition has the potential to include legitimate scheduled transactions, such as bill payments, and does not purport to have any connection to illicit activity. Without more specificity, this definition is plainly overbroad.

### c. The Definition of "Covered Transaction" in Proposed §1010.662(a)(5) Is Vague and Overbroad.

The Proposed Rule defines a "covered transaction" as a transaction "in CVC by, through, or to the covered financial institution that the covered financial institution knows, suspects, or has reason to suspect involves CVC mixing within or involving a jurisdiction outside the United States."[39] Notably, the proposal does not define "involves." As written, "involves" functionally becomes "involves <u>any</u>" and is essentially without limitation. The NPRM states that FinCEN expects covered financial institutions to continue to use a risk-based approach to determining when a transaction "involves CVC mixing," for example, by using blockchain analytics tools.[40] Given this explicit regulatory expectation, covered financial institutions are likely to rely on those blockchain analytics tools to identify transactions that "involve CVC mixing." However, blockchain forensics allows transaction chains to be traced through multiple wallets or "hops," meaning that such analysis can show when a set of funds is sent from Point A to Point E with four "hops" along the way. If a user has funds that at some point in their transaction history were sent through a "mixer," how many "hops" away from that mixer counts for the definition

[37] NPRM at 72709.

[38] *Id.*

[39] NPRM at 72710.

[40] *Id.*

of “involves”? As a result, this ambiguity, together with the all-encompassing definition of “CVC mixing,” will cause financial institutions, without more clarity and relief from potential liability, to flag an excessive number of transactions.

Covered transactions also appear to include all those between U.S.-based financial institutions and foreign financial institutions, as the (a)(3)(ii) exception appears to be afforded only to domestic financial institutions.[41] The Proposed Rule is unclear whether the (a)(3)(ii) exception applies to those “banks, broker-dealers, or money services businesses, including virtual asset service providers”[42] that fall outside of the United States and, therefore, outside of the BSA. If it does not, the Proposed Rule sweeps in all cryptocurrency transactions between U.S. financial institutions and financial institutions domiciled in a jurisdiction outside of the United States. Simply occurring in a jurisdiction outside of the United States is not an inherent indicator of illicit activity nor obfuscation, nor has FinCEN demonstrated it is in this NPRM. Moreover, the breadth and ambiguity will leave the market guessing as to what transactions in foreign jurisdictions, and with what type of financial institution, are covered by the Proposal.

#### d. These Cumulative Failures Amount to an Arbitrary and Capricious Rule.

Regardless of its intentions, if there are indications that complying with a regulation would be unworkable—such as when the definition used in the regulation does not comport with reality—then that regulation is arbitrary and capricious.[43] Moreover, a failure to “consider an important aspect of the problem” is also arbitrary and capricious[44], and where an agency reverses its prior position, it would be arbitrary and capricious to not provide a “detailed justification.”[45] As noted throughout this Section, the definitions in the Proposed Rule are vague and overbroad. Some definitions are utterly confusing. Others lack nuance and conflict with

[41] *See* NPRM at 72722.

[42] (a)(3)(ii) applies to certain “transactions by banks, broker-dealers, or money services businesses, including virtual asset service providers… provided that these financial institutions” preserve certain information about the relevant transactions. *Id*. The term “virtual asset service providers” is not currently defined in US law or regulation nor in this rulemaking, and the Treasury Department has stated that “virtual asset service providers” are not “financial institutions.” *See* U.S. Dep’t. of the Treasury, *Potential Options to Strengthen Counter-Terrorist Financing Authorities* (Nov. 28, 2023).

[43] *See, e.g.*, *Almay, Inc. v. Califano*, 569 F.2d 674, 682 (D.C. Cir. 1977) (finding that the regulation at issue was arbitrary and capricious in part because the definition at issue was unrealistic, and because “compliance would be unworkable.”)

[44] *California v. Bernhardt*, 472 F. Supp. 3d 573, 610 (N.D. Cal. 2020) (citing *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co*., 463 U.S. 29, 43 (1983)).

[45] *F.C.C. v. Fox Television Stations, Inc*., 556 U.S. 502, 515–16 (2009) (noting that “a reasoned explanation is needed for disregarding facts and circumstances that underlay or were engendered by the prior policy”).

existing FinCEN regulation and guidance. Together, they amount to an unworkable and potentially unlawful Proposal that makes risk-based compliance impossible for a financial institution to effectuate in reality.[46]

## IV. FinCEN's Assessment of the Compliance Burden Fails to Take Into Account the Overbreadth of the Definitions.

The NPRM specifically invites comment on the regulatory impact analysis included in the proposal. As stated above, the sheer breadth of the Proposed Rule's definitions has the potential to capture nearly all cryptocurrency transactions including DeFi transactions. And covered financial institutions, lacking clarity on what constitutes "involves mixing," may very well include transactions with only indirect exposure to the vast universe of transactions "involving mixing," as defined, or in which funds are many hops away from in identifying covered transactions. As a result, the Proposed Rule is likely to create a deluge of reporting that the NPRM does not take into account in its regulatory impact analysis. FinCEN should re-assess the compliance burden to take these into account.

The Proposed Rule would also suppress development of and investment in privacy-enhancing technologies in the United States. Requiring financial institutions to report such detailed financial information will further suppress the use of and stigmatize privacy-enhancing technologies, which has the significant potential to push the development of these technologies offshore. Covered financial institutions may face a choice of reporting on all transactions or refusing to effectuate all or a subset of transactions involving "CVC mixing," first and foremost transactions that "involve" the use of any privacy-enhancing technologies. If financial institutions trend towards the latter, at best, the use of and investment in technologies that can be used to enhance the privacy of legitimate transactions will be suppressed. This phenomenon is already occurring and will accelerate if this rulemaking is finalized.[47] At worst,

[46] *See* 5 U.S.C. § 706(2)(A) (reviewing courts shall hold unlawful and set aside agency action, findings, and conclusions found to be arbitrary or capricious).

[47] *See, e.g.*, *OKX to delist several spot trading pairs*, OKX (Dec. 29, 2023), https://www.okx.com/help/okx-to-delist-several-spot-trading-pairs-12-29; *Binance Will Extend the Monitoring Tag to Include ANT, FIRO, KP3R, MDX, MOB, REEF, VAI, XMR, ZEC & ZEN, and Remove the Seed Tag for GMX & SUSHI on 2024-01-04*, Binance (Jan. 4, 2024), https://www.binance.com/en/support/announcement/binance-will-extend-the-monitoring-tag-to-include-ant-firo-kp3r-mdx-mob-reef-vai-xmr-zec-zen-and-remove-the-seed-tag-for-gmx-sushi-on-2024-01-04-fd710b5e647c480ab9fe2d87e3cd4b39; Vince Dioquino, *Binance places privacy coins Monero, Zcash and others for possible delisting*, Crypto Briefing (Jan. 5, 2024), https://cryptobriefing.com/binance-places-privacy-coins-under-monitoring-list/. *See also* Crystal Kim, *Privacy coins test crypto exchanges' comfort with compliance*, Axios (Sep. 15, 2022), https://www.axios.com/2022/09/15/privacy-coins-test-crypto-exchanges-comfort-with-compliance.

the Proposal would de facto prohibit U.S. financial institutions from providing any cryptocurrency-related services to their customers.

### V. The Proposed Rule Is An Unreasonable Intrusion Into Users' Privacy and Violates the Fourth Amendment.

As written, the Proposed Rule would be a significant and unreasonable intrusion into the privacy of cryptocurrency users and would cause Fourth Amendment violations. As FinCEN itself has acknowledged, the proposal "could affect more than 300 million users of unhosted CVC wallets."[48] This is an extraordinary number of users—many of whom use privacy-enhancing technology for legitimate purposes—and would not otherwise be suspected of any potential wrongdoing. For instance, in its analysis of value received by "mixers" by source for Q1 2017 through Q2 2022, Chainalysis found that the majority (~77%) of funds received by "mixers" in 2022 were not from illicit addresses.[49] But the NPRM fails to consider or even mention that requiring companies to collect details about private or personal financial transactions and report those details to the government would violate users' Fourth Amendment rights. This is particularly the case as companies will likely *over-comply* with these requirements, thereby turning over massive amounts of data that the government may not have even requested but will then have control over. And in violating the privacy of these users, FinCEN is undermining and undervaluing the legitimate business activities in this class of transactions.

Cryptocurrency users specifically utilize privacy-enhancing technology to address a core privacy concern with cryptocurrency: that, unlike traditional financial transactions, cryptocurrency transactions are posted on a public ledger for anyone in the world to view. As such, if someone can link a person's real-world identity to their pseudonymous wallet address, they would be able to trace that user's complete financial history on the blockchain. Consequently, cryptocurrency users might prefer privacy-enhancing protocols to guard against the threats of fraud, hacking, and scams. For instance, if a hacker knows the real-world identity of a cryptocurrency user and sees that they recently made a high-value transaction, that hacker may then track that user's cryptocurrency transactions and attempt to hack into their wallet or even attempt to locate that user geographically. In choosing to use privacy-enhancing protocols, cryptocurrency users actually clearly manifest their expectation of privacy through

[48] NPRM at 72716.

[49] Chainalysis Team, *Crypto Mixer Usage Reaches All-time Highs in 2022, With Nation State Actors and Cybercriminals Contributing Significant Volume*, CHAINALYSIS (July 14, 2022), https://www.chainalysis.com/blog/crypto-mixer-criminal-volume-2022/. Chainalysis defines "mixers" as "a service that blends the cryptocurrencies of many users together to obfuscate the origins and owners of the funds." *See* Chainalysis Team, *Crypto Mixers and AML Compliance*, CHAINALYSIS (Aug. 23, 2022), https://www.chainalysis.com/blog/crypto-mixers/.

their choice to use privacy-enhancing protocols more than users of credit cards, bank wires, or other forms of digital fiat payments.

There are a number of legitimate use cases for privacy-enhancing protocols. For example, one user used the Tornado Cash protocol to anonymize his transfer of cryptocurrency assets to run an Ethereum validator, which he describes as a valuable activity that may attract attention from malicious actors.[50] Another user had a large presence in the Ethereum community and was concerned about hacking and the safety of his family—and, after previous instances where individuals found his wallet addresses, he used Tornado Cash to protect his security and privacy while making cryptocurrency transactions.[51]

Cryptocurrency users may also use privacy-enhancement technology to anonymously participate in sensitive or risky activities, like journalism, civil disobedience, or protest. For instance, a third Tornado Cash user used the privacy-enhancement protocol to anonymously donate to the Ukrainian government's cryptocurrency wallet address, out of fear that he would be targeted by Russian state-sponsored hacking groups monitoring Ukraine's public address for donations.[52] This use case was relatively common: Vitalik Buterin, the Russian-Canadian co-founder of Ethereum, also said he used Tornado Cash to donate to Ukraine.[53] In fact, according to the 2023 Elliptic Report, "Crypto in Conflict," approximately 1.8% of a sample of $95.8 million of BTC, ETH and USDT, USDC and DAI donations to pro-Ukrainian causes were sent through mixers.[54]

As constructed, the Proposed Rule would violate these users' Fourth Amendment rights by constituting a warrantless search through user information in which users have a reasonable expectation of privacy. The Proposal's requirement to collect information like transaction hashes and wallet addresses is uniquely revealing in that it ties personal information to not just one transaction, but to any transaction the wallet in question has ever conducted or will conduct. Moreover, collecting information like IP addresses and email addresses is unduly invasive and reveals personally identifying information that is unrelated to the covered financial transactions.

[50] Complaint ¶14, *Van Loon v. Dep't of Treasury*, No. 1:23-CV-312-RP (W.D. Tex. Aug. 17, 2023).

[51] *Id*. ¶ 22.

[52] *Id*. ¶ 18.

[53] Vitalik Buterin (@vitalik.eth), X (Aug. 9, 2022, 4:49am) https://x.com/VitalikButerin/status/1556925602233569280?s=20.

[54] *Crypto in Conflict: How the role of cryptoassets has evolved in the Russia-Ukrainian War*, Elliptic Report 2023, at 15.

The "touchstone" of the Fourth Amendment inquiry is whether a person has a "reasonable expectation of privacy in the information that the government collects."[55] If he does, then the government must get a warrant or fall within an exception to collect his information.[56] Although the Fourth Amendment has generally protected information shared with third parties, *Smith v. Maryland*, 442 U.S. 735 (1979) and *United States v. Miller*, 425 U.S. 435 (1976) created a narrow exception that allowed for circumstances under which the government can overcome the general rule if: (1) the information accessed was limited in terms of the amount of data gathered;[57] (2) the information accessed was limited in number of people affected;[58] and (3) the information accessed was limited in the nature of the information revealed.[59] In *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the Supreme Court confirmed this rule by holding that cell-site location information was protected from disclosure because it did not involve "comparable limitations."

The Proposed Rule seeks a huge swath of personal and private financial information from users and does not include limitations as contemplated by *Smith*, *Miller*, and *Carpenter, necessitating* violations of the Fourth Amendment. This proposal would result in the government unconstitutionally searching and collecting information over which users have a reasonable expectation of privacy and enable the government to have complete surveillance over the cryptocurrency transactions of these hundreds of millions of cryptocurrency users for all time. Once the government connects a user with a pseudonymous address, it would be able to identify every transaction that the user has ever made and every transaction that the user will ever make in the future with that public key, because that information will be posted and searchable on the public ledger. And even if a person creates another address, blockchain forensics software and analysis can easily identify and connect different addresses controlled by the same person based on interactions between the addresses.[60] As such, by collecting the information required by the NPRM, the government is in effect collecting *all* transactions, now

[55] *California v. Ciraolo*, 476 U.S. 207, 211 (1986).

[56] *See Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[57] In *Miller*, 425 U.S. at 438, the government collected only two financial statements, three monthly statements, and checks and deposit slips. The papers covered less than four months of intermittent activity. *Id*.

[58] In *Miller*, 425 U.S. at 437, the government got bank records of one man because they had discovered enormous evidence of criminal wrongdoing in his warehouse. In *Smith*, 442 U.S. at 737, the government got one day's worth of phone numbers from one man because he was visually identified as the person making calls in connection with a crime.

[59] In *Smith*, 442 U.S. at 742, the information collected were dialed numbers without further context or intimate information. In *Miller*, 425 U.S. at 442, the Court emphasized that the checks collected were not confidential communication and did not reveal intimate details about the individual's life.

[60] *E.g.*, *Matter of Search of Multiple Email Accts.*, 585 F. Supp. 3d 1, 8 (D.D.C. 2022) (detailing ledger analysis).

and forever, of the impacted users—even if they have no connection whatsoever to suspicious activity and even if the transaction was not related to a "CVC mixer." This degree of information collection is far from limited in the amount of data gathered, the number of people affected, and the nature of the information revealed—falling outside of the exceptions established in Supreme Court precedent—and its implications clearly violate the Fourth Amendment.

When old rules meet new technology, courts and lawmakers must "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[61] For instance, while the Fourth Amendment does not protect against outside visual surveillance, it does once the government uses thermal-imaging technology.[62] While it does not protect against manually following a car on public roads, it does once the government uses a GPS tracker.[63] And while the Fourth Amendment does not protect against searches of items in pockets incident to arrest, it does when those items include modern-day cell phones.[64] In cases where new technology would lead the government to obtain vastly more information than earlier cases anticipated, the Fourth Amendment's protections are recalibrated to account for that change in technology and access. Here, FinCEN should consider the ways in which digital asset technology requires it to recalibrate Fourth Amendment protections to address the privacy concerns of cryptocurrency (who are often using such protocols specifically to preserve the privacy of their financial transactions), and regulatory agencies like FinCEN should be careful to narrowly tailor requests like this NPRM to balance reporting needs with the privacy protections afforded to cryptocurrency users.

## VI. FinCEN Should Not Finalize This Proposal.

As made clear in this comment letter, DEF urges FinCEN not to proceed with this Proposed Rule. FinCEN should first allow for the development of privacy-preserving identification solutions, such as zero-knowledge proofs, that are currently in progress and create unique, privacy-protecting, and effective opportunities to combat illicit finance. *See* Appendix II.

FinCEN itself recognizes that financial institutions are already in a position to provide the information that FinCEN seeks to compel from them by the operation of this special measure. FinCEN should instead focus on enforcing compliance with existing rules and at most, propose a revised SAR form for notice and comment.

[61] *Kyllo v. United States*, 533 U.S. 27, 34-35 (2001).

[62] *Id*. at 35.

[63] *See United States v. Jones*, 565 U.S. 400 (2012).

[64] *See Riley v. California*, 573 U.S. 373 (2014).

* * *

DEF sincerely appreciates the opportunity to provide comments on the Proposal, and we stand ready and willing to assist FinCEN and its government partners in addressing these challenges.

Sincerely,

Miller Whitehouse-Levine
Amanda Tuminelli
Lizandro Pieper

DeFi Education Fund
miller@defieducationfund.org
www.defieducationfund.org

cc: AnnaLou Tirol, O'Melveny & Myers LLP
Anna Xie, O'Melveny & Myers LLP

## APPENDIX I:
## Examples of Common Blockchain Transactions

### 1. Standard Wallet-to-Wallet Transfer

A payment from one cryptocurrency wallet to another is the most "basic" cryptocurrency transaction against which other types of transactions can be compared to assess whether they accomplish any obfuscation of transaction information. As the NPRM notes, for transactions that are conducted without the use of any privacy-enhancing methods, "the public nature of most CVC blockchains, which provide a permanent, recorded history of all previous transactions, make it possible to know someone's entire financial history on the blockchain."[65]

When a user conducts a transfer of cryptocurrencies to another wallet, a unique transaction hash is generated that can be used to identify the transaction on-chain. In this on-chain example, we conducted this type of transaction, which is recorded permanently on-chain and associated with a unique identifier. The information recorded permanently on-chain about the transaction and available to be examined on a free block explorer includes (1) the transaction hash, (2) the transmitter wallet, (3) the recipient wallet, (4) the date and time of the transaction, (5) the amount and type of cryptocurrency used, (6) the dollar value of the assets used in the transaction, and (7) the type of transaction conducted.

**Transaction Hash:** 0x5f3a8…
**Time of transaction:** Jan-09-2024 03:46:06 PM +UTC

| | |
|---|---|
| transmittor address | 0xc206A |
| recipient address | 0x78Bc9 |
| cryptocurrency | 1 MATIC |
| type of transaction | Transfer |

Wallet-to-wallet transfers also happen with "single use wallets." In this example chain of transactions involving two single use wallets, Example Wallet 2 received a transfer from Example Wallet 1. Next, Example Wallet 2 (itself a "single use wallet" as defined) sends a transfer of its assets to Example Wallet 3 (also a single use wallet), which in turn transfers the assets back to Example Wallet 1.

[65] NPRM at 72702.

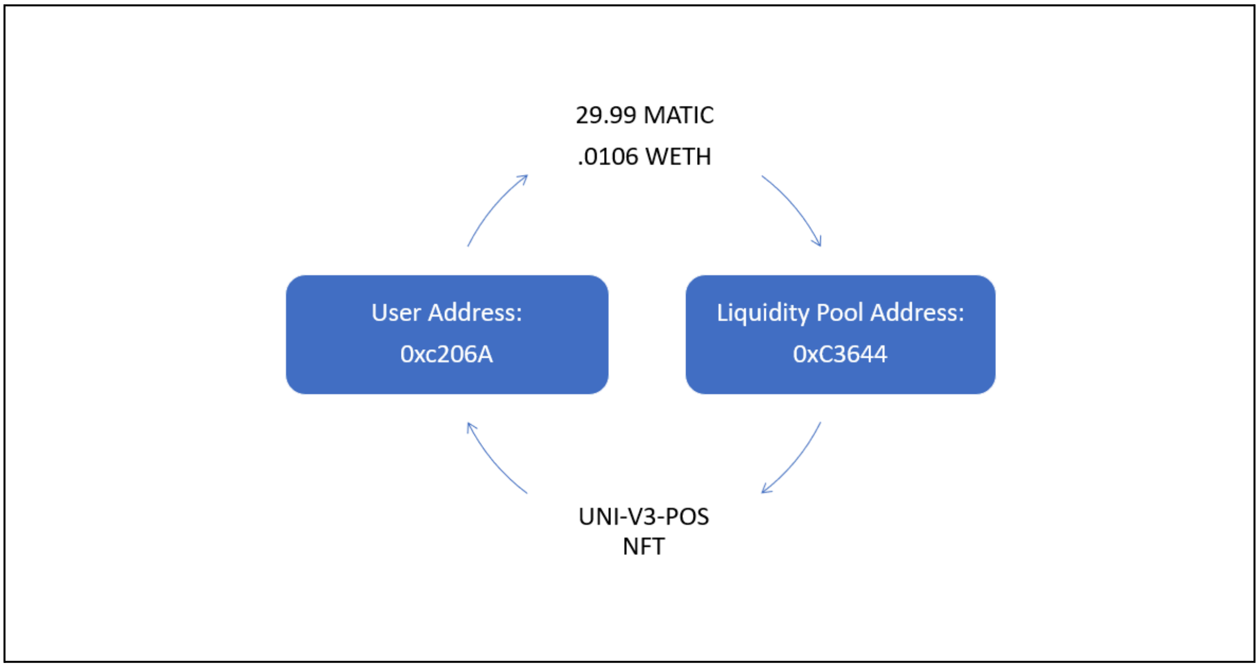
### 2. Providing Liquidity to an Automated Market Maker Pool

Providing liquidity to and withdrawing liquidity from automated market maker pools are on-chain activities that the Proposal would define as "CVC mixing." While this on-chain activity involves the "aggregating" of multiple users' assets, it does not in any way "obfuscate" the link between the two transactions necessary to provide and withdraw liquidity, as shown in the example below.

In the example below, two transactions take place: 1) a transfer of assets from wallet 0xc206A (the liquidity provision transaction) and 2) wallet 0xc206A receives those assets at a later point in time (the liquidity withdrawal transaction).

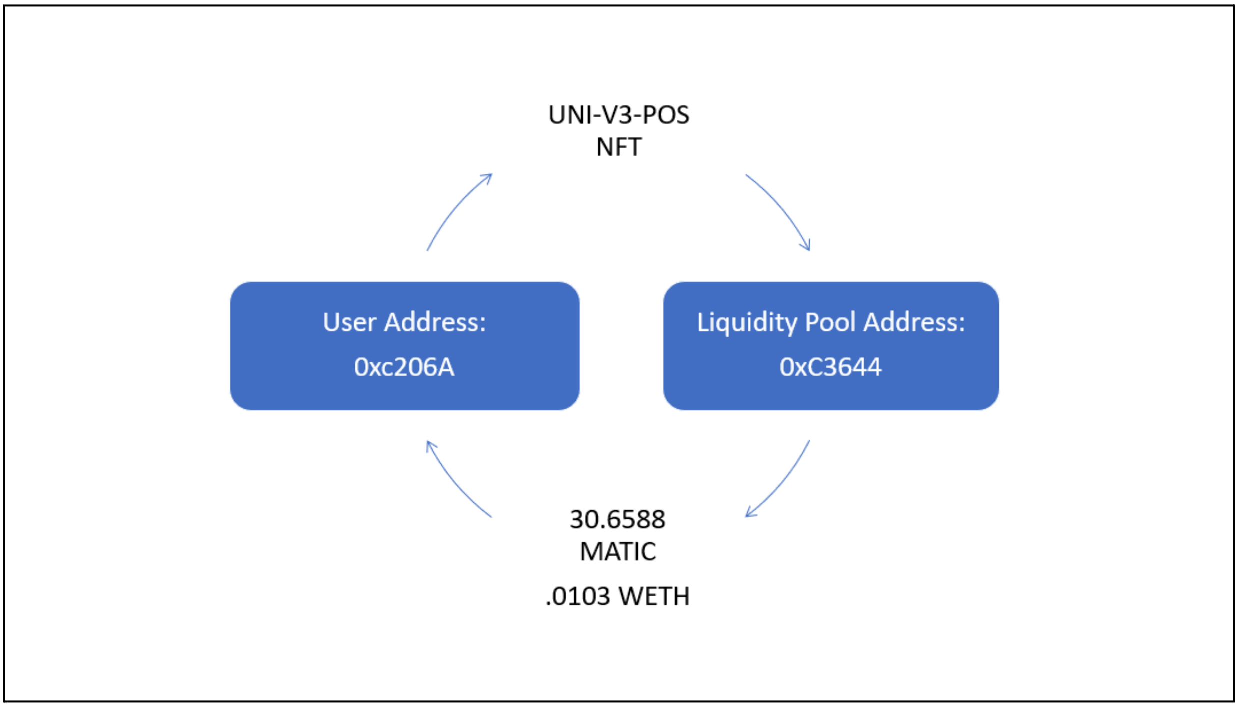
**Provision of Assets - Transaction 1**: In this example, in a single transaction, we provided assets (MATIC and WETH) to an AMM pool and received a newly-generated non-fungible token (NFT) (UNI-V3-POS) representing the portion of the AMM pool our contribution amounted to. Conducting this activity does not "obfuscate" any transaction information.

**Transaction hash:** 0xb29ce…
**Time of transaction:** Jan-08-2024 04:24:16 PM +UTC



**Withdrawal - Transaction 2**: Next, in a single transaction, we withdrew the assets we provided to the AMM pool using the NFT that represented the portion of the AMM pool our contribution amounted to. Conducting this activity does not "obfuscate" any transaction information.

**Transaction hash:** 0xe20bb…
**Time of transaction:** Jan-09-2024 04:47:38 PM +UTC



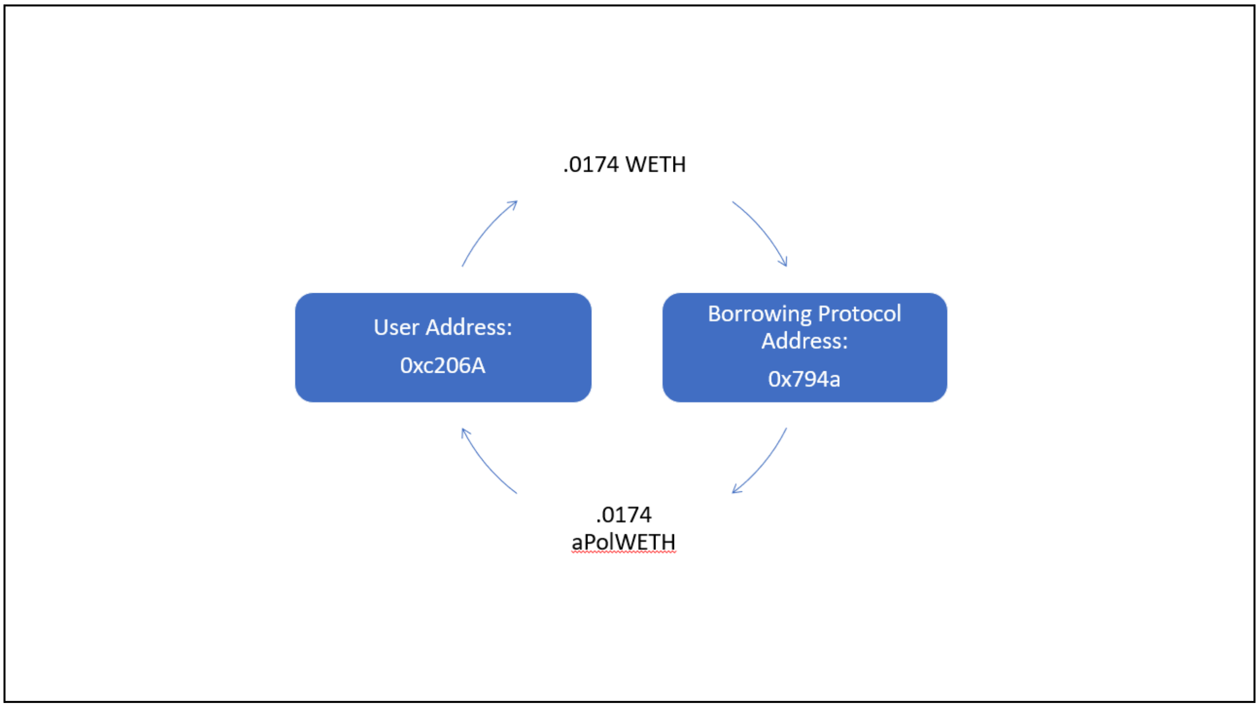
As you can see from the above examples, providing and withdrawing liquidity did not obfuscate the transaction history. Any person viewing the two public blockchain transactions would be able to link the transfer of assets to the pool and the withdrawal from the pool.

### 3. Borrowing Tokens From a Borrowing Protocol

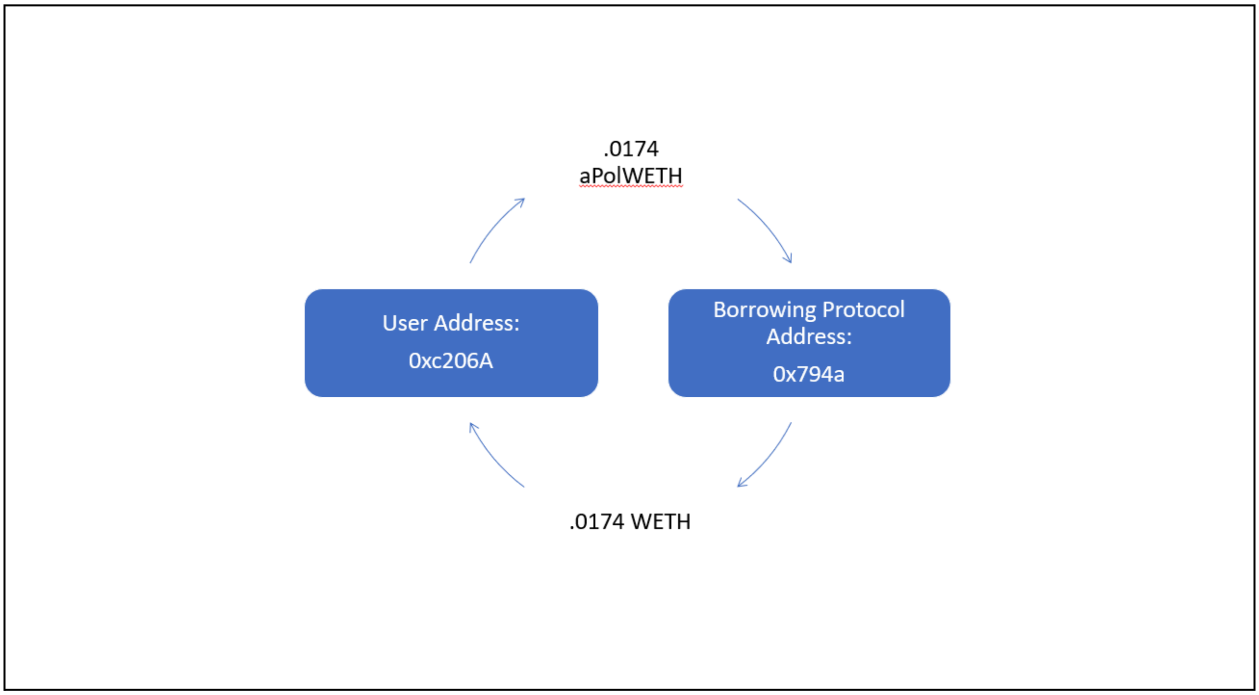
Providing liquidity to and withdrawing liquidity from borrowing protocols are on-chain activities that the Proposal would define as "CVC mixing." While this on-chain activity involves the "aggregating" of multiple users' assets and involves "using programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction," it does not in any way "obfuscate" the link between the two transactions necessary to provide and withdraw liquidity, as shown in the example below.

In the example below, two transactions take place: (1) a transfer of assets from wallet 0xc206A (the liquidity provision transaction) and (2) wallet 0xc206A withdraws those assets at a later point in time (the liquidity withdrawal transaction).

**Provision of Assets - Transaction 1**: In this step, in a single transaction, we provided assets (WETH) to a borrowing protocol and received a newly-generated non-fungible token (NFT) (aPolWETH) representing the portion of the pool our assets amounted to. Conducting this activity does not "obfuscate" any transaction information.



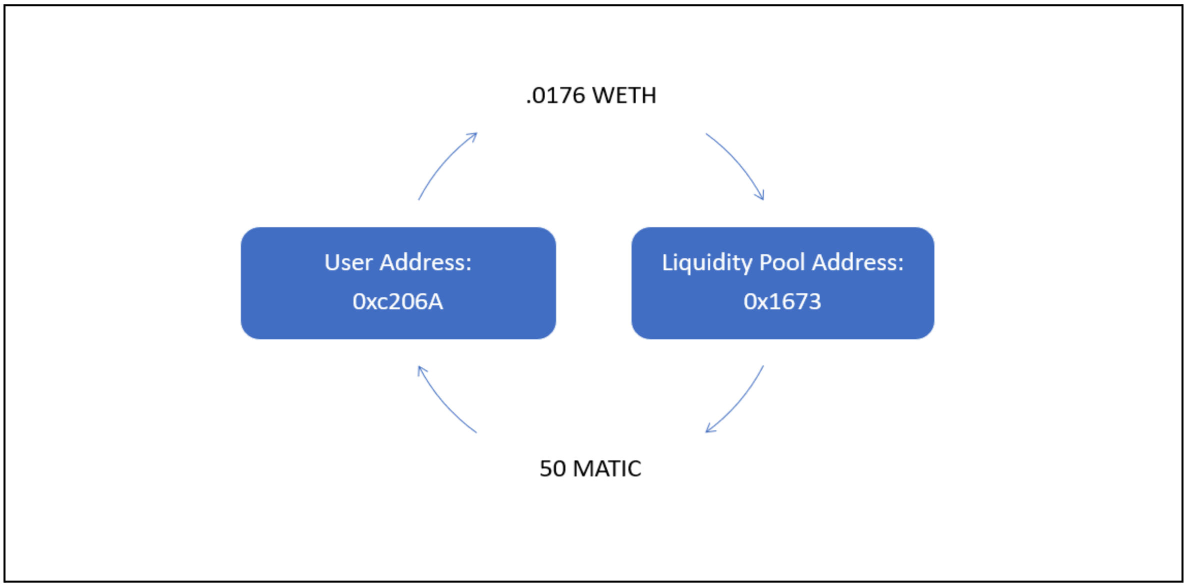
**Withdrawal - Transaction 2**: Next, in a single transaction, we withdrew the assets we provided to the borrowing pool using the aPolWETH we received in the previous transaction. Conducting this activity does not "obfuscate" any of the key transaction information described in the NPRM.



### 4. "Exchanging" or Swapping Tokens

Swapping one cryptocurrency for another using a decentralized exchange protocol is an on-chain activity that would meet the Proposal's definition of "CVC mixing." While conducting such a transaction involves "exchanging between types of CVC or other digital assets," it does not "obscur[e] the connection between the CVC wallet addresses" or "obfuscate" key transaction information (and necessarily only involves one wallet), as shown below.

In this example transaction, we swapped WETH for MATIC using an AMM:



## APPENDIX II:
## Technological Solutions

As described above, FinCEN's current Proposed Rule effectively bans privacy-enhancing technology (PET) and pushes innovation and development offshore. Instead of finalizing this Proposal, FinCEN should focus on recognizing and/or providing workable technological solution guidelines for privacy-enhancing protocol developers / application developers (such as a "proof of innocence" solution discussed below) to comply with existing obligations.

Failing to take new technologies into account in formulating regulation threatens to create gaps in investor protection and capital formation, and it undermines the preeminence of the United States' financial markets. For regulations to vindicate the policy objectives motivating them, they must adapt to how an activity is conducted. While both car and airline manufacturers produce vehicles for the same reason—to provide transportation—cars and airlines facilitate transportation in distinct ways. Fortunately, the regulations applicable to car manufacturers and airline manufacturers are responsive to the functional differences through which the vehicles transport people. The same concept should be applied to distinguish regulations for traditional financial services and blockchain-based or decentralized finance protocols.

Rather than finalizing the Proposed Rule, FinCEN should recognize that there are technological innovations that can be used to increase compliance with reporting requirements and combat illicit finance. A key feature of technological solutions is that they will allow FinCEN to focus on applications (gateways/endpoints/interfaces) rather than protocols.[66] As such, a technological solution would address FinCEN's concerns without implicitly banning PETs and hampering innovation.

[66] This would also be structurally consistent with the United States' 1996 Communications Decency Act, Section 230, the 1998 Digital Millennium Copyright Act, Section 512, and the European Union's 2000 E-Commerce Directive, which protect Internet intermediaries from liability for the actions of their users. Just as network intermediaries are treated as conduits for information and are not responsible for their users' content or transactions, blockchain protocols should also not be responsible for content, including a particular user's intent to engage in "mixing" or obfuscation.

## A Technological Solution to FinCEN's Concerns

FinCEN's concerns can be addressed through a technological solution centered around zero-knowledge proofs (ZKPs).[67] Applications built on blockchain protocols could utilize ZKPs to screen deposits and withdrawals and better safeguard the ecosystem from illicit usage.

### *ZKPs as a Tool to Mitigate Illicit Finance and Money Laundering Risks*

ZKPs are cryptographic techniques that allow one party (the prover) to prove to another party (the verifier) that a statement is true, without revealing any additional information beyond the validity of the statement itself. The "statement" will typically include claims about encrypted information. Numerous publications have recognized their value.[68] For instance, a person may want to prove that he or she voted without revealing what the vote was, or a company might want to prove its solvency without revealing its balance sheet. In essence, ZKPs enable the prover to demonstrate knowledge of a secret without actually disclosing the secret.

The U.S. Department of the Treasury has also highlighted how ZKPs might be used to help law enforcement agencies combat illicit financing in its recent report on "Illicit Finance Risk Assessment of Decentralized Finance"[69]:

*"Technological innovation of this kind could potentially bolster the accessibility, transparency, and security of the U.S. financial system, but most tools remain too nascent for definitive conclusions on their promise. Many potential solutions are designed to support various elements of compliance with AML/CFT obligations while maximizing user privacy, including through digital identity technology to support identity verification by DeFi services that can be informed by a user's transaction history on the public blockchain. Zero-knowledge proofs can also enable a DeFi service user to confirm that their identity has been verified without revealing personal information. Industry solutions may also enable illicit finance risk mitigations to be integrated into smart contract code, such as restricting transaction frequency; placing*

[67] A cryptographic scheme where a prover is able to confirm that a statement is true to a verifier without providing any additional information. *See Zero-Knowledge Proof*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/zero_knowledge_proof (last visited Jan. 19, 2024).

[68] *See, e.g.*, Aleksander Berentsen et. al., *An Introduction to Zero-Knowledge Proofs in Blockchains and Economics*, FED. RESERVE BANK OF ST. LOUIS REVIEW, Fourth Quarter 2023; Shafi Goldwasser et al., *The Knowledge Complexity of Interactive Proof Systems*, SIAM J. COMPUT. (Apr. 18, 1988), https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf; Maksym Petkus, *Why and How zk-SNARK Works*, CORNELL UNIV. (June 17, 2019), http://arxiv.org/abs/1906.07221.

[69] U.S. Dep't. of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* (April 2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

*threshold limits for certain customer types; or using oracles to screen against virtual asset wallet addresses appearing on sanctions lists and to prevent sanctioned addresses from using a DeFi service. While some of these solutions may be applicable to the broader virtual asset ecosystem and financial system, DeFi services may provide an interesting use case given the use of smart contracts and the wealth of data available via the public blockchain. Such solutions could support compliance with BSA and sanctions obligations for obliged DeFi services but could also be used voluntarily by DeFi services not subject to AML/CFT obligations to mitigate risks*."[70]

For instance, by implementing privacy-enhancing measures, ZKPs can be tailored to reduce certain risks associated with exposure to illegal financial activity and economic sanctions. In particular, ZKPs can help FinCEN, Treasury's Office of Foreign Assets Control, and law enforcement agencies with the identification, prevention, and prosecution of money laundering, terrorist financing, and fraud activity. They can also help identify and block assets belonging to sanctioned parties in the U.S. financial system in accordance with foreign policy and national security objectives. The general set-up of ZKP is very flexible. By creating specific association sets of verifiable information to be proved, an application on a blockchain protocol can be customized to suit a large variety of use cases. A workable use case of ZKPs to mitigate FinCEN's concerns flagged in the Proposed Rulemaking is discussed below.

***Proof of Innocence***

ZKPs can be customized to prove that a withdrawal is not associated with illicit activities by proving that the withdrawn funds do not originate from deposits on a 'black list.' This concept is known as "Proof of Innocence," which aims to establish the innocence of the individual / user / application involved.[71]

In this context, ZKPs, through the Proof of Innocence concept, can act as the "notary on the blockchain" and ensure that the identities underlying the transactions on a specific application on a protocol are innocent. ZKP technology uses state-of-the-art cryptographic techniques to issue "green light codes"—given with every transaction—to validated users.

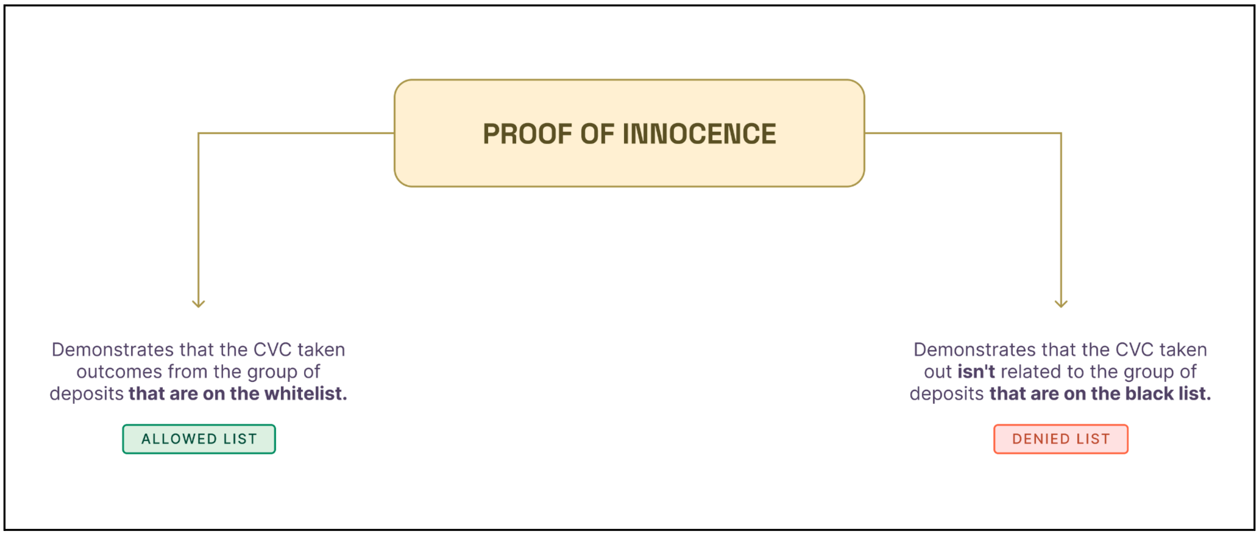
The concept of Proof of Innocence can be conceptualized in two ways:

- demonstrating that the withdrawn cryptocurrency comes from the group of deposits that are on the whitelist (the "Allowed List"); and

[70] *Id*. at 35.

[71] Vitalik Buterin et al., *Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium*, SSRN (Sept. 9, 2023), https://ssrn.com/abstract=4563364.

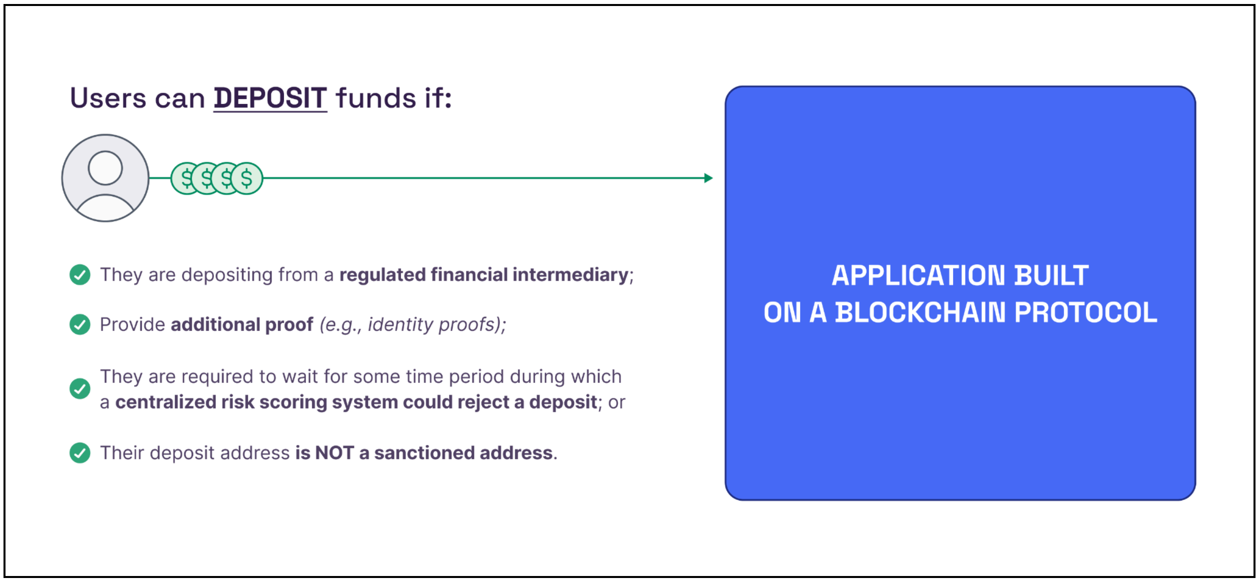
- demonstrating that the withdrawn cryptocurrency is not related to the group of deposits that are on the black list (the "Denied List").


PROOF OF INNOCENCE
Demonstrates that the CVC taken outcomes from the group of deposits **that are on the whitelist.**
ALLOWED LIST
Demonstrates that the CVC taken out **isn't** related to the group of deposits **that are on the black list.**
DENIED LIST

In this example, the ZKPs can use Proof of Innocence to establish the legitimacy and legality of any financial transactions on a blockchain application by proving that the withdrawn funds are either (1) not associated with deposits on a Denied List or (2) are associated with deposits on an Allowed List.

An Allowed List can be designed to regulate which users are allowed to deposit funds into an application built on a blockchain protocol.  For instance, the Allowed List can (1) require users to confirm they are depositing from a regulated financial intermediary (such as a regulated cryptocurrency exchange wallet address), (2) require users to provide additional proof (e.g., identity proofs), or (3) require deposits to wait for some time period, during which a centralized risk scoring system could reject a deposit.  An effective Allowed List which would address FinCEN's concerns could  consist of wallet addresses associated with regulated financial intermediaries (e.g., Coinbase) that perform thorough KYC screening as part of their onboarding procedures, thereby eliminating the need for the privacy-preserving protocol to screen those addresses, as shown below.[72]

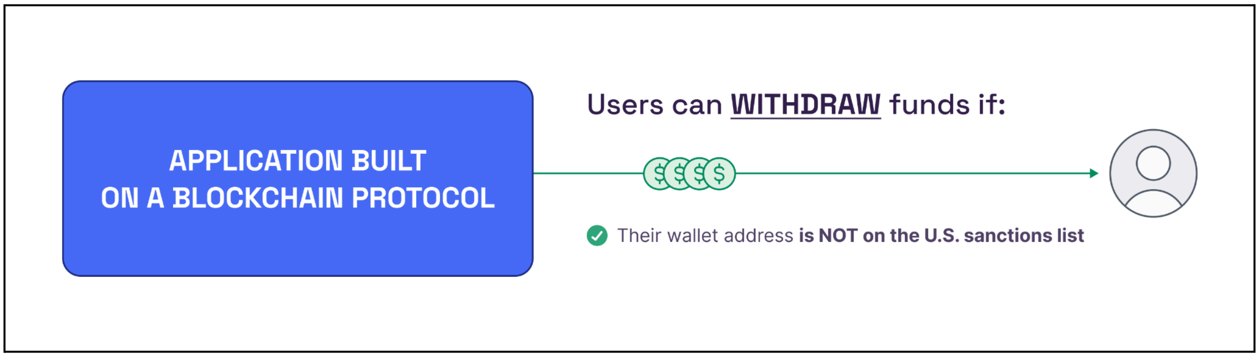
[72] Joseph Burleson et. al., *Privacy-Protecting Regulatory Solutions Using Zero-Knowledge Proofs*, A16Z CRYPTO (Nov. 16, 2022), https://a16zcrypto.com/posts/article/privacy-protecting-regulatory-solutions-using-zero-knowledge-proofs-full-paper/.



Users can **DEPOSIT** funds if:

- ✓ They are depositing from a **regulated financial intermediary**;
- ✓ Provide **additional proof** *(e.g., identity proofs);*
- ✓ They are required to wait for some time period during which a **centralized risk scoring system could reject a deposit**; or
- ✓ Their deposit address **is NOT a sanctioned address**.

Conversely, a Denied List can be set up so that if a user whose wallet address is on the U.S. sanctions list, the user will not be able to withdraw its funds from an application which is accessible to US persons.



Users can **WITHDRAW** funds if:

- ✓ Their wallet address **is NOT on the U.S. sanctions list**