EXPERT REPORT OF COIN CENTER AND DEFI EDUCATION FUND

Amanda Tuminelli, Esq.
Lizandro Pieper
DEFI EDUCATION FUND
1155 F St. NW, Suite 300
Washington, DC 20004
tuminelli@defieducationfund.org
lizandro@defieducationfund.org

Peter Van Valkenburgh, Esq.
COIN CENTER
700 K St. NW
Washington, D.C. 20001
peter@coincenter.org

Dated: May 16, 2025

TABLE OF CONTENTS

ASSIGNMENT **1**
COIN CENTER AND DEFI EDUCATION FUND BACKGROUND **2**
INTRODUCTION **5**
I. BACKGROUND ON RELEVANT TECHNOLOGY **8**
A. Technical Background on Ethereum 8
B. Overview of Decentralized Finance ("DeFi") 10
C. Distinct Components of a DeFi Network: Smart Contracts 12
D. Smart Contract Immutability and DeFi Protocols Upgradability 13
E. Distinct Components of a DeFi Network: the User Interface 16
F. The Benefits of Self-Custodial DeFi 18
II. PRIVACY PRESERVING TECHNOLOGY **20**
A. Privacy Tools Are Particularly Important When Transacting On-Chain 21
B. zk Proof Technology Pre-Dated Tornado Cash 22
III. ANALYSIS RELATED TO TORNADO CASH **26**
A. How Tornado Cash Works 26
B. What does a person need to use Tornado Cash smart contracts? 29
C. The Immutability and Security of the Tornado Cash Protocol 31
D. Upgradability and Decentralized Governance in Tornado Cash 33
E. How does the Tornado Cash tool enhance privacy? 35
F. Why Privacy Is A Good Thing: Law-Abiding People Want to Retain Privacy 37
G. Tornado Cash Is Not A "Service" or Properly Classified as a Compliance- Obligated Entity 39
IV. CONCLUSION **43**

ASSIGNMENT

The defense of A.O. Pertsev asked Coin Center and the DeFi Education Fund to provide an expert opinion that addresses certain key aspects of Ethereum and the Tornado Cash Protocol, as well as the broader context of privacy-preserving tools within decentralized finance (DeFi). The defense requested to examine these technologies in light of the current regulatory environment, providing detailed analysis and insights on the following key areas:

1. **Neutrality of Technologies**:
    - Assess whether Ethereum and Tornado Cash, particularly in their design and operational principles, can be classified as neutral technologies.
    - Explore how Tornado Cash functions as a privacy tool, and whether it can be considered an inherently neutral technological solution.
2. **Privacy Benefits for Users**:
    - Analyze how Tornado Cash is used by individuals to protect their privacy when transacting on-chain.
    - Provide examples of legitimate, non-illicit uses of Tornado Cash by individuals seeking to preserve privacy in a decentralized ecosystem.
3. **Societal and Financial Benefits of DeFi Protocols**:
    - Discuss the societal value of self-custodial DeFi protocols such as Tornado Cash.
    - Provide background on the components of a decentralized finance ecosystem and the role that privacy tools like Tornado Cash play within this structure.
4. **Compliance and Regulatory Framework**:
    - Examine whether Tornado Cash can be classified as an “entity,” particularly in relation to its status under existing financial regulations.

COIN CENTER AND DEFI EDUCATION FUND BACKGROUND

Coin Center is a Washington, DC-based non-profit research and advocacy center focused on the public policy issues facing cryptocurrency and decentralized computing technologies such as Bitcoin and Ethereum. Our mission is to defend the rights of individuals to build and use free and open cryptocurrency networks: the right to write and publish code – to read and to run it. The right to assemble into peer-to-peer networks. And the right to do all this privately. In November 2023, Coin Center sued the United States Office of Foreign Assets Control (OFAC) to remove the Tornado Cash pool addresses from the Specially Designated Nationals and Blocked Persons list (SDN List). Coin Center argues that OFAC's action exceeds its statutory authority by blocking things like immutable smart contracts that are neither sanctioned persons nor their property, violates the Administrative Procedure Act, and is unconstitutional. *See Coin Center et al. v. Secretary, Dep't of Treasury, et al*., Case No. 23-13698-E (11th Cir.). While the case addresses some of the same facts as the criminal case against A.O. Pertsev, the legal issues are completely different and the outcome of one will not affect the other. Since OFAC delisted sanctions against the Tornado Cash protocol and website on March 21, 2025, active motion practice in the case is currently held in abeyance (stayed).

Peter Van Valkenburgh is the Executive Director of Coin Center, the leading non-profit research and advocacy group focused on the public policy issues facing cryptocurrency technologies such as Bitcoin and Ethereum. Previously, he was a founding board member of the Zcash Foundation, a non-profit charity dedicated to building financial privacy infrastructure for the public good, and an advisor to StarkWare, a company developing trust-minimized scaling solutions using zero-knowledge proof cryptography. Due to his expertise in these subjects, he has been invited to testify before the U.S. Congress on six different occasions. He testified before the

Senate Banking Committee and was the first witness before that body to offer a detailed explanation of Bitcoin and its financial regulatory implications. He has also testified before the Joint Economic Committee of Congress, the Financial Services and Energy and Commerce Committees of the House of Representatives.[1] Internationally, he has briefed staff and members of the EU parliament, the Financial Action Task Force, and educated policymakers and regulatory staff around the world on the subject of cryptocurrency regulation and decentralized computing systems. He has guest lectured on these topics at various law schools and engineering schools, including Yale, Harvard, NYU, Columbia, Cornell, Carnegie Mellon, U.C. Berkeley, Stanford, and the University of Maryland.

Peter Van Valkenburgh thus has a profound and a deep understanding of blockchain technology, cryptocurrency, smart contracts and policy and legal issues related to these topics. As a co-writer of this report he has used this experience and knowledge on the topics as listed. His resume is attached to this report.

DeFi Education Fund (DEF) is a nonpartisan nonprofit organization based in the United States that advocates for and educates about sound policy for decentralized finance (DeFi). DEF's mission includes advocating for the interests of DeFi users, participants, and software developers working to innovate using blockchain technology that is decentralized and open to all users. Among other things, DEF educates the public about DeFi through editorials, podcasts, and print media, meets with members of Congress to discuss DeFi technology, and submits

[1] *See, e.g.*, Written Testimony of Peter Van Valkenburgh before the U.S. House of Representatives Subcommittee on Digital Assets, Financial Technology and Inclusion, hearing titled, *Decoding DeFi: Breaking Down the Future of Decentralized Finance* (Sep. 10, 2024), *available at* https://democrats-financialservices.house.gov/uploadedfiles/hhrg-118-ba21-wstate-vanvalkenburghp-20240910.pdf; Written Testimony of Peter Van Valkenburgh, U.S. House of Representatives Committee on Financial Services Subcommittee on Oversight and Investigations, hearing titled, *America on "FIRE: Will the Crypto Frenzy Lead to Financial Independence and Early Retirement or Financial Ruin?* (Jun. 30, 2021), *available at* https://democrats-financialservices.house.gov/uploadedfiles/hhrg-117-ba09-wstate-vanvalkenburghp-20210630.pdf.

public comments on proposed rulemakings that impact DeFi. DEF also regularly files amicus briefs in court cases that raise legal issues of broad importance for DeFi.

Amanda Tuminelli is the Executive Director and Chief Legal Officer of DEF, where she oversees DEF's policy and advocacy efforts. Prior to joining DEF, Amanda was a lawyer at Kobre & Kim, where she defended clients against criminal and regulatory investigations, government enforcement actions, and large scale litigation, particularly in the crypto and blockchain space. Through these representations, she developed a comprehensive understanding of the legal and regulatory landscape related to digital assets and software developers. She previously served as a law clerk for the Honorable Ann M. Donnelly of the U.S. District Court for the Eastern District of New York and practiced at Dechert LLP in their white-collar and securities litigation group. Because of her expertise related to DeFi technology, Ms. Tuminelli was asked to testify before the House Financial Services Subcommittee on Digital Assets, Financial Technology and Inclusion in Congress in the first-ever Congressional hearing related to DeFi, and asked to provide an overview of DeFi technology, its benefits, and the related regulatory environment.[2]

Lizandro Pieper is the Research Director at DEF, where he leads the organization's efforts to conduct research and write reports related to DeFi and blockchain technology. Under DEF, his research is largely focused on U.S. national security laws, as well as financial privacy and inclusion. Lizandro received his Bachelor of Arts in Political Science at Colorado State University. He is currently obtaining his Bachelor of Science in Applied Computer Science from the University of Colorado, where he has programmed software using public-key cryptography

[2] *See* Written Testimony of Amanda Tuminelli before the U.S. House of Representatives Subcommittee on Digital Assets, Financial Technology and Inclusion, hearing titled *Decoding DeFi: Breaking Down the Future of Decentralized Finance* (Sep. 10, 2024), *available at* https://www.defieducationfund.org/_files/ugd/84ba66_1cfcccd3ef8b4f4899e6dcfc02686158.pdf.

and Secure Hashing Algorithms (SHA) employed in blockchains. Prior to joining DEF, Lizandro worked in various areas of politics, but most relevant was his Asian geopolitical research in his internship at A. Kain & Partners and U.S.-Asian foreign policy research at the Heritage Foundation. In both research experiences, Lizandro specifically focused on human rights and freedom, as well as cyber, information, and economic warfare with regards to China and North Korea. Lizandro was introduced to cryptocurrency in early 2020 while researching Bitcoin's global humanitarian uses. Given his research in foreign policy, national security, and privacy, as well as his studies in computer science, Lizandro has developed a keen understanding of blockchains and cryptocurrency, and their development around the world.

As co-authors of this report, Ms. Tuminelli and Mr. Pieper have used their respective experience and knowledge on the topics included in this paper. Each of their resumes are attached to this report.

Both organizations have an independent interest in educating about the nature of the digital asset and DeFi industries, public blockchain technology generally, and privacy-preserving technology specifically. Each organization has a further interest in protecting the rights of all digital asset market participants, including users and software developers, to interact with and build software tools that take advantage of the security, efficiency, accessibility, resiliency, and privacy of decentralized networks.

INTRODUCTION

This case presents a novel question: when should software developers be held criminally liable for the actions of third parties who use their software to commit crimes? Outside the world of software development, it is not common for liability to be imposed on the creators of neutral tools. For example, automobile manufacturers are not liable for drivers who use their vehicles as weapons; construction companies are not liable for businesses that use their offices to perpetrate

fraud; and television manufacturers are not liable for newscasters who use their screens to publish false or defamatory statements. It is *not* the norm for designers, inventors, and developers of new technologies to be liable for third-party misuse of their inventions.

For this reason, this case has drawn significant attention, as understanding the boundaries of what developers can and cannot do is of critical importance. The lines appear blurred in these instances, prompting questions about whether DeFi innovations are being treated the same as those in other industries. While blockchain technology plays a central role in this case, the liability issues at stake have far-reaching implications for software developers across all industries. Writing computer code is both a technical skill and an act of creative expression, and software developers are as much writers as they are engineers. For them, code is speech – the means by which they invent, innovate, and instantiate their ideas into the world.

DeFi Education Fund and Coin Center work directly with members of the DeFi and digital asset industries and are concerned that a ruling criminalizing the development of software later used by third-party bad actors will have a chilling effect on the technological innovations of this young industry. The chilling effect of the initial verdict on the development of free and open-source software is already significant, and developers are left with no indication of where their liability begins or ends.

It is also important to recognize that many concepts related to digital assets and DeFi technology, which is a relatively new technology, do not align with traditional legal frameworks. Both Europe and the U.S. are actively working on new rules to address digital assets and DeFi, striving to find a balance between fostering innovation and addressing the challenges posed by the unknown. As regulators attempt to apply existing laws to new technology, difficult questions like the ones raised in this case will arise. For example, the U.S. Fifth Circuit Court of Appeals in

Van Loon v. Department of the Treasury recently held that smart contracts are not property or interests in property under the law and that the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) had overstepped its regulatory authority in issuing the sanctions in the first place, which led to OFAC delisting of Tornado Cash smart contracts from its Specially Designated Nationals (SDN) list.[3] The reality is that so long as the law does not clearly or comprehensively grapple with the realities of blockchain technology or DeFi, and give software developers fair notice of what the law is as applied to their technologies, this shifting regulatory environment will continue.

For example, if software developers are held liable for third-party misconduct, the following actions could unexpectedly result in criminal charges for software developers, who would be surprised to learn that they violated the law:

- A video game developer creates an online game where users can interact live and barter in-game goods, and pays for hosting services. A criminal actor makes an account to play the game using stolen funds. The developer continues to pay for website hosting services after finding out this occurred.
- An email client such as Gmail continues to provide their software and pay for server space after finding out that an individual used their email client to buy and sell stolen goods or defraud other persons.
- An iPhone app developer creates a general purpose payments app available in the App Store. Despite Apple's efforts to comply with applicable laws, an individual uses the app to launder funds, and the app's development team continues to fix bugs and put out updates for the app.

Taking the theory of this case to its logical end, the law would require developers of any tool to, at the time of creation, anticipate the myriad ways that bad actors might someday use their tool and wall off all possible entry points. If it turns out that their efforts to exclude bad actors were insufficient, the developers must cease operations the day that a bad actor uses their tool, lest they be found liable for a third party's use of that tool. Should we remove everything

[3] *See* U.S. Dep't of Treasury, *Tornado Cash Delisting*, (March 21, 2025), *available at* https://home.treasury.gov/news/press-releases/sb0057.

from the market that is known to be used by criminals for illegal activities? As mentioned, with this expert opinion, we aim to provide the background and insights into this emerging industry, to foster a better understanding and reach a clear judgment on these kinds of liability issues.

In Section I, the report provides a background on the technology related to the Ethereum network, including what smart contracts are and what it means for a smart contract to be immutable, and related to decentralized finance ("DeFi"). In Section II, the report explains privacy-preserving technology, including zero knowledge ("zk") cryptography, why it is important, and why it should always be properly categorized as a neural tool. In Section III, the report discusses how Tornado Cash works, how it assists users in creating private transactions, provides real use cases of the software helping people, explains that even with the Tornado Cash tool available for public use, obligated entities can still meet compliance obligations, and concludes that Tornado Cash is not properly considered "service" or obligated entity of any kind.

I. BACKGROUND ON RELEVANT TECHNOLOGY

A. Technical Background on Ethereum

Ethereum is a network of nodes on the internet. The nodes collectively work together to create a shared public database of user data, including financial transactions. That database is typically referred to as Ethereum's "blockchain," a term referencing the specific technological methods used to encode and verify the data in the database.

Ethereum is used by tens of millions of people around the world.[4] It facilitates

[4] Anyone can generate a public address and start using Ethereum with their own wallet software. There is no authoritative list of individual wallets on Ethereum and one person may have several wallets. It is therefore difficult to arrive at a precise estimate of how many people use Ethereum. Consensys is a software development company that provides wallet software called Metamask. Their data on unique users suggests that around 30 Million people use Metamask to access Ethereum. There are many alternative software wallets as well as hosted wallet accounts, such as those provided by companies like Coinbase. 30 Million users would, therefore, be an extremely conservative lower bound. *See* David Canellis, *MetaMask Monthly Active Users Nears All-Time High - Over 30 Million*, Blockworks (Feb. 20, 2024), https://blockworks.co/news/metamask-monthly-active-users-blockaid.

transactions involving ether, the second most common cryptocurrency after Bitcoin. It also facilitates transactions involving a wide range of additional digital assets often referred to generally as "tokens." To use Ethereum, a person needs only to have an internet-connected device and freely available software. That software is "free and open-source" which means it is in gratis, *i.e.* available for users to download from a multitude of sources without any cost. It is also free as in freedom, *i.e.* it is released under open-source copyright licenses that allow anyone to use, modify, distribute, and copy it without permission and as they see fit.

Using this free software on her own computer, a person can begin transacting on Ethereum. As a first step the user must have their computer cryptographically generate a "private key" and a corresponding "public key." The private key is the basis for mathematically generating the corresponding public key. And while public key generation is easily computed, it is infeasible to reverse-engineer the private key from the public key. Importantly, the public and private keys act as mathematical proofs of authority over digital assets on a blockchain: the private key is used to create digital signatures that authorize transactions, while the public key is used to generate receiving addresses and verify digital signatures.

To make sending Ether more user-friendly, an Ethereum blockchain address is mathematically generated from a public key as a shorter string of characters. This serves as a more practical representation used for securely sending and receiving transactions. By sharing an address, users are able to receive a transaction from anyone, anywhere in the world. Unlike a traditional payment service, sending and receiving tokens on Ethereum does not require an intermediary. Instead, the sender broadcasts their intent to transfer tokens, digitally signs their message using the corresponding private key, and Ethereum's network collectively updates the blockchain records of the sender and receiver addresses with the new balances. In this

peer-to-peer transfer example, none of the participants are "financial institutions" as that term is defined across the European Union, United States, United Kingdom, or in any of the member nations of the Financial Action Task Force ("FATF").[5]

Furthermore, unlike in traditional finance, Ethereum's records are completely transparent: anyone can download and view the balances and transaction history of user accounts. Although user addresses are pseudonymous, if a real-world identity is linked to a user address, it becomes possible to tie that user's complete transaction history, and any transactions they make in the future, to their real-world identity. By default, a record of a casual transaction today, like paying with cryptocurrency for Wi-Fi access at the airport, reveals records of earlier (and any future) cryptocurrency transactions, which may include any intimate, revealing, or sensitive transactions made by the same user long ago. Among the many different applications smart contracts may support, some provide an avenue for users to regain the privacy they expect when using blockchains, discussed below.

B. Overview of Decentralized Finance ("DeFi")

DeFi is an umbrella term generally used to describe blockchain-based software protocols that allow people to engage in peer-to-peer economic activities online while self-custodying their assets. To do so, DeFi builds on the innovations of public blockchains, which are software protocols that first enabled people to engage in peer-to-peer value transfer over the internet.[6] Because there is no need for a central server in a peer-to-peer network, no single entity has control over the data stored on a public blockchain. Instead, all computers (nodes) participating in a peer-to-peer blockchain network (1) hold a record of the history of data stored on the

[5] Nor does FATF recommend that member states require licenses for these entities.
[6] *See* Peter Van Valkenburgh, *Open Matters: Why Permissionless Blockchains Are Essential to the Future of the Internet*, Coin Center (Dec. 2016), https://www.coincenter.org/open-matters-why-permissionless-blockchains-are-essential-to-the-future-of-the-internet.

network; and (2) reach consensus as to the validity of that data. No single entity participating in the network has control over, or can alter, the data record.

"Self-custody" refers to individuals' ability to directly custody the cryptographic keys (public and private) that maintain control of digital assets without the involvement of any third-party. A custodial arrangement, on the other hand, refers to situations in which a person uses the services of a third-party to store keys on their behalf, therefore, giving up some measure of control over their digital assets. Using a basic analogy, cash in a person's bi-fold wallet is "self-custodied" whereas a person's cash held by a bank on their behalf is "custodied" by a third-party. In both instances, the cash belongs to the person; the differentiation lies in whether the owner of the cash has free access to and independent control over it.[7]

As with any decentralized protocol and associated user interfaces or other connected applications, it is important to distinguish each component of a blockchain-based network precisely. This exercise is particularly important in the context of open-source software development, where it is common for different software developers to work on different components of a network at different times. For example, the software developer who begins to write code for a smart contract protocol may not be the same developer who finishes the code or reviews it for bugs years later. Often, the developer who works on the smart contracts for the protocol is different from the developer who creates a user interface for the protocol. These distinct components are discussed in detail below.

[7] *See* Barabander et al., S*ecret Notes And Anonymous Coins: Examining FinCEN's 2019 Guidance On Money Transmitters In The Context Of The Tornado Cash Indictment*, The International Academy of Financial Crime Litigators (Sep. 2023), https://www.cravath.com/a/web/qyCBWVBLEMsqxPHtd9ykoc/87ntut/the-international-academy-of-financial-crime-litigators.pdf.

C. Distinct Components of a DeFi Network: Smart Contracts

In addition to sending and receiving tokens, users can create and interact with "smart contracts," which are software programs that extend the functionality of Ethereum. When software developers program smart contracts, they decide what operations the smart contract will support and what rules those operations must follow. These rules and operations are written using code that is broadcast to Ethereum's network, just like the token transactions described above. Once a smart contract's code is added to Ethereum's records, it receives its own unique address, and any user can interact with it to automatically carry out the rules and operations it supports.

Both people and smart contracts can have Ethereum addresses. The difference is that when a person has an address, they have the private key that controls any tokens sent to that address. Any person that holds the private key will ultimately decide if and when any transactions are made with those tokens. When a smart contract has an address, the rules and operations written in the smart contract code control the tokens. They could be simple rules, such as "automatically return the tokens to the sender," or more complicated rules. There could be rules that include human operations and human decisions – such as "send the tokens back if 3 out of 5 of these human-controlled addresses send a signed message saying they agree." The rules could also, however, be fully and permanently outside of any human being's control. In that case, so too are any tokens sent to that address until and unless the contract sends them to some human according to the rules. When a smart contract's rules are programmed to operate without an intermediary, the contract is often referred to as being "non-custodial," as in no human participant custodies or controls any assets on behalf of the users of the contract.[8]

[8] Nick Szabo, a computer scientist and legal researcher, wrote extensively about the concept of a "smart contract" in the 1990s and is commonly credited with inventing the term. *See, e.g.*, Nick Szabo, *The Idea of Smart Contracts*, (1997), available at https://nakamotoinstitute.org/library/the-idea-of-smart-

Smart contracts are often compared to a vending machine that automatically releases a bag of chips on the condition that it receives €2: the user relies on the machine to operate according to the "code" in place and dispense an item once the user has inserted €2. But unlike a vending machine, no one can "unplug" a smart contract or modify the underlying code, making smart contracts "immutable."

D. Smart Contract Immutability and DeFi Protocols Upgradability

By default, smart contracts are immutable, which means their code cannot be changed by anyone once they are "deployed," a term used for publishing code to the Ethereum blockchain. DeFi protocols – which are collections of smart contracts that operate in conjunction for users to conduct their own financial activities – can be designed with upgradable components such that the smart contracts employed in a protocol may be replaced by new smart contracts. This upgradable component ensures that any bugs or inefficiencies can be dealt with by replacing a smart contract, since smart contracts' code cannot be changed directly. Importantly, upgradeability is typically designated only to smart contracts that conduct auxiliary functions – *i.e*., functions that are not critical to the protocol, but support the core functions. The core smart contracts themselves, which are fundamental to the protocol, are not typically upgradable so as to ensure the security and integrity of the protocol.

For protocols to be upgradable, they may be constructed with smart contracts that are *initially* deployed with an update capability assigned to some human-controlled address. This is to allow for flexibility in the protocol's initial construction. However, this update capability may be subsequently revoked and reassigned to a "zero" address, without an owner, which results in permanent removal of any authority to upgrade the smart contracts. This is typically the process

---

contracts; Nick Szabo, *Smart Contracts*, (1994), available at https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

employed on a protocol's core smart contracts. Revocation and reassignment makes it so the protocol is truly decentralized – where upgrades for auxiliary smart contracts can only come from the consensus of independent token holders and not any one person or group under common control, and core smart contracts are permanently cemented in the protocol.

To revoke update capability, the person or group of persons who have the power to update the contract must transfer that update permission to a placeholder Ethereum address for which it is mathematically infeasible to derive a private key – the zero address. All the computing power in the world could be dedicated exclusively to creating a corresponding private key for the next billion years and yet still no computer would likely succeed at creating that matching key. Without a corresponding private key, it is impossible for any person to forge a correct digital signature updating the contract. Once the ability to update a contract has been assigned to the zero address, it is effectively revoked, cannot be reclaimed, and the contract can no longer be changed.

With regards to auxiliary smart contracts, their upgradability is secured through the decentralized infrastructure of the DeFi protocol. In other words, no one person or corporation could unilaterally upgrade the protocol and replace the auxiliary smart contracts. This is because DeFi protocols employ decentralized governance mechanisms in which anyone can participate by simply acquiring a token native to the protocol. A governance smart contract – *i.e.*, a smart contract that encodes the rules for token holders to propose and vote on protocol upgrades for auxiliary smart contracts – is also deployed and assigned to an address that employs the decentralized governance mechanism for the protocol. Token holders are then able to propose and vote on upgrades to the protocol just as they would in a direct democracy, where the token

serves as a proof-of-citizenship. Decentralization ensures that there is no barrier to participation and therefore no unilateral human discretion dictating upgrades to the protocol.

Immutability and non-upgradability is a positive attribute; it ensures the security and integrity of DeFi protocols by significantly reducing the need to trust third-parties with maintaining important software functions for financial activities. Users can be sure that no one can maliciously manipulate the code or mistakenly modify it such that it causes financial injury. This also means that anyone can enjoy the benefit of the smart contract's functionality, because no one is empowered to screen or prevent people from using it. Centralized control over access to financial systems can be abused by corporations or nation-states to systematically deny lawful citizens access to finance and banking for discriminatory reasons. While such systematic denials are possible today in an intermediated financial system, DeFi and blockchain technology imagine an alternative to that traditional financial system. Hence, with over one billion people unbanked globally, DeFi has largely been adopted by those in developing countries as a means to protect themselves from political instability, corruption, hyperinflation, and inadequate financial infrastructure caused by centralized control.[9]

For these reasons, many important and widely used Ethereum protocols employ smart contracts that are non-upgradable, which are attractive to many users.[10] This preference is not unlike an ordinary person's preference for cash over credit card payments: neither the payor nor the payee need to trust a card-issuing bank in order to complete the payment. Similarly, many people prefer physical books despite the availability and convenience of e-books because they

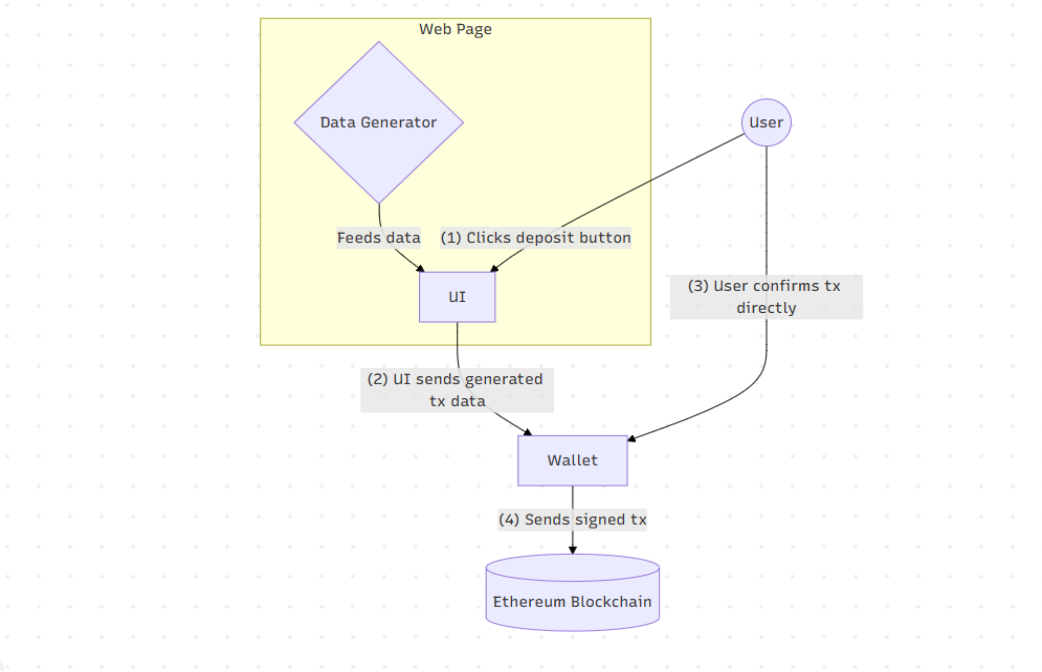
[9] DeFi Education Fund, *DeFi, Inclusion, and Financial Democracy* 1 (June 2024), https://www.defieducationfund.org/_files/ugd/84ba66_61d78b323b244c16994e2dc0373519a3.pdf.
[10] For example, the smart contracts that power the decentralized cryptocurrency exchange protocol called Uniswap are immutable. As of this declaration, Uniswap's immutable smart contracts have facilitated 1.738 Trillion USD worth of trading for users. *See* https://defillama.com/dexs/uniswap.

would rather own and fully control their reading material rather than be beholden to an electronic retailer like Amazon's Kindle platform for the continued availability of their library.

E. Distinct Components of a DeFi Network: the User Interface

User interfaces ("UIs") are front-end websites or applications that can link to a smart contract protocol, and consist of entirely separate code from the protocol itself. Because of this, UIs are referred to as "off-chain," meaning they are typically owned and controlled by the developers who built them, are stored by a centralized cloud provider (such as Amazon Web Services, for example), and operate only so long as their developers provide for their maintenance and upkeep; they are not stored and maintained on a blockchain.

When seeking to conduct a DeFi transaction, a person can use a UI that makes it easier to interact with the relevant smart contracts. UIs are composed not only of visual elements (*i.e.*, a website) but also of the code that powers interactive features like forms and buttons. A UI typically serves two roles: as a browser and as a data object generator. In its browser role, a UI shows the user information about the state of the blockchain relating to a set of smart contracts and provides an intuitive visual interface for users to indicate what actions they would like to perform (a user's "input") through the smart contracts. In its data object generator role, a UI "translates" a user's input into a data object, *i.e.*, a set of data with the necessary information to submit a transaction for inclusion on-chain. Typically, UIs with data object generators include a "connect wallet" button, which, when selected, establishes a secure connection between the UI and the user's crypto wallet. The data object generator uses that connection to send the data object to the user's wallet, which a user may or may not cryptographically pair with their private key and then submit their transaction through their wallet for inclusion on-chain.



Crucially, a UI solely generates a data object based on people's interactions with the front end, and therefore, users have total discretion over whether to complete their transaction. Any deployment of a data object to the blockchain is done by the user through the user's wallet and without a UI's involvement whatsoever. UIs only generate and display information in response to a user's actions, providing an informational service like Google, Yahoo! Finance, or Wikipedia.

Because of the distinction between UIs and their underlying protocols, control over a UI does not equate to control over the underlying protocol. Often, smart contract protocols are accessible through many different UIs created and maintained by developers who had no role in coding the underlying protocol and may not even know each other. Changes to a UI usually do not have any effect on the protocol itself. Furthermore, more technical users can access a DeFi protocol locally from their computer using a command-line interface (CLI)[11] and do not need to depend on a UI to access a protocol. In other words, UIs provide a form of access to a protocol,

[11] In a UI – or graphical user interface (GUI) – a user *shows* the computer what to do by interacting with its visual design features. While in a CLI, the user *tells* the computer what to do through text-based instructions. A CLI is typically accessed locally on one's computer through a terminal.

but they do not and cannot authorize access to a protocol, control the functions of the protocol, or act on behalf of the users of the protocol.

F. The Benefits of Self-Custodial DeFi

DeFi technology was developed in response to the many challenges and risks inherent in the structure of intermediated financial services, be it centralized finance or traditional finance – including limited and unequal access, slow settlement cycles, inefficient price discovery, liquidity challenges, a lack of assurance around underlying assets, opaqueness, broker risk, and uptime issues.

Traditional financial intermediaries establish trust between transacting counterparties – the knowledge that a transaction will occur as both parties expect – by acting as a middleman between them. For example, making a payment with a credit card involves a minimum of four separate financial intermediaries in addition to the two parties to a transaction. However, instead of relying on specialized intermediaries to establish trust between counterparties, blockchains establish trust via rules-based, encoded software protocols – in other words, the technical design provides the trust. These novel features enable people to use public blockchains to engage in digital transactions and economic activities without reliance on third-party intermediaries. Users of DeFi protocols have open, transparent access to systems that allow people to conduct various types of financial activities without requiring specialized intermediaries or institutions.

Moreover, by allowing people to transact directly with their peers utilizing open-source software, all while maintaining custody over their own funds, DeFi protocols provide numerous benefits.[12] For example, DeFi protocols increase transparency about the mechanics of market

[12] *See generally* Caitlin Ostroff & Jared Malsin, *Turks Pile Into Bitcoin and Tether to Escape Plunging Lira*, Wall St. J. (Jan. 12, 2022), https://www.wsj.com/articles/turks-pile-into-bitcoin-and-tether-to-escape-plunging-lira-11641982077; Roger Huang, *Dissidents Are Turning to Cryptocurrency As Protests Mount Around The World*, Forbes (Oct. 19, 2020) https://www.forbes.com/sites/rogerhuang/2020/10/19/

infrastructures and associated fees by using open-source software, wherein the code for each protocol is transparent and auditable.[13] Transactions using DeFi protocols are also recorded on immutable public blockchains, the records of which live forever and cannot be manipulated or amended, offering greater certainty to users.

DeFi protocols are open and available to anyone in the world with an internet connection, significantly expanding global access to transactional services.[14] That access empowers people from all backgrounds and in varying circumstances to use financial services without having to go through intermediaries, who often gatekeep participation through unfair or discriminatory treatment, absolute prohibitions, or excessive pricing.[15] It also means that people have access to finance even in challenging conditions, such as in countries where " local currencies are collapsing, broken, or cut off from the outside world," "legacy financial systems falter[]," or "the horrors of monetary colonialism, misogynist financial policy, frozen bank accounts, exploitative remittance companies, and an inability to connect to the global economy" are a constant reality.[16]

---

dissidents-are-turning-to-cryptocurrency-as-protests-mount-around-the-world/; Timour Azhari, *Young Lebanese driving crypto 'revolution' after banks go bust*, Reuters (Sept. 20, 2021), https://www.reuters.com/article/lebanon-crypto-currency-youth/feature-young-lebanese-driving-crypto-revolution-after-banks-go-bust-idUSL8N2QH1MW/; Carlos Hernández, *Bitcoin Has Saved My Family*, N.Y. Times (Feb. 23, 2019), https://www.nytimes.com/2019/02/23/opinion/sunday/venezuela-bitcoin-inflation-cryptocurrencies.html; Jillian Deutsch & Aaron Eglitis, *Putin's Crackdown Pushes Independent Russian Media Into Crypto*, Bloomberg (May 10, 2022), https://www.bloomberg.com/news/articles/2022-05-10/putin-s-crackdown-pushes-independent-russian-media-into-crypto; Cristina Criddle & Joshua Oliver, *How Ukraine Embraced Cryptocurrencies in Response to War*, Financial Times (Mar. 19, 2022), https://www.ft.com/content/f3778d00-4c9b-40bb-b91c-84b60dd09698.

[13] *Decentralized Finance: Innovations and Challenges*, Bank of Canada (Oct. 2023), *https://www.bankofcanada.ca/2023/10/staff-analytical-note-2023-15/.*

[14] *See, e.g.*, Bitange Ndemo, *The role of cryptocurrencies in sub-Saharan Africa*, Brookings Inst. (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.").

[15] *Letter in Support of Responsible Crypto Policy*, Open Letter to 117th Congressional Leadership (June 2022), https://www.financialinclusion.tech/ ("Bitcoin provides financial inclusion and empowerment because it is open and permissionless. Anyone on earth can use it. Bitcoin and stablecoins offer unparalleled access to the global economy for people in countries like Nigeria, Turkey, or Argentina, where local currencies are collapsing, broken, or cut off from the outside world."); *see also* Huang, *supra*.

[16] *See Letter in Support of Responsible Crypto Policy*, *supra* note 14; *see also* Azhari, *supra* note 11 ; Hernández, *supra* note 11.

The absence of intermediaries and self-custodial nature of DeFi protocols provides individual users greater control over their tokens and certainty that the transactions they expect to happen will happen. Users do not have to trust a third-party to safely store and transact. However, because users self-custody their tokens and cannot rely on a centralized institution to protect their personal information or shield their transactions from public view, they need to take action in order to preserve their privacy.

II. PRIVACY PRESERVING TECHNOLOGY

In the simplest terms, the Tornado Cash protocol is a neutral tool that allows users to engage in private transactions on a public blockchain without the rest of the world peering over their shoulders. Like all tools, the Tornado Cash protocol can be used for benign purposes or misused to commit crimes. However, the intention of third parties who use a tool does not change the neutrality of the tool itself.

There is nothing illicit about building tools that preserve financial privacy. The right to privacy or a private life is a core value in the E.U., and enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8) and the European Charter of Fundamental Rights (Article 7).[17] An April 2021 report by the European Central Bank calling for public comment on a digital euro noted that privacy was "the most important feature" to E.U. citizens and professionals, and that privacy was identified by respondents as the "main challenge" associated with its creation.[18]

[17] UN General Assembly, Resolution 217A (III), Universal Declaration of Human Rights, A/RES/217(III) (December 10, 1948), https://www.un.org/en/about-us/universal-declaration-of-human-rights; Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms*, Council of Europe Treaty Series 005, Council of Europe, 1950, https://www.echr.coe.int/documents/d/echr/Convention_ENG; European Union, Charter of Fundamental Rights of the European Union, Official Journal of the European Union C83 (Vol. 53, p. 380)(2010), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.

[18] European Central Bank, *Eurosystem report on the public consultation on a digital euro*, (April 2021) at 3, 10-11, https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_e

The ability to transact privately is a core component of protecting a private "family life, home and communications."[19] And it is relatable: we all want to give to political causes or religious entities without unwanted attention, buy personal items without others knowing or having to feel embarrassed, and speak freely to our friends without fear our words may be taken out of context at some later point in time. People already use cryptocurrency for all of these sensitive purposes.[20]

The European Union's recent affirmation of a data protection right of erasure, exemplified by the Court of Justice's March 2024 ruling empowering authorities to mandate deletion of unlawfully stored personal transaction data, underscores a strong commitment to individual privacy in the context of financial transactions and records.[21] Criminalizing the development of privacy tools such as Tornado Cash directly undermines this very commitment, as these technologies are some of the *only* effective means and methods to allow individuals to 'delete' their transaction histories in public blockchain environments.

A. Privacy Tools Are Particularly Important When Transacting On-Chain

Privacy preservation is particularly important when transacting on public blockchains because of their transparent nature. Traditional economic transactions (off-chain) can provide substantially more privacy than on-chain transactions: traditional cash transactions are virtually untraceable, and transactions involving financial institutions like banks, credit card networks,

---

uro~539fa8cd8d.en.pdf. 43% of respondents cited privacy as what they want most from a digital euro. *Id.* In fact, "When confronted with a specific choice between an offline digital euro focused on privacy, an online one with innovative features and additional services," E.U. citizens chose the more private, off-line version. *Id.*

[19] *See supra* note 9.

[20] *See, e.g.*, Healthcare Bus. Today, *Cryptocurrencies And Medical Bills: The New Way To Pay For Healthcare?*, (Nov. 3, 2022), perma.cc/72S8-DWSS (describing cryptocurrency payments for private healthcare services); The Giving Block, perma.cc/XP9U-GGYE (facilitating cryptocurrency donations to religious and charitable organizations).

[21] *See* Case C-60/23, Autoriteit Persoonsgegevens, ECLI:EU:C:2024:219 (Mar. 14, 2024), https://curia.europa.eu/juris/document/document.jsf?docid=283833.

and payment processors expose sensitive information only to the institution, not to the public at large. But blockchain-based transactions are posted to a public ledger that anyone can see; all of a user's transactions can be viewed by anyone with access to the internet and who knows the user's wallet address, for all time.

The unique transparency of public blockchains creates major privacy concerns that can expose individuals to exploitation, invite retaliation for politically-sensitive contributions, and leave users' private and sensitive affairs exposed. For example, thieves can identify cryptocurrency users with large holdings and threaten them unless they send them their assets. Popper, *Bitcoin Thieves Threaten Real Violence for Virtual Currencies*, N.Y. Times (Feb. 18, 2018), perma.cc/3KCU-3ELC. And dangerous groups, like Russians who target donations to Ukraine for cyber attacks, for example, can use public cryptocurrency transactions as a basis for retaliation. *See Cybersecurity Advisory: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, CISA (May 9, 2022), perma.cc/C5TN-QL62.[22] Software that solves these problems by preserving user privacy in public transactions should in itself be viewed as valuable and neutral tools.

B. zk Proof Technology Pre-Dated Tornado Cash

The privacy-enhancing aspects of the Tornado Cash protocol are built in part on zk proofs. In the simplest terms, zk proofs enable one party to cryptographically prove to another that they possess knowledge about a piece of information without revealing the actual underlying

[22] In fact, using Tornado Cash and other mixers was relatively common for donations to Ukraine: a notable example is that Vitalik Buterin, the Russian-Canadian co-founder of Ethereum, used Tornado Cash to donate to Ukraine. *See* Vitalik Buterin (@vitalik.eth), X (Aug. 9, 2022, 4:49am), *available at* https://x.com/VitalikButerin/status/1556925602233569280?s=20. In addition, 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. *See* Elliptic, *Crypto in Conflict: How the role of cryptoassets has evolved in the Russia-Ukrainian War*, Elliptic Report 2023, 15, *available at* https://www.elliptic.co/resources/crypto-in-conflict.

information.[23] With respect to the Tornado Cash protocol specifically, zk proofs are the cryptographic mechanism by which a party can withdraw deposited funds from the Tornado Cash protocol without revealing a link between those two actions. In other words, zk proofs are one element of the Tornado Cash protocol that enables users to transact while preserving their individual privacy. However, the Tornado Cash protocol's developers did not invent zk proof technology, which existed for years prior to the creation of Tornado Cash.

People once believed that blockchains preserved a measure of privacy despite their transparent nature because they offer "pseudonymity": a person does not need to reveal information about her offline identity to use a blockchain because users are identified by numerical "addresses."[24] However, it has become increasingly clear that "this level of privacy has proven to be far insufficient in the face of modern clustering and analysis tools," which group together public wallet "addresses" thought to be associated with one particular user and make tracing blockchain transactions much easier.[25] And just as there has been a rise in tools that make tracing blockchain transactions easier, there has been an increase in the development of tools meant to protect individuals' privacy while transacting on-chain.[26] One such advancement was the incorporation of zk proofs into blockchain technology.

There is a world of academic scholarship exploring the general potential of zk proofs dating back to the 1980s.[27] In 1985, the original concept for zk proofs emerged in a

[23] zK proofs are 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; Chainlink, *What is a Zero-Knowledge Proof?* https://chain.link/education/zero-knowledge-proof-zkp.
[24] Vitalik Buterin, Jacob Illum, Matthias Nadler, Fabian Schär, Ameen Soleimani, *Blockchain privacy and regulatory compliance: Towards a practical equilibrium*, Blockchain: Research and Applications, Volume 5, Issue 1, 2024, https://doi.org/10.1016/j.bcra.2023.100176.
[25] *Id.*
[26] *See* Buterin et al. Section 2.1 for a discussion of the evolution of various types of privacy-preserving technology, leading to the creation of zK cryptography.
[27] *See, e.g.,* Shafi Goldwasser et al., *The Knowledge Complexity of Interactive Proof Systems*, SIAM J. Comput. (Apr. 18, 1988),

peer-reviewed academic paper titled, "The Knowledge Complexity of Interactive Proof Systems," marking a breakthrough in cryptography.[28] Early examples of projects implementing zk cryptography to increase privacy on blockchains are Zerocash, first published in May 2014, and the related implementation of similar technology in Zcash, launched in 2016.[29] These projects allow a user to send digital assets without revealing the destination or amount, in a decentralized manner, using zk proof technology. Tens of millions of dollars continue to be traded on the Zcash blockchain every day.[30]

Today, there are numerous projects and software development teams building new tools using zk proofs.[31] 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.[32] zk proofs can enhance the security of a supply chain by validating suppliers' credentials and authenticity of products without disclosing transaction information or proprietary information about a production process.[33]

---

https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf; Aleksander Berentsen et al., *An Introduction to Zero-Knowledge Proofs in Blockchains and Economics*, Fed. Reserve Bank of St. Louis Review, Fourth Quarter 2023; Maksym Petkus, *Why and How zk-SNARK Works*, Cornell Univ. (June 17, 2019), http://arxiv.org/abs/1906.07221.

[28] *See* Shafi Goldwasser et al.

[29] Buterin et al. (citing E. Ben Sasson et al., *Zerocash: decentralized anonymous payments from bitcoin,* Proceedings of the 2014 IEEE Symposium on Security and Privacy, IEEE (2014), https://ieeexplore.ieee.org/document/6956581, and Zcash, https://z.cash (2023)), *see also* Zellic, *Zcash: An Implementation of Zerocash*, https://www.zellic.io/blog/how-does-zcash-work/#zcash-an-implementation-of-zerocash).

[30] *See* Blockworks, https://blockworks.co/price/zec.

[31] The Crypto Times Team, *The New Era of ZK-Proofs: How Cryptographic Technology Moves Ahead*, https://www.cryptotimes.io/2024/05/21/the-new-era-ofzkk-proofs.

[32] For additional examples of zK technology use cases, *see* Aztec Network, *Can blockchains and zero-knowledge help humanity survive? 47 real-world use cases*, https://aztec.network/blog/can-blockchains-and-zero-knowledge-help-humanity-survive-47-real-world-use-cases.

[33] Chainalysis, *Introduction to Zero-Knowledge Proofs*, https://www.chainalysis.com/blog/introduction-to-zero-knowledge-proofs-zkps/#ZKP-applications.

To give a concrete example, JP Morgan Chase has built and tested a computer system, called "Quorum," for privately settling accounts between banks using the very same zero-knowledge proof cryptography as the Tornado Cash protocol. They are also testing a zero-knowledge system that, like the Tornado Cash protocol, runs on the Ethereum network, called "AZTEC."[34] These tools are widely regarded by top researchers in cryptography[35] and finance[36] as state-of-the-art and essential for providing privacy safeguards when using blockchains to transact. To suggest that the Tornado Cash protocol is a mere tool for criminals rather than a series of innovative privacy tools for the world is inaccurate.

It comes to no surprise that a variety of individuals and entities choose to employ cryptography into their software and computer systems. Cryptography has served as the backbone for a safe internet since the 1990s, particularly with the cryptographic protocol Transport Layer Security (TLS). TLS was developed in 1999 to provide end-to-end encryption of data being sent over the internet and allow for secure web browsing, which is used by all major web browsers today.[37] In doing so, web browsers are protecting their users from malicious actors who wish to intercept their data.[38]

---

[34] Allison, Ian, *JP Morgan Is Quietly Testing Cutting-Edge Ethereum Privacy Tech*, Coindesk (Feb. 28, 2019) https://www.coindesk.com/tech/2019/02/28/jp-morgan-is-quietly-testing-cutting-edge-ethereum-privacy-tech.

[35] *See* Miers, et al., *Zerocoin: Anonymous Distributed E-cash from Bitcoin*, Proceedings of IEEE Symposium Security and Privacy, at 397–411 (2013) ("Decentralized currencies should ensure a user's privacy from his peers when conducting legitimate financial transactions. Zerocash [a progenitor of Tornado Cash] provides such privacy protection, by hiding user identities, transaction amounts, and account balances from public view.").

[36] *See, e.g.,* Nadler & Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers*, Fed. Reserve Bank of St. Louis Rev., at 122-136 (2023) ("We conclude that non-custodial crypto asset mixers are an interesting innovation and demonstrate the power of zero knowledge proofs. They provide honest users with the option not to share their transaction history publicly and use public blockchains similarly to other electronic payment systems.").

[37] Internet Society, *TLS Basics*, https://www.internetsociety.org/deploy360/tls/basics/.

[38] Heimdal, *What is Transport Layer Security (TLS)? Strengths and Vulnerabilities Explained*, https://heimdalsecurity.com/blog/what-is-transport-layer-security/#:~:text=TLS%20advantages:,its%20destination%20without%20any%20losses (last visited May 8, 2025).

Importantly, cryptography is not merely a tool for private actors to protect themselves but is largely developed and funded by governments around the world. For example, the United States government has been instrumental in developing cryptographic algorithms like Data Standard Encryption (DES) in 1972[39] and the Advanced Encryption Standard (AES) in 2001 to protect sensitive government data.[40]

Ultimately, employing and advancing cryptography is a normal part of developing software that transmits information over the internet. Criminalizing its use would undermine years of effort by both the public and private sectors to protect sensitive information from malicious actors. Zero-knowledge proofs are only the most recent development of cryptographic security, and given the exposure of public blockchains, it is reasonably deployed in developing blockchain software applications.

III. ANALYSIS RELATED TO TORNADO CASH

A. How Tornado Cash Works

Tornado Cash is a set of smart contracts that can be accessed via off-chain software tools that allow users of Ethereum to protect their privacy when transacting despite the inherent public visibility of transactions on Ethereum's blockchain. It is to Ethereum users what a set of drapes would be to someone with large picture windows in their bedroom. All of the Tornado Cash smart contracts that receive tokens, the "pool" addresses, have been deployed to the Ethereum blockchain such that they are both non-custodial and immutable. Therefore, when a user sends tokens to these addresses, the user and the user alone is in control of their assets; no third-party has any ability to redirect those assets, and no one can alter the smart contract rules that control their movement.

[39]William E. Burr, *Data Encryption Standard*, Nat. Inst. of Standards and Tech. (1972).
[40] Miles E. Smid, *Development of the Advanced Encryption Standard*, 126 J. of Rsch. of the Nat. Inst. of Standards and Tech. (Aug. 16, 2021).

To obtain transactional privacy using the tool, the user first generates on their own device a "note" (which is simply a random number and is not shared with anyone). The note is created using cryptographic functions similar to those used for generating public and private keys, producing a sequence of numbers that is unpredictable and practically impossible to guess. And similar to public and private keys, note generation is done locally on a user's device.

Using either a UI or CLI, the user generates a "commitment," which is the first of two critical elements for interacting with the Tornado Cash protocol. The commitment represents the user's deposited funds, which allows the protocol's verifier smart contract to verify the deposit's existence and ownership upon withdrawal. After it is generated, the user can broadcast their commitment along with their deposit to the Ethereum blockchain. Just like any other transaction, the transaction details – e.g., sender address, recipient (*i.e.*, Tornado Cash smart contract) address, transaction value, and gas fees – are visible to the validator for the purpose of validating the transaction.

Once the transaction is included in a block and validated, the commitment within the transaction is communicated to the Tornado Cash smart contract. Upon receiving the commitment, the smart contract records the commitment where it serves as a marker or placeholder for the deposited funds within the protocol's logic. Meanwhile, the deposited funds are added to an anonymity pool corresponding to the deposit amount. Tornado Cash protocol organizes deposits based on their amount (denomination) – e.g., there could be different pools for 0.1 ETH, 1 ETH, or 10 ETH. This approach ensures that all deposits within a pool are of the same value, making individual transactions indistinguishable within the pool.

While the commitment is the first of two elements critical to using the Tornado Cash protocol, the second is known as a nullifier. A nullifier is also a unique identifier generated from

a user's note but plays a distinct role apart from the commitment. Commitments are related to the deposit process, creating a record that allows for future withdrawal without directly linking back to the depositor; whereas, nullifiers are related to the withdrawal process, ensuring that each deposit can only be withdrawn once. When a user decides to withdraw their deposit, the nullifier is generated locally on their device. Once the nullifier is generated, it is incorporated into the privacy-enhancing technology known as a zero-knowledge succinct non-interactive arguments of knowledge ("zk-SNARK").

A zk-SNARK is a form of zk proof technology that allows one party (the prover) to prove to another party (the verifier) that a statement is true without revealing any information beyond the validity of the statement itself. The Tornado Cash protocol leverages zk-SNARKs to prove ownership of a deposit represented by a commitment, without revealing which specific deposit is being withdrawn. When a user decides to withdraw their deposit, they generate a zk-SNARK proof that mathematically demonstrates that a user knows a deposit's note and the corresponding nullifier without revealing those values. Specifically, the user proves they know a note that matches one of the commitments stored in the Tornado Cash smart contract. Additionally, they prove knowledge of the nullifier associated with that note and ensure the nullifier hasn't been used before to prevent double-spending.

Much like generating a commitment and a nullifier, the user uses cryptographic libraries through a UI or CLI to construct the zk-SNARK proof that the Tornado Cash verifier smart contract can verify but not reverse-engineer. Once the proof is ready, the user uses a UI or CLI to present a summary of the withdrawal transaction for the user's review and confirmation. Upon confirmation, the user submits the transaction – including the zk-SNARK proof and nullifier as function arguments – to the Ethereum blockchain for verification.

To enhance privacy in the withdrawal process, a user can *choose* to use a relayer – which is a third party software application that communicates the user's withdrawal message on behalf of a user without taking custody of the user's funds. Instead of submitting the withdrawal transaction directly from their wallet, the user provides the transaction details, including the zk-SNARK and a newly generated destination address, to the relayer. The relayer then communicates this transaction's information to the Ethereum network. The relayer pays the transaction's gas fee and the user compensates the relayer with a small portion of the withdrawal amount. Once the transaction is validated and included on the Ethereum blockchain, the funds are transferred to the specific withdrawal address, and the relayer's service fee is received through the previously agreed upon arrangement.

It is helpful to think of the Tornado Cash protocol as an extension of the Ethereum protocol: Ethereum allows users to send tokens from address to address, and Tornado Cash allows users to do that with enhanced privacy if and only if the user wields these tools in a specific way. Neither Ethereum nor Tornado Cash requires users to put their trust in anyone while transacting, and neither allows any third party to control the user's tokens while transacting. It is not a service that is being provided, it is a piece of technology which users can decide to use when transacting on the Ethereum blockchain. This is exactly what separates disintermediated finance from the traditional financial sector in which intermediaries such as banks provide a service to facilitate transactions. In this peer-to-peer network, users transact directly without third party involvement.

B. <u>What does a person need to use Tornado Cash smart contracts?</u>

Users can interact with Tornado Cash smart contracts with nothing but an internet-connected computer. Users need nothing else to write and broadcast a transaction

message that obeys the syntactic rules of the Ethereum protocol and the Tornado Cash smart contracts. This means that Tornado Cash users can have the benefit of transactional privacy while using *only* the immutable and non-custodial smart contracts on Ethereum and no other third-party software, websites, or infrastructure. This was explained in the preceding section as the CLI used locally on a user's computer.

Alternatively, users can write and broadcast these transaction messages by using Tornado Cash UI software, which is what you might think of when asked to picture the Tornado Cash "website," or any other user interface. Importantly, because the Tornado Cash protocol is deployed on the Ethereum blockchain, anyone can also build and operate their own UI for others to write and broadcast their own transactions,[41] and some already have.[42]

In all cases, the user is the only person who can initiate the transaction by signing the message with cryptographic keys they have stored on their computer. The UI is, in this sense, rather like an early version of TurboTax, which is a program in the US that helps you file your taxes. It will help you fill out your tax forms by prompting you with non-technical questions, but you are ultimately responsible for printing out the results, filing your return, and paying your taxes yourself.

As previously discussed, users also have the option of paying a third party relayer. This relayer is, however, merely relaying already formed and user-signed transaction messages to the Ethereum network and paying the associated Ethereum transaction fees. In other words, the user provides the relayer with all the information they need to communicate between the Tornado

[41] This is generally true of publicly available protocols. For example, email protocols are structurally similar to DeFi protocols in the sense that they define open, permissionless standards that anyone can build a UI to communicate with. For email, popular UIs include Gmail and Microsoft Outlook. In both cases, the UI merely translates human-readable input to machine-readable data, and communicates it to the protocol.

[42] For example, https://1.tornadowithdraw.eth.limo is a UI that is not affiliated with the original Tornado Cash developers.

Cash protocol and the Ethereum blockchain (including the new blockchain address the user generates). The relayer is not tasked with creating or generating any of this information, the user is. The relayer is just an independent third party that communicates information between networks, nothing more.

It is the user rather than the relayer or any other third party choosing to create privacy through their actions and choices. To continue the tax preparation metaphor, the relayer is like a private courier service the taxpayer hires to deliver their tax documents to the Belastingdienst. At no point can a relayer alter the signature of the transaction, control the underlying funds, or otherwise manipulate the transaction that was initiated by the user. If a relayer fails to relay the message, the user can always broadcast the transaction message themselves or find an alternative relayer.

Furthermore, the Tornado Cash protocol includes a relayer registry smart contract. In order for a relayer to be listed in the registry, they must stake – *i.e.*, place collateral in the form of TORN tokens – to signal their commitment to providing a reliable service. Registered relayers are then algorithmically ranked based on the amount they've staked and the fees they charge. Users can refer to the registry to find the most reliable or cost-effective relayers. However, relayers are not required to register in order to operate – the registry simply serves as a resource for users to select a relayer and has full autonomy to choose a relayer that is not registered.

C. The Immutability and Security of the Tornado Cash Protocol

As discussed, no one can rewrite the Tornado Cash core smart contracts in order to change how they work or gain control over user funds stored therein. These core smart contracts include each of the anonymity pools for deposits and the verifier smart contract that is tasked with verifying the validity of zk proofs.

The pool smart contracts were made non-upgradable upon deployment to the Ethereum blockchain. In May 2020, the verifier contract's operator address was reassigned to the zero address, making it so the smart contract could not be upgraded[43] – as explained above. This means that no one – including the Tornado Cash developers – has had any ability to modify the pool smart contracts since deployment, nor the verifier smart contract, since May 2020. This is an important way of maintaining the integrity and security of a decentralized software protocol, and is both an ethos and industry standard for DeFi developers.

Furthermore, the protocol's cryptographic security was decentralized and protected under a process known as a *trusted setup*, which is required for the security of zk-SNARKs. The trusted setup generates cryptographic data that allows a zk-SNARK to create valid zk proofs.[44] This cryptographic data consists of proving and verification keys[45] that are generated from random numbers – known as *secrets* – that serve as hidden inputs in a software function to generate the keys. These secrets must be destroyed after the setup; if retained, they could be exploited by a malicious actor to generate fake proofs and compromise the protocol.[46]

To mitigate this risk, protocols undergo a *trusted setup ceremony*, which consists of multiple participants generating the required data with their secrets.[47] As long as *one* participant acts honestly by destroying their secret after generating the required data, the zk proof system remains secure from malicious actors, because generating fake proofs would require *all* the secrets used, not just one.[48]

---

[43] Medium: Tornado Cash, *Tornado.cash Trusted Setup Ceremony*, https://tornado-cash.medium.com/tornado-cash-trusted-setup-ceremony-b846e1e00be1 (last visited Apr. 3, 2025).
[44] Vitalik Buterin, *How do trusted setups work?*, Vitalik Buterin's Website (Mar. 22, 2022), https://vitalik.eth.limo/general/2022/03/14/trustedsetup.html
[45] In cryptography, a key is a piece of information used to encrypt and decrypt data.
[46] Panther Protocol Blog, *Understanding Trusted Setups: A Guide*, https://blog.pantherprotocol.io/a-guide-to-understanding-trusted-setups/ (last visited Apr. 3, 2025).
[47] *Id.*
[48] *Id.*

In zk-SNARK implementations, the trusted setup process is a cryptographic requirement, and the multi-party ceremony is an industry standard. The purpose of a ceremony is to make a protocol truly trustless in the sense that users do not need to depend on the good will of any one person for the security of the protocol, thereby contributing to its decentralization. Hence, the Tornado Cash protocol completed its trusted setup ceremony in 2020, with a record 1,114 contributions.[49]

D. Upgradability and Decentralized Governance in Tornado Cash

As explained above, auxiliary smart contracts can be designed to be upgradable within a protocol, given that they are not fundamental to the core operations, and therefore, not a security risk. For these smart contracts to be upgradable, protocols are often designed with what is known as a *proxy pattern*. In a proxy pattern, two smart contracts work together to perform the functions of one smart contract: the proxy contract and the implementation contract. One way to understand the two contracts' relationship is to imagine the proxy contract as a universal remote and the implementation contract as a TV – the remote adds a layer of convenience and functionality to controlling what the TV does, but does not need to be changed when the TV's system is upgraded.

In more practical terms, the proxy contract serves as the front-facing smart contract for users and other smart contracts, and maintains the smart contract's state (data) while delegating execution to the implementation contract. The implementation contract holds the business logic and can be replaced upon a protocol upgrade. The proxy pattern allows for smart contract upgrades without changing the front-facing smart contract (and address), preserving the smart contract's state (data) and ensuring continuity for users.

[49] Medium: Tornado Cash, *Tornado.cash Trusted Setup Ceremony*, https://tornado-cash.medium.com/tornado-cash-trusted-setup-ceremony-b846e1e00be1 (last visited Apr. 3, 2025).

The Tornado Cash protocol was designed with the proxy pattern to *only* upgrade auxiliary smart contracts, and the authority to prompt such upgrades was designated to a decentralized governance mechanism consisting of independent, unaffiliated token holders who voluntarily participate in the maintenance of the protocol. The governance smart contract then sets the rules for proposals and voting such that the protocol governance was decentralized, and does not allow an administrator to force proposals or override the voting process. The governance smart contract also makes it so its governance parameters cannot be changed by an administrator.

Importantly, changes to the protocol could not result in users losing access to tokens; nor could changing these smart contracts deny any potential users future access to the immutable pool contracts and the primary benefits of the privacy protocol generally. Nor would rewriting the off-chain UI software prevent misuse of the privacy tool by criminals. Releasing new versions of the UI would not automatically replace previously released or downloaded versions of the software that may be retained by users or obtained from other third-party websites. Additionally, users could always use older versions of the interface or use the immutable pool contracts directly through a CLI. For this reason Tornado Cash protocol continues to be used to this day.[50]

[50] There was—and is—nothing anyone can do to stop someone from using the smart contracts. There have been numerous reports of people still using the protocol and in fact, usage is on the rise. *See* Brady Dale, *Sanctions have slowed Tornado Cash, but usage is rising*, Axios (Aug. 8, 2024), https://www.axios.com/2024/08/08/sanctions-tornado-cash-crypto-privacy-application; Anders Brownworth, Jon Durfee, Michael Junho Lee, and Antoine Martin. 2024. *Regulating Decentralized Systems: Evidence from Sanctions on Tornado Cash*, Federal Reserve Bank of New York Staff Reports, no. 1112, August. https://doi.org/10.59576/sr.1112 ("Despite gross drops in flows to and from Tornado Cash addresses, we find an increase in the total value deposited in Tornado Cash addresses, relative to presanction levels, for all but the largest denominated pool. Recovery from drops at announcement, and secular increases in net flows into Tornado Cash contracts suggest that Tornado Cash remains viable as a privacy tool, particularly in the view of users."). For example, last March, someone used the protocol to send funds to a wallet associated with Blackrock. See Young, *Wallet Associated With BlackRock's Tokenized Fund Spammed With Unsolicited ETH From Tornado Cash*, Unchained (Mar. 21, 2024), https://tinyurl.com/2jxz52au.

This is not a feature unique to Tornado Cash; essentially all blockchain technologies – by virtue of being decentralized and open-source – "escape" the control of the person or company who first develops and publishes them. The pseudonymous inventor of Bitcoin, Satoshi Nakamoto, disappeared in 2010 yet the protocol continued to function unbothered. This is not even a cryptocurrency-specific phenomenon; it's the nature of all open-source software development. Even if everyone outside of Iran agreed that the developers of the Linux operating system should publish a new version of Linux that prevents Iranian scientists from using Linux to run machines that enrich uranium, and even if those developers agreed and did publish that new version of Linux, it would not, somehow magically, prevent the existing unrestricted software already used by Iran from continuing to operate.

Accordingly, dating back to May 2020, the developers (1) have no control over the Tornado Cash core smart contracts on the Ethereum blockchain; (2) have no control over users' choice of any supporting software: anyone could publish a new version of the UI, but users would be free to use previous versions of the Tornado Cash protocol with previous functionality if they so desire; and (3) do not have the means to implement protocol-level checks on the cryptocurrency going into the pools.

E. How does the Tornado Cash tool enhance privacy?

The ability to transact privately using Tornado Cash is created by the users themselves in the process of their transactions. The Tornado Cash developers created software that allowed any third party to use it to transact peer-to-peer with varying levels of privacy, dependent on multiple user-controlled factors, such as those described below.

- Unified denominations: every TC pool has its own denomination (e.g. 0,1, 1, 10, 100 ETH) in order to simplify the user experience. If the denominations were not

uniform, the user's particular amount deposited and withdrawn could help third party observers to connect a deposit with a withdrawal. Because the denominations are automatically standardized, transaction amounts are indistinguishable from one another.

- Third party withdrawals (*i.e.*, a relayer): All transactions on Ethereum require fee payments to the validators who maintain that network and incorporate transactions into the Ethereum blockchain. A Tornado Cash withdrawal transaction, like any other Ethereum transaction, also requires payment of this network fee. These fees are thus not paid to the original Tornado Cash developers.[51] If users input the same address to both deposit into a Tornado Cash fee and pay the network fee on withdrawal, a third party could observe the fact that a certain deposit address paid the fee for a certain withdrawal address and assume that these addresses are controlled by the same user, thereby undoing transaction privacy. For this reason, the Tornado Cash smart contracts are designed so that any Ethereum address can pay the withdrawal fee to the Ethereum network. That fee-paying address can be a relayer, another Tornado Cash user, an address of the user, or any other address.
- Zero-knowledge cryptography: Tornado Cash smart contracts use zk cryptography to allow users to mathematically authorize a withdrawal without revealing any information that can be used to link the withdrawal to the corresponding deposit. However, even zk cryptography does not provide privacy on its own and is just one element of engaging with Tornado Cash smart contracts.

[51] Specifically, users always pay transaction fees to the Ethereum network, which go to its validators. If a user chooses to withdraw using a relayer, a portion of the withdrawal is paid to the relayer. None of these fees are designed to go back to the Tornado Cash developers.

- Anonymity set: The anonymity set is a number of deposits that a particular withdrawal might originate from. The more deposits, the more data needs to be analyzed before a withdrawal can be linked to a particular deposit. For example, if a Tornado Cash Pool does not have any deposits, the anonymity set would be 0. This means if only one person makes a deposit into that pool, that person will invariably and necessarily be the same person who withdraws; thus no privacy is achieved no matter what kind of brilliant technology is used. However, even a high anonymity set provides limited privacy on its own because the blockchain is transparent and each transaction into and out of a smart contract is easily traced.

The above capabilities are available to all users of Tornado Cash smart contracts. It is not the case that one technological element of the tool creates privacy on its own, but it is instead the synergy of the technological elements and the user's choices that create privacy. It is up to the user to choose which wallet addresses to use to interact with the smart contracts; if the user chooses unaffiliated wallet addresses or a relayer in order to withdraw, they will maintain privacy; but if the user chooses previously affiliated wallet addresses, they will compromise their privacy. In other words, the user can leverage the above tools to create privacy by using Tornado Cash, or choose not to leverage them and no privacy will be created.

F. Why Privacy Is A Good Thing: Law-Abiding People Want to Retain Privacy

Regular people used and continue to use the Tornado Cash protocol to protect their privacy when using cryptocurrency. People value the Tornado Cash protocol because it solves an important problem: because Ethereum transactions are posted on a public ledger that anyone in the world can view, if someone can link a person's real-world identity to an Ethereum address, it becomes possible to trace that user's complete transactional history.

For example, if Bob's employer makes a payment to Bob, the employer will know which address belongs to Bob and can then go review the public ledger to see all the other transactions he has made from the same address. The employer can therefore see that Bob's a millionaire, that Bob donates to a certain religious denomination, or that Bob is seeing a mental health counselor. For obvious reasons, people don't like having all their transactions easily traceable on the public ledger.

The Tornado Cash protocol solves that problem. It allows users to make it more difficult for third-party observers to connect past and future transactions, so others cannot survey them all with ease. While transactions are still happening on-chain and are still publicly recorded and visible, depending on how the user interacts with the protocol, there does not have to be an obvious public link between a specific deposit and a specific withdrawal.

People use the protocol, in transactions like Bob's above, for many reasons. For one, it protects them from violence and affords them personal privacy in everyday transactions. Coin Center has used Tornado Cash to privately accept donations that support our non-profit mission. Coin Center has brought a lawsuit in United States federal court to have OFAC remove the Tornado Cash pool addresses from the sanctions list so that we can continue to use them for that purpose and so that other Americans can use them for any legitimate privacy purposes.[52] As a US-based non-profit, Coin Center has a right to deny the government access to a comprehensive list of our donors; that is our First Amendment right of association. Cryptocurrency donations, by virtue of traveling over a transparent blockchain, would reveal that comprehensive list to the government and others; therefore, until the sanctions Coin Center was willing to accept donations via the Tornado Cash protocol and even encouraged large donors to use the privacy

[52] *See Coin Center v. Yellen*, 2023 WL 7121095 (N.D. Fla. Oct. 30). The lawsuit is currently on pause following the delisting of sanctions on Tornado Cash smart contracts and the website.

tool. Coin Center has co-plaintiffs in that lawsuit who wish to use the Tornado Cash protocol to be privately paid their salary and who have used it to privately make donations to the war effort in Ukraine without becoming targets of Russian cyber attacks.[53] Until OFAC imposed sanctions in August 2022, the Tornado Cash protocol was the most popular privacy-protecting tool on Ethereum.[54] According to Chainalysis, the Tornado Cash protocol was and is used primarily for legitimate and socially valuable reasons.[55] Even after Tornado Cash smart contracts were sanctioned, usage continued and even surpassed pre-sanction levels.[56]

G. Tornado Cash Is Not A "Service" or Properly Classified as a Compliance-Obligated Entity

It is improper to group distinct software components that run autonomously to package them as an interoperable "service." As previously explained, the Tornado Cash network consists of separate technical components – the various smart contracts, governance mechanism, UIs, underlying blockchain network, users, relayers, etc. – in which the developers have little-to-no touchpoints at all. Developing the software for one component – *e.g.,* the UI – does not equate to controlling the underlying protocol.[57] Therefore, to consider the developers liable for each separate technical component is to mistakenly assume that the entire network is one operating "service" or "entity" when it is not. For this reason as well as the reasons laid out below, Tornado Cash is not properly classified as any kind of compliance-obligated entity.

---

[53] *Id.*; *see also supra* note 19.
[54] *See* Kaloudis & Oosterbaan, *How Popular Are Crypto Mixers? Here's What the Data Tells Us*, Coin Desk (Nov. 7, 2022), https://bit.ly/3Xb0iok; Coin Market Cap, *Today's Cryptocurrency Prices by Market Cap*,(last visited May 8, 2025), https://bit.ly/3IFcoSs.
[55] Chainalysis, *OFAC Sanctions Popular Ethereum Mixer Tornado Cash for Laundering Crypto Stolen by North Korea's Lazarus Group*,(Aug. 8, 2022), https://bit.ly/3EqpUHd.
[56] Anders Brownworth, Jon Durfee, Michael Junho Lee & Antoine Martin, *Regulating Decentralized Systems: Evidence from Sanctions on Tornado Cash*, Federal Reserve Bank of New York Staff Report No. 1112, at 3 (August, 2024).
[57] *See* Brief Of The Defi Education Fund As Amicus Curiae In Support Of Defendant Roman Storm's Motion To Dismiss The Indictment, No 1:23-cr-00430-KPF (S.D.N.Y. April 5, 2024), at 8-9, 23-24 *available at* https://www.defieducationfund.org/_files/ugd/84ba66_063f9d1fd563466cadfa3f5434f918e9.pdf.

In the context of financial services, the plain meaning of compliance is "conformity in fulfilling official requirements."[58] Compliance is not something one does for strictly personal, moral, or ethical reasons; it is something mandated by law. While everyone should take care to avoid transacting with criminals, only regulated financial institutions have affirmative anti-money-laundering due diligence and know your customer obligations (hereinafter "AML/KYC" obligations). The Tornado Cash developers, however, were not engaged in any activities that were or are currently regulated as financial services under the law. No jurisdiction has yet classified the activities Tornado Cash as operating a financial institution – not the government of the Netherlands, the Anti-Money Laundering Directives of the European Union, the Financial Action Task Force in any of its recommendations on digital assets, nor the United States financial crimes regulator, the Financial Crime Enforcement Network (FinCEN). Obligated businesses must comply with their AML/KYC obligations; the developers of the Tornado Cash protocol, however, were not and have never been an obligated business under the law.

The data availability objectives of the EU-US agreement, the Terrorist Finance Tracking Program (TFTP), and similar financial crime regulations are likely already satisfied by the inherently transparent nature of open blockchain networks paired with the compliance tool that was made available by the Tornado Cash developers. Transactions emerging from Tornado Cash's pool contracts are inherently detectable by the recipient and by third parties such as banks, financial intelligence units, or, indeed, the public at large. Because of the privacy technology built into the Tornado Cash pools anyone can, assuredly, know that they are coming from the Tornado Cash protocol. These transactions can therefore be easily screened and flagged

[58] *Compliance*, Merriam-Webster.com Dictionary, https://www.merriam-webster.com/dictionary/compliance (last visited Sept. 30, 2024).

by any and all regulated parties just as any large and undocumented physical cash transaction can and should raise the alarm at a regulated bank. Just as in traditional finance, one can rely on the obligated entities, the banks, brokers, and on-ramps and off-ramps[59] from cryptocurrency networks to do their part in scrutinizing these messages.

Moreover, the developers of the Tornado Cash protocol have never had control over the funds users deposit into the immutable pool contracts, *i.e.,* the Tornado Cash protocol has always been quintessentially non-custodial, and therefore, should not be regulated as if it were custodial. It was not until the Fifth Anti-Money Laundering Directive in 2020 that the EU classified *custodial* wallet providers as obligated entities for purposes of AML/KYC regulation.[60] The most recent Sixth Anti-Money Laundering Directive did not alter the scope of obligated entities any further and certainly did not create new compliance obligations for developers of non-custodial tools and protocols such as the Tornado Cash protocol or people running a UI to interact with these smart contracts.[61] Nor do the recommendations of the Financial Action Task Force[62] or the

[59] On- and off-ramps refer to centralized exchanges that operate as financial institutions and hold public and private keys on behalf of their customers. These are known as on- and off-ramps because they allow customers to exchange fiat for cryptocurrency.

[60] *Directive 2018/843 of the European Parliament and of the Council, amending Directive (EU) 2015/849, art. 1(1)(h), 2018 O.J. (L 156) 43 (EU)* (adding "custodian wallet providers" to the list of obligated entities).

[61] *Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, 2018 O.J. (L 284) 22 (EU).*

[62] FATF defines the category of obligated entities as "Virtual asset service provider[s]" and characterizes that term as "any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

> i. Exchange between virtual assets and fiat currencies;
> ii. Exchange between one or more forms of virtual assets;
> iii. Transfer of virtual assets; and iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;
> v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

FATF (2019), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, Paris, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html. Footnote 4 further clarifies that the term "transfer" is intended to extend only to those who "conduct" the transaction on behalf of another rather than someone who merely relays a signed transaction message: "In this context of virtual assets, transfer means to *conduct a transaction on behalf*

Bank Secrecy Act regulations of the U.S. government[63] call for any particular compliance obligations from persons engaged in non-custodial activities.

Recently, even the U.S. has removed the sanctions designations on Tornado Cash smart contracts and the website, recognizing that smart contracts are not "property" capable of being owned by a developer or anyone else. In March 2025, the Treasury Department's Office of Foreign Assets Control (OFAC) delisted the Tornado Cash smart contracts from its Specially Designated Nationals (SDN) list.[64] This came after the Fifth Circuit Court of Appeals ruling in *Van Loon v. Department of the Treasury* that Tornado Cash smart contracts are not property or interests in property under the IEEPA and that OFAC had overstepped its regulatory authority in issuing the sanctions in the first place.[65]

It is also worth noting that even though Tornado Cash is not a compliance-obligated entity, traditional financial institutions and other compliance-obligated entities can still meet their requirements when dealing with customers' digital assets that may have come through Tornado Cash. It would be perfectly reasonable for banks and other financial institutions to freeze any and

---

of another natural or legal person that moves a virtual asset from one virtual asset address or account to another." *Id.* at 14, n. 4 (emphases added). As discussed above, Pertsev and the other developers of Tornado Cash have no ability to conduct transactions on behalf of the users of Tornado Cash. Their software and server infrastructure is utilized simply to communicate transaction messages after they have been signed by users. Accordingly, Pertsev is clearly not a VASP under the FATF recommendations.

[63] FinCEN, the relevant division of the US Treasury, has offered extensive guidance on the question of whether a software developer or other non-custodial entity is obligated under the Bank Secrecy Act to do AML/KYC. It has said that software developers are not money transmitters: "The production and distribution of software, in and of itself, does not constitute acceptance and transmission of value, *even if the purpose of the software is to facilitate the sale of virtual currency.*" *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001, FinCEN (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf. FinCEN also clearly articulated that partial control over virtual currency was insufficient to classify wallet developers as money transmitters because: "the person participating in the transaction to provide additional validation at the request of the owner does not have *total independent control over the value*." *Id.*

[64] *See* U.S. Dep't of Treasury, *Tornado Cash Delisting*, (March 21, 2025), *available at* https://home.treasury.gov/news/press-releases/sb0057

[65] *See Van Loon v. Department of the Treasury*, No. 23-50669, Doc No. 123-1 (5th Cir. Nov. 26, 2024), *available at* https://www.ca5.uscourts.gov/opinions/pub/23/23-50669-CV0.pdf.

all incoming funds from the Tornado Cash pool addresses on Ethereum, pending further evidence that such funds are unrelated to crime, terrorism, or sanctions evasion. Transactions may be traced as funds are deposited into and withdrawn from the Tornado Cash protocol publicly on the blockchain.[66] There are a number of blockchain forensic analytics tools already widely used by law enforcement, such as those offered by Elliptic, Chainalysis, TRM, and Merckle.[67] This is, no doubt, already de rigueur in traditional finance with respect to unusual and suspicious activity or under-documented incoming physical cash deposits.

IV. CONCLUSION

Neither Ethereum nor Tornado Cash requires users to put their trust in anyone while transacting, and neither allows any third party to control the user's tokens while transacting. This lack of intermediaries and gatekeepers is exactly what separates decentralized, disintermediated finance from the traditional financial sector. In peer-to-peer networks, users transact directly without third party involvement, ensuring free and open access to financial services.

The design and operational principles of Tornado Cash, and the underlying Ethereum network, classify the protocol as neutral technology. Ethereum's decentralized nature ensures that users can execute peer-to-peer transactions without the involvement of an intermediary. Tornado Cash, built on Ethereum, merely provides the privacy layer, serving as a tool for users to

---

[66] *See* Bitquery, *How to Use Bitquery to Follow the Money in Tornado Cash*, (April 18, 2024), *available at* https://bitquery.io/blog/track-money-tornado-cash-bitquery. Additionally, the Tornado Cash UI did offer a compliance tool for users to be able to show a compliance-obligated entity (*i.e.*, a centralized exchange) the origin of their assets with a cryptographically verified proof of transactional history. Medium: Tornado Cash, Tornado.cash Compliance (June 3, 2020), https://tornado-cash.medium.com/tornado-cash-compliance-9abbf254a370.

[67] *See,* Elliptic, *Blockchain Intelligence for Law Enforcement*, https://www.elliptic.co/industries/law-enforcement; Chainalysis, *Law Enforcement Crypto Solutions*, https://www.chainalysis.com/law-enforcement; TRM, *TRM Forensics*, https://www.trmlabs.com/blockchain-intelligence-platform/forensics; Merkel Science, *What is Blockchain Forensics? An In-Depth Guide*, (Dec. 17, 2024) https://www.merklescience.com/blog/what-is-blockchain-forensics-an-in-depth-guide#:~:text=Blockchain%20forensics%20is%20used%20by,in%20a%20court%20of%20law.

conduct private transactions. This is particularly valuable in a global environment where financial transparency can lead to exploitation and retaliation for a person's beliefs and associations.

The societal and individual benefits of decentralized software protocols are substantial. These tools offer users control over their assets, expand global access to financial services, and reduce the risks associated with traditional intermediated financial systems. Privacy protocols like Tornado Cash are integral to this ecosystem, as they protect users' dignity and well-being without providing anyone with unilateral authority over their transactions. Imposing existing financial regulatory regimes upon the developers of this decentralized software inhibits its development, and subsequently, its use by lawful citizens who simply wish to protect themselves and their finances from malicious actors who exploit the vulnerabilities of centralization and transparency. While obligated businesses must comply with their AML/KYC obligations, the developers of the Tornado Cash protocol were not and have never been an obligated business under the law. Tornado Cash is not a "service" but is instead a network of technologies that allows users to transact privately on the Ethereum blockchain.

We hope this report has effectively conveyed this truth: that software developers should not be held criminally liable for the actions of third parties who use their software to commit crimes.