CAUGHT IN A STORM: THE MISAPPLICATION OF EXECUTIVE ORDER 13694 AND THE DEPARTMENT OF TREASURY’S RECENT SANCTIONS ON TORNADO CASH.

Catherine E. Nicholson*

I. Introduction

The increase in popularity of cryptocurrency created a wave within the financial technology ("Fintech") community and currently presents a challenge to our legislative bodies.⁴ Although

* J.D. Candidate, Suffolk University Law School, 2024, Gratitude is expressed to Professor Joseph Glannon and Bradley Bostwick for their editorial and research assistance.

⁴ See What Is the Economic Impact of Cryptocurrency?, PELICION (Oct. 18, 2022), archived at https://perma.cc/UQT3-ZHPC (commenting on the economic impact on job markets). “The rise of cryptocurrency has brought with it an entire industry that is dedicated to supervising cryptocurrency exchanges that take place throughout the world.” Id. See also Sofija Vidjikant, Bitcoin Regulation: What is Happening and What to Expect?, SOFTJOURN (May 13, 2022), archived at https://perma.cc/H3SR-MSRW (proposing that the government can impact the price of a cryptocurrency by either regulating digital assets via buying and selling actions through global marketplaces or imposing strict regulations that could increase the cost). Although there is a potential to make an impact, this would not impact cryptocurrency on a larger scale in that the digital asset is traded internationally, and regulation in this area would require consensus from a number of countries. Id. See also Andrew Singer, Congress may be ‘ungovernable,’ but US could see crypto legislation in 2023, Cointelegraph (Jan. 12, 2023), archived at https://perma.cc/K7LN-F8YY (explaining the difficulty Congress has had thus far in regulating cryptocurrency and
cryptocurrency is a desirable alternative to other online payment methods, there are also concerns such as fraud, massive heists, and money laundering.\textsuperscript{2} Currency Mixers have been increasingly associated with these types of crimes.\textsuperscript{3} This software, which was originally designed to enhance user anonymity, has since transformed into a tool used by criminals to facilitate and perpetuate these crimes.\textsuperscript{4} Legislators and law enforcement now target these Currency Mixers as a way to solve these financial crimes; however, this seems to be placing the blame in an inappropriate place.\textsuperscript{5}

\textsuperscript{2} See Nathan Reiff, \textit{How to Pay with Cryptocurrency}, INVESTOPEDIA (Sept. 6, 2022), \textit{archived at} https://perma.cc/DP9T-TUFN (listing the conveniences of transacting with cryptocurrency such as increased anonymity, peer-to-peer transactions, reduced fees, ability to pay from any location – domestic or international, and that cryptocurrency is available to everyone). \textit{See also} Emma Fletcher, \textit{Reports show scammers cashing in on crypto craze}, FED. TRADE COMM'N (June 3, 2022), \textit{archived at} https://perma.cc/WX9X-9ZV4 (reporting that between 2018 and 2019, almost four out of every ten dollars reported lost were stolen as a result of fraud stemming from social media that was lost in cryptocurrency, which was far more than any other form of payment).


This Note argues that policymakers and law enforcement should focus their attention on the malicious actors rather than the technology that allowed their crimes to come to fruition. In order to properly regulate the cyber-crimes perpetuated by these malicious actors, targeted penalties must apply to the criminals, not the technology used in the commission of their crimes. Misinterpreting or stretching already-existing legislation to justify regulation upon software is a misapplication of the law and undermines the legislative

“Virtual currency mixers that assist illicit transactions pose a threat to U.S. national security interests. We are taking action against illicit financial activity by the DPRK and will not allow state-sponsored thievery and its money-laundering enablers to go unanswered.” Id.

6 See Paul Grewal, Sanctions Should Target Bad Actors. Not Technology., THE COINBASE BLOG (Sept. 8, 2022), archived at https://perma.cc/9BWR-C2B3 (arguing that the Department of Treasury should address its sanctions toward the criminals who used this technology for illicit purposes, not the technology itself). See also Jerry Brito & Peter Van Valkenburgh, U.S. Treasury sanction of privacy tools places sweeping restrictions on all Americans, COIN CENTER (Aug. 8, 2022), archived at https://perma.cc/ZLA6-QTHF (arguing that there is a potential violation of due process and describing the flaws in the logic of sanctioning a piece of technology that could be used for illicit or licit means.)

It appears, instead, to be the sanctioning of a tool that is neutral in character and that can be put to good or bad uses like any other technology. It is not any specific bad actor who is being sanctioned, but instead it is all Americans who may wish to use this automated tool in order to protect their own privacy while transacting online who are having their liberty curtailed without the benefit of any due process.

Id.

7 See Brian Armstrong, Defending Privacy in Crypto, THE COINBASE BLOG (Sept. 8, 2022), archived at https://perma.cc/TZ4E-9A6P (criticizing the Treasury Department for overreaching and sanctioning an entire piece of technology as opposed to the specific criminals).
and regulatory process. Continuing to impose penalties upon inanimate pieces of technology creates a worrying precedent for future legislators, innovators, and software developers.

II. History

A. An Overview of the Blockchain and its Emergence in Cryptocurrency

On October 31, 2008, an anonymous author under the pseudonym of Satoshi Nakamoto published the Bitcoin White Paper, which described a new application of a technology called a blockchain, creating a decentralized peer-to-peer network that would eliminate the necessity of a financial institution to send and receive payments.

---

8 See 23 Tenn. Juris. § 36 (2022) (codifying the Rule of Lenity). “A statute should be construed as a whole giving effect to each word. In construing a statute, the intention of the General Assembly is to be gathered from words it has used and not from words it has chosen not to include.” Id. See also Ryan Haar, U.S. Officials Send Mixed Messages on Crypto Regulation. Here’s What It All Means for Investors, TIME (Apr. 18, 2022), archived at https://perma.cc/5F5D-8G4V (echoing the concern of cryptocurrency investors that legislation that is applied to digital assets should be new and created with the intention of digital assets being regulated, not other securities or other assets).

9 See What Happened to Tornado Cash?, I DENTITY REV. (Aug. 9, 2022), archived at https://perma.cc/B86K-XT7B (echoing the concern that if we create a precedent that it is okay to sanction an entire piece of technology rather than the individual bad actors that used the technology for harm, that it could stifle innovation and hold inventors liable for harms that they did not cause).

10 See SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 1 (2008) (describing the rise of internet commerce, and rather than relying on financial institutions to process electronic payments, what is needed is an electronic payment system allowing for two users to transact directly with each other). Before describing the functionalities and technicalities of the blockchain technology, Nakamoto’s vision was simple: a cryptographically secured peer-to-peer system that
Blockchain, invented in 1991, was originally created to timestamp documents so that it was infeasible for a user to back-date or forward-date his document.\footnote{See Chris Gaetano, Inventors of Blockchain Explain Project’s Humble Beginnings, Sound Warnings About Its Future, THE TRUSTED PRO. (Oct. 29, 2019), archived at https://perma.cc/79LD-VCQJ (indicating that the two inventors of the blockchain were Stuart Habert and W. Scott Stornetta). Although the original purpose of the blockchain was to timestamp documents, the blockchain technology is mainly associated today with cryptocurrency. \textit{Id.} See also Stuart Haber & W. Scott Stornetta, \textit{How to Time-Stamp a Digital Document I}, J. CRYPTOLOGY 99, 106 (1991) (describing the purpose of the blockchain technology which was to authenticate and verify records so that when recorded, the time-stamp would not be able to be back-dated or forward-dated).} Blockchain is a database that collects and holds sets of information in groups known as blocks – as new information comes in, that data is entered into a new block, and once that new block is filled, it is chained onto the previous block, allowing for data to be linked together in chronological order.\footnote{See Adam Hayes, Blockchain Facts: What Is It, How It Works, and How It Can Be Used, INVESTOPEDIA (Sept. 27, 2022), archived at https://perma.cc/CJ9V-JGYK (outlining the structure of the blockchain and how information is structured in blocks, and when those blocks are filled to their maximum capacity with data, they are subsequently chained to the previously filled block, and all together, the blocks form a chronological chain of data known as the blockchain). It is important to contrast the structure of the blockchain with that of a typical database in that a database takes data and is stored into tables, whereas the blockchain allows for an unchangeable timeline of data. \textit{Id.} See also Robert Sheldon, A timeline and history of blockchain technology, TECHTARGET (Aug. 9, 2021), archived at https://perma.cc/LB4F-857D (articulating that the initial block in a blockchain structure is often referred to as the Genesis block within this is the first recorded transaction, and an assignment of a hash: an alphanumeric designation that is based on the timestamp of the block).} Blockchain is decentralized...
in that no person or entity has control over the block.\textsuperscript{13} The blockchain is immutable in that the data that is entered is irreversible, allowing for permanent recordation and viewability by anyone.\textsuperscript{14} As more people discovered Nakamoto’s whitepaper describing this framework, blockchain technology now had its first real-world application: cryptocurrency.\textsuperscript{15}

Although blockchains are beneficial in their permanence and accessibility, the true facet of cryptocurrency transactions via blockchain is that parties may transact directly with each other without

\begin{footnotes}
\footnote{See Mally Anderson, \textit{Exploring Decentralization: Blockchain Technology and Complex Coordination}, JODS (Feb. 6, 2019), \textit{archived at} https://perma.cc/YTZ7-V9MQ (defining decentralization as the “process of dispersing functions and power away from a central location or authority.”) Although a decentralized technology will not be a total solution for all of society’s problems, the adoption of this type of technology can further social decentralization and facilitate democratization of the users which will allow for the decision-making to be placed back in the hands of the people. \textit{Id.}} \footnote{See Nupur Pal, \textit{Understanding Immutable Ledger In Blockchain in Depth}, CRONJ (June 2022), \textit{archived at} https://perma.cc/2G4V-WNDF (highlighting the aspect that made the blockchain technology successful as a ledger is its capability to record transactions and remain unchanged making the process of auditing fast, authentic, and cost-effective).} \footnote{See Vinay Gupta, \textit{A Brief History of Blockchain}, HARV. BUS. REV. (Feb. 28, 2017), \textit{archived at} https://perma.cc/9QAH-HB7K (noting that the first major innovation that transformed the blockchain was bitcoin, characterized as a “digital currency experiment.”). \textit{See also Cryptocurrency}, TREND MICRO (Nov. 20, 2022), \textit{archived at} https://perma.cc/DFK6-ZFUM (defining cryptocurrency).

A cryptocurrency is an encrypted data string that denotes a unit of currency. It is monitored and organized by a peer-to-peer network called a blockchain, which also serves as a secure ledger of transactions, e.g., buying, selling, and transferring. Unlike physical money, cryptocurrencies are decentralized, which means they are not issued by governments or other financial institutions.

\textit{Id.}}
the need for a trusted third party like a financial institution.\textsuperscript{16} Because each transaction is permanently stored and irreversible, sellers and buyers would be protected from fraud as there is computational proof of the chronological order of transactions.\textsuperscript{17} All transactions recorded on the blocks are agreed upon by a consensus algorithm, warranting that each transaction is valid and accurate.\textsuperscript{18}

The unique aspects that separate cryptocurrency transactions from other online payment transactions are that money can be transferred internationally almost instantaneously, and transacting parties can

\textsuperscript{16} See NAKAMOTO, supra note 10, at 1 (proposing that with this new technology, the necessity for a financial institution in transactions would be rendered obsolete due to the fact that the blockchain in it of itself acts as this trusted third-party in these peer-to-peer transactions). “A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.” Id.

\textsuperscript{17} See Hayes, supra note 12 (articulating that the blockchain prevents fraudulent transactions because the structure of the blockchain allows for data to be stored in an irreversible timeline, that is “set in stone. . . .”).

\textsuperscript{18} See What is Blockchain Security, IBM (Oct. 15, 2022), archived at https://perma.cc/5N9J-9WRM (observing that the principles of consensus allow for users to have trust in their transaction, and that the consensus algorithm serves as a mechanism that validates each transaction and confirms its authenticity). See also What Makes a Blockchain Secure?, Binance Acad. (Nov. 16, 2020), archived at https://perma.cc/CC8Z-PF6H (defining consensus as the ability of a node within the blockchain technology to mutually agree on the valid state of the network and on the validity of the transactions between the users allowing for authenticity and validity in transactions between parties). See also Jake Frankenfield, Block (Bitcoin Block), Investopedia (Jan. 9, 2022), archived at https://perma.cc/V34V-QDZ7 (explaining that although the information in a given block records the data of the transaction it is only when that data is validated by the consensus algorithm that the block will then be closed). Upon validation of the block, it is then closed and a new block of information can now be created. Id. A new block cannot be created until the data on the preceding block is verified and thereby closed. Id.
maintain a sense of anonymity.\textsuperscript{19} Traditionally, parties interested in sending money overseas would transact through a bank wire, which requires that the party sending money provide their institution with the recipient’s name, bank details, other personal information, the amount they are sending, and incur fees due to the interbank exchange rate.\textsuperscript{20} Now, with cryptocurrency transactions, parties interested in sending money overseas can do so simply by entering the amount of cryptocurrency, “Tokens”, typing or scanning the recipient’s wallet

\textsuperscript{19} See Okane Pay, Advantages of money transfer using cryptocurrency., DATADRIVENINVESTOR (Nov. 14, 2018), archived at https://perma.cc/R73E-3EM4 (contrasting the process of transferring money overseas via a bank wire where such transactions could take multiple days to get to the recipient with the process of sending cryptocurrency, where money can be sent anywhere on the blockchain within minutes). See also Julian Dossett, Are Cryptocurrency Transactions Actually Anonymous?, CNET (June 7, 2022), archived at https://perma.cc/6WNM-YW9L (acknowledging that although transactions via cryptocurrency are not linked to a real-world identity which provides this sense of anonymity, there is still potential for users’ identities to be linked to their transactions). For example, when users seek to convert their cryptocurrency into U.S. dollars, this creates a distinct paper trail. \textit{Id.} Furthermore, when interacting with an institution that will convert cryptocurrency into dollars, institutions like this tend to have “Know Your Customer” (“KYC”) mechanisms in place which mandate identity verification to use the service. \textit{Id.}

\textsuperscript{20} See also Julia Kagan, What Is a Wire Transfer? How it Works, Safety, and Fees, INVESTOPEDIA (Aug. 17, 2022), archived at https://perma.cc/IL2B-4WDH (listing the typical information that a sender must provide to their financial institution upon initiating a wire transfer).

The recipient’s name, address, contact number, along with any other personal information[,] . . . The recipient’s banking information, including their account number and branch number[.] The receiving bank’s information, which includes the institution’s name, address, and . . . routing number . . . [and] [t]he reason for the transfer[.]

\textit{Id.} See also Artiom Pucinskij, International Wire Transfers, MONEYTRANSFERS.COM (Sept. 27, 2022), archived at https://perma.cc/56PS-BQ4N (conceding that one of the burdens of sending money overseas through a bank wire is that there are various fees associated with performing with this transaction: an exchange rate markup and a fixed transfer fee).
address – a long string of characters similar to that of a bank account number – and pressing send on their device. Once this amount is sent, the transaction is verified by the consensus algorithm, then recorded on the blockchain displaying the wallet address of the sender and the recipient, and the amount sent during that transaction which provides users with a sense of anonymity. Cryptocurrency transactions provide anonymity in that your wallet address will not reveal anything about your identity in the transactions recorded on the

\[21\] See How to send crypto, COINBASE (Oct. 15, 2022), archived at https://perma.cc/6J2A-V4YT (warranting that the process of sending cryptocurrency to another individual is an easy process that requires the user to have the wallet address of the recipient, entering or scanning the wallet address, selecting the amount of crypto the user desires to send, and upon pressing send, the transaction is complete.) It is important to note that cryptocurrency does not have any exchange rates or physical borders in the way that bank wires do when converting dollars to pesos or euros. \(\text{Id.}\) Furthermore, there is a small fee associated with sending cryptocurrency known as a “gas fee” which is much less than other methods like wire transfers or Western Union. \(\text{Id. See also Lyle Daly, What is a Wallet Address?, THE MOTLEY FOOL (June 9, 2022), archived at https://perma.cc/2R2Y-WR43 (defining a wallet address as, “[A] randomly generated string of characters [and numbers] connected to a blockchain wallet. It’s used to receive cryptocurrency transactions to that wallet. . . ”). In a wallet, there is a public key that is comparable to an account number, and there is a private key that acts as a password that allows a user to access the funds within the wallet. \(\text{Id.}\)\]

\[22\] See Noelle Acheson, John Biggs, & Hoa Nguyen, How Do Bitcoin Transactions Work?, COINDESK (Dec. 6, 2022), archived at https://perma.cc/HK7H-DN8J (reviewing the three key variables in a cryptocurrency transaction: an amount, an input, and an output). “An input is the address from which the money is sent, and an output is the address that receives the funds.” \(\text{Id.}\) Once the cryptocurrency is sent, the consensus algorithm validates the transaction, and then it is subsequently published on the public ledger: the blockchain. \(\text{Id.}\)
However, wallet addresses may be linked to a real-world identity by registering that address to exchange platforms or posting a wallet address online.24

B. An Overview of Currency Mixers and Their Surrounding Controversy

1. History of Currency Mixers

To preserve the anonymity and privacy of the individual, parties sending cryptocurrency can obfuscate the origin of these funds by using a cryptocurrency mixing service (“Currency Mixer”).25 A Currency Mixer is a smart contract that operates as a third-party

---

23 See How Anonymous Is Cryptocurrency?, ACUANT (Dec. 9, 2020), archived at https://perma.cc/Q9N9-VB36 (clarifying that cryptocurrency is anonymous in that a user’s wallet address will not, de facto, reveal anything about the user’s identity in that address). “Sending and receiving virtual currency is like writing under a pseudonym. If an author’s pseudonym is ever linked to their identity, everything they ever wrote under that pseudonym will be linked to them.” Id. There are several ways in which wallet addresses can be connected to real-world identities, for example, exchanges that require Know Your Customer and Anti-Money Laundering policies when interacting with that institution. Id. See also How to verify your identity on Coinbase, COINBASE (Oct. 12, 2022), archived at https://perma.cc/V4J6-8ZVE (declaring their commitment to remain a trusted cryptocurrency platform and as such their KYC procedures require that there must be a valid identification of the country the user is residing in and subsequently verified by Coinbase employees).

24 See Jt Clough, How Identity Can Get Linked To your Bitcoin Address, LINKEDIN (Apr. 23, 2018), archived at https://perma.cc/9FPJ-9HHA (characterizing users engaging in cryptocurrency transactions as pseudonymous rather than anonymous in that there is still a potential for users’ real-world identity to be linked to their wallet address).

25 See Sean Stein Smith, Crypto Mixers Are Making Headlines, But What Are They?, FORBES (Aug. 14, 2022), archived at https://perma.cc/9YXM-LBBR (describing a Currency Mixer as a tool that serves to increase anonymity of users when engaging in cryptocurrency transactions). Currency Mixers may be centralized or decentralized, and the mechanics of each Currency Mixer may differ. Id.
service that takes different streams of Tokens and mixes them with others in order to obscure the Token’s original source. Once the Tokens leave the sender’s wallet, they get mixed with the Tokens of other transactors using that Currency Mixer, and the equivalent amount of mixed Tokens is deposited into the recipient’s wallet. When a sender transfers Tokens to a recipient via a Currency Mixer, the blockchain records that a sender sent some Tokens to a mixer, as did several other people at that time, and a recipient received some Tokens from a mixer. Though the Currency Mixer acts as a nexus

---

26 See Max Raskin, The Law and Legality of Smart Contracts, 1 GEO L. TECH. REV. 305, 309–10 (2017) (defining smart contracts and explaining how they work). “A smart contract is an agreement whose execution is automated. This automatic execution is often effected through a computer running code that has translated legal prose into an executable program. This program has control over the physical or digital objects needed to effect execution.” Id. See also Jason Nelson, What Are Coin Mixers and How Do They Work?, Decrypt (Aug. 12, 2022), archived at https://perma.cc/4ZPJ-QEW2 (detailing the way Currency Mixers work). “These smart contracts work as a pool where all the deposited Tokens get mixed together. When funds are withdrawn from those pools, the on-chain link between the source and the destination is broken, anonymizing the transaction.” Id. See also Stuart D. Levi & Alex B. Lipton, An Introduction to Smart Contracts and Their Potential and Inherent Limitations, HARV. L. SCH. FORUM ON CORP. GOVERNANCE (May 26, 2018), archived at https://perma.cc/XDS8-BF2Z (defining smart contracts as a technology that performs all or segments of an agreement on a blockchain).

27 See Dan Goodin, Cryptocurrency flowing into “mixers” hits an all-time high. Wanna guess why?, ARS TECHNICA (July 14, 2022), archived at https://perma.cc/C243-HZBJ (setting forth the way in which Currency Mixers work in that the mixers pool together Tokens that are submitted by several different users and those Tokens are randomly mixed).

28 See Stevens, supra note 4 (simplifying the concept of what occurs when a Currency Mixer is used). “The idea is that, by shuffling bitcoin through a black box, it’s difficult to work out that person A sent 10 bitcoins to person B.” Id.
between the sender and the recipient in its application, the transaction recorded on the blockchain does not reveal the direct connection of a sender to a recipient in a given transfer, which makes it more difficult for viewers to track where the Tokens came from and who received them.  

2. The Criticisms and Acclimations of Currency Mixers

The use of Currency Mixers has sparked a wave of tension and division in the technology community, raising questions of legality and ethics in their use. Critics of Currency Mixers argue that users of this service are interested in obfuscation for the purposes of money laundering, fraud, evading taxes, and covering illegal financing.

---

29 See What Is a Bitcoin Mixer – And How Does It Work?, BYBIT LEARN (Aug. 29, 2022), archived at https://perma.cc/9E3Y-SLJ7 (observing that after there has been transfer of cryptocurrency from one user to another, the blockchain records that the sender sent Tokens from their wallet to a recipient’s wallet). See Stevens, supra note 4 (juxtaposing what is recorded on the blockchain during a regular peer-to-peer transaction with that of a transaction via a currency mixer). “All a public explorer will show is that person A sent some bitcoin to a mixer, as did a dozen other people, and that person B received some bitcoin from a mixer, as did a dozen other people.” Id.

30 See USMAN W. CHOAHAN, THE CRYPTOCURRENCY TUMBLERS: RISKS, LEGALITY AND OVERSIGHT 1 (2017) (stipulating that Currency Mixers beckons review about their legality, the necessity for oversight, and accountability). However, there is a tension between the “cryptoanarchist roots” of cryptocurrency that embodies the spirit of freedom and privacy of the individual. Id. See also Nelson, supra note 26 (quoting Lia Holland, who opined that, “[H]ackers and cybercriminals, as well as those that support them, are deplorable and should be stopped . . .”).

31 See Jessica Lyons Hardecastle, Cryptocurrency laundromat Blender shredded by US Treasury in sanctions first, THE REG. (May 6, 2022), archived at
Critics have gone so far as to compare Currency Mixer to a money laundering service in that users are able to mix tainted Tokens with other users’ Tokens, allowing for facilitation in moving and storing illicit finances.\(^\text{32}\) Additionally, Currency Mixers have been used to facilitate fraudulent transactions and massive rug-pull heists.\(^\text{33}\) Critics argue that this increase in fraud, vulnerability, and illicit activity massively outweighs the benefit of privacy and anonymity.\(^\text{34}\)

Proponents of Currency Mixers, in turn, stress that users have legitimate, non-illicit reasons for wanting an increased level of

---

\(^\text{32}\) See Andrea Rebora, *The Use of Cryptocurrency for Money Laundering*, MEDIUM (Dec. 29, 2019), archived at https://perma.cc/Z2ZZ-JPBA (opining that Currency Mixers have vastly facilitated criminals in that after they obtain illicit funds, they begin the “cleansing” process by moving cryptocurrency into Currency Mixers).

\(^\text{33}\) See Benjamin Pimentel, *Anatomy of an NFT art scam: How the Frosties rug pull went down*, PROTOCOL (Feb. 24, 2022), archived at https://perma.cc/3XR6-8LAV (recounting a recent heist that frauded several purchasers of a digital artwork known as an “NFT”).

\(^\text{34}\) See Goodin, *supra* note 27 (weighing the factors of privacy and money laundering risks in cryptocurrency transactions and Currency Mixers).

[F]inancial privacy is valuable, and that in a vacuum, there’s no reason services like mixers shouldn’t be able to provide it. However, the data shows that mixers currently pose a significant money laundering risk, with 25 percent of funds coming from illicit addresses, and that cybercriminals associated with hostile governments are taking advantage.

*Id.*
privacy. Some users who hold large amounts of Tokens fear that they may be a target of theft or scam, so using Currency Mixers allows for an increased level of anonymity and privacy. Other arguments include that those living under repressive regimes may want to ensure that their financial activity is free from scrutiny. For example, Vitalik Buterin, the co-founder of Ethereum, a decentralized open-source blockchain that offers peer-to-peer transactions, stated that he elected to use a Currency Mixer when donating to Ukraine to protect recipients from scrutiny from the Russian government. Supporters voiced their concern, noting that there is a worrying precedent being

35 See Rose Perper, Are Crypto Mixers Legal?, COINDESK (Aug. 14, 2022), archived at https://perma.cc/M426-X4C3 (setting forth that Currency Mixers serve to increase the privacy of users and enhance the anonymity of those transacting through this service allowing for an additional layer of safety from potential threats from people looking to steal the users’ funds or those who may have access to the users’ personal information).

36 See Osato Avan-Nomayo, Cryptocurrency Mixers and Why Governments May Want to Shut Them Down, Cointelegraph (May 28, 2019), archived at https://perma.cc/PV75-W36M (admonishing the physical assaults on owners of cryptocurrency, with some even leading to the death of the owner). “From Dubai to Singapore, and even the United Kingdom, cryptocurrency owners have fallen victim to armed bandits looking to steal their valuable virtual coins.” Id.

37 See Eric Johansson, Tornado Cash ban is just the beginning: Regulators take aim at cryptocurrency mixers, RETAIL BANKER INT’L (Aug. 26, 2022), archived at https://perma.cc/LMT8-YQ6E (arguing that Currency Mixers allow for those living under oppressive regimes the power to make legal transactions anonymously without fear of scrutiny from their government).

38 See Lachlan Keller, Vitalik Buterin says he used Tornado Cash to donate to Ukraine, FORKAST (Aug. 10, 2022), archived at https://perma.cc/Y49K-M2ZG (providing an example of a prominent figure in the Web 3 community, Vitalik Buterin, that donated money to Ukraine during the Russian invasion, and his reason for doing so was to protect the recipients from scrutiny from the Russian government). “Even if the government where you live is in full support, you might not want [the] Russian government to have full details of your actions . . . .” Id.
set in that anonymity and privacy are incorrectly being conflated with criminal intent. Though proponents and users may have different reasons as to why they elect to transact via a Currency Mixer, they all harken to the same principle of wanting to maintain privacy in their transactions.

C. Possibility of Locating Persons Who Use Currency Mixers

Although the use of Currency Mixers tends to make it more difficult for law enforcement to locate the origin and destination of mixed funds, it is not impossible and has been done before. In 2017, Felix Maduakor illustrated several ways to attack or analyze coin

---

39 See John McAfee, TWITTER (May 24, 2019), archived at https://perma.cc/2E8C-ML94 (declaring that “anonymity itself is slowly being considered a crime [and] [t]he word ‘privacy’ will soon mean ‘criminal intent’”). See also Esther Kim, Authorities Seize Dutch Bitcoin Mixer in ‘Worrying Precedent’, BITCOINIST (May 23, 2019), archived at https://perma.cc/NSL5-R7YJ (quoting Dutch software developer Sjors Provoost’s opinion that “[b]anning [currency] mixers is akin to banning cryptography . . .”).

40 See Cryptocurrency Mixers And Anonymity? How Do They Work?, NDTV (Jan. 22, 2022), archived at https://perma.cc/M3DT-HZ9D (noting the effect of the cryptocurrency mixer in that transactions that are recorded on the blockchain ledger are a lot more difficult to track, which in turn allow for increased levels of anonymity and privacy).

41 See Laura Shin, How Chainalysis Helps Solve Crimes: Jonathan Levin Tells, UNCHAINED (May 29, 2018), archived at https://perma.cc/N6KR-ELKE (stating that even though Currency Mixers enhance anonymity in a transaction, it is not impossible to locate the origin and destination of the coins in the transaction). “‘Okay. So if they do use a tumbler, does it make it more difficult for you?’ ‘Yeah, it definitely makes it difficult for us.’ ‘Impossible or difficult?’ ‘Nothing is ever impossible.’” Id.
mixers. Using a simple heuristic process to deanonymize the mixer transactions, Maduakor was able to identify flaws in the coin mixing process. Maduakor’s algorithm incorporated different factors such as timing, coin transaction amounts, and corresponding fees to filter the destination wallet. Additionally, Maduakor concluded that some services had web-based vulnerabilities that could lead to identifying mixed transaction data via exploiting internal record keeping.


We are going to show, that even though the internals of a mixing service could be based on a secure mixing algorithm, the implementation of this algorithm as a centralized service could easily lead to vulnerabilities. Even a small information leak could lead to the deanonymization of every transaction which the service ever processed.


See id. (identifying that the methods relied upon in Maduakor’s algorithm were timing, Bitcoin transaction amounts, and the associated fees that acts as a filter to identify the destination wallet).

See Maduakor, supra note 42, at 25–26 (explaining that session hijacking and fixation, XSS, SQL and other code injections, and broken authentication may lead to information disclosure). “CMS are typically accessible through a website. Web security bugs and vulnerabilities could compromise the service . . . [Session hijacking / fixation, XSS, SQL and other code injections, and Broken authentication are] some vulnerabilities which could lead to deanonymization of customers.” Id. It is also worthy to note that the aforementioned list is not exhaustive and that based on Maduakor’s algorithm, “even bugs which [do] not seem to be vulnerabilities could be used in combination with other attacking approaches like blockchain analysis or sybil attacks to deanonymize customers.” Id.
Without identifying a precise algorithmic method, the Office of Internal Revenue Service, Criminal Investigation Division, (“IRS-CI”) in the Southern District of New York was able to locate and reveal the identities of two cybercriminals despite them using the Currency Mixing service. In January of 2022, the two defendant cybercriminals marketed and sold Non-Fungible Tokens, (“NFTs”) online with promises to customers that they would receive certain benefits if they purchased their products. Approximately three hours after the last sale of their NFT, the proceeds of the sales were transferred from the company’s Cryptocurrency Wallet to a separate wallet address, and the website marketing their product was subsequently deactivated, making the purchasers victims of fraud.

---

46 See Complaint at 16, U.S. v. Ethan Nguyen, (S.D.N.Y. 2022) (No. 22 mag 2478), [hereinafter Frostie Complaint] (identifying that defendants Nguyen and Llacuna used Tornado Cash to launder money subsequent to their NFT rug pull fraud). “[O]ne week after the Frosties NFT rug pull fraud, Intermediary Wallet Address-1 sent cryptocurrency to Tornado Cash.” Id.

47 See id. at 2 (listing the benefits that were associated with the purchase of a Frostie NFT). “[T]he purchaser would receive certain benefits, including giveaways and access to metaverse game, when in reality there were no such benefits.” Id.

48 See Frostie Complaint, supra note 46, at 10 (recounting the events that happened immediately after the last sale of the Frostie NFT).

That same day . . . the proceeds of the Frosties NFT sale that had been transferred to Frosties Wallet Address-1 were then transferred to a separate cryptocurrency wallet address . . . certain Frosties purchasers observed the suspicious transfer of all the Frosties proceeds at or near real-time, which coincided with the deactivation of the Frosties Website[.]

Id.
the following weeks, the proceeds of the sales were transferred to several intermediary cryptocurrency wallets, masked by VPNs, and the money was sent through Tornado Cash.\textsuperscript{49} Despite the utilization of Tornado Cash, the IRS-CI was able to follow the path of the stolen funds and saw that they were ultimately deposited into the cryptocurrency wallets of the defendants.\textsuperscript{50} With this, it is apparent that although the use of Currency Mixers increases the difficulty of identifying cybercriminals, it is not impossible to do.\textsuperscript{51}

\textit{D. An Overview of the Department of Treasury and the Office of Foreign Assets Control}

In 1789, the Constitution established with ratification The Department of Treasury, ("Treasury Department") which was tasked

\textsuperscript{49} \textit{See generally id.} at 15–17 (tracking the various transfers and different techniques defendants used subsequent to defrauding their customers).

\textsuperscript{50} \textit{See Frostie Complaint, supra note 46, at 18 (following the path of the defendant’s stolen funds through various wallet transfers and use of Tornado Cash). Based on, among other things, (i) the purchase and use of VPN services, (ii) the timeline of the Frosties NFT sales proceeds transfer from Frosties Wallet-1 to Fraud Wallet Address-1 and -2, and then to Tornado Cash, (iii) the use of Tornado Cash, which is designed to further anonymize the source of cryptocurrency funds, and (iv) the receipt of multiple cryptocurrency transactions from Tornado Cash, I believe that NGUYEN and LLACUNA took deliberate steps to conceal their true identities and receipt of the Frosties NFT sales proceeds.}

\textit{Id.}

\textsuperscript{51} \textit{See Shin, supra note 41 (indicating that the use of mixing services indeed enhances anonymity, but it does not make it impossible for law enforcement to identify and locate cybercriminals who use Currency Mixers). See also generally Maduakor, supra note 42 (stating the various methods to reveal user identities via his algorithm).}
to find a way to repair the American government’s $75 million war
debt.\textsuperscript{52} Since then, the Treasury Department has evolved into a
prominent executive agency and has an array of responsibilities with
the goal of promoting economic growth.\textsuperscript{53} The Treasury Department
is divided into two departments: the operating bureaus and the
departmental offices.\textsuperscript{54} The operating bureaus make up the majority
of the Treasury Department and take on a variety of tasks like
managing federal finances, collecting taxes, the production of coin and
currency, advising the President on domestic and international
financial issues, enforcing federal finance and tax law, and
investigating and prosecuting tax evaders, counterfeiters, and
forgers.\textsuperscript{55} The departmental offices are responsible for creating policy

\textsuperscript{52} See Congress founds U.S. Treasury, HISTORY (Nov. 13, 2009), archived at
https://perma.cc/C5RY-N7CQ (clarifying that the Department of Treasury’s origin
can be drawn back to 1775 when looking to find ways to fund the Revolutionary
War, and after taking out loans from other U.S. countries, the Department was tasked
with finding a way to pay off the subsequent debt).
\textsuperscript{53} See Treasury Department, FED. REG. (Oct. 18, 2022), archived at
https://perma.cc/D3C8-8GZN (stating the mission of the Department). “The
Treasury Department is responsible for promoting economic prosperity and ensuring
the soundness and security of the U.S. and international financial systems.” Id.
\textsuperscript{54} See Role of the Treasury, U.S. DEP’T OF THE TREASURY (Oct. 18, 2022), archived
at https://perma.cc/UT9Z-4EY2 (outlining the structure of the Treasury Department
and how it is organized).
\textsuperscript{55} See id. (listing the functions of the operating bureaus and how as a whole, this
sector executes specific tasks).
and overseeing the management of the Department as a whole.\textsuperscript{56} The Office of Foreign Assets Control (“OFAC”) exists within the departmental offices.\textsuperscript{57}

OFAC was officially created in December of 1950 under the name, “Division of Foreign Assets Control” after President Truman declared a national emergency when China entered into the Korean War, thereby blocking all Chinese and North Korean assets subject to United States jurisdiction.\textsuperscript{58} OFAC issues and enforces economic and trade sanctions to further United States foreign policy and national security objectives to deter those that threaten the national security,

\begin{quote}
The basic functions of the Department of the Treasury include: Managing Federal finances; Collecting taxes, duties and monies paid to and due to the U.S. and paying all bills of the U.S.; Currency and coinage; Managing Government accounts and the public debt; Supervising national banks and thrift institutions; Advising on domestic and international financial, monetary, economic, trade and tax policy; Enforcing Federal finance and tax laws; Investigating and prosecuting tax evaders, counterfeiters, and forgers.
\end{quote}

\textit{Id.}

\textsuperscript{56} See \textsc{Dep’t of the Treasury, Departmental Off. Program Summary by Budget Activity} (2014) (stating the overarching responsibility of the departmental offices). “Departmental Offices (DO), as the headquarters bureau for the Department of the Treasury, provides leadership in economic and financial policy, terrorism and financial intelligence, financial crimes, and general management.” \textit{Id.}


\textsuperscript{58} See \textsc{Frequently Asked Questions, U.S. Dep’t of the Treasury} (May 2, 2006), archived at https://perma.cc/5E5J-EYKQ (recounting the history of OFAC and how its roots can be found in 1940 after the German invasion of Norway, but its formal creation came about in 1950 during the Korean War).
foreign policy, or economy of the United States. These sanctions are typically aimed toward individuals and entities, regimes, traffickers of narcotics, people in foreign nations who threaten democratic progress, individuals involved in the propagation of weapons of mass destruction, or against specific countries.

OFAC’s authority derives from the President’s war powers and national emergency powers. OFAC may impose controls on

---

59 See Cortez v. Trans Union, LLC, 617 F.3d 688, 696 (3rd Cir. 2010) (articulating the purpose and functions of OFAC). “We note now that OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against threats to the national security, foreign policy, or economy of the United States.” Id.

60 See Court E. Golumbic & Robert S. Ruff III, Leveraging the Three Core Competencies: How OFAC Licensing Optimizes Holistic Sanctions, 38 N.C.J. INT’L L. & COM. REG. 729, 733 (2013) (indicating that there are two types of sanctions: smart sanctions and “holistic” sanctions). Smart sanctions are employed to target specific areas, entities, or individuals that pose a threat to the national security of the United States. Id. Contrast with holistic sanctions that impact an entire nation, or an entire nation’s government. Id. See also Jason C. Nelson, The United Nations and the Employment of Sanctions as a Tool of International Statecraft: Social Power Theory as a Predictor of Threat Theory Utility, 29 L. & PSYCH. REV. 105, 115 (2005) (giving examples of smart sanctions). “[F]inancial sanctions (e.g., asset freezes and financial restrictions), travel sanctions (e.g., visa bans and airline restrictions), commodity boycotts (e.g., commodities such as oil, diamonds, and lumber products), and arms embargoes.” Id. Although there are less ramifications from a humanitarian vantage point, it is unclear whether it is more effective to employ smart sanctions from a political standpoint. Id.

61 See Office of Foreign Assets Control– Overview, FFIEC BANK SECRECY ACT/ANTI-MONEY LAUNDERING INFOBASE (Oct. 18, 2022), archived at https://perma.cc/C2PB-Z2NU (overviewing OFAC, its purpose, and how the office draws its authority under the President’s war and national emergency powers and other various statutory grants of authority). See also 50 U.S.C. 34 §§ 1621-1622 (conferring power to the President to declare a national emergency and expounding upon the national emergency’s superseding effect on other laws).
transactions and freeze assets within the jurisdiction of the United States pursuant to relevant statutes and legislation. The International Emergency Economic Powers Act (“IEEPA”), in particular, gives OFAC authority to impose penalties and economic sanctions. With regard to cyber-enabled activity threats to national security, OFAC has exercised the authority to impose and enforce sanctions under Executive Order 13694.

E. An Overview of Executive Order 13694 and its Applicability

1. History of Executive Order 13694

Executive Order 13694, (“EO 13694”), was enacted in April of 2015 to impose “sanctions on individuals and entities determined to be

---

62 See Golumbic & Ruff, supra note 60 (addressing the characteristics of OFAC’s financial sanctions and in accordance with this, may freeze the assets of individuals, entities, or entire nations).

63 See Christopher A. Casey et al., Cong. Rsch. Serv., R45618, The International Emergency Economic Powers Act: Origins, Evolution, and Use (2020) (overviewing the International Emergency Economic Powers Act, and how it confers authority to the President regulate once there has been a declaration of a national emergency and confers authority to OFAC to block assets pursuant to this Act). See also 50 U.S.C. 35 § 1701(b)(1) (addressing the imposition of sanctions to those engaging in economic or industrial espionage in cyberspace). “[B]lock and prohibit all transactions in all property and interests in property of a person . . . if such property and interests in property are in the United States, come within the United States, or come within the possession or control of a United States person.” Id.

64 See Frequently Asked Questions, U.S. Dep’t of the Treasury (Oct. 18, 2022), archived at https://perma.cc/HN3C-TKE5 (using Executive Order 13694 as a basis for imposing sanctions upon those found to be responsible for or complicit in harmful cyber activities, and that OFAC has the authority to take action upon those whose action fits this criterion).
responsible for or complicit in malicious cyber-enabled activities that result in enumerated harms that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.\textsuperscript{65} Since its enactment, EO 13694 has been amended by Executive Order 13757, ("EO 13757") which allows for sanctioning of individuals or entities engaging in cyber-enabled activities that have the goal of interfering or threatening with the election process.\textsuperscript{66} EO 13694 is intended to thwart potential threats to United States national security through the imposition of economic sanctions and limit malicious cyber activities.\textsuperscript{67} Since its enactment in 2015, OFAC has issued sanctions pursuant to EO 13694 in several

\textsuperscript{65} See Exec. Order No. 13694, 3 C.F.R. § 1(a)(i) (2015) (providing the criterion for conduct that allows for the application of EO 13694, and the appropriate actions that may be taken by OFAC to halt this illicit behavior).

\textsuperscript{66} See Exec. Order No. 13757, 3 C.F.R. § 1(a) (2016) (amending EO 13694 to allow for sanctions to be imposed on individuals or entities that are deemed to be responsible for meddling or changing information with the goal or effect of impeding upon the election process).

\textsuperscript{67} See Sanctions related to Significant Malicious Cyber-Enabled Activities, VISUAL OFAC (Oct. 18, 2022), archived at https://perma.cc/5SRT-HHZ2 (summarizing the intended goals of EO 13694 and noting that it is addressed to those whose cyber activities have had a harmful impact on national security).
instances against malicious actors to impede their goals and threats to United States national security.68

2. Previous Usage of Executive Order 13694

In the past, EO 13694 was only applied to persons and entities.69 OFAC first used EO 13694 to impose sanctions against individuals that were members of ANO PO KSI, Federal Security Service (“FSB”), Main Intelligence Directorate (“GRU”), Special Technology Center (STC, LTD), and ZOR Security for its cyber-enabled activities to undermine the 2016 United States presidential elections and harassment of United States officials.70 Subsequently, in 2018, OFAC used EO 13694 to impose sanctions upon the Internet Research Agency, (“IRA”) and Concord Management and Consulting for interference in the 2016 presidential election and for assessed attribution for the NotPetya cyberattack.71 In 2018 OFAC issued

68 See Executive Order 13694, WIKIPEDIA (Aug. 27, 2022), archived at https://perma.cc/B8XV-83S3 (listing a handful of the most recent and notable sanctions OFAC has implemented pursuant to EO 13694).
69 See Office of Foreign Assets Control, supra note 57 (outlining the persons and entities that have received sanctions pursuant to EO 13694 since its enactment).
70 See Press Release, Barack Obama, President, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016) (on file with the White House Archives) (responding to the Russian government’s malicious actions against U.S. government officials, their interference with the 2016 presidential elections, and imposing sanctions in response to these activities).
71 See Tamara Keith, U.S. Imposes New Sanctions On Russia Over Election Interference, Cyberattacks, NAT’L PUB. RADIO (Mar. 15, 2018), archived at
sanctions against two Iranian hackers pursuant to EO13694 for accumulating over 7,000 Bitcoins in ransom payments. In June 2020, Nigerian nationals were sanctioned pursuant to EO 13694 for conducting an elaborate scheme to steal over six million dollars through deceptive global threats by impersonating potential romantic partners to gain the trust of potential victims.

https://perma.cc/EQ7D-4U8X (reporting that OFAC under former President Trump’s administration took actions to impose sanctions pursuant to EO 13694 against thirteen people and three entities: one of which being the IRA due to their alleged influence during the 2016 presidential elections and their “NotPetya” attack). “Among the cyberattacks for which U.S. is trying to punish Russia was the “NotPetya” attack, which targeted computers in Ukraine. The U.S. attributes that attack to the Russian military.” Id.

See Nikhilesh De, US Regulators Tie Two Bitcoin Addresses to Iranian Ransomware Plot, COINDESK (Nov. 28, 2018), archived at https://perma.cc/BYY6-LZ5R (linking Khorashadizadeh and Ghorbaniyan to their wallet addresses, and as a result of such link, OFAC has been able to sanction them due to their malicious ransomware plot). “[They] converted more than 7,000 bitcoin transactions into Iranian rial, processing roughly 6,000 bitcoin, worth millions of U.S. dollars . . . . These transactions included bitcoin received as part of the payment from SamSam’s victims.” Id.


American citizens lost over $6,000,000 due to these individuals’ BEC fraud schemes, in which they impersonated business executives and requested and received wire transfers from legitimate business accounts. Money was also stolen from innocent Americans by romance fraud, in which the designees masqueraded as affectionate partners to gain trust from victims. Id.
III. FACTS

A. OFAC Sanctions Currency Mixers Blender.io & Tornado Cash

Over the course of 2022, two different Currency Mixers have been sanctioned pursuant to EO 13694.\(^74\) This is the first time in history that the United States government has sanctioned a virtual Currency Mixer.\(^75\) Accordingly, such unprecedented sanctions have caused a flurry of controversy among United States Government officials, lawyers, and members of the cryptocurrency community.\(^76\)

---

\(^74\) See Chris Duckett, Crypto mixer Blender sanctioned by US Treasury for involvement in $600m Ronin theft, ZDNET (May 8, 2022), archived at https://perma.cc/KRM2-2AAW (reporting that U.S. Treasury sanctioned Blender for providing services for the North Korean Lazarus group, and that as a result of these sanctions, Blender is blocked from transactions involving US persons). See also Richard Gibbon et al., OFAC Sanctions Virtual Currency Mixer “Tornado Cash”, SQUIRE PATTON BOGGS (Oct. 4, 2022), archived at https://perma.cc/6S6U-SJTD (explaining that sanctions were imposed after the Lazarus Group used this Tornado Cash to launder their illicit proceeds).

\(^75\) See Reynaldo Marquez, A First for Crypto, U.S. Treasury Sanctions Mixer Blender IO, BITCOINIST (Nov. 16, 2022), archived at https://perma.cc/68UL-62GK (stating that following OFAC’s sanctions, Blender.io has officially become the first entity in cryptocurrency to be sanctioned because of their connection to the Lazarus Group’s virtual currency heist).

\(^76\) See Brooke Becher, U.S. Sanctions on Tornado Cash: What Does This Mean for Crypto?, BUILTIN (Nov. 1, 2022), archived at https://perma.cc/2ZJR-P9DW (citing developer, software engineer, and founder of Modulus, Richard Gardner, “The call to sanction Tornado Cash is justified . . . A mixer, operating as Tornado Cash does, can’t be allowed to operate, as it would allow for a bypass of international sanctions. It can directly be used to facilitate hacks perpetrated by enemy nation states.”). Other commentators, like Marcel Harmann, founder and CEO of ThorWallet DEX have taken the opposite approach and defend Tornado Cash by arguing that OFAC must first understand where liability attaches before issuing sanctions. Id. It is clear that authorities are still trying to discern where liability lies when it comes to decentralization, particularly as it relates to
1. OFAC Sanctions Blender.io

In May of 2022, Blender.io (“Blender”), a Currency Mixer, faced sanctions after the Lazarus Group, a Democratic People’s Republic of Korea (“DPRK”) state-sponsored cyber hacking group, used Blender’s mixing service to launder over $20.5 million illicit proceeds.77 These illicit proceeds came from what is the largest known cyber-enabled virtual currency heist to date which has now become known as the Axie Infinity Heist.78

Criminals have leveraged technological developments throughout history for illicit activity and to ban the technology would be more detrimental than constructive.

Id. See also Kurt Opsahl, Code, Speech, and the Tornado Cash Mixer, EFF (Aug. 22, 2022), archived at https://perma.cc/CQL5-ES6P (advancing the argument that because Tornado Cash is computer code, it is therefore protected by the First Amendment as precedent has already determined that computer code is speech and enjoys those same constitutional protections); Bernstein v. U.S. Dept. of State, 922 F.Supp. 1426, 1436 (1996) (holding that the plaintiff’s computer code was speech for the purposes of First Amendment protection). See also Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000) (reasoning that because computer code is an “expressive means for the exchange of information and ideas about computer programming”, it is therefore considered speech and is protected by the First Amendment).

77 See Sanctions on Blender, supra note 5 (estimating an amount of $20.5 million in illicit proceeds have been laundered by Lazarus Group by using Blender so they may generate revenue for their ballistic missile programs and weapons of mass destruction).

78 See Alexander Culafi, Axie Infinity hack highlights DPRK cryptocurrency heists, TECHTARGET (May 18, 2022), archived at https://perma.cc/GT8C-7NAP (describing how the hackers orchestrated the attack).

The breach occurred when attackers gained control of a series of validator nodes attached to Axie Infinity to conduct fake withdrawals. Hackers stole . . . approximately $620 million at the time . . .
According to OFAC’s investigation, Blender has been used to launder a total of $500 million worth of Tokens in illicit proceeds. OFAC also identified that several Russian ransomware groups, including Trickbot, Conti, Ryuk, Sodinokibi, and Grandcrab, used Blender to launder. These groups include Trickbot, Conti, Ryuk, Sodinokibi, and Grandcrab. Given the repeated use of Blender by

But the Axie Infinity hack represents an enormous theft on behalf of Kim Jong Un’s regime, and acts as the latest in a long line of big-game heists against cryptocurrency platforms.

Id.

79 See Sanctions on Blender, supra note 5 (totaling the amount of Tokens that have been laundered by using Blender). See also Mengqi Sun, U.S. Blacklists Mixer Used to Launder Proceeds from Axie Infinity Crypto Hack, WALL ST. J. (May 6, 2022), archived at https://perma.cc/FB3V-J5KX (reporting that since its creation in 2017, Blender.io has been used to process over $500 million worth of Tokens and was used by Lazarus Group to launder $20.5 million of illicit proceeds).

80 See Sanctions on Blender, supra note 5 (linking Blender to other ransomware groups based in Russia). See also Joe Warminsky, US Treasury sanctions cryptocurrency for first time, citing Ronin Network hack, THE REC. (May 6, 2022), archived at https://perma.cc/F59H-B5MN (hypothesizing that Blender was used to launder Tokens from Hydra market, which is a Russian language darknet that OFAC has previously sanctioned). See also Joe Tidy, Hydra: How German police dismantled Russian darknet site, BBC (Apr. 6, 2022), archived at https://perma.cc/BF49-UYLX (listing the services that Hydra offered: “same-day ‘dead drop’ services, where drug dealers hide packages in public places before informing customers of their pick-up location[,] . . . drugs, hacked materials, forged documents . . .”).

81 See Sanctions on Blender, supra note 5 (listing the groups of cyberhackers, darknets, and ransomware that has been linked to Russian individuals and groups). See also Advisory: Trickbot, NAT’L CYBER SEC. CTR. (Feb. 12, 2020), archived at https://perma.cc/QC4K-HRJ8 (cautioning the public about Trickbot as a computer malware that aims to steal banking details and other credentials and has been found to be connected with Russian intelligence agencies). See also Christopher Bing, Russia-based ransomware group Conti issues warning to Kremlin foes, REUTERS (Feb. 25, 2022), archived at https://perma.cc/ZP3V-MRVN (defining Conti as a Russian cyber hacking group that has previously used ransomware to extort money from companies in the United States and in Europe). “[The] Conti hackers invaded networks and encrypted data, disrupting operations and demanding payments to
cybercriminals and ransomware groups, OFAC has deemed Blender to be a significant threat to the national security and financial stability of the United States. Consequently, Blender is being sanctioned pursuant to EO 13694 for being complicit in or having materially restored access.” Id. See also Lucian Constantin, Ryuk explained: Targeted, devastatingly effective ransomware, CSO (Mar. 19, 2021), archived at https://perma.cc/94BJ-L62L (articulating the origins and application of Ryuk). “Ryuk is a sophisticated ransomware threat that has been targeting businesses, hospitals, government institutions and other organizations since 2018 . . . Ryuk is now generally believed to be the creation of a Russian-speaking cybercriminal group . . . .” Id. See also Lawrence Abrams, Another Ransomware Will Now Publish Victims’ Data If Not Paid, BLEEPING COMPUT. (Dec. 12, 2019), archived at https://perma.cc/2Y9M-4999 (explaining that Sodinokibi, also known as REvil operated as a Russian-based ransomware service that would steal confidential information from its victim, and would threaten to publish the information on their webpage unless the victim paid them a ransom). See also Juha Saarinen, No let up on REvil ransomware-as-a-service attacks, iTNEWS (Jan. 29, 2020), archived at https://perma.cc/E4BT-E7R3 (stating that Sodinokibi are thought to be a Russian-based group because they do not attack Russian organizations). “The United States, South Korea and China are the hardest REvil-hit countries followed by Canada and France; the malware checks computers’ system language settings and won’t run if it’s set to Russian or one of the Commonwealth of Independent States countries.” Id. See also Brian Krebs, Who’s Behind the GandCrab Ransomware?, KREBS ON SEC. (July 8, 2019), archived at https://perma.cc/36FY-FG4A (determining that GandCrab is a ransomware service that corrupted systems, and the group behind GandCrab would hold such systems hostage until its victim paid the ransom). There were several individuals that belonged to the GandCrab software development team, and it is likely that this team was Russian-based because, “[t]he GandCrab affiliate program took measures to prevent the installation of its ransomware on computers residing in Russia or in any of the countries that were previously part of the Soviet Union . . . .” Id.

82 See Sanctions on Blender, supra note 5 (characterizing Blender.io as a threat to U.S. national security because the service has been used on multiple occasions by several different criminal organizations to launder their illicit proceeds following a cyberattack or ransomware scheme). Quoting Brian E. Nelson, Under Secretary of the Treasury for Terrorism and Financial Intelligence, “Virtual currency mixers that assist illicit transactions pose a threat to U.S. national security interests. We are taking action against illicit financial activity by the DPRK and will not allow state-sponsored thievery and its money-laundering enablers to go unanswered.” Id.
assisted the aforementioned cyber-criminals and ransomware groups, among others.83

2. OFAC Sanctions Tornado Cash

In August of 2022, Tornado Cash, another Currency Mixer, was sanctioned by OFAC pursuant to EO 13694.84 Like Blender, Tornado Cash was used by the DPRK and other cyber criminals to launder a total of $7 billion Tokens.85 Tornado Cash was also used to launder over ninety-six million dollars in illicit proceeds from the

83 See Sanctions on Blender, supra note 5 (designating Blender pursuant to E.O. 13694). See also Exec. Order No. 13757 3 C.F.R. § 1(i)(i) (2015) (setting forth the applicability of the conduct that allows the government to sanction a person or entity pursuant to this grant of authority).

Any person determined by the Secretary of the Treasury . . . to be responsible for or complicit in, or to have engaged in, . . . or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States . . .

Id.

84 See U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash, U.S. DEP’T OF THE TREASURY (Aug. 8, 2022), archived at https://perma.cc/VPT4-3MBG [hereinafter Sanctions on Tornado Cash] (announcing that pursuant to E.O. 13694, OFAC will be designating the currency mixing service for its use in laundering $7 billion worth of virtual currency since its creation in 2019). See also Cryptocurrency Mixer Tornado Cash Sanctioned by U.S. Treasury Department, FTI CONSULTING (Aug. 19, 2022), archived at https://perma.cc/3L8R-3S7P (reporting that on August 8, 2022 Tornado Cash faced sanctions by the Office of Foreign Assets Control and quotes Ari Redbord, the head of legal and government affairs at TRM who described the government’s sanctions the “‘largest, move impactful action’ in crypto to date.”).

85 See Nikhilesh De, Crypto-Mixing Service Tornado Cash Blacklisted by US Treasury, COINDESK (Aug. 8, 2022), archived at https://perma.cc/9RP8-GL56 (tying Tornado Cash to the Lazarus Group by characterizing it as a “key tool” for the Lazarus Group they used Tornado Cash’s mixing service as a way to launder their illicit proceeds). ‘Blockchain analysis showed that tens of millions of dollars’ worth of crypto stolen from Ronin flowed through Tornado Cash . . . .” Id.
Harmony Bridge Heist and approximately $7.8 million Tokens from the Nomad Heist.\footnote[86]{See Elizabeth Howcroft, Tom Wilson & Hannah Lang, \textit{U.S. crypto firm Harmony hit by $100 million heist}, \textit{REUTERS} (June 24, 2022), archived at https://perma.cc/822B-XPSW?type=image (explaining that Harmony is a cryptocurrency firm with a specialized tool called a “bridge” that was hacked into and stolen). “The California-based company said the heist hit its Horizon ‘bridge’, as a tool for transferring crypto between different blockchains – the underlying software used by digital [T]okens such as bitcoin and ether.” \textit{Id.} See also Sebastian Sinclair, \textit{Funds From $100M Horizon Bridge Exploit Sent to Tornado Cash Mixing Service}, \textit{BLOCKWORKS} (June 27, 2022), archived at https://perma.cc/63KF-SLQM (revealing that after the Harmony Bridge Heist, the stolen $100 million in Tokens were subsequently transferred to a wallet address belonging to Tornado Cash, indicating that the stolen proceeds were subsequently laundered). See also Sumeet Wadhwani, \textit{Bad Code Update Lets Hackers Steal $190M From Cryptocurrency Bridge Nomad}, \textit{SPICEWORKS} (Aug. 3, 2022), archived at https://perma.cc/76JT-B268 (observing the flaw that hackers found in Nomad’s computer code that allowed them to gain access to steal almost $200 million Tokens).}

Like Blender, Tornado Cash was deemed to be a major threat to United States national security and United States financial security.\footnote[87]{See Sanctions on Blender, supra note 5 (comparing Tornado Cash to Blender in that both services have been used by ransomware and fraud groups and therefore

Nomad, which operates under parent company Illusory Systems, had over $190 million in its smart contracts when hackers identified a flaw that allowed them to carry out transactions . . . . 

The significance of the flaw is that it allowed hackers to send a small amount, as little as 0.1 bitcoin, from one blockchain on Nomad and receive an arbitrary, higher amount of as much as 100 bitcoin on another blockchain.

\textit{Id.} See also Shiraz Jagati, \textit{Tornado Cash saga highlights legal issues affecting the crypto market}, \textit{COINTELEGRAPH} (Aug. 23, 2022), archived at https://perma.cc/SG5N-EGU8 (linking Tornado Cash as the tool used to launder stolen Tokens in both the Nomad Heist and the Harmony Bridge Heist). “Additionally, Tornado Cash was also used to launder over $96 million of ill-gotten funds derived from . . . [the] Harmony Bridge hack and $7.8 million from this month’s Nomad heist.” \textit{Id.}
Cash for being complicit in or having materially assisted the aforementioned cyber-criminals and ransomware groups, among others.⁸⁸ Accordingly, OFAC determined that Tornado Cash’s threat resulted in or is likely to result in enumerated harms.⁸⁹

3. The Effect of Sanctions on a Currency Mixer

Once sanctions are imposed upon a Currency Mixer, the assets held within that mixer are frozen and effectively inaccessible.⁹⁰

constitute a threat to the United States’s financial security). “Treasury is committed to exposing components of the virtual currency ecosystem, like Blender, that are critical to the obfuscation of the trail of stolen proceeds from illicit cyber activity.”

Id.

⁸⁸ See Sanctions on Blender, supra note 5 (providing EO 13694 as the basis of authority to issue sanctions on this Currency Mixer). See also Tornado Cash Sanctions May Signal Enforcement Shift, LAW360 (Sept. 2, 2022), archived at https://perma.cc/PZB2-V8KP (noting that under United States law, in order to legally prosecute for money laundering or criminal sanctions violations, there must be proof of criminal intent).

⁸⁹ See Exec. Order. No. 13757 3 C.F.R. § 1(a) (2016) (amending EO 13694 to enumerate harms that allow OFAC to take action to sanction the malicious actor).

[Ｃ]ompromising the provision of services by, a computer . . . that support one or more entities in a critical infrastructure sector; . . . significantly compromising the provision of services by one or more entities in a critical infrastructure sector; . . . causing a significant disruption to the availability of a computer or network of computers; . . . causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; or . . . tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions . . .

Id.

⁹⁰ See Dalia Ramirez, Tornado Cash Sanctions: What Crypto Investors Need to Know, NERD WALLET (Sept. 22, 2022), archived at https://perma.cc/B2ZG-JQU8 (articulating that effects of what a sanction does to a Currency Mixer such as Tornado Cash). “When Tornado Cash was sanctioned, the government seized control of all its addresses and froze the associated assets, which could set a standard for future government crackdowns on crypto.” Id.
Furthermore, entities and individuals within the United States are unable to utilize the platform to transact with other users.  

Currently, approximately $437 million worth of virtual currency assets are locked up within Tornado Cash’s mixing service. As a result, users who have initiated a transaction involving Tornado Cash may request a license from OFAC to retrieve whatever assets they have within the mixing service or complete the transaction. However, OFAC has made it clear that completing a transaction or otherwise withdrawing virtual currency from Tornado Cash is

91 See Marquez, supra note 75 (noting the effect the ban has on users who transacted using the mixing service Tornado Cash that were unable to complete the transaction before the sanctions were imposed, and what procedures are available to retrieve their assets). “All transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons are prohibited unless authorized by a general or specific license issued by OFAC, or exempt.” Id.

92 See Zhiyuan Sun, Circle freezes blacklisted Tornado Cash smart contract addresses, COINTELEGRAPH (Aug. 8, 2022), archived at https://perma.cc/S66Y-URDZ (estimating the amount of cryptocurrency assets that have been seized by the government and are currently inaccessible unless the user retrieves a special license issued by OFAC to get a return on his assets).

93 See OFAC License Application Page, U.S. DEP’T OF THE TREASURY (Nov. 20, 2022), archived at https://perma.cc/4HDJ-YKF5 (providing an application to allow for users with frozen assets in Tornado Cash to retrieve those seized assets back). “If your funds have been blocked or ‘frozen’ by a financial institution or other party due to a possible link to OFAC-administered sanctions, you may apply for a specific license by clicking . . . above.” Id.
conditioned on the fact that the transaction did not involve other sanctionable conduct.\footnote{See Frequently Asked Questions, U.S. DEP’T OF THE TREASURY (Sept. 13, 2022), archived at https://perma.cc/CQ2J-CV62 [hereinafter Qualifiers to Retrieve Seized Assets] (clarifying that in order to receive a special license from OFAC to complete a transaction using Tornado Cash, users must provide certain information regarding the sender and recipient of the transaction, and that such transactions did not involve other sanctionable conduct).}

\textbf{B. Defining Complicity and Materially Assisting}

Recent case law and years of precedent have allowed for a comprehensive understanding of what it means to be an accomplice to a crime and what it means to materially assist a crime, both of which will be addressed in turn.\footnote{See People v. R.V., 635 P.2d 892, 895 (Colo. 1981) (stressing the key factors in imposing criminal liability under the theory of accomplice liability). \[T\]he critical factor in imputing criminal responsibility . . . is the offenders ‘intent to promote or facilitate the commission of the offense.’ In this respect, the statutory definition is consistent with the prevailing judicial doctrine on complicity, which requires a purposive attitude or conscious objective on the part of the offender towards the completion of the crime. \textit{Id.} See also Apollo Capital Fund LLC v. Roth Capital Partners, LLC, 158 Cal. App. 4\textsuperscript{th} 226, 253 (Cal. Dist. Ct. App. Div. 8, 2007) (clarifying that in order to impose liability on an agent materially assisting in an act or transaction that there must be an intent to deceive or defraud).} Complicity is not a substantive crime or offense; rather, it is a theory of liability in which a defendant becomes liable for a criminal offense committed by another.\footnote{See Grissom v. People, 115 P.3d 1280, 1283 (Colo. 2005) (clarifying that complicity is not a separate and distinct crime, and it is used to hold the accomplice legally accountable for the criminal offense[s] of the principal). \textit{“A person is legally accountable as principal for the behavior of another constituting a criminal offense if, with the intent to promote or facilitate the commission of the offense, he or she aids, abets, advises, or encourages the other person in planning or committing the offense.” \textit{Id.}}} With this, there
is an elevated requirement that the accomplice or assistant must actually intend his action to further the criminal conduct of the principal.  

1. Complicity

To establish accomplice liability, there must be both an accomplice and a principal, and the accomplice must purposefully aid, abet, or encourage the principal to commit the offense. An accomplice is one who has the intent to assist the principal in the commission of the crime and actually does verbally or physically aid, counsel, or encourage the principal before or during the commission of the crime. A principal is one who, with the requisite mental state,

---

97 See United States v. Coats, 8 F.4th 1228, 1252 (11th Cir. 2021) (clarifying the requisite intentionality for the accomplice to impose liability). “[A]n accomplice must either intentionally cause the crime, intentionally aid or abet in its commission, or intentionally advise, encourage, hire, counsel or procure another to commit the crime.” Id.

98 See Model Penal Code § 2.06 (3) (Am. L. Inst. 1962) (setting forth how accomplice liability is established). “A person is an accomplice of another person in the commission of an offense if: (a) with the purpose of promoting or facilitating the commission of the offense, he (i) solicits such other person to commit it, or (ii) aids or agrees or attempts to aid such other person in planning or committing it . . . .” Id.

99 See Riley v. State, 60 P.3d 204, 210 (Alaska Ct. App. 2002) (holding that an accomplice must intend to promote the commission of the crime, and even though there may have been some assistance or encouragement, the accomplice may only be held liable if she did so with the criminal intent).

It is universally acknowledged that accomplice liability can not [sic] be based solely on the fact that a person’s words or actions had the effect of encouraging or assisting another to a crime. The government must also prove, at a minimum, that the accomplice
actually engages in the act or omission that causes the criminal result.\textsuperscript{100}

In order to be found as an accomplice to a crime, the accomplice must physically or verbally encourage, abet, aid, or assist the principal in his crime.\textsuperscript{101} Additionally, he must be purposeful in his actions and have a conscious purpose for the crime to occur.\textsuperscript{102} Although it is not necessary for the accomplice to be physically present at the commission of the crime, a conviction is dependent upon proof that there is the accomplice and the principal and that the accomplice acted in connection with the principal to accomplish the crime.\textsuperscript{103} In

\textsuperscript{100} See \textit{Coats}, 8 F.4\textsuperscript{th} at 1244 (defining the principal as one who is the perpetrator of the criminal conduct).

\textsuperscript{101} See \textit{State v. Hatfield}, 2022-Ohio-148 1, 51 (2022) (maintaining that in order to convict on accomplice liability by aiding and abetting, there must be evidence that indicates the defendant accomplice either supported, assisted, encouraged, cooperated with, advised, or incited the principal in the commission of the crime, and that the defendant shared the criminal intent of the principal). \textit{See also} \textit{People v. Lauria}, 251 Cal. App. 2d 471, 483 (1967) (holding that knowledge of the principal’s purpose would not suffice for aiding and abetting of just any crime).

\textsuperscript{102} See \textit{Direct Sales Co. v. United States}, 319 U.S. 703, 709 (1943) (holding that the seller’s knowledge of the illegal use of goods alone was insufficient to make the sellers participants in a conspiracy with the distillers who purchased goods from them). “[B]y the sale he intends to further, promote, and cooperate in it. This intent, when given effect by overt act, is the gist of conspiracy.” \textit{Id.}

\textsuperscript{103} See \textit{State v. Galisia}, 63 Wn. App. 833, 839 (1992) (asserting that physical presence and awareness of the criminal conduct alone are insufficient to support a conviction for accomplice liability, and that accomplice liability is supported where the accomplice is purposeful in promoting or facilitating the commission of the crime). \textit{See also} \textit{Riley}, 60 P.3d at 210 (reinforcing that the accomplice must intend that her acts have the impact of assisting or encouraging the principal).
attempting to prove that the accomplice had the objective to further or complete the crime, courts may look towards whether or not the accomplice had a “stake in the venture”. 104

2. Material Contribution

“Material” in its plain meaning is defined as being of real significance, and “contribution” is defined as help that is supplied or given to another to bring about a particular result. 105 Materially contributing to the commission of a crime, like complicity, allows for liability to be imposed on the person or entity who aids another in the commission of unlawful conduct.106 Case law has helped in defining

---

104 See United States v. Renteria-Alvarez, No. 89-10433, 1990 U.S. App. LEXIS 21632 at 11 (9th Cir. Dec. 11, 1990) (indicating that criminal responsibility for abetting a crime requires that the defendant “associated himself with the venture, that he participated in it as something that he wished to bring about, that he [sought] by his action to make it succeed.”).
105 See People v. Lofton, 1975 N.Y. Misc. LEXIS 2428 at 5–6 (defining the terms “material” and “assistance” in its plain meaning). “The words ‘material assistance’ must be given their plain and usual meaning. ‘Material’ is defined as being of real importance or great significance and ‘assistance’ is defined as help supplied or given. To ‘assist’ is defined as an act or circumstance that helps to bring about a desired result . . . .” Id.
106 See Jordan-Benel v. Universal City Studios, Inc., No. CV-14-5577-MWF, 2015 U.S. Dist. LEXIS 82220, 1, 31 (C.D. Cal. 2015) (holding that in order to be held liable for contributory infringement, there must be evidence that there was a material contribution of the unlawful conduct). See also Doe v. MindGeek USA, Inc., 574 F.Supp. 3d 760, 768 (2021) (asserting that if an internet software contributes materially to unlawful content, liability will be imputed to the third-party internet software).
what is required to characterize one’s conduct as a material contribution to the commission of a crime or other tortious conduct.\textsuperscript{107}

Several circuits have adopted a “material contribution” test to determine whether or not services provided by interactive computer software rise to the requisite level to impute liability for materially contributing to unlawful content.\textsuperscript{108} Under the material contribution test, merely taking action that is necessary to the display of the allegedly illegal content is insufficient to impute liability; rather, the

\textsuperscript{107} See Doe, 574 F.Supp. 3d at 768 (stating that in order to materially contribute to an unlawful act, the defendant must have a direct connection to the unlawful conduct). See also In re Brand Name Prescription Drugs Antitrust Litig., 123 F.3d 599, 1035 (synonymizing materially assisting with aiding and abetting). “Aiding and abetting . . ., which means materially assisting a known-to-be-illegal activity in the hope that it will flourish to the benefit, pecuniary or otherwise, of the aider.” Id. See Perfect 10, Inc. v. Visa Int’l Serv. Ass’n, 494 F.3d 788, 797-98 (2007) (holding that although payment systems make it easier for copyright infringement to take place, payment processing does not constitute a “material contribution”). We acknowledge that Defendants’ payment systems make it easier for such an infringement to be profitable, and that they therefore have the effect of increasing such infringement, but because [copyright] infringement[s] . . . can occur without Defendants’ payment system, we hold that payment processing by the Defendants . . . does not constitute a “material contribution” . . . .


. . . [T]he material-contribution test fits well within our broader . . . jurisprudence. Zeran and Nemet rest on the principle that liability for an interactive computer service user or provider must turn on “something more than . . . its traditional editorial function.” . . . All the material-contribution test does is put a more helpful name to this “something more” standard. And defining “something more” as a material contribution makes sense.

\textit{Id.}

See also Jones v. Dirty World Entm’t Recordings LLC, 755 F.3d 398, 413 (2014) (adopting the material contribution test).
actor or service provider must be responsible for what makes the displayed content allegedly unlawful.\textsuperscript{109} This test creates a crucial distinction between, on the one hand, displaying actionable content and, on the other hand, assisting with the creation or development of illegal or actionable content.\textsuperscript{110} Courts adopting this test acknowledge that making a material contribution does not mean “merely taking action that is necessary to the display of the allegedly illegal content” but rather “being responsible for what makes the displayed content allegedly unlawful.”\textsuperscript{111}

\textsuperscript{109} See Henderson, 53 F.4th 110 at 128 (holding that an interactive computer software is not liable for developing the unlawful content unless the software has gone beyond the exercise of traditional editorial functions and instead materially contributed to what made the content unlawful). See also Roca Labs, Inc. v. Consumer Op. Corp., 140 F. Supp. 3d 1311, 1322 (2015) (articulating the material contribution test). “Under the material contribution test, a service provider or user becomes an information content provider when it is ‘reasonable for what makes the displayed content allegedly unlawful.’” \textit{Id.}

\textsuperscript{110} See Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (1997) (noting that liability is barred against companies that serve as intermediaries for other parties’ potentially injurious messages). However, where a company materially contributes to a message’s unlawful content, the company stops being a mere “intermediary” for another party’s message. \textit{Id.} Instead, the company is adding new content to the message that harms the plaintiff. \textit{Id.} Legislation already exists for plaintiffs seeking to put the third-party computer service in the shoes of the person who used the service to commit a harm. \textit{Id.} “[Legislation] precludes courts from entertaining claims that would place a computer service provider in a publisher’s role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher’s traditional editorial functions such as deciding whether to publish, withdraw, postpone or alter content are barred.” \textit{Id.}

\textsuperscript{111} See Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1121-22 (addressing whether or not liability is imputed on a third-party dating website that was used by a prankster to make a fake profile with libelous information about the plaintiff).
IV. ANALYSIS

A. OFAC’s Two Big Mistakes in Interpreting EO 13694

OFAC’s decision to use EO 13694 as a basis for imposing sanctions upon Tornado Cash is a misapplication of the law.\(^{112}\) Moreover, it seems as though OFAC is attempting to stretch already existing legislation to present a legal justification for the sanctions on Tornado Cash and Blender.io.\(^{113}\)

1. OFAC’s First Mistake: Inability to Establish Accomplice Liability Against Open-Source Technology

Plaintiff asserted the theory that the website materially contributed to this libelous content, and that therefore liability should attach. \(Id.\) The court reasoned that even though the website’s matchmaking functionality allowed the libelous content to be more effectively disseminated, this in and of itself did not constitute a material contribution because the third-party prankster was the developer and creator of the libelous content and the website served to be more of a neutral tool that did not encourage the posting of the defamatory content. \(Id.\) See also Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1172 (2008) (determining that the roommate-seeking website service was a neutral tool that was specifically designed to allow users to input qualifications such as race, gender, and religion, and did not materially contribute to illegal or discriminatory conduct).

\(^{112}\) See Armstrong, supra note 7 (arguing that OFAC has exceeded the authority conferred by Congress by sanctioning Tornado Cash as it is an open-source technology rather than the cybercriminals themselves).

\(^{113}\) See Exec. Order No. 13694 3 C.F.R. § 1(a)(i) (2015) (providing the Executive Order applies to individuals and entities, not to open-source technology). See also Grewal, supra note 6 (asserting that Tornado Cash as a smart contract does not qualify as an individual, an entity, nor a piece of property). “First, at the risk of stating the obvious, Tornado Cash open source smart contracts are not persons. They are lines of code, not humans, corporations, or organizations . . . Tornado Cash smart contracts are also not property.” \(Id.\)
OFAC’s first mistake in using EO 13694 to impose sanctions upon Tornado Cash was their failure to establish the basic elements of accomplice liability between Tornado Cash and a cybercriminal principal.\textsuperscript{114} EO 13694 provides in part that the individual or entity be complicit in malicious cyber-enabled activities to receive sanctions.\textsuperscript{115} Complicity requires that the accomplice has the intent to assist the principal and actually render that assistance to the principal before or during the commission of the crime.\textsuperscript{116}

Tornado Cash is not a human capable of forming an intent as it is a piece of technology.\textsuperscript{117} Taking the application of EO 13694 to its logical end, it seems as though OFAC formed the theory that Tornado

\textsuperscript{114} See Exec. Order No. 13694 3 C.F.R. § 1(a)(i) (2015) (providing that sanctions will be imposed on individuals or entities that are complicit in the commission of cybercrimes). See also Grissom v. People, 115 P.3d 1280, 1283 (Colo. 2005) (outlining the elements necessary to establish accomplice liability upon a defendant). “A person is legally accountable as principal for the behavior of another constituting a criminal offense if, with the intent to promote or facilitate the commission of the offense, he or she aids, abets, advises, or encourages the other person in planning or committing the offense.” \textit{Id.}

\textsuperscript{115} See Exec. Order No. 13694 3 C.F.R. § 1(a)(i) (2015) (setting forth that those that are complicit in cybercrimes that result in a significant threat to national security or national financial health of the United States can be sanctioned).

\textsuperscript{116} See Riley v. State, 60 P.3d 204, 210 (Alaska Ct. App. 2002) (ruling that liability will not be imputed where someone’s words or actions had the effect of assisting the principal, and that intent to encourage or assist the principal is necessary for liability to attach to the accomplice).

\textsuperscript{117} See Becher, \textit{supra} note 76 (characterizing Tornado Cash as a Currency Mixer); Smith, \textit{supra} note 25 (defining Currency Mixers as a piece of technology that serves to increase anonymity). See also Opsahl, \textit{supra} note 76 (maintaining that Tornado Cash is computer code).
Cash established an accomplice-principal relationship with a cybercriminal, formed an intent to assist said cybercriminal, and rendered assistance to the cybercriminal for the commission of that crime.  

118 Tornado Cash is an open-source smart contract and, more importantly, lacks that purposive attitude or conscious objective toward the completion of the crime; it merely executes a program based on computer code.

119 While it could be argued that Tornado Cash increased anonymity by obfuscating the identity of the cybercriminals, thereby providing assistance to the cybercriminals, this alone is not sufficient to impose accomplice liability.  

120 It is a necessary element of accomplice liability that the assistance rendered be done with the conscious

---

118 See Exec. Order No. 13694 3 C.F.R. § 1(a)(i) (2015) (declaring accomplice liability as a method of imposing sanctions). See also Grissom, 115 P.3d at 1280 (articulating the elements of necessary to impute accomplice liability on a defendant). “A person is legally accountable as principal for the behavior of another constituting a criminal offense if, with the intent to promote or facilitate the commission of the offense, he or she aids, abets, advises, or encourages the other person in planning or committing the offense.” Id.

119 See Raskin, supra note 26, at 309–10 (providing that a smart contract is simply just a computer running code into an automated executable program). See also People v. R.V., 635 P.2d 892, 895 (Colo. 1981) (affirming the prevailing judicial doctrine on complicity which requires either a purposive attitude or conscious objective on the part of the accomplice towards the completion of the crime).

120 See Harcastle, supra note 31 (condemning Currency Mixers that are used to launder illicit finances to escape “Uncle Sam’s watchful eye.”). See also Rebora, supra note 32 (criticizing Currency Mixers as a money laundering service that cleanses illicit funds and facilitates criminals). See also R.V., 635 P.2d at 895 (distinguishing that the conscious objective to promote or facilitate the commission of the crime is the critical factor in imputing criminal liability).
objective of the successful completion of the crime. Tornado Cash as a smart contract is merely executing programs based on computer running code regardless of whether or not the transaction is criminal or perfectly legal in nature. With this, there is no preference for certain users’ transactions or purposive attitude that one particular transaction be executed over another, and therefore no ability to form an intent necessary for accomplice liability.

---

121 See People v. Lauria, 251 Cal. App. 2d 471, 483 (1967) (holding that knowledge of the principal’s intent is insufficient for the purpose of imputing criminal liability on the accomplice); State v. Galicia, 63 Wn. App. 833, 839 (1992) (declaring that accomplice liability attaches where the accomplice is purposeful in facilitating the principal in the commission of the crime and that knowledge of the conduct alone are insufficient to support liability).

122 See Raskin, supra note 26, at 306–312 (likening a smart contract to that of a vending machine: where the terms of a contract are written into programming languages that are communicated to a machine). “One example of a smart contract is the humble vending machine. If the machine is operating properly and money is inserted into the machine, then a contract for sale will be executed automatically. This is a smart contract.” Id. at 306. The vending machine example shows that the computer code is merely automated on a condition precedent, money being inserted into the machine, to perform the rest of the contract: dispensing the soda. Id. at 307. See also Grewal, supra note 6 (noting that Tornado Cash is used by both innocent people and bad actors).

123 See Brito & Valkenburgh, supra note 6 (noting that Tornado Cash is a tool that is neutral in character). See also Nelson, supra note 26 (detailing the way that Currency Mixers like Tornado Cash work, users determine when funds are withdrawn from the mixing pools).
2. OFAC’s Second Mistake: Precedent Does Not Support the Notion that the Role of Tornado Cash’s Software in the Commission of Cybercrimes Rises to the Level of Material Contribution

OFAC again stretches the meaning of material contribution in EO 13694 to justify their choice to impose sanctions on Tornado Cash when precedent does not support this interpretation of the phrase, “material contribution”. OFAC may impose sanctions upon individuals or entities that

124 See Gonzalez v. Google LLC, 2 F.4th 871, 893 (2021) (reciting Plaintiff’s argument that although Google did not create the illegal content, they created the “mosaics” by which that content is delivered and therefore materially contributed to the unlawfulness of the ISIS content). The court points out the flaw in the plaintiff’s argument by stating that although Google does make the content more accessible to audiences, this service of making the content more accessible does not equate with a material contribution. Id. The software is a neutral tool that delivers content to its users, and Google is neither a content creator nor developer of the unlawful content and is therefore not responsible for what makes the content allegedly unlawful. Id. See also Zeran, 129 F.3d at 330-31 (discussing that Congress has a strong public policy interest in allowing Internet communication to flourish by keeping government interference in the medium to a minimum, targeting the bad actors themselves that use the internet for harms, and decline to impose liability on third parties that serve as intermediaries for the software users).

While Congress acted to keep government regulation of the Internet to a minimum, it also found it to be the policy of the United States “to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.” Congress made a policy choice, however, not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties’ potentially injurious messages. Id. See also 23 Tenn. Juris. § 36 (2022) (explaining that when construing a statute, words should be given their plain meaning). See also Sanctions on Tornado Cash, supra note 84 (announcing that Tornado Cash is being designated pursuant to Exec. Order 13694 for having materially assisted in illicit cyber-enabled activity).
materially assist in malicious cyber-enabled activities. On its face, OFAC has a more convincing basis for sanctioning Tornado Cash on the theory that this technology materially assisted cybercriminals in the commission of their crimes rather than the theory of accomplice liability. However, years of case law and precedent defining what it means to materially assist indicate that the services provided by Tornado Cash do not rise to the level of material contribution.

Under the material contribution test, it must be determined whether or not Tornado Cash was either the host for which the commission of the illegal activity occurred or has done “something more than” its

---

125 See Exec. Order No. 13694 3 C.F.R. § 1(a)(i) (2015) (setting forth that individuals or entities that materially assist in the commission of a malicious cyber-enabled activity may receive sanctions from OFAC).
126 See Jordan-Benel, 2015 U.S. Dist. LEXIS 82220, at 31 (ruling that there must be a material contribution of the unlawful act and a direct connection between the unlawful act and the defendant to impute liability on a charge of contributory infringement).
127 See Jones, 755 F.3d at 411 (giving an example of what a material contribution would look like for a website that solicits, edits, and displays content originating from the third-party users).

A website operator who edits user-created content—such as by correcting spelling, removing obscenity or trimming for length—retains his immunity for any illegality in the user-created content, provided that the edits are unrelated to the illegality. However, a website operator who edits in a manner that contributes to the alleged illegality—such as by removing the word “not” from a user’s message reading “[Name] did not steal the artwork” in order to transform an innocent message into a libelous one—is directly involved in the alleged illegality and thus not immune.

*Id.*
traditional function of mixing coins and making it responsible for the commission of the crime.\(^{128}\) When applying this test, the evidence does not support the inference that Tornado Cash did “something more” beyond its traditional function of mixing Tokens to be characterized as “responsible” for the commission of the alleged cybercrimes.\(^{129}\) Tornado Cash’s computer code dictates that it receives, mixes, and disperses users’ Tokens and nothing more.\(^{130}\) It is against the very nature of the computer code that Tornado Cash is written, and it is outside the realm of possibility for Tornado Cash to deviate from its computer code to perform some other function that constitutes a material contribution.\(^{131}\) With this, it is more appropriate

\(^{128}\) See Doe, 574 F. Supp. 3d at 768 (announcing that material contribution does not refer to merely augmenting or displaying content posted on their website but to actually go beyond and be responsible for what makes the displayed content unlawful).

\(^{129}\) See Henderson, 53 F.4th at 127–28 (distinguishing that liability will attach when the interactive computer service does “something more” than its traditional function).

\(^{130}\) See Opsahl, supra note 76 (computer code). See also Nelson, supra note 26 (specifying that Tornado Cash was using smart contracts to operate and that the software would not be able to begin mixing coins until a user deposited Tokens and specified a destination wallet address). “Before Tornado Cash was taken down, it used smart contracts to accept token deposits from one address and enable their withdrawal from a different address. . . . When ready to withdraw from the Tornado Cash pool, the user provides a recipient address.” Id.

\(^{131}\) See generally Raskin, supra note 26 (stating that smart contracts are written into programming languages that are communicated to the machine). With this, the smart contract performs is running on conditional statements that are translated to the machine into computer code, and once a circumstance occurs, it is then and only then that the smart contract will begin to execute a program. Id. See also Levi & Lipton, supra note 26 (explaining that for a smart contract to work there are certain
to characterize Tornado Cash as a “neutral tool” as it does not encourage or discourage mixing illicit Tokens; rather, it provides a means by which the users may mix their Tokens – licit or illicit.\textsuperscript{132}

\textbf{B. The Concern Regarding Implementation of this Legislation}

Current legislation seems to have no ability to resolve or adequately address the problem that is posed by cybercriminals using Currency Mixers to carry out their financial crimes.\textsuperscript{133} Fraudulent and criminal behavior has become a tangible concern for many parameters that are translated into computer code, and that the smart contract cannot carry out the task until the predetermined condition precedent must occur). “At present, the input parameters and the execution steps for a smart contract need to be specific and objective. In other words, if ‘x’ occurs, then execute step ‘y’. . . . [W]e are, at the very least, many years away from code being able to determine more subjective . . . criteria. . . .” \textit{Id.}

\textsuperscript{132} See Roommates, 521 F.3d at 1186 (explaining that neutral tools merely deliver content in response to the user’s inputs). \textit{See also} Carafano, 339 F.3d at 1121-22 (determining that the dating website in this matter provided neutral tools aimed to match romantic partners depending on their voluntary inputs). More importantly, the website was not transformed into the creator or developer of defamatory content contained in users’ profiles, even though its matchmaking functionality allowed that content to be more effectively dispersed. \textit{Id. See also} Gonzalez, 2 F.4th at 893 (2021) (discussing neutral tools as seen in Carafono). “Critically, Carafano’s ‘neutral tools’ were neutral because the website did not ‘encourage the posting of defamatory content’ by merely providing a means for users to publish the profiles they created.” \textit{Id.}

\textsuperscript{133} See Singer, supra note 1 (outlining the difficulty Congress has had in properly regulating cryptocurrency and other digital assets). “Care must be taken, though. Not any sort of lawmaking will do. It’s important that Congress takes the time to really learn about cryptocurrencies and blockchain technology. Otherwise, ‘reactive policies that do not take into consideration the unique aspects of the industry could have disastrous impacts . . .’.” \textit{Id.}
cryptocurrency users. With this, members of the financial technology community have advocated for new legislation within a federal regulatory framework that is tailored specifically to digital assets so it better addresses the situation.

Tornado Cash, like the Internet, is a tool that is used by several users, both innocent and cybercriminals. When the Internet is used to commit a cybercrime, government agencies do not respond by shutting down or sanctioning the Internet because criminals have used

134 See Haar, supra note 8 (echoing the concern of cryptocurrency investors).

For many crypto enthusiasts, the decentralized nature of digital currencies—which, unlike traditional currencies, aren’t backed by any institution or government authority—is a big draw. But regulatory guidance can help protect investors. ‘... I am glad that they are paying attention because unfortunately with cryptocurrency, there are a lot of scams,’ says Kiana Danial...

Id.

135 See Singer, supra note 1 (arguing that in order to properly regulate this emerging area of law, legislators must educate themselves on blockchain technology and cryptocurrency, and in turn, tailor new legislation to match this new area of law). See also Haar, supra note 8 (proposing that legislation should be new and intended for digital assets not other traditional securities).

136 See Grewal, supra note 6 (articulating that Tornado Cash is a neutral technology that is used for licit and illicit means). “Tornado Cash... [is] a tool legitimately used by many innocent people even if also by some bad actors.” Id. See also Perper, supra note 35 (taking the position that there are several legitimate and licit reasons that one would want to use a Currency Mixer, one of the most prevalent reasons being user privacy).
its services for an illicit purpose. Rather, law enforcement tends to respond by going after the individual bad actor.

If federal regulatory agencies continue regulating in this holistic way, this creates a concerning precedent for future software developers and innovators. For example, how is the developer of a future technology supposed to know that his technology will be used

---

137 See Grewal, supra note 6 (establishing that the government typically enforces punishments on individual bad actors rather than a whole technology). “After all, we do not shut down email or the internet code because among its many users are some criminals.” Id. See Armstrong, supra note 7 (comparing OFAC’s sanctions against Tornado Cash to shutting down a highway because it was used to flee a crime scene). “Sanctioning open source software is like permanently shutting down a highway because robbers used it to flee a crime scene. It’s not the best way to solve a problem. It ends up punishing people who did nothing wrong and results in people having less privacy and security.” Id.

138 See Armstrong, supra note 7 (characterizing OFAC’s choice to sanction an entire piece of technology as opposed to the specific individual bad actors as an “unprecedented step”). See also Grewal, supra note 6 (expressing the concern in OFAC’s precedent method of regulating these cybercrimes by sanctioning an entire piece of open-source technology, and the concerns that come along with electing to do this rather than targeting specific actors). “However, in the Tornado Cash action, OFAC did not target the bad actors or the property controlled by those actors; instead, it took the unprecedented step of sanctioning open source technology – a tool legitimately used by many innocent people even if also by some bad actors.” Id.

139 See Armstrong, supra note 7 (expressing a concern for how the sanctions against Tornado Cash pose a threat to future technology innovators in that they cannot anticipate whether or not their technology will be used for licit or illicit means).

Finally, sanctioning open-source code has a chilling effect on innovation. Right now, developers are worried that they could be held responsible for something they had nothing to do with, and no ability to control. At a time when we should be encouraging innovation, this kind of fear and uncertainty will do the opposite – making developers wonder if, by pushing the industry forward, they could be putting themselves at risk.

Id.
to commit illicit acts?\textsuperscript{140} We do not want to set a precedent that sanctions the technology and, therefore, punishes the developer who did not intend for his technology to be used for harm.\textsuperscript{141} With this, any proposed regulation that is drafted should be kept in the context of punishing the malicious actors, not the technology that made itself possible.\textsuperscript{142} Furthermore, OFAC should remove Tornado Cash from their designated list as the technology is a neutral tool that was used by malicious actor to carry out illicit activities.\textsuperscript{143} Legislators and government officials need to take the time to work with financial technology companies and scholars to educate and familiarize

\begin{quote}
Tornado [Cash] itself isn’t “good” nor “bad”, it is just a tool that allows for privacy in financial transactions. Setting the precedent that individual developers are liable for the actions other’s take using open source software is dangerous. It stifles innovation by making creators fearful of what might happen should they push the boundaries or invent something new.
\end{quote}

\textit{Id.}

\textsuperscript{140} See id. (articulating the worrying environment that now surrounds future software developers and innovators in that they do not know their invention will put them at legislative and regulatory risk).

\textsuperscript{141} See What Happened to Tornado Cash?, supra note 9 (evaluating the stifling effects this sanctioning can have on future software developers and technology innovators).

\textsuperscript{142} See Brito & Valkenburgh, supra note 6 (pointing out the danger in sanctioning a tool that is of neutral character that can be put to bad or good use). See Singer, supra note 1 (stressing the importance of lawmakers becoming educated on cryptocurrency and blockchain technology before enforcing regulation).

\textsuperscript{143} See Sanctions on Tornado Cash, supra note 84 (placing Tornado Cash on their designated list pursuant to EO 13694). See also Roommates, 521 F.3d at 1171 (defining a neutral tool as a technology that responds to the users’ inputs).
themselves with digital assets and other new areas of technology.\textsuperscript{144} It is only until this is done that OFAC and other government agencies can properly draft rules and regulations rather than superimposing inapplicable existing legislation onto digital assets and other blockchain technology, effectively putting the blame in an inappropriate place.\textsuperscript{145}

\textbf{V. CONCLUSION}

Cryptocurrency, Currency Mixers, and the rise of digital assets have made an incredible impact on the Fintech community and will continue to do so in our financial, regulatory, and judicial systems. The challenge now lies in our legislative systems to create an independent regulatory framework to address the concerns that belies the digital asset market: fraud, massive heists, and money laundering. Right now, software that was intended to increase user anonymity has now become equated with the perpetrator of these types of crimes. While Currency Mixers are used by cyber criminals to commit such

\textsuperscript{144} See Singer, \textit{supra} note 1(beckoning legislators to take the time to learn and understand cryptocurrencies and blockchain technology before attempting to regulate them).

\textsuperscript{145} See Grewal, \textit{supra} note 6(arguing that by applying this legislation to designate Tornado Cash, OFAC is effectively targeting a neutral piece of technology rather than targeting the malicious actors who used the technology for illicit purposes).
cybercrimes, placing the blame on a piece of technology is placing the fault in an incorrect place. Instead, OFAC and other regulatory agencies must address these penalties on the malicious actors rather than the software that assisted in the commission of their crime. Extending pre-existing legislation, such as EO 13694, is a misapplication of the law. It is quite apparent that cryptocurrency and the digital asset market are going to continue to expand. With this, ill-informed regulation such as this creates an alarming precedent for future software developers. Instead, regulators must adapt by creating a separate regulatory framework to tailor their legislation to digital assets and its appurtenances.