

Are Crypto Anti-Money Laundering Policies Effective?^{*}

John M. Griffin[†]

Kevin Mei[‡]

Zirui Wang[§]

September 6, 2026

Abstract

We evaluate two major types of crypto enforcement actions: policies targeting services and policies targeting users. First, sanctions against the Tornado Cash mixer resulted in an 80.4% decline in hacker illicit inflows and shifted their usage toward more traceable swaps and bridges. Second, overseas exchange acceptance of illicit funds declines only after the U.S. DOJ settlements. Third, OFAC sanctions against individuals are relatively rare and often after the funds have left the wallets. Fourth, after Tether freezes, criminals continue to use related wallets. Overall, anti-money laundering policies targeting services like mixers and exchanges appear more effective than policies targeting users.

JEL classification: G18, G23, G28, K24, K42

keywords: Anti-Money Laundering Policies, Crypto Flows, DeFi, Tornado Cash, Stablecoins

^{*}We thank Zahi Ben-David, Ben Charoenwong, Sudheer Chava (discussant), Sanjiv Das (discussant), Darrell Duffie, Cesare Fracassi, Zhiguo He, Sam Kruger, Chen Lin, Yukun Liu (discussant), Yiming Ma, Tom Meling, Andrey Ordin, Aaron Pancost, Alex Pettyjohn, Daniel Rabeti (discussant), Fahad Saleh, Amin Shams, René Stulz, Qiang Wang (discussant), and Stefan Zeume (discussant), as well as conference and seminar participants at the Asian Blockchain & Crypto Conference (ABC²), 2025 CEAR-CenFIS Conference at Georgia State University, Financial Intermediation Research Society (FIRS) 2026 Annual Meeting, JOIM Fall Conference 2025, Midwest Finance Association (MFA) 2026 Annual Meeting, NBER Economic Analysis of Regulation 2026, Northern Finance Association (NFA) 2025 Annual Meeting, Stanford Institute for Theoretical Economics (SITE) Financial Regulation Conference, the Ohio State University, and the University of Texas at Austin for their helpful comments. We especially thank J. A. Artero Calvo for excellent research assistance. Mei thanks the University of Texas, where he performed much of this research as a PhD student. We additionally thank Integra FEC for the use of their tracing tools and for substantial crypto-research support. Griffin is an owner of Integra FEC and Integra Research Group, which engage in financial consulting, research, and recovery on a variety of issues related to the investigation of financial fraud, including crypto-related activities.

[†]McCombs School of Business, University of Texas at Austin. John.Griffin@utexas.edu

[‡]Gatton College of Business and Economics, University of Kentucky. Kevin.Mei@uky.edu

[§]McCombs School of Business, University of Texas at Austin. Zirui.Wang@utexas.edu

Whereas the traditional banking sector has well-established anti-money laundering (AML) procedures, policies, and protocols, those in the crypto arena are relatively nascent and in flux. There is a general lack of understanding regarding whether crypto AML policies are enforced, useful, and effective in accomplishing their goals. What are the economic magnitudes of their impact? Through which channels do they operate? What substitutes emerge in response? Answering these questions could help inform policy design and enforcement priorities. Recent changes in the regulatory and enforcement environment provide an empirical testing ground to examine the implementation and efficacy of different forms of AML enforcement protocols.

Money laundering is the process of moving and concealing the origins of illicit proceeds to integrate them into the legitimate financial system and enable their unrestricted use. Anti-money laundering laws are deeply ingrained in the modern financial system, particularly following September 11, 2001, as controls to reduce terrorist financing and other criminal capital flows. The theoretical motivation from the [Becker \(1968\)](#) crime model suggests that to deter crime, one needs to increase the likelihood of being caught and the fine when punished. The goal of AML policies and their enforcement is to increase the probability of detecting both criminals and money launderers, and to punish, to the extent that it results in the forfeiture and possible fine of funds ([Ferwerda, 2009](#)).

Evaluating the AML framework is difficult because of the limited availability of reliable and detailed data. [Chong and Lopez-De-Silanes \(2015\)](#) outline two contrasting views on whether AML laws matter: A) the conventional view, which holds that AML laws reduce crime by blunting their profitability, and B) the skeptical view, which emphasizes that efforts are best spent on targeting the root sources of crime and not on regulating money services.¹ [Levi, Reuter, and Halliday \(2017\)](#) detail how there is little reliable data to evaluate AML efforts and that regulation is largely unguided by analysis. Within the cryptocurrency environment, we compile a large amount of detailed data on illicit funds that is typically private within banks and not available for researchers.

In this paper, we empirically evaluate the effectiveness of crypto AML policies and procedures by

¹Consistent with the skeptical view, [Cuéllar \(2002\)](#) argues that there is a tenuous relationship between AML regulations and reducing crime, despite the large costs of implementation, reduction in privacy, and negative externalities such as reducing access to the banking system. [Pol \(2020\)](#) argues that there are few outcome metrics to measure AML effectiveness, criminals keep up to 99.95% of criminal proceeds, and that the policies actually enable all forms of serious criminal activity.

utilizing regulatory and court orders as policy shocks. We process 6.19 terabytes of Ethereum transaction and event data as of December 31, 2025, to trace the flow of illicit funds through the blockchain. We organize our analysis around two types of policies: policies targeting *services*, including the high-profile 2022 Tornado Cash sanctions and 2023-2025 U.S. Department of Justice (DOJ) settlements with exchanges, and policies targeting *users*, including sanctions by the U.S. Treasury’s Office of Foreign Assets Control (OFAC), and stablecoin freezes. We define services as the intermediaries that facilitate the flow of funds and users as specific individuals or organizations with dark money that attract scrutiny from OFAC and other regulators. We evaluate both direct effects and substitution effects of policies.

Our first hypothesis and line of inquiry for each enforcement event is whether the amount of criminal activity through the targeted money laundering channel decreased after the enforcement event at the sanctioned service or user wallet. Alternatively, if crypto users ignore the sanction, activity by the entity or user wallet may remain unchanged after the sanction. Our second hypothesis for each event is whether and where criminal activity migrated. If criminal activity migrated, we examine (when possible) if the alternative channel is more or less transparent than the original channel.² For example, for the Tornado Cash sanction, we examine if the sanction reduced criminal activity in Tornado Cash or alternatively if the amount of criminal activity is similar after the ban. To test for substitution effects of sanctions against Tornado Cash, we analyze other potential avenues that criminals could use to evade sanctions and examine whether there was an increase or decrease in privacy coin usage, and in other forms of evasion such as decentralized finance (DeFi) bridges and swaps.³

Our findings show that Tornado Cash, an Ethereum mixer that obfuscates the origin of funds, handles considerable criminal flows from more sophisticated cyber-criminal gangs, with the Lazarus Group from North Korea being the largest identified user. In the six months following the August 2022 sanctions, total Tornado Cash inflows declined by 85.95%, while hacker-originated inflows declined

²A key challenge in studying AML is that while we observe some flagged criminal activity, we do not observe total criminal activity, nor off-chain money laundering such as cash-based methods. When examining entities, we can examine if criminal activity migrates to alternative mechanisms, but this is difficult to analyze for individual actions against users.

³Bridges accept deposits on one blockchain and remit them to addresses on a different blockchain. Swaps exchange one type of crypto for another on the same blockchain. Mixers accept deposits from customers into a common liquidity pool and remit to other addresses such that inbound and outbound transactions cannot be linked.

by 80.38%, relative to the preceding six months. A formal difference-in-differences (DiD) analysis comparing hacker flows to Tornado Cash with flows from the same hackers to overseas exchanges further shows that hackers reduced their use of Tornado Cash. Western exchanges handled far fewer Tornado Cash receipts after the ban.⁴ The probability of correctly matching transactions from the largest mixer user during a given week increases from 12.9% before the sanctions to 21.3% afterward, indicating that the decline in volume renders the mixer less useful for obfuscation.

After documenting the direct effects of the Tornado Cash sanctions, we next turn to study substitution effects by measuring whether illicit flows migrate to privacy chains and bridges. We find that the privacy coins Monero, Dash, and Zcash surprisingly on average experience a decline in the number of transactions following sanctions. Instead, hackers move money through DeFi swaps and bridges, outlets that obfuscate transactions for standard tracing tools, but are nevertheless traceable with additional work. Additionally, we examine the recent Bybit hack by North Korea and find that the funds did not utilize Tornado Cash. After a long series of obfuscating transactions, the majority of flows used the Thorchain bridge to move from Ethereum to Bitcoin and are stored across multiple wallets that are mostly observable on the blockchain. Overall, the sanctions against Tornado Cash decreased the amount of criminal flows to Tornado Cash, and hackers switched to more traceable methods.

Our analyses focus on the potential effects on criminals. However, the ban may have had negative externalities on those using Tornado Cash for legitimate purposes. This is difficult to assess, but as a limited case study, we analyze Ukrainian crypto donations. Various Ukrainian donation addresses received a total of \$113 million in crypto, but only \$1.77 million utilize Tornado Cash as compared to over \$2 billion in criminal hacker flows.

We next consider whether U.S. DOJ settlements with centralized exchanges deter illicit behavior. Centralized exchanges are potentially important because they are the main off-ramp and source of liquidity to convert crypto funds to fiat. The largest overseas exchange, Binance, continued to receive considerable sanctioned funds from Tornado Cash after sanctions were enacted and flows persisted

⁴We use Western exchanges to refer to Coinbase, Crypto.com, Gemini, and Kraken because they are some of the largest exchanges that can be accessed from North America and Europe over the 2020 to 2025 sample period and are registered with the Financial Crimes Enforcement Network (FinCEN).

all the way up to the month that Binance settled with the DOJ in November 2023. These findings support the claims in the DOJ settlement that Binance ignored AML monitoring procedures and are inconsistent with claims that the charges against Binance were without merit. OKX also continues to receive large amounts of sanctioned Tornado Cash flows after the 2022 ban, but experiences a sharp decline in flows four months prior to OKX's February 2025 DOJ settlement. Overall, stricter enforcement of AML in exchanges appears to reduce tainted flows.

The second main type of enforcement is investigations into specific individuals or organizations. We examine crypto addresses of individuals or organizations on the OFAC sanctions list, which includes 522 Bitcoin addresses and 183 Ethereum addresses. We find sanctions are often imposed too late and after funds have left addresses. Approximately 58,000 Bitcoin (BTC), worth \$1.1 billion, and 234,000 Ether (ETH), worth \$593 million, have passed through sanctioned addresses associated with users, after netting flows recirculated between sanctioned addresses. 51% of sanctioned BTC flows remain on-chain without being off-ramped to a service. For sanctioned Ethereum assets, 78% of capital flowing through wallets moves to Tornado Cash to evade sanctions and only 3.96% of total funds moving through the addresses (or \$27 million) remains observable on-chain.

We next study freezes by stablecoin issuers.⁵ In total, we find that over \$1.92 billion in Tether and \$113 million in USDC have been frozen. Stablecoin freezes are much more sizeable than OFAC sanctions but still appear small relative to the underlying criminal flows. We also analyze substitution effects to other addresses related to the criminal freeze and find that related deposit address activity increases by more than 48.4% compared to the control group. The flow to DeFi swaps and services also increased by 11.48 percentage points compared to a control group, presumably to obfuscate their flows.

Overall, anti-money laundering policies that target services appear more effective at reducing criminal activity in those entities than those that target users primarily because services reduce feasible substitutes for users. After sanctions against Tornado Cash, illicit actors like hackers sponsored by North Korea have switched to more transparent venues, like bridging to Bitcoin, and we do not

⁵Stablecoins are cryptocurrency tokens that can be redeemed for a defined fiat amount, such as \$1.

observe an increase in activity on privacy-focused blockchains. On the other hand, while policies targeting users restrict the targeted assets, we find that sanctions are infrequent, late, and commonly evaded by switching to new wallets or using mixers such as Tornado Cash. Our analysis has limitations in that we observe only a subset of illicit crypto activity and do not observe off-chain illicit activity; our results capture displacement across the observable crypto channels we study and not changes in total illicit activity. Additionally, we examine only the potential effectiveness of sanctions and not the costs of sanctions in terms of spending by government agencies, compliance costs by services, nor the costs on potentially legitimate users.

We speak to ongoing policy debates. First, as of September 2026, the Senate is deliberating the Digital Asset Market Clarity Act (CLARITY Act), which is new legislation that would determine whether DeFi services should be exempt from AML requirements.⁶ Our findings show that DeFi, including mixers, bridges, and swaps, obfuscate substantial criminal flows. Criminals do not appear to be concerned that these services will reject their transactions, and illicit funds including those from foreign actors coming out of DeFi services often go directly to major crypto exchanges, suggesting self-policing by exchanges has been ineffective. Second, the GENIUS Act, signed on July 18, 2025, requires stablecoin issuers to comply with U.S. law enforcement requests for asset freezes.⁷ Our findings indicate that requiring services such as stablecoin issuers to comply with law enforcement is likely useful, but insufficient if illicit flows quickly switch to non-seizeable venues. Third, on April 7, 2025, a DOJ order by then-Deputy Attorney General Todd Blanche, who was later elevated to Attorney General, stated that the DOJ “will no longer target virtual currency exchanges, mixing and tumbling services, and offline wallets for the acts of their end users or unwitting violations of regulations,” but will instead hold accountable individuals who cause harm to digital asset investors or use digital assets for various forms of organized crime.⁸ At the same time, the U.S. government appears to be taking a more

⁶Arguments for exempting DeFi from AML requirements are that compliance is too onerous for DeFi startups, that exemptions are necessary because builders will simply move to jurisdictions with weaker laws, or that the ecosystem will self-enforce. Major industry participants have advanced self-regulation proposals asserting that the crypto ecosystem can effectively police itself. Examples include Gemini’s [Proposal for a Self-Regulatory Organization](#) (2018), Coinbase’s [Digital Asset Policy Proposal](#) (2021), and the INATBA’s proposal on [DeFi Self-Regulation](#) (2025).

⁷See [Congress.gov website](#) for more details about the Guiding and Establishing National Innovation for U.S. Stablecoins Act of 2025, or GENIUS Act.

⁸More information is available in the [pdf linked here](#).

aggressive stance on drug cartels and foreign actors such as Iran and North Korea. Given our findings, the DOJ's goal of pursuing organized crime, including foreign actors, may be substantially impeded without also targeting the mixing and tumbling services that obfuscate their funds. As suggested by the judge who issued the ruling lifting the Tornado Cash ban, Congress should consider legislation that will ban mixers and other technologies that specialize in laundering funds from criminal actors.⁹

Related Literature. Our paper relates to two main strands of literature. First, in addition to the literature outlined above, we further contribute to the literature on crime and money laundering. [El Siwi \(2018\)](#) notes that recognizing “money is the lifeblood of organized crime” led to the adoption of the AML regime in Italy.¹⁰ [Campbell-Verduyn \(2018\)](#), [Al-Tawil \(2022\)](#), and [Wronka \(2023\)](#) overview money-laundering laws and procedures, the potential challenges of application to cryptocurrencies, and policies across countries. [Levi \(2015\)](#) surveys the literature on financing for organized crime and notes that empirical evidence is primarily limited to prosecuted case records. Our paper focuses on understanding the efficacy of money-laundering policies in the crypto space, where criminal activities can actually be partially measured and the regulatory landscape is rapidly evolving.

Second, there is a literature examining dark market activity in the crypto space. [Meiklejohn, Pomarole, Jordan, Levchenko, McCoy, Voelker, and Savage \(2013\)](#), [Sokolov \(2021\)](#), and [Amiran, Jørgensen, and Rabetti \(2022\)](#) examine the role of Bitcoin in the Silk Road (2011-2013), ransomware, and terrorism financing. [Foley, Karlsen, and Putniņš \(2019\)](#) find that 46% of non-exchange-related Bitcoin activity from January 3, 2009 to April 2017 is associated with darknet websites from 27 million Bitcoin users. [Makarov and Schoar \(2025\)](#) find substantially less criminal activity in Bitcoin from 2009-2025.¹¹

⁹The judge issuing the ruling that OFAC did not have the authority to ban code noted that “OFAC’s concerns with illicit foreign actors laundering funds are undeniably legitimate. Perhaps Congress will update IEEPA, enacted during the Carter Administration, to target modern technologies like crypto-mixing software.”

¹⁰[Mirenda, Mocetti, and Rizzica \(2022\)](#) show how organized crime utilizes cash and shell companies to obfuscate transactions entering the banking system. [Moore, Clayton, and Anderson \(2009\)](#) survey the economic structure of online crime and recommend more private data sharing and police enforcement focused on online gangs. [Leukfeldt, Kleemans, Kruisbergen, and Roks \(2019\)](#) find that technological knowledge for cybercrime in the Netherlands is often gained through a smaller set of technically skilled enablers in online marketplaces. [Draca and Machin \(2015\)](#) survey a growing literature on the economic incentives for crime. Dirty money also distorts macroeconomic capital allocations ([Tanzi, 1996](#); [Quirk, 1996](#)) and [Fracassi, Lee, and Roukny \(2025\)](#).

¹¹[Griffin, Wang, and Artero Calvo \(2026\)](#) measure the total illicit flows in Ethereum, Tron, and Bitcoin from various types of illicit activity moving through exchanges. [Chainalysis \(2026\)](#) provides an industry survey and examples of various types of criminal activity and calculates total illicit activity.

Griffin and Mei (2025) map the flows of pig butchering scams by tracing the flows and showing how criminal flows are leaving Western-based exchanges and entering centralized exchanges after moving through DeFi swaps. Cong, Harvey, Rabetti, and Wu (2025) show that 43 ransomware gangs carried out 2,690 attacks from May 2019 to July 2021. They also describe how ransomware gangs may rebrand to avoid enforcement such that sanctions may backfire, which is a theme we explore in investigating how hackers may move to more or less transparent arenas. Cong, Grauer, Rabetti, and Updegrave (2023a) provide a useful overview as well as concrete examples of various crypto investment scams, Ponzi schemes, ransomware, money laundering, and dark markets. Nguyen and Putniņš (2023) study 123 hacks and document that investors respond by systematically withdrawing assets from exchanges.¹² Charoenwong, Kim, Kirby, and Reiter (2026) examine the timing of OFAC blacklist enforcement in DeFi and argue that wallet creation and fund dispersions outpace address-based enforcement. We provide the first systematic examination of AML laws in the crypto space.

1. Crypto AML Background, Hypotheses, Data, and Methodology

This section describes the background of crypto AML policies, hypotheses, data, and methodology.

1.1 Crypto AML Policy Background

After the terrorist attacks on September 11, 2001, the U.S. extended the existing anti-money laundering framework of the Bank Secrecy Act and increased cooperation across countries through new international initiatives from the Financial Action Task Force (FATF). Anti-money laundering laws and enforcement may be the primary means of deterring activity in important settings such as terrorism and crimes committed by foreign nationals, where authorities may not have the ability to apprehend criminals in non-cooperative nations. Many of the basic principles are now being questioned by a crypto industry born as an alternative financial system and growing in size and political influence.

Cryptocurrency’s appeal is in its potential as an alternative financial system free from regulation.

¹²This literature also fits within a larger literature of other types of nefarious trading activity in crypto, including price manipulation (Gandal, Hamrick, Moore, and Oberman, 2018; Griffin and Shams, 2020), pump-and-dump schemes (Li, Shin, and Wang (2025), Hamrick, Rouhi, Mukherjee, Feder, Gandal, Moore, and Vasek (2021)), scams (Phua, Sang, Wei, and Yu, 2025), insider trading (Félez-Viñas, Johnson, and Putniņš, 2022), and wash trading (Pennec, Fiedler, and Ante, 2021; Cong, Li, Tang, and Yang, 2023b) as briefly surveyed by Griffin and Kruger (2024).

However, to interact with the global banking system, centralized crypto exchanges must authenticate the identities of new users through anti-money laundering and know your customer (AML/KYC) processes. Most exchanges purport to monitor transactions through know your transaction (KYT) policies to avoid receiving funds from known criminals. Since investors need trust for meaningful investments to occur, the crypto ecosystem also has an incentive to root out bad actors as it seeks to be an alternative means of raising capital for legitimate activity. The trade-off is that monitoring can be costly, reputational risk may be less pertinent with new players in the crypto world, and lax monitoring may lead to more transactions and fees for crypto intermediaries.

The regulatory and enforcement environment is in flux. On August 8, 2022, OFAC sanctioned Tornado Cash in response to its use by hackers sponsored by the Democratic People’s Republic of Korea (DPRK) and thus prohibited the U.S. financial system from accepting related funds. A lawsuit challenging the sanctions, with the financial backing of large players in the crypto industry, argued that such a precedent would put undue responsibility on developers to prevent criminals from using their services.¹³ The sanction designation was overturned on November 26, 2024, when an appellate judge ruled that Tornado Cash’s immutable smart contracts are not “property” and thus OFAC did not have authority to ban their use, and OFAC lifted sanctions on March 21, 2025.^{14,15} On a separate track, the U.S. DOJ prosecuted and fined large international crypto exchanges such as Binance (November 21, 2023) and OKX (February 24, 2025) for their lax AML procedures. As part of their settlements, the exchanges agreed to more rigorous monitoring procedures and DOJ oversight. We use these shocks to study how users and exchanges respond to AML enforcement actions.

1.2 Hypotheses

We next develop hypotheses that follow from [Becker \(1968\)](#) and the policies described above. The market for crypto money laundering consists of many types of users and types of money laundering

¹³As reported [by Reuters](#) and discussed in a [Coinbase blog post](#).

¹⁴More information can be found [in this court ruling](#).

¹⁵When the Fifth Circuit ruled, Paul Grewal, Chief Legal Officer at Coinbase, remarked that: “Privacy wins. Today the Fifth Circuit held that U.S. Treasury’s sanctions against Tornado Cash smart contracts are unlawful. This is a historic win for crypto and all who cares about defending liberty. Coinbase is proud to have helped lead this important challenge.” More information can be found [here](#).

services. Users pick services by comparing the expected benefits of successful laundering to the expected costs, which include transaction costs and risks of being detected. The following hypotheses consider how regulation impacts user decisions based on the types of services available.

Anti-money laundering (AML) policies increase the probability that illicit activity is detected, which may lead to subsequent enforcement and reduce the expected profitability of illicit activity. Thus, rational criminals facing strong AML policies in a specific channel may choose to reduce or cease activity in that channel.¹⁶

Hypothesis 1. *Total flows and observable illicit flows decline after AML policies are enacted against a crypto service or user.*

In our setting, we interpret declines in activity within a given venue as the direct effects of AML policies. Alternatively, if the policies have weak enforcement mechanisms and entities do not abide by the policies, we may not see a decrease in activity.

The many types of users of a service may also differ in the strength of their preferences for privacy and in the benefits they derive from successful money laundering. Observed post-policy activity may increasingly reflect the behavior of users with the strongest incentives to obtain privacy or launder funds. In a frictionless competitive market, impacted users may migrate to new substitute venues for money laundering, particularly in crypto, where barriers to entry are relatively low compared with those in the traditional financial system. However, liquidity (Easley, O'Hara, Yang, and Zhang, 2026) and coordination (Auer, Monnet, and Shin, 2025) are also important for the crypto market in general, especially in privacy services that require liquidity from a variety of players to properly hide funds. Criminals face trade-offs between choosing venues that vary in liquidity, security (in whether digital assets can be feasibly seized or frozen), and transparency (in whether transactions are opaque or can be traced). We hypothesize that illicit funds migrate to alternative areas.

Hypothesis 2A. *Illicit flows may migrate to alternative channels for money laundering after AML policies are*

¹⁶As the costs of regulation increase, those with relatively low benefits from private transactions may leave to find other venues for privacy, while those with relatively high benefits may remain, such as illicit actors with very large flows.

enacted against a given crypto service or user.

If criminals previously relied on opaque venues and sanctions began to target opacity, then illicit flows may be forced to re-optimize to more liquid venues. Liquid venues may then attract more types of users and thus overall flows may be more transparent.

Hypothesis 2B. *After sanctions, illicit activity migrates to more transparent venues.*

Alternatively, if a multitude of liquid privacy options exist, sanctions could have the reverse effect of criminals moving into other channels of similar or even less transparency, such as privacy coins. It is important to note that substitution effects may be difficult to detect empirically as there are many possible avenues to which activity could migrate. We test Hypothesis 2B primarily for services because we can examine changes in levels of each service or channel in aggregate. At the user level, it is difficult to ascertain changes in transparency (in the form of rotation to privacy chains) because we typically do not observe user-level flows to these venues.

The extent of substitution may depend on frictions in the market for that service. For example, spillovers may arise if privacy services are complements or depend on a common pool of liquidity or coordination. Regulation in one domain may also increase the perceived or actual costs of using related services. Overall, for each policy targeting services and users, we evaluate the hypotheses by measuring direct effects and substitution effects.

1.3 Data

We primarily use two types of data: blockchain transaction data and attribution data. Blockchain transaction data is sourced from the Bitcoin and Ethereum blockchains. Importantly, the fields include the blockchain address of the sender and receiver, which allows us to construct paths of flows between addresses. We study both Bitcoin and Ethereum, with greater emphasis on Ethereum because that is where Tornado Cash, a high-profile mixer, exists. We analyze the Bitcoin blockchain for an analysis of additional OFAC addresses, the Bybit hack, and for additional robustness tests. We additionally use data on the Monero, Dash, and Zcash blockchains from bitinfocharts.com and validate the Monero

data using moneroblocks.info. We use data from coingecko.com on end-of-day cryptocurrency prices to convert Ethereum and Bitcoin values to dollars.¹⁷ Beyond cryptocurrency transfers, we also process data on swaps and bridges to follow relevant funds. On Google Cloud BigQuery, our current mode of access, the total Ethereum blockchain amounts to 6.19 terabytes of data as of December 31, 2025.¹⁸

We use a rich set of sources for attribution data. First, we use data from online sources, such as blockchain.com and etherscan.io, to label addresses that belong to known entities. We focus on service providers such as centralized exchanges, decentralized exchanges, bridges, or mixers. Second, we collect all addresses sanctioned by OFAC, as well as all Ethereum-based addresses where the stablecoin issuers of Tether and USDC have seized assets. Third, we use and extend the hacker data collected in [Griffin and Mei \(2025\)](#). We identify hacker addresses using OFAC and FBI reports, Chainalysis, and Chainabuse. In Chainalysis, we include addresses labeled as stolen funds or illicit actors, and in Chainabuse, we use victim reports classified as contract exploits. We use these reported hacker addresses to trace their flows and study changes in behavior around the Tornado Cash sanctions.

1.4 Methodology

We use blockchain data to construct a network of related addresses and analyze their characteristics to understand how the network responds to AML regulations. In this subsection, we provide an overview of the methodologies used to identify related addresses, including tracing and address clustering.¹⁹

Tracing organizes transaction-level data into a framework that delineates the path of transaction flows of subsequent addresses. Tracing methods are an area of growing academic research ([Anderson, Shumailov, and Ahmed, 2018](#); [Möser and Narayanan, 2019](#); [Tironsakkul, Maarek, Eross, and Just, 2022](#)) and are commonly used by law enforcement, through service providers like Chainalysis and TRM Labs, to follow capital flows. Tracing is essentially a program with a series of steps to follow crypto fund flows to stopping points such as centralized exchange hot wallets. We utilize data from the tracing

¹⁷When converting cryptocurrency value to dollars, we assume prices for the stablecoins Tether, USDC, and DAI are \$1.

¹⁸The Ethereum blockchain data consists of two primary tables on Google Cloud BigQuery: the *transactions* table (3.28 TB), which records transaction-level details such as sender, recipient, ETH value transferred, and contract interactions; and the *logs* table (2.91 TB), which stores all smart contract event logs, including token transfers, swaps, and other contract events, emitted during transaction execution.

¹⁹Additional information about tracing and clustering (including gas clustering, deposit address clustering, and co-spending) are in Internet Appendix [A](#).

platform more fully described by [Griffin and Mei \(2025\)](#) in the context of pig butchering scams.²⁰ By using tracing data, we seek to only follow flows that are highly likely to be controlled by reported criminal addresses, instead of implicating all downstream addresses and their respective funds. In the analysis below, we “trace” all outflows from Tornado Cash and OFAC-sanctioned addresses. We also “backtrace” all funds entering Tornado Cash and OFAC-sanctioned addresses to their originating source. For services like Uniswap, Wrapped ETH, and bridge contracts, we trace through DeFi to continue following the paths of tainted transactions.

In addition to tracing, we apply clustering methods to extend our network to find addresses that are highly likely to be related to an address of interest, similar to [Foley, Karlsen, and Putniņš \(2019\)](#). We use three clustering methods: gas clustering and deposit address clustering heuristics on Ethereum, and co-spending on Bitcoin. Gas clustering arises when two addresses may share the same “funding” address, or the first instance of receiving a small amount of Ether, the native currency of Ethereum.²¹ Deposit address clustering arises when two exchange deposit addresses receive funds from the same sender. The rationale is that deposit addresses are sensitive information like a bank account number, and therefore, if one sender transfers funds to two different deposit addresses, then it is likely that the two deposit addresses are linked, as discussed in [Victor \(2020\)](#) and applied at large scale by [Griffin and Mei \(2025\)](#).²² The co-spending heuristic relies on the unspent transaction output (UTxO) properties of Bitcoin such that input addresses on a transaction are deemed to have a common owner. We use all three methods to define related addresses that serve as a “treated” group when measuring substitution effects for OFAC sanctions against users and stablecoin freezes.

2. Policies Targeting Services

We first examine AML enforcement actions directed at crypto services. We study two settings: OFAC sanctions against Tornado Cash and DOJ enforcement against centralized exchanges. We examine

²⁰The platform for collecting tracing data has been developed and maintained by Integra FEC.

²¹The rationale is that all addresses need Ether because blockchain transaction costs can only be paid in Ether. Therefore, we associate the first funder to link potentially related addresses. This idea is incorporated in services like Etherscan, the most popular service to view Ethereum transactions, where they display the first gas funder for every wallet.

²²On most centralized exchanges, each deposit address is linked to a specific customer account, and users can often generate new deposit addresses at no cost.

both their direct effects on targeted flows and the substitution channels.

2.1 Tornado Cash Sanctions

Tornado Cash is the most well-known mixer on Ethereum. On August 8, 2022, OFAC sanctioned Tornado Cash, citing its use to launder more than \$7 billion in virtual currency since 2019, including more than \$455 million stolen by North Korea’s Lazarus Group. The sanctions prohibited the U.S. financial system from accepting related funds. This ban was overturned by a U.S. appeals court on November 26, 2024, and lifted by OFAC on March 21, 2025. We use this regulatory timeline to study how crypto activity interfaces with Tornado Cash before, during, and after the ban. We begin with an overview of aggregate fund flows, then address the hypotheses around direct effects and substitution effects, and transparency of potential substitutes.

We first provide an overview of Tornado Cash flows. Figure 1 visualizes the transaction network surrounding Tornado Cash and highlights identifiable addresses and services connected to the mixer. To keep the visualization exercise manageable, the figure samples the 2,500 largest nodes within the network. To the left of the central Tornado Cash node, we observe that many addresses sending funds to Tornado Cash are recognizable hackers and illicit organizations, including the top user, the North Korean Lazarus Group.²³ Given their prominence and OFAC’s emphasis on hacked funds in its designation, our analysis of illicit-flow substitution focuses on these technically sophisticated hackers. Among paths entering Tornado Cash, many are intertwined in more complicated networks, while outgoing paths are more discernible. Users appear to funnel more money from decentralized exchanges (i.e., Uniswap, 1inch) than from centralized exchanges. Further, Tornado Cash withdrawals are commonly funneled back to DeFi within one hop. Funds also move to centralized exchanges. If exchanges enforce sanctions, then we should expect this flow to nearly cease after sanctions.

2.1.1 Do Sanctions Reduce Flows to Tornado Cash?

Figure 2, Panel A, shows the time series of total inflows to Tornado Cash. Following the August 2022 sanctions, inflows to the mixer declined sharply. In the six months before the ban, Tornado Cash

²³Of the identified tainted flows to Tornado Cash, Figure 1A.1 plots the top 50 individual senders, with the North Korean Lazarus Group as the largest sender.

handled approximately 957,000 ETH (\$2.17 billion); however, in the six months after the ban, volume declined to approximately 134,000 ETH (\$197 million), representing a decline of 85.95% in ETH terms and 90.91% in USD terms.²⁴

A decline in total volume also may impact the ability for illicit actors to hide within a broad pool of liquidity. We estimate the likelihood that large, concentrated inflows can be correctly linked to subsequent outflows by modeling individual time-to-withdrawal and fitting the aggregated estimates to historical data. The resulting likelihood implies a probability of detection, and we plot the probability of detection for the largest sender as the blue line in Figure 2.²⁵ Following the August 2022 U.S. Treasury sanctions and the subsequent drop in liquidity, the average probability of matching withdrawal transactions to the top depositor increased from 12.9% to 21.3%.

We also decompose total Tornado Cash inflows in Figure 2, Panel A, into inflows originating from identified hacker addresses and other unidentified inflows, while the red line plots the hacker share of total inflows. Beginning around April 2022, this share increased substantially, consistent with OFAC's stated concern about the use of Tornado Cash to launder proceeds from hacks. Following the sanctions, hacker-originated inflows declined sharply in levels even as their share of total inflows increased. In the six months before the sanctions, hacker-originated inflows totaled 246,010 ETH and accounted for 25.70% of Tornado Cash inflows. In the subsequent six months, these flows fell by 80.38% to 48,276 ETH, while their share increased to 35.90%. The increase in share partly reflects an even larger decline in unattributed flows composed of a mixture of smaller-scale illicit activity and legitimate users that we cannot separate. Overall, both total Tornado Cash inflows and inflows originating from identified hacker addresses declined sharply following the sanctions.²⁶

However, the decline in hacker inflows to Tornado Cash could reflect either a change in hackers'

²⁴We state dollar amounts based on the price of ETH on the day of each transaction. A formal DiD estimates a 70.0% decline in total Tornado Cash volume compared to all other aggregate Ethereum volume as shown in Table IA.1. It also shows comparisons between Bitcoin and Ethereum and in dollar values, which yield similar results. [Brownworth, Durfee, Lee, and Martin \(2024\)](#) and [Cristodaro, Kraner, and Tessone \(2025\)](#) also show the decline in Tornado Cash volume after sanctions.

²⁵Internet Appendix Section B provides the methodology for calculating probability of detection. Note that there are other heuristics, such as transaction reporting, timing differences, and transaction clustering, which may further increase the probability of detection.

²⁶The decline in the measured hacker share in 2025 is likely partly a by-product of reporting lags, because illicit addresses are often identified only after some delay, as previously discussed.

choice of laundering services or a broader decline in hacker activity. To formally test whether the sanctions changed hackers' destination choices, we estimate a DiD design comparing hacker flows to Tornado Cash with hacker flows to overseas exchanges. We use data on 5,867 unique hacker addresses.²⁷ For each reported hacker address in our dataset, we trace monthly flows both to Tornado Cash as well as to all other destinations on Ethereum. We construct a balanced panel dataset where the unit of observation is the flows from each labeled hack, to each destination, per month. Tornado Cash is the treated destination, while overseas centralized exchanges serve as the comparison group because they were not directly targeted by the Tornado Cash sanctions and provide a benchmark for broader changes in hacker activity. Specifically, we estimate a regression of the form as follows:

$$\begin{aligned} \log(1 + TaintedFlows)_{i,d,t} = & \sum_{t \neq \text{July}2022} \beta_t \times \mathbb{1}(\text{Month} = t) \times Tornado_d \\ & + \delta \times Tornado_d + \mu_i + \gamma_t + \varepsilon_{i,d,t} \end{aligned}$$

where $\log(1 + TaintedFlows)_{i,d,t}$ is the log of one plus the amount of ETH traced from hacker address i to destination d in month t , $\mathbb{1}(\text{Month} = t)$ is an indicator for calendar month t , $Tornado_d$ is an indicator equal to one if the destination is Tornado Cash, and zero if the destination is an overseas centralized exchange, and μ_i and γ_t are hacker address and month fixed effects, respectively.

Figure 2, Panel B, plots the estimated DiD coefficients (β_t), which capture the change in hacker flows to Tornado Cash relative to hacker flows to overseas exchanges in each month compared to the baseline month. After the ban in August, we find that hackers send significantly less to Tornado Cash relative to overseas exchanges, with the relative decline reaching approximately 8% lower and persisting for a year. This result indicates a shift in the destinations of hacker flows away from Tornado Cash, rather than simply a decline in aggregate hacker activity.

Given that the probability of detection increased while hacker usage of Tornado Cash decreased, we also examine whether subsequent enforcement actions against Tornado Cash-linked addresses in-

²⁷Constructing a user-level sample based on addresses that interact with Tornado Cash would be problematic because sophisticated users often rotate wallets and avoid address reuse. Our hacker sample instead starts from addresses attributed to specific hack incidents, compiled from multiple public and proprietary sources, and traces funds from these reported incidents forward. Although attribution is necessarily incomplete, this approach does not require the same hacker address to persist over time.

creased, focusing on OFAC sanctions and Tether freezes of Ethereum addresses. We find no statistical difference in these enforcement actions before and after the Tornado Cash ban.²⁸ One possibility is that flows migrate to alternative channels, as we analyze below. Additionally, Tether freezes and OFAC sanctions against individual wallets are rather idiosyncratic (as shown below) and may hinge on institutional factors such as the number of DOJ attorneys and their priorities.

We also analyze Tornado Cash activity after sanctions were overturned and subsequently lifted. Returning to Figure 2, Panel A, we observe that aggregate volume did not change substantially immediately after sanctions were overturned by the court on November 26, 2024, but rose slowly after OFAC lifted the ban on March 21, 2025. Between May and December 2025, Tornado Cash activity averaged approximately 73,000 ETH per month, still well below the average monthly volume of approximately 151,000 ETH observed before the sanctions. To control for aggregate Ethereum activity, a DiD specification (in Figure IA.2 and Table IA.1) shows that flows have only partially returned to the activity level prior to sanctions. Since mixer usage requires coordinated liquidity among users, a shock like sanctions that weakens liquidity may discourage further use. The slow recovery of volume can also be consistent with continued regulatory risk, such as from the EU's Transfer of Funds Regulation, the possibility of new sanctions in the future, and lingering stigma around Tornado Cash-linked funds at exchanges. Additionally, Tornado Cash users may have already migrated to a new platform and be reluctant to incur the costs of adopting new routines.

2.1.2 Where Does Illicit Activity Migrate After the Tornado Cash Sanctions?

Having documented a decline in hacker flows to Tornado Cash, we next examine whether activity shifts toward privacy-focused blockchains that could provide more opaque substitutes for Tornado Cash. We evaluate whether users increase or decrease their activity on Monero, Dash, and Zcash, which are prominent privacy-focused blockchains.

Ex ante, it is not clear whether activity on privacy-focused blockchains would increase or decrease. On one hand, if these services are competitive substitutes, then users with preferences for privacy may

²⁸We identify addresses that directly interact with Tornado Cash, as well as addresses connected within five transaction hops, and count those that are subsequently sanctioned by OFAC or frozen by Tether. We compare the mean number of such addresses in the seven quarters before and after the ban using a t-test (see Figure IA.3).

switch between privacy services when one is rendered infeasible, and thus activity on privacy-focused blockchains may increase following Tornado Cash sanctions. On the other hand, if these privacy services are complements such as requiring coordinated liquidity among different privacy chains, then activity may decrease after sanctions were enacted. Additionally, activity may also decline if users perceive a greater risk of future regulations targeting Monero, Dash, or Zcash, especially if the expected costs of regulation exceed the benefits of transacting privately, which we discuss in the next section.

We formally test for changes in privacy-chain activity using a DiD design. We construct a blockchain-by-day panel in which Monero, Dash, and Zcash are the treated blockchains and Bitcoin and Ethereum serve as comparison blockchains to absorb broad changes in aggregate crypto activity. The outcome is the log daily number of transactions, and the regressions include blockchain and date fixed effects. Figure 3, Panel A, plots the corresponding dynamic coefficients and shows no increase in transaction activity on the privacy-focused blockchains following the sanctions. If anything, activity generally declines relative to Bitcoin and Ethereum after the event. Table 1, Panel A, reports the corresponding average effects. Monero declines by 30.2%, Dash by 24.1%, and Zcash by 29.7% relative to Bitcoin and Ethereum; pooling the three privacy-focused blockchains yields an overall decline of 28.0%.²⁹ Given other possible reasons for a change in volume, we do not draw causal conclusions or attribute the observed declines causally to the Tornado Cash sanctions.³⁰ It is difficult to evaluate the full scope of activity in privacy-focused blockchains because we can only observe the number of transactions and lack visibility into the dollar-volume of transactions.

We return to the hacker-level analysis above to examine where hackers redirect their funds after reducing their use of Tornado Cash. We separately consider decentralized exchange swaps, bridges, and wrapped Ether as alternative destinations. For each test, the relevant destination serves as the treated group, while overseas centralized exchanges provide the comparison group. Figure 3, Panel B, plots the corresponding dynamic coefficients. Following the sanctions, hacker flows increase to swaps

²⁹We also note that there are some positive pre-trends for Zcash, whose activity rises relative to the comparison blockchains shortly before the Tornado Cash sanctions.

³⁰While the previous findings are for changes in activity, Figure IA.4 plots the levels of daily number of transactions for each of these three blockchains. The levels also exhibit a decrease around the enactment of sanctions against Tornado Cash. We also plot effects of the sanctions lifting, as shown in Figure IA.5 and find negative effects for Monero, while Dash and Zcash later trend higher, as summarized in Table IA.2.

(by 4.6%), bridges (6.0%), and wrapped Ether (4.2%) as shown in Table 1, Panel B.

We now summarize the evidence on hacker destinations before and after the Tornado Cash ban. Figure 4, Panel A, compares two cohorts: (i) hackers active before the ban, and (ii) those who started moving funds after the ban. We plot the traced dollar flows of each group to various destinations, highlighting sizable shifts in blue and entirely new top destinations in red. The pre-ban group relied heavily on Tornado Cash. By contrast, the post-ban group uses Tornado Cash at lower rates and shifts to other major services. We see that Wrapped Ether experiences the largest jump. Hackers appear to convert their stolen Ether into Wrapped Ether, possibly as an intermediate step before onward transfers. Among the newly popular destinations, Thorchain stands out the most. Thorchain is a bridging protocol that enables cross-chain transfers without going through centralized intermediaries. Hackers likely hope that moving funds across different blockchains via bridges will obscure the trail and make their activities more difficult to trace. One limitation of our analysis is that there could be migration to other opaque crypto structures, or off-chain venues that we do not observe. Overall, the evidence suggests that hackers substitute away from Tornado Cash, but primarily toward alternative on-chain channels that, while complicating tracing, remain relatively traceable.

2.1.3 Largest Crypto Heist Case Study

North Korean hackers are an emblematic example that encapsulates how the environment has evolved. Not only were North Korean hackers prolific users of Tornado Cash before the software was sanctioned, but a high-profile North Korean hack was also the precipitating event that led to the 2022 sanctions.³¹ In February 2025, North Korea is alleged to have stolen \$1.4 billion from the exchange Bybit, marking the largest crypto heist in history.³² We trace these flows to uncover the subsequent destinations. Figure 4, Panel B, plots these flows, with stolen funds initially exiting Bybit on Ethereum and being forwarded by hackers through Ethereum-based wallets and services, represented in the center. Within Ethereum, \$42.8 million was transferred to OKX, but \$968 million, or 69% of the stolen amount, bridged through Thorchain to addresses on the Bitcoin blockchain, likely to minimize seizure

³¹North Korea hacked Harmony Bridge and used Tornado Cash to launder the funds in June 2022, and Tornado Cash was sanctioned in August 2022. Details are available in the [OFAC Press Release](#).

³²Details are available in this [FBI Press Release](#).

risk. We calculate the transaction costs of this operation: transfers on Ethereum cost approximately \$12,000, using Thorchain to bridge to Bitcoin incurred \$3.79 million (42 basis points of the bridged amount), and subsequent Bitcoin transfers added another \$67,000 in fees to block miners, for a combined \$3.87 million. Notably, North Korea seems to have substituted from Tornado Cash, a service with relatively low cost (30 basis points), to bridges, which are more costly. The excessive splitting into over 34,000 transactions was likely an attempt to cheaply obfuscate their flows. Additionally, speed appeared to be a priority, given that, after thousands of transactions, the Ethereum proceeds were bridged to Bitcoin within 24 hours following the hack. Once on the Bitcoin blockchain, the funds continued to circulate through a wide network. However, the vast majority of funds remain on the Bitcoin blockchain as of August 2025, six months after the initial hack.³³

The limited liquidity in mixers is unlikely to support the laundering of \$1.4 billion within a short time horizon without attracting enforcement action. Instead, the hackers bridged the funds into Bitcoin, which, due to its decentralized consensus mechanism, offers greater protection against transaction censorship and seizure. Ultimately, the episode seemingly highlights that, without substantial liquidity in mixers, even high-profile and extremely sophisticated attacks like the Lazarus Group are potentially traceable.

2.1.4 Ukrainian Usage

Our analysis is focused on the potential costs to criminal networks. Nevertheless, there are legitimate reasons users may prefer privacy. These may be difficult to measure. We examine one prominent and well-defined use case: borderless remittances of donations to the Ukrainian relief effort.³⁴ In this setting, users may prefer privacy to conceal their wallets from potential Russian hackers. We compile a list of 24 Ethereum addresses that collected donations for Ukraine, including those associated with the Ukrainian government and well-known news organizations. Figure IA.6, Panel A, presents this list of addresses and the denominations of funds received. These addresses received a total of \$113 million.

³³Approximately \$98.7 million was deposited in Freebitco.in, a Bitcoin-based wallet and gambling service as of August 2025.

³⁴Donating to the Ukrainian war effort through Tornado Cash appears as a major use case in articles such as [in this linked WSJ article](#) as mentioned by the founder of Tornado Cash, and [in this linked Fortune article](#), where donations to Ukraine are mentioned in the court case that overturned the sanctions against Tornado Cash. One famous example of donors to Ukraine via Tornado Cash includes Vitalik Buterin, the Russian-born founder of Ethereum, as he [tweeted](#).

Tracing transactions backward from these addresses, we find that \$1.77 million was routed through Tornado Cash before arriving at the destination, implying that 1.56% of Ukrainian donations relied on Tornado Cash. The \$1.77 million is small compared to the \$2.04 billion in tagged hacker flows that flowed through Tornado Cash over our sample period.³⁵ Overall, sanctions may harm legitimate users, but these costs are difficult to detect empirically.

2.2 U.S. Department of Justice Settlements with Exchanges

We now turn to a second form of service-level enforcement: U.S. Department of Justice (DOJ) settlements with centralized exchanges. Centralized exchanges are particularly important AML enforcement points because they provide deep liquidity and are a primary channel through which on-chain assets can be converted into fiat currency and reintegrated into the traditional financial system. They are also well positioned to conduct KYC and transaction-monitoring procedures because they operate at the interface between crypto markets and the traditional financial system. However, some exchanges have historically maintained weak compliance processes, potentially allowing money launderers to convert tainted crypto assets into fiat without detection. We use sanctioned Tornado Cash outflows first to characterize how exchanges handle sanctioned funds and then to examine whether their behavior changes following DOJ enforcement.

2.2.1 Do Exchanges Continue to Receive Sanctioned Tornado Cash Outflows?

We begin with descriptive evidence on the ultimate destination of Tornado Cash outflows, which were labeled as illicit flows following sanction designation. We identify and trace transaction paths from Tornado Cash to their eventual destinations. Figure 5 summarizes these paths using Sankey diagrams that visualize outflows from Tornado Cash before and after the August 8, 2022 sanction. Flows originate from Tornado Cash, pass through intermediate hops, and ultimately reach centralized exchanges in blue, decentralized exchanges in red, bridges in purple, or wrapped ETH in gray. When flows reach a decentralized exchange, we continue to follow the funds in the new token. Before the

³⁵We further plot the timing of transactions in Figure IA.6, Panel B. Donations were concentrated in February and March 2022, at the beginning of the Russo-Ukrainian War. Donations to Ukraine routed through Tornado Cash had already slowed substantially by the time OFAC sanctioned the mixer.

ban, we observe relatively large direct flows to centralized exchanges. After the ban, the composition of destinations changes, with a greater role for decentralized exchanges and bridges, while centralized exchanges continue to receive a meaningful share of Tornado Cash outflows.³⁶

Western exchanges reduce their exposure to Tornado Cash relatively quickly after the ban: the average monthly share of outflows reaching Western exchanges falls from 3.99% in the twelve months before the ban to 2.14% in the twelve months after, a 46.30% reduction (as shown in Figure [IA.7](#)). In contrast, overseas exchanges do not exhibit the same immediate decline and continue to receive meaningful Tornado Cash flows well after the sanctions are imposed. These flows decline substantially only by the end of 2023.³⁷ The persistence of these flows motivates a sharper test of whether enforcement directed at the exchanges themselves changes their behavior.

2.2.2 Do DOJ Settlements Reduce Sanctioned Flows to Exchanges?

On November 21, 2023, Binance pleaded guilty to anti-money laundering and sanctions violations as part of a settlement with the U.S. Department of Justice. As part of the agreement, the company’s founder and CEO resigned, Binance paid over \$4 billion in penalties, and the company admitted to violations of KYC and AML requirements. At the time, Attorney General Merrick Garland stated, “Binance became the world’s largest cryptocurrency exchange in part because of the crimes it committed. Now it is paying one of the largest corporate penalties in U.S. history.” On May 17, 2024, the DOJ appointed two independent compliance monitors to oversee Binance for a three-year term. Similarly, on February 24, 2025, OKX pleaded guilty to violating U.S. anti-money laundering laws.³⁸ We use these enforcement events to evaluate whether the targeted exchanges reduce their receipt of sanctioned Tornado Cash outflows.³⁹

³⁶Figure [IA.8](#) provides a more granular breakdown of Tornado Cash outflows reaching specific destination services before the sanctions, during the sanctioned period, and after the November 2024 court ruling, and also reports transaction hop counts.

³⁷Table [IA.3](#) formally compares paths originating from Tornado Cash withdrawals and terminating at Western exchanges with those terminating at overseas exchanges in a DiD framework. After the Tornado Cash ban, paths terminating at Western exchanges use approximately 0.29 more hops, require about 120 additional days, and incur 77-87 basis points in additional transaction costs relative to paths terminating at overseas exchanges.

³⁸See [here](#) for the DOJ press release on Binance settlement, and [here](#) for the DOJ press release on OKX settlement.

³⁹Customers may choose not to remit funds to these exchanges either because of the announcement effect, or due to direct tighter post-plea compliance measures that deter future transactions.

A sharp test of Binance’s sanctions compliance is whether it continued to receive flows from Tornado Cash after the settlement. Panel A of Figure 6 focuses on Tornado Cash flows to Binance, while Panel B shows flows to all other overseas exchanges over the same period. The blue and yellow bars plot the monthly share of Tornado Cash outflows reaching Binance and all other overseas exchanges, with yellow denoting paths that swapped through a DEX. In 2023 and before the DOJ settlement with Binance, Binance received an average of 3.98% of all Tornado Cash outflows. In the months after the DOJ’s settlement with Binance and before the Tornado Cash ban was overturned by the court in November 2024, this share declined sharply to 0.75%, representing an 81.29% reduction. The decline is even larger when measured after the start of the compliance monitorship in June 2024, as the share fell further to 0.54%.

Table 2 tests these changes in a monthly DiD design that compares Binance with other overseas exchanges and includes exchange and year-month fixed effects. The outcome is an exchange’s share of traced Tornado Cash flows, defined as the percentage of all traced Tornado Cash volume reaching any destination in a given month that arrives at that exchange. Column (1-2) uses six-month windows before and after the Binance settlement, while Column (3-4) retains the same pre-settlement period but defines the post-period as the six months beginning with the compliance monitorship. Binance’s share falls by 1.57 percentage points after the settlement, about 44% of its pre-settlement level, and by 2.92 percentage points after the monitorship, about 83%, while the shares of other overseas exchanges barely move.

Additionally, the red line in Figure 6, Panel A, shows that the Tornado Cash flows that continued to reach Binance traveled through more intermediate hops after the monitorship began. We formally test this pattern using a dynamic DiD framework, with estimated monthly coefficients plotted in Figure IA.9. The outcome variable is the number of intermediate hops for transfer paths from Tornado Cash to centralized exchange destinations. The treatment group consists of flow paths to Binance, and the control group consists of flow paths to other overseas centralized exchanges. The estimates show no significant change in the number of hops immediately after the settlement, but a clear increase following the start of the compliance monitorship. This pattern suggests that users who continued

sending Tornado Cash flows to Binance began adopting more complex routing paths to obscure the origin of funds, and that users became more hesitant to send sanctioned funds to Binance.

We next evaluate similar tests around the DOJ settlement with OKX and find similar results. After OFAC sanctioned Tornado Cash in 2022, we continue to observe sizable flows from Tornado Cash entering OKX (as seen in Figure [IA.10](#)). In the year before the OKX settlement, OKX accounted for an average 1.53% of Tornado Cash outflows. Interestingly, flows from Tornado Cash fell four months prior to the DOJ settlement with OKX in February 2025. By February 2025, the Tornado Cash flows to OKX were nearly nonexistent. In a formal test, we find that the flows declined by 99.03% (t-statistic = 3.515, p-value = 0.0048) after the settlement. Over the same window, the combined share to other overseas exchanges fell from 4.84% to 3.04%, which is not statistically significant.

Overall, the fact that outflows from Tornado Cash to exchanges did not decline sharply after Tornado Cash sanctions but only after the exchanges settled or neared settling with the DOJ indicates that crypto exchanges do not always self-police and that enforcement can be useful to ensure compliance.

2.2.3 Do Sanctioned Flows Shift to Other Overseas Exchanges?

The decline in flows to Binance and OKX raises the possibility that Tornado Cash users simply redirect sanctioned funds to overseas exchanges that are not subject to the same enforcement actions. If such substitution were important, we would expect the receipt of Tornado Cash outflows by other overseas exchanges to increase as flows to the targeted exchanges decline.

We do not observe such an increase in Figure 6, Panel B. Following the Binance settlement and subsequent compliance monitorship, Tornado Cash outflows to other overseas exchanges do not rise; if anything, they decline over the same period. Thus, we find no evidence that other overseas exchanges systematically replace Binance as destinations for sanctioned Tornado Cash flows. This evidence is descriptive, however, and we are reluctant to overinterpret the null result. Other market developments may have affected exchange flows over the same period, and we lack a natural comparison group that would allow for a clean causal test of substitution.

3. Policies Targeting Users

We next turn from enforcement directed at crypto services to policies targeting individual users. We study two forms of user-level enforcement: OFAC sanctions on criminal actors and stablecoin freezes by issuers. We examine whether these actions reduce activity in directly designated wallets and whether targeted users substitute toward other, non-designated wallets they control.

3.1 OFAC Sanctions Against Criminal Organizations and Individuals

The U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) began adding digital-currency addresses to its sanctions list in 2018. Once an address is sanctioned, U.S. persons and entities are generally prohibited from transacting with it. In total, the list contains 71 sets of sanctions involving Bitcoin or Ethereum addresses. We hand-label each set according to whether it targets an organization or individual engaged in criminal activity or a specific crypto service. We identify 54 sanctions targeting crypto addresses associated with organizations or individuals, including North Korea’s Lazarus Group, ISIL, the Sinaloa Cartel, and other transnational criminal organizations involved in drug trafficking and terrorism.⁴⁰ The remaining 17 sanctions target services, including Tornado Cash; Hydra, a darknet marketplace; and centralized exchanges associated with Russia and Iran. Because this section focuses on policies targeting users, we restrict our analysis to the organizations and individuals.

3.1.1 How Timely Are OFAC Sanctions?

We begin by describing when OFAC sanctions are imposed relative to the transaction activity of designated wallets. Sanctions were imposed on 54 entities of criminal organizations or individuals that include a total of 522 Bitcoin addresses and 183 Ethereum addresses. In Figure 7, Panel A, we plot the sanctioned Bitcoin (left) and Ethereum (right) addresses. Each bubble represents a sanctioned address, with the bubble size proportional to the address’s total lifetime inflow in dollars. The scatterplots illustrate sanction timing by plotting the address age at the time of last transaction, or the number

⁴⁰A prominent recent addition is the Prince Group, which was sanctioned on October 14, 2025, for operating online investment scams and forced-labor compounds in Cambodia. OFAC sanctioned 29 Bitcoin addresses holding approximately \$2.1 billion. The DOJ additionally announced the seizure of 127,000 Bitcoin, worth approximately \$15 billion, in connection with an action that occurred in July 2024, which does not appear in the sanctions list.

of days between an address’s first and last transactions (x-axis), and age at the time of sanctions, or number of days between the first transaction and the sanction date (y-axis). Addresses positioned directly on the 45-degree line were last used to transact exactly on the sanction date, which means users halted all activity after sanctions. In contrast, if an address is far above the 45-degree line, then sanctions are imposed significantly after the last active date. The darker red shaded triangular regions highlight addresses that are sanctioned for more than one year and for more than two years after the last transaction date. Bitcoin addresses exhibit significant lags in sanction timing. Specifically, 67.06% of sanctioned Bitcoin addresses and 50% of Ethereum addresses had no transactions after they were sanctioned, and 44.71% of BTC and 11.67% of ETH addresses ceased activity more than one year before sanctions. Sanctions on Ethereum addresses were historically more likely to impact funds, as they are often imposed while addresses are still active.

3.1.2 Do OFAC Sanctions Prevent Funds from Leaving Designated Wallets?

We next examine where their funds move after sanctions, how activity changes after designation, and how much remains trapped on-chain. In Figure 7, Panel B, we plot the balances of sanctioned addresses and the destinations of their trace outflows with Bitcoin in the left subpanel and Ethereum in the right subpanel. The bars are cross-sectional snapshots of the destinations of flows that transit sanctioned addresses, as of each month, indexed against the sanction date.⁴¹ In the figure, we remove inflows from other sanctioned addresses to remove double counting, which results in total inflows of more than 58,000 BTC, or about \$1.1 billion.⁴² In Ethereum, we observe total inflows of more than 234,000 ETH (\$593 million) after netting flows from other sanctioned wallets.⁴³

This figure highlights four main results about the timing of sanctions relative to the total flows.

⁴¹For example, consider bars at -18 months. The light blue bars show the amount held in the sanctioned addresses 18 months before sanctions are imposed. The gold bars show flows transferred from sanctioned addresses, potentially through other on-chain addresses, and ultimately to Bitfinex, an exchange, 18 months before sanctions were imposed.

⁴²Because our analysis of OFAC addresses involves tracing flows of sanctioned addresses to their end destination, we are cautious to avoid double counting flows that move between multiple sanctioned addresses. For example, if \$100 moves through three different addresses on the sanctions list, then we would not want to recount the same funds three times as \$300. Our analysis presents net flows and hence we would report the flows in this example as \$100. The total inflow to sanctioned addresses (with double counting) totals more than 91,000 Bitcoin, or about \$2.4 billion at the time of the transaction.

⁴³Total inflows, including double-counting, total over 380,000 ETH. We also observe \$114 million in net USDT, which we display in Appendix Figure IA.11.

First, the light-blue bars show the amounts held in the sanctioned wallets at the time of sanctions. For Bitcoin, sanctioned wallets held approximately 20,000 BTC at the time of sanction, representing 34.8% of the total inflows to these wallets. The majority of aggregate BTC inflows were no longer held in the sanctioned wallets but had instead been transferred elsewhere on-chain prior to sanctions. For Ethereum, substantial funds, or 63.2% of the ETH total inflow (or 148,000 ETH), are in the addresses prior to the sanction. At the wallet level, the median sanctioned address on Bitcoin and Ethereum had a balance of \$0 and \$91, respectively. Further, 79.2% of BTC addresses and 28.8% of ETH addresses held less than \$1 at the time of sanctions.⁴⁴ In sum, sanctions often target empty or low-balance addresses.

Second, aggregate flows commonly transited through addresses and entered exchange or service destinations, which are indicated in hatched bars, before sanctions were imposed. This is visible in the amounts entering HTX, Binance, Bitfinex, and other services. The red lines on the right-hand axis indicate the share of inflow that we observe moving to a service. In the month before sanctions, approximately 28,000 BTC (49.2%) of Bitcoin inflows and 80,000 ETH (34.2%) of Ethereum inflows had already been remitted to an identifiable service or to a large unidentifiable address.⁴⁵ Funds exited the Ethereum and Bitcoin blockchains through centralized exchanges before sanctions were imposed.⁴⁶

Third, funds are moved right after the sanction. After the sanction, approximately 9,300 BTC (15.9% of total inflows) move from a sanctioned wallet to another wallet on-chain (as visible in the transition from light blue to dark blue), and approximately 144,600 ETH were sent to Tornado Cash, or 78.8% of total inflows in dollars (as visible by the transition from light blue to bright orange). The large movement into Tornado Cash illustrates an important limitation of sanctions imposed on individual wallets: sanctioned users can route funds through a mixer to obscure the link between the designated address and subsequent transactions, potentially allowing the underlying user to continue

⁴⁴We plot address balances at the time of sanctions and the prevalence of sanctioning empty wallets in Figure [IA.12](#). We also show a time series of total sanctions against criminal users and find a steady increase in sanctions for both BTC and ETH.

⁴⁵We do not follow trace paths through large unidentifiable addresses to mitigate the risk of tracing shadow exchanges.

⁴⁶Figure [IA.13](#) and Figure [IA.14](#) show the total inflow to sanctioned addresses and their services of choice, as well as the dollarized value of the respective amounts stuck on-chain in event time. Panel A of both figures plots the Bitcoin and Ethereum outflows over calendar time, respectively. Importantly, the large inflows to Tornado Cash during the middle of 2022 correspond to a series of hacks targeting DeFi platforms in the Ethereum network. The largest of these was the Axie Infinity Ronin bridge hack perpetrated by the Lazarus Group.

moving funds through new addresses.⁴⁷ Insofar as sanctioned users increase reliance on mixers, sanctions may lead to less transparency. This behavior also highlights the importance of enforcement directed at laundering services such as Tornado Cash itself.

Fourth, in contrast to flows that were transferred to services, we still observe approximately 29,000 BTC (50.56% of inflow, worth \$2.6 billion as of the end of 2025) and 9,000 ETH (3.96% of inflows, or \$27.5 million) on chain. Thus, forensic researchers and law enforcement can still observe the majority of sanctioned Bitcoin, but we cannot observe substantive ETH flows. The funds that remain on-chain are seemingly frozen, as sanctioned entities have been unable to transfer these funds through centralized exchanges and convert them into fiat currency.

We next formally estimate the direct effect of sanctions on address outflows using a DiD framework. We first develop a testing framework for Ethereum, which we subsequently mirror for testing stablecoin freezes. For each sanctions date, we define a cohort whose treatment group consists of all addresses sanctioned on that date. Because sanctioned addresses are often inactive, our treatment group includes active addresses within the preceding year, or 44 treated cohorts. We construct the corresponding control group by first identifying addresses that were active during the preceding year before the sanctions date, thereby ensuring that the controls reflect broader address activity around the time sanctions were imposed. We then randomly select 50 control addresses for each treated address. Our DiD regressions include cohort-by-address fixed effects, which absorb time-invariant differences across addresses within each cohort, and cohort-by-time fixed effects, which absorb cohort-specific aggregate activity in each period. Consistent with the relatively muted activity around sanctions, we find no meaningful effect in outflows, as shown in Column (1) of Table 3.⁴⁸ We additionally present formal tests for sanctioned Bitcoin addresses and find a 35.3% decrease in outflows after sanctions.⁴⁹

⁴⁷We present a formal test of the flows to Tornado Cash in Figure IA.15 and Table IA.4. Because there are only 17 OFAC addresses within a year that use Tornado Cash, the test has low power. Further, sanctioned addresses also use Tornado Cash prior to the imposition of sanctions, which also attenuates any treatment effect. Nevertheless, the test shows a positive coefficient, and the aggregate statistics show a clear increase in Tornado Cash use after sanctions.

⁴⁸We observe a positive, but statistically insignificant response in the first month after sanctions, as shown in dynamic coefficients in Figure IA.16, which is consistent with funds being transferred immediately after sanctions were imposed. The inclusion of inactive addresses in the treated group likely attenuates the average treatment effect.

⁴⁹Results on sanctioned BTC are shown in Table IA.5, Column (1), which states a change of -35.3%. Dynamic coefficients in Figure IA.17, Panel A exhibit more active volume prior to the shock, and low volume and low variation after the event, which is consistent with the aggregate observation of many periods of zero transactions after sanctions are imposed.

3.1.3 Do Sanctioned Users Shift Activity to Related Wallets?

We next ask whether sanctions on individual wallets constrain the underlying users or instead induce them to shift activity toward related, non-designated wallets. We examine three sets of addresses plausibly linked to sanctioned users: (i) gas-clustered addresses related to the sanctioned wallet, (ii) downstream deposit addresses that receive tainted funds from sanctioned wallets, and (iii) additional deposit addresses identified through deposit-address clustering. We estimate a separate DiD for each setting using cohorts defined by OFAC sanction dates. Within each cohort, the related addresses form the treated group. For each treated address, we form a candidate pool of unlabeled, never-sanctioned addresses that were active in the window immediately preceding the sanction date and that fall in the same transaction-count and dollar-volume bins as the treated address. We draw 50 random addresses from the pool for each treated address to serve as the control group in that cohort.

We present results in the last three columns of Table 3. In Column (2), we do not observe a decline in activity among gas-clustered addresses related to the sanctioned address compared to a control group. Next, we examine changes in activity among related tainted deposit addresses in Column (3) and clustered deposit addresses in Column (4), which increase by 17.9% and 228.7%, respectively. Figure 8 presents dynamic coefficients. Prior to the sanctions, related deposit addresses exhibited some activity despite the focal address being inactive. Additionally, related deposit addresses exhibit an increase in activity after sanctions. These increases are consistent with sanctioned actors shifting activity toward other wallets, with downstream deposit addresses subsequently receiving more funds from those alternative wallets after a focal address is designated for OFAC sanctions. We also find an increase in clustered Bitcoin activity after sanctions.⁵⁰ Considering both the Ethereum and Bitcoin evidence together, the results suggest that underlying users continue operating through related, non-designated wallets.

⁵⁰For sanctioned Bitcoin addresses, we rely on co-spending clustering to identify related addresses to serve as the treated group. The control group is constructed by drawing 50 random addresses per treated address, conditional on pre-period activity. Table IA.5, Column (2) shows an increase of 93.5% relative to the control group. Figure IA.17, Panel B, has a decline in the pre-period as addresses may be inactive prior to sanctions, and a sharp increase at the shock, especially when focusing on the few months around the event.

3.2 Stablecoin Asset Freezes

The risk of asset seizure is a critical consideration in money laundering schemes. Stablecoin issuers such as Tether, the issuer of Tether USD (USDT), and Circle, the issuer of USD Coin (USDC), have the technical ability to freeze these assets and prohibit specific users from future transactions with that stablecoin. However, stablecoin issuers have historically not been held to the standards of traditional banks, and “the absence of a regulated financial institution, subject to AML/CFT obligations can limit authorities’ collection of and access to information. It can also reduce the effectiveness of preventive measures” ([U.S. Department of the Treasury, 2024](#)). In this section, we consider how illicit flows respond to asset freezes enacted by stablecoin issuers.

3.2.1 How Common Are Stablecoin Freezes?

We begin by documenting the scale and timing of stablecoin freezes. Figure 9, Panel A, plots the cumulative number of Ethereum addresses frozen by Tether (red line) and the cumulative value of USDT held by these addresses at the time of freeze (stacked bars). Across the 2,654 addresses frozen as of December 31, 2025, \$1.92 billion in USDT was held at the time of the freeze. Of this amount, only \$714 million was subsequently destroyed, indicating that frozen balances do not necessarily lead to destruction of the underlying tokens. In total, 10.07% of addresses were inactive for more than one year at the time their balances were frozen, and the median address held a balance of approximately \$31,000. Purple bar segments denote freezes that overlap with known OFAC sanctions or funds related to reported hacks. Of the 2,654 frozen addresses, only 173 are related to OFAC and 141 are related to hacks. To gauge the scale of Tether’s freezes, we compare their average annual value with existing estimates of illicit activity. Tether froze \$1.92 billion over five years, equivalent to approximately \$384 million per year. By comparison, [Griffin and Mei \(2025\)](#) document \$94.6 billion transferred into deposit addresses linked to pig butchering scams, primarily in Tether, or \$27.8 billion per year. [Griffin, Wang, and Artero Calvo \(2026\)](#) estimate \$167 billion in total crypto criminal activity per year. Thus, Tether’s average annual freezes amount to approximately 0.23%-1.38% of the total annual estimates. The Tether freezing activity, while reasonable, is small in scale relative to the underlying

criminal flows.

Given this relatively limited scale, we next examine whether changes in Tether’s freezing policy help explain when and how frequently freezes occur. As shown in Figure 9, the pace of Tether freezes increased in December 2023. Between January 2021 and November 2023, Tether froze an average of 22 addresses per month. During this period, Tether’s stated policy was not to proactively freeze sanctioned addresses, but instead to act when specifically requested by law enforcement. However, on December 9, 2023, Tether announced a new policy under which it would voluntarily freeze addresses appearing on the OFAC sanctions list.⁵¹ At that time, we see a marked increase of 220 addresses frozen, as seen in Figure IA.18, Panel A. Since then, addresses added to the OFAC list are generally frozen within a day of being announced (as shown in Panel B). The average number of Tether freezes also approximately tripled to 65 addresses per month between December 2023 and December 2025. It is additionally worth noting that OFAC sanctions are only a small share of all Tether freezes, so the broader increase cannot be attributed solely to the new OFAC policy. This shift in policy by Tether on OFAC sanctions may have coincided with Tether becoming more responsive to law enforcement and/or with law enforcement adopting a more aggressive approach to asset seizures.

We also examine freezing activity by Circle, the issuer of USDC. We document 244 frozen USDC addresses containing \$113 million (as shown in Figure IA.19). However, Circle appears to have adopted a different approach to OFAC designations: as early as 2022, it consistently froze designated addresses within three days after sanctions were announced.

3.2.2 Do Targeted Addresses Cease Activity After Tether Freezes?

We next examine the direct effects of Tether freezes on the targeted addresses. A freeze mechanically prevents the address from transacting in Tether, but a broader question is whether the targeted address also ceases activity in other crypto tokens and cryptocurrencies.⁵²

Figure 9, Panel B, plots the cumulative inflows received by frozen addresses over their observed

⁵¹See the archived [2022 announcement](#) regarding awaiting law enforcement instructions before freezing addresses and [2023 announcement](#) of the new policy to freeze sanctioned addresses.

⁵²To be consistent with the tracing framework that conservatively excludes large addresses, for the remainder of the analyses, we only keep frozen addresses with less than 2,000 transactions. This ensures that we do not trace paths associated with shadow exchanges.

lifetimes. Each bubble represents an individual transfer into an address, with its vertical position and size reflecting the cumulative inflow received by that address at that point in time. Sequences of bubbles therefore trace the inflow trajectory of a single address, while the red cross marks the freeze date. Prior to being frozen, addresses vary substantially in both the duration of activity and the amount of flows received, with many addresses accumulating substantial inflows. Following the freeze, most trajectories end, particularly for USDT activity, although a small number of addresses continue to transact in other assets, primarily USDC and Ether.

As another look at individual wallet activity around Tether freezes, Figure 10, Panel A, presents a more granular event-time analysis of inflows and outflows in the hours immediately before and after each freeze. Bars above zero on the horizontal axis indicate inflows and bars below zero indicate outflows. Hatched bars denote flows that arise from token swaps rather than simple transfers. Activity rises sharply around the freeze event, with substantial movement of funds shortly before the address is frozen. After the freeze, USDT is immobilized and thus USDT activity at the targeted addresses largely disappears, while some activity continues in other assets.⁵³ Within the first hour, frozen addresses swap USDC into DAI; in the following hours, they transfer ETH and DAI out of the frozen wallets. Reliance on the stablecoin DAI is especially notable because the issuer of DAI tokens does not possess the functionality to freeze the tokens.⁵⁴

3.2.3 Do Targeted Users Shift Activity to Related Wallets After Tether Freezes?

Even if a targeted address becomes inactive following a freeze, the underlying user may remain active in crypto markets by shifting activity to other wallets under their control. We therefore examine whether activity moves to non-frozen addresses plausibly controlled by the same users and whether these addresses change the assets and services they use.

Figure 10, Panel B, provides initial evidence from addresses linked to the frozen wallets through

⁵³Examining all the activity in the addresses, we also formally test and find some evidence for a decrease in address activity utilizing a formal DiD design as described in the OFAC sanctions analysis. The DiD estimates indicate that treated group outflows decline after the freeze by 10.8% statistically significant at only the 10% level, as seen in Table 4, Column (1). There is also an increase in outflows prior to the freeze consistent with the spike in activity likely precipitating the freeze (as shown in Figure 1A.20).

⁵⁴The issuer has since rebranded and now focuses on the stablecoin USDS, which contains the functionality required to freeze tokens.

gas clustering. Two patterns stand out. First, unlike the frozen addresses themselves, these related addresses remain active after the freeze, with elevated inflows and outflows during the first 24 hours. This continued activity is consistent with users maintaining access to crypto markets by shifting transactions to other wallets under their control. Second, the composition of activity changes: related addresses swap both USDC and TUSD into DAI shortly after the freeze.⁵⁵ Thus, in addition to substituting across wallets, users appear to substitute from freezable stablecoins toward assets less exposed to issuer seizure, using DeFi swaps to make this transition.

Motivated by the continued activity of gas-clustered wallets, we next test wallet-level substitution more comprehensively. Using the same design as in the analysis on OFAC sanctions, we identify three sets of non-frozen addresses plausibly linked to the targeted user: (i) gas-clustered addresses related to the frozen wallet, (ii) downstream deposit addresses that receive tainted funds from frozen addresses, and (iii) additional deposit addresses clustered around those tainted deposit addresses. These measures capture progressively broader channels through which the same underlying user may continue moving funds after the focal wallet is frozen. For each freeze cohort, we compare activity in these related addresses with random control addresses that were active in USDT prior to the freeze.

Figure 11 plots the corresponding dynamic DiD estimates, and Table 4 reports the average effects. Across all three definitions, activity increases following the freeze rather than declining. Gas-clustered addresses exhibit a 43.9% increase in outflows. Downstream deposit addresses and clustered deposit addresses exhibit increases in inflows of 48.4% and 69.6%, respectively. The increasing effects as we move from closely related wallets to downstream deposit channels are consistent with targeted users redirecting funds through alternative wallets and continuing to move those funds into crypto-market deposit channels after the original address is frozen.

The observed token substitution from freezable stablecoins toward non-freezable tokens in clustered wallets raises the question of whether affected users also increase their broader use of DeFi services after a freeze. To formally study the use of DeFi services like swaps or bridges, we trace frozen addresses and their gas-clustered addresses to determine their downstream activity. The weighted

⁵⁵TUSD refers to TrueUSD, a U.S. dollar-backed stablecoin that can also be frozen by its issuer.

or dollar-volume share of flows routed to DeFi services increases by approximately 11.48 percentage points compared to the control group following the freeze (as shown in Table IA.6). We do not observe differences between treated and control groups prior to the shock (as shown in Figure IA.21). This pattern is consistent with affected users relying more heavily on decentralized services as they shift away from assets subject to issuer freezes. The result also highlights the importance of coordination across stablecoin issuers: if some stablecoins remain outside the reach of seizure mechanisms, targeted users may redirect assets toward those alternatives.⁵⁶

Overall, Tether freezes sharply restrict activity in USDT at the designated address and often coincide with the address becoming largely inactive. However, related wallets become more active, funds continue to reach downstream deposit addresses, and users shift toward DeFi and tokens less exposed to issuer freezes. Substitution to other observable wallets and tokens implies that activity after enforcement has a similar level of transparency; however, because we cannot observe all possible user channels, we cannot draw a definitive conclusion on overall blockchain transparency.

4. Comparing Policies Targeting Services and Users

Having presented the results across the four policy settings, we next summarize and compare their main patterns. Table 5 organizes the findings into direct effects on targeted services or wallets and substitution toward alternative channels. For policies targeting services, the direct effects are substantial. The Tornado Cash sanctions are followed by large declines in both aggregate and hacker flows to Tornado Cash relative to overseas exchanges. Although Western exchanges reduced their receipt of Tornado Cash flows after the sanctions, overseas exchanges continued to receive substantial flows until subsequent DOJ settlements, after which flows to the targeted exchanges declined.

Turning to substitution effects, hackers shift toward other channels following the Tornado Cash sanctions, particularly swaps, bridges, and wrapped Ether, while activity on privacy-focused blockchains such as Monero, Dash, and Zcash does not increase. Following DOJ exchanges settlements, we do not

⁵⁶In the U.S., the GENIUS Act was signed on July 18, 2025, requiring stablecoin issuers to comply with U.S. law-enforcement requests for asset seizure. However, other stablecoins may be issued and operated under foreign regulatory regimes, such as the ruble-pegged A7A5 stablecoin commonly associated with Russian sanctions evasion.

find a noticeable increase in illicit activity flowing through other exchanges, but the setup lacks power because of the disparate nature of volume to various exchanges. Overall, these results indicate that policies directed at major services are followed by substantial declines in usage and illicit flows, as criminal users reduce their use of the targeted services. Interestingly, the substitution that we observe following the Tornado Cash sanctions is primarily toward alternative on-chain channels that remain relatively transparent and more traceable.

Policies targeting users produce a different pattern. For the direct effects, OFAC sanctions often arrive after substantial funds have already left the designated wallet, and many sanctioned wallets are already inactive by the time of designation. For sanctioned Ethereum wallets, we also observe substantial funds moving through Tornado Cash after designation, illustrating how users can evade wallet-level sanctions by obscuring their identity. Stablecoin freezes similarly restrict activity at the directly frozen address: USDT can no longer be transferred, and most targeted wallets subsequently exhibit little activity. The substitution effects, however, show that restrictions on the focal wallet do not stop the underlying user. Activity in related non-designated wallets does not decline following OFAC sanctions, and downstream deposit addresses associated with sanctioned users actually become more active. Following stablecoin freezes, users similarly shift activity toward related wallets and downstream deposit addresses. They also use DeFi services to substitute from freezable to non-freezable stablecoins. The aggregate scale of stablecoin freezes, while sizeable, remains small relative to observable illicit flows.

Overall, policies targeting users can restrict particular wallets and immobilize some funds, but the underlying users often retain access to crypto markets through related, non-designated addresses. Policies directed at services can remove a particular laundering channel, forcing users to substitute toward alternative channels that, in our setting, are generally more transparent and traceable. Policies directed at individual wallets leave greater scope for users to continue operating through substitute addresses. We do not evaluate the relative costs and externalities of these policies.

5. Conclusion

We provide the first empirical investigation of crypto anti-money laundering policies. Policies targeting services are followed by substantial declines in illicit use of the targeted channels. Hackers migrate to alternative channels of bridges and swaps that are generally more transparent and traceable. Policies targeting individual users are often applied to addresses after the funds have been moved and, with the exception of stablecoin freezes, are not that successful at stopping criminals from moving funds. Additionally, users quickly migrate to related addresses and appear relatively unconstrained in their subsequent transactions. Policies targeting services appear more disruptive to criminal flows than policies targeting users.

Our findings imply several areas for interface with policy. First, the proposed CLARITY Act largely exempts mixers and DeFi from AML laws. Given that our findings indicate that mixers and other DeFi services, such as swaps and bridges, are frequently utilized by illicit foreign actors, this appears to be granting immunity to players that help facilitate illicit activity and will likely make the job of anti-terrorism and law enforcement much more difficult. Second, current U.S. DOJ policy indicates a pivot to focus primarily on sanctioning users rather than actions against entities or service providers. Our findings indicate that this approach is significantly hampered if users can easily access mixing channels to evade tracing technology. Finally, crypto industry exchanges commonly state that they can self-police and stop illicit activity without regulatory oversight. Our findings indicate that historically the reputation and goodwill of exchanges to stop crime do not appear to be an effective deterrent. Thus, rule of law and enforcement, though seemingly old fashioned, have not been replaced by the governance structure of blockchain technology.

Our research demonstrates how the blockchain makes forensic tracing and monitoring more straightforward than in other contexts, such that large-scale monitoring could be automated. The crypto criminal and regulatory landscape appear to be rapidly changing. We hope additional research will further analyze different types of enforcement mechanisms, crypto crime, obfuscation methods, and policies to help enact reasonable guidelines that both facilitate legitimate capital flows and deter crime.

References

- Al-Tawil, Tareq Na'el, 2022, Anti-money laundering regulation of cryptocurrency: Uae and global approaches, *Journal of Money Laundering Control* 26, 1150–1164.
- Amiran, Dan, Bjørn N. Jørgensen, and Daniel Rabetti, 2022, Coins for bombs: The predictive ability of on-chain transfers for terrorist attacks, *Journal of Accounting Research* 60, 427–466.
- Anderson, Ross, Ilia Shumailov, and Mansoor Ahmed, 2018, Making Bitcoin Legal, *Security Protocols XXVI* 11286, 243–253.
- Auer, Raphael, Cyril Monnet, and Hyun Song Shin, 2025, Distributed ledgers and the governance of money, *Journal of Financial Economics* 167, 104026.
- Becker, Gary S., 1968, Crime and punishment: An economic approach, *Journal of Political Economy* 76, 169–217.
- Béres, Ferenc, István A Seres, András A Benczúr, and Mikerah Quintyne-Collins, 2021, Blockchain is watching you: Profiling and deanonymizing ethereum users, in *2021 IEEE international conference on decentralized applications and infrastructures (DAPPS)*, 69–78, IEEE.
- Brownworth, Anders, Jon Durfee, Michael Junho Lee, and Antoine Martin, 2024, Regulating decentralized systems: Evidence from sanctions on tornado cash, *Staff Reports (Federal Reserve Bank of New York)*.
- Campbell-Verduyn, Malcolm, 2018, Bitcoin, crypto-coins, and global anti-money laundering governance, *Crime, Law and Social Change* 69, 283–305.
- Chainalysis, 2026, The 2026 Crypto Crime Report, Technical report, Chainalysis.
- Charoenwong, Ben, Daehan Kim, Robert M Kirby, and Jonathan Reiter, 2026, Enforcement speeds in defi: Limits to a race against time, Working Paper.
- Chong, Alberto, and Florencio Lopez-De-Silanes, 2015, Money laundering and its regulation, *Economics & Politics* 27, 78–123.
- Cong, Lin, Kimberly Grauer, Daniel Rabetti, and Henry Updegrave, 2023a, Blockchain forensics and crypto-related cybercrimes, World Scientific Publishing.
- Cong, Lin William, Xi Li, Ke Tang, and Yang Yang, 2023b, Crypto wash trading, *Management Science* 69, 6427–6454.
- Cong, Will, Campbell Harvey, Daniel Rabetti, and Zong-Yu Wu, 2025, An anatomy of crypto-enabled cybercrimes, *Management Science* 71, 3622–3633.
- Cristodaro, Raffaele, Benjamin Kraner, and Claudio J. Tessone, 2025, The impact of sanctions on decentralised privacy tools: A case study of tornado cash, Working Paper.
- Cuéllar, Mariano-Florentino, 2002, The tenuous relationship between the fight against money laundering and the disruption of criminal finance, *J. Crim. L. & Criminology* 93, 311.

- Draca, Mirko, and Stephen Machin, 2015, Crime and Economic Incentives, *Annual Review of Economics* 7, 389–408.
- Easley, David, Maureen O'Hara, Songshan Yang, and Zhibai Zhang, 2026, Microstructure and market dynamics in crypto markets, *Journal of Financial Markets* 101071.
- El Siwi, Yara, 2018, Mafia, money-laundering and the battle against criminal capital: the Italian case, *Journal of Money Laundering Control* 21, 124–133.
- Ferwerda, Joras, 2009, The economics of crime and money laundering: Does anti-money laundering policy reduce crime?, *Review of Law & Economics* 5, 903–929.
- Foley, Sean, Jonathan R Karlsen, and Tālis J Putniņš, 2019, Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?, *Review of Financial Studies* 32, 1798–1853.
- Fracassi, Cesare, Eric Lee, and Tarik Roukny, 2025, No Country for Dirty Money? The Economic Footprint of Anti-Money Laundering Standards, Working Paper.
- Félez-Viñas, Ester, Luke Johnson, and Tālis J. Putniņš, 2022, Insider Trading in Cryptocurrency Markets, Working Paper.
- Gandal, Neil, JT Hamrick, Tyler Moore, and Tali Oberman, 2018, Price manipulation in the bitcoin ecosystem, *Journal of Monetary Economics* 95, 86–96.
- Griffin, John M, and Samuel Kruger, 2024, What is Forensic Finance?, *Foundations and Trends® in Finance* 14, 137–243.
- Griffin, John M., and Kevin Mei, 2025, How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering, Working Paper.
- Griffin, John M., and Amin Shams, 2020, Is Bitcoin Really Untethered?, *Journal of Finance* 75, 1913–1964.
- Griffin, John M., Zirui Wang, and J.A. Artero Calvo, 2026, Is Criminal Crypto a Sideshow? Illicit Activities across Three Major Blockchains, Working Paper.
- Hamrick, J.T., Farhang Rouhi, Arghya Mukherjee, Amir Feder, Neil Gandal, Tyler Moore, and Marie Vasek, 2021, An examination of the cryptocurrency pump-and-dump ecosystem, *Information Processing and Management* 58, 102506.
- Leukfeldt, E. Rutger, Edward R. Kleemans, Edwin W. Kruisbergen, and Robert A. Roks, 2019, Criminal networks in a digitised world: on the nexus of borderless opportunities and local embeddedness, *Trends in Organized Crime* 22, 324–345.
- Levi, Michael, 2015, Money for crime and money from crime: Financing crime and laundering crime proceeds, *European Journal on Criminal Policy and Research* 21, 275–297.
- Levi, Michael, Peter Reuter, and Terence Halliday, 2017, Can the aml system be evaluated without better data?, *Crime, Law and Social Change* 69, 307–328.

- Li, Tao, Donghwa Shin, and Baolian Wang, 2025, Cryptocurrency Pump-and-Dump Schemes, *Journal of Financial and Quantitative Analysis* Forthcoming.
- Makarov, Igor, and Antoinette Schoar, 2025, Blockchain Analysis of the Bitcoin Market, Working Paper.
- Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage, 2013, A fistful of bitcoins: characterizing payments among men with no names, *Proceedings of the 2013 conference on Internet measurement conference* 127–140.
- Mirenda, Litterio, Sauro Mocetti, and Lucia Rizzica, 2022, The economic effects of mafia: Firm level evidence, *American Economic Review* 112, 2748–2773.
- Moore, Tyler, Richard Clayton, and Ross Anderson, 2009, The Economics of Online Crime, *Journal of Economic Perspectives* 23, 3–20.
- Möser, Malte, and Arvind Narayanan, 2019, Effective cryptocurrency regulation through blacklisting, Working Paper.
- Nguyen, Khanh Quoc, and Tālis J. Putniņš, 2023, Stealing digital assets: Evidence from cryptocurrency exchange hacks, *SSRN Electronic Journal* .
- Pennec, Guénolé Le, Ingo Fiedler, and Lennart Ante, 2021, Wash trading at cryptocurrency exchanges, *Finance Research Letters* 43, 101982.
- Phua, Kenny, Bo Sang, Chishen Wei, and Gloria Yang Yu, 2025, The Economics of Financial Scams: Evidence from Initial Coin Offerings, Working Paper.
- Pol, Ronald F., 2020, Anti-money laundering: The world’s least effective policy experiment? Together, we can fix it, *Policy Design and Practice* 3, 73–94.
- Quirk, Peter J., 1996, Macroeconomic implications of money laundering, *IMF Working Papers* 96, 1.
- Sokolov, Konstantin, 2021, Ransomware activity and blockchain congestion, *Journal of Financial Economics* 141, 771–782.
- Tanzi, Vito, 1996, Money Laundering and the International Financial System, *IMF Working Papers* 1996, 1.
- Tironsakkul, Tin, Manuel Maarek, Andrea Eross, and Mike Just, 2022, Context matters: Methods for bitcoin tracking, *Forensic Science International: Digital Investigation* 42–43, 301475.
- U.S. Department of the Treasury, 2024, 2024 National Money Laundering Risk Assessment.
- Victor, Friedhelm, 2020, Address Clustering Heuristics for Ethereum.
- Wronka, Christoph, 2023, Financial crime in the decentralized finance ecosystem: new challenges for compliance, *Journal of Financial Crime* 30, 97–113.

Figure 1. Tornado Cash Transaction Networks

This figure visualizes flows involving Tornado Cash. It illustrates the network of flows involving Tornado Cash, with senders positioned on the left and receivers on the right. Edges concave down represent flows moving from left to right (e.g., the curve moves as if going from 9 o'clock to 3 o'clock), while edges concave up indicate flows moving from right to left (e.g., from 3 o'clock to 9 o'clock). This is a sample constructed by selecting the largest 2,500 nodes within 5 hops from Tornado Cash and keeping connected paths. This was selected to reflect the largest ~10,000 edges related to Tornado Cash.

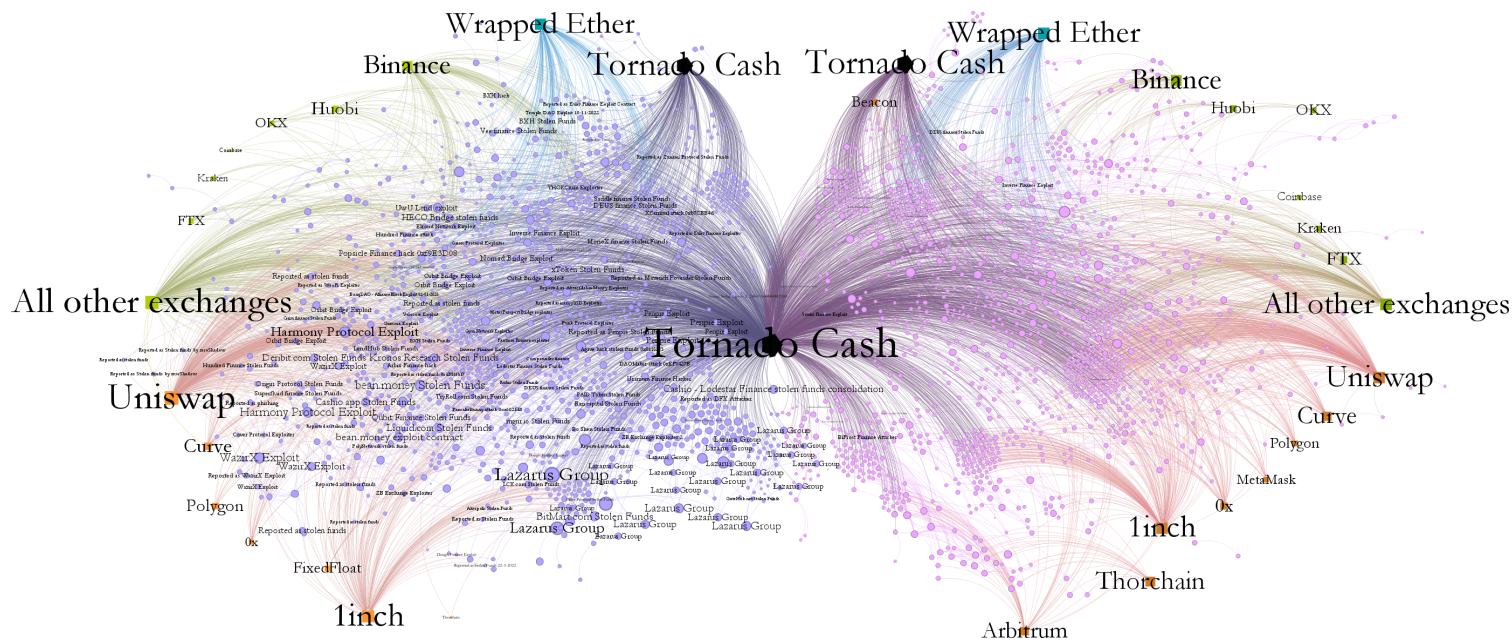
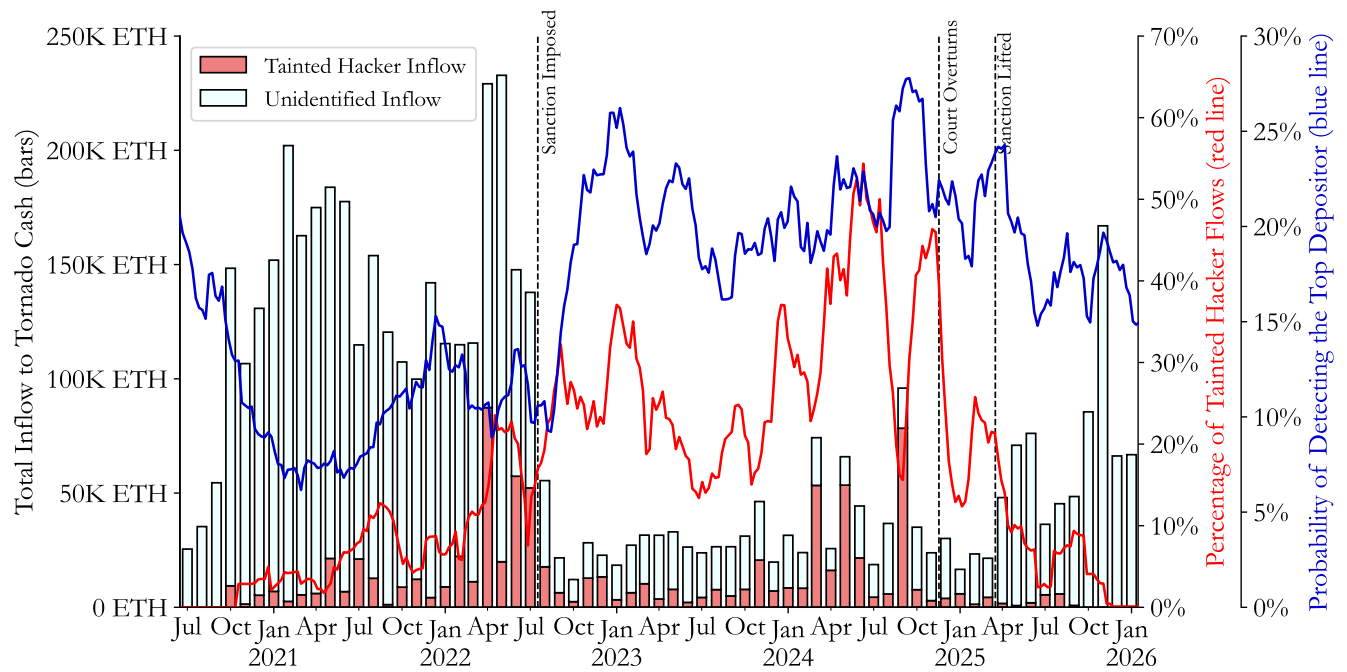


Figure 2. Tornado Cash Sanctions: Direct Effects on Inflows and Hacker Usage

This figure examines Tornado Cash activity and hacker use around the U.S. Treasury sanctions. Panel A plots monthly ETH inflows to Tornado Cash, decomposed into flows that are linked to proceeds from reported hacks, and all other flows. The red line reports the share of total inflows originating from identified hacker addresses, while the blue line reports the estimated probability of matching a withdrawal to the largest depositor. Both lines are calculated weekly and displayed as ten-week moving averages. The vertical dashed lines mark the imposition of sanctions on August 8, 2022, the November 26, 2024 court ruling overturning them, and their removal on March 21, 2025. Panel B plots monthly difference-in-differences coefficients comparing log ETH flows from reported hacks to Tornado Cash with flows from the same hacks to overseas centralized exchanges. July 2022 is the omitted month. The regression includes hacker-address and month fixed effects; standard errors are double-clustered by hacker address and month, and the error bars report 95% confidence intervals.

Panel A: Tornado Cash Inflows



Panel B: Hacker Flows to Tornado Cash Relative to Overseas Exchanges

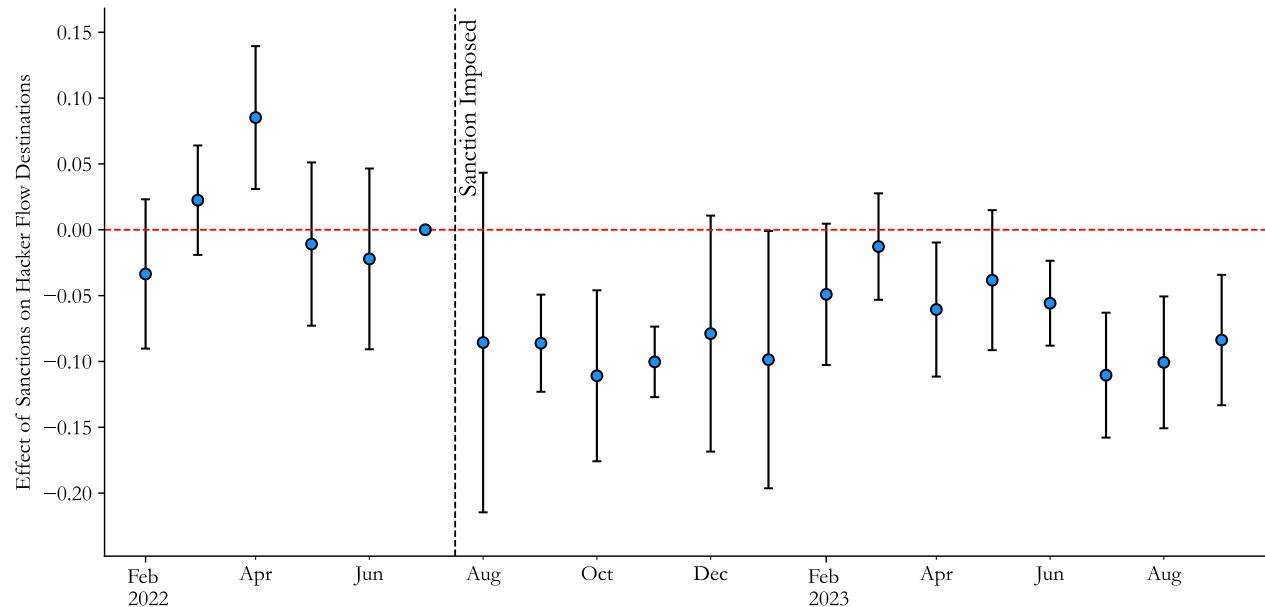
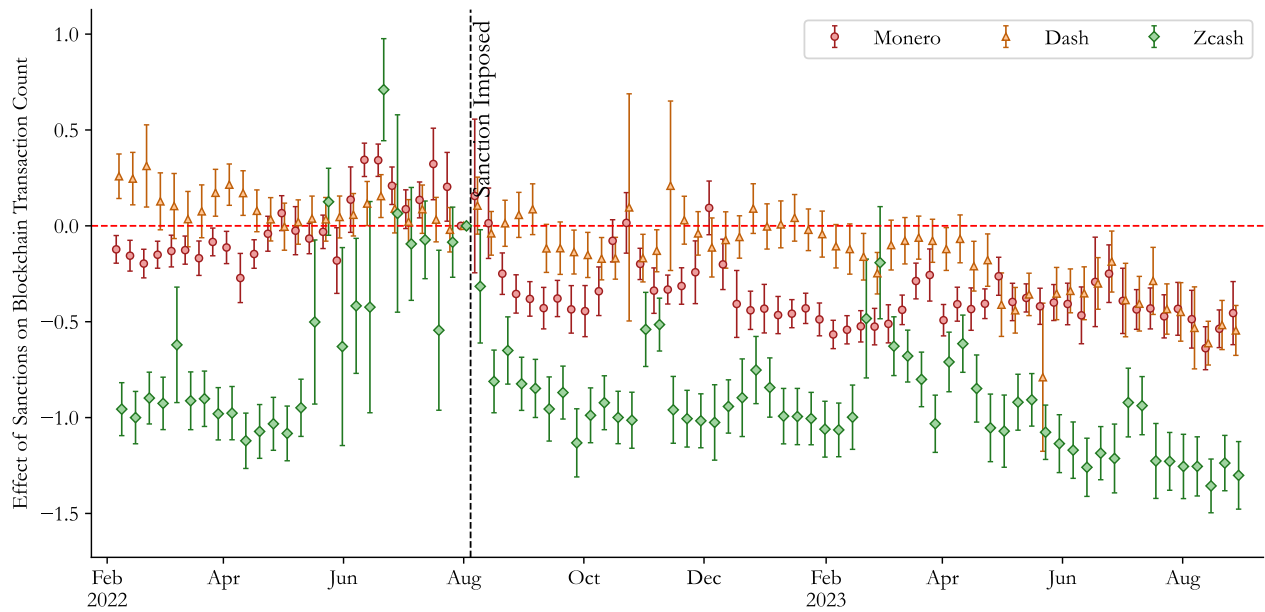


Figure 3. Tornado Cash Sanctions: Substitution Effects on Privacy Coins and Hacker Flows

This figure examines changes in privacy-focused blockchain activity and hacker destination choices following the U.S. Treasury's August 8, 2022 sanctions on Tornado Cash. Panel A plots weekly difference-in-differences coefficients for transaction activity on Monero, Dash, and Zcash, with Bitcoin and Ethereum serving as comparison blockchains. The dependent variable is the log daily number of transactions. Panel B plots monthly difference-in-differences coefficients for ETH flows from reported hacker incidents to decentralized-exchange swaps, bridges, and wrapped ETH. Each destination is separately compared with overseas centralized exchanges. The dependent variable is the log amount of ETH traced from a reported hacker incident to the respective destination in a given month. For both panels, July 2022 is the omitted baseline. Regressions in Panel A include a treated-chain indicator and date fixed effects, with standard errors clustered by date. Regressions in Panel B include hacker-address and month fixed effects, with standard errors double-clustered by hacker address and month. Error bars report 95% confidence intervals, and the vertical dashed line marks the imposition of the Tornado Cash sanctions.

Panel A: Privacy-Chain Activity Relative to Bitcoin and Ethereum



Panel B: Hacker Flows to Alternative Channels Relative to Overseas Exchanges

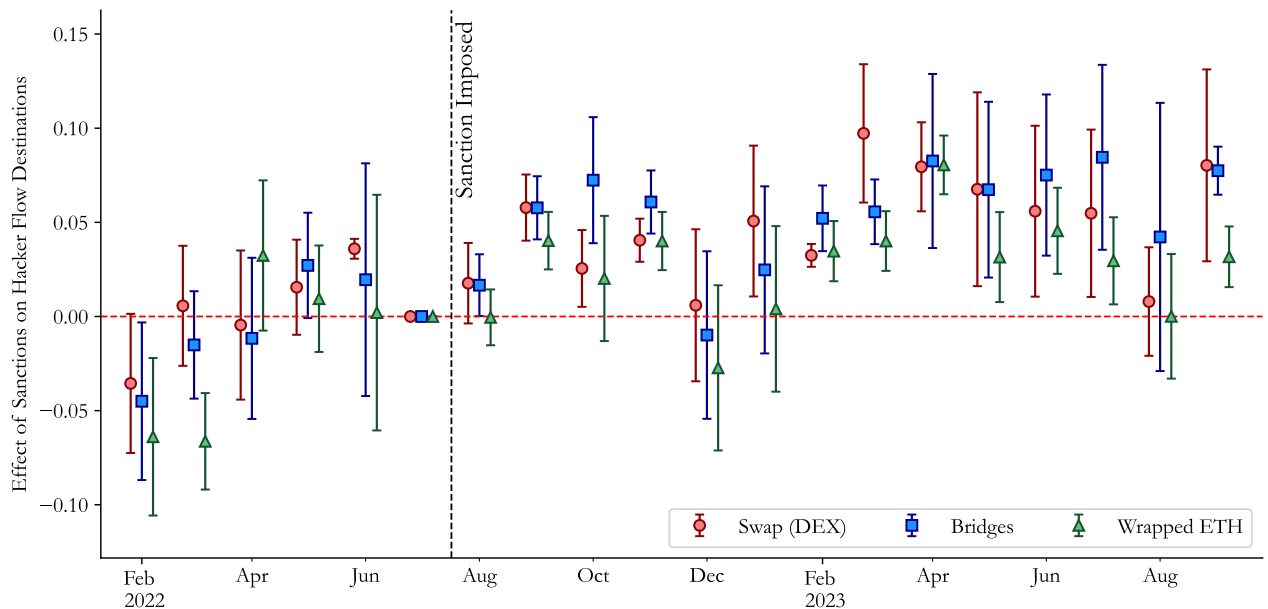
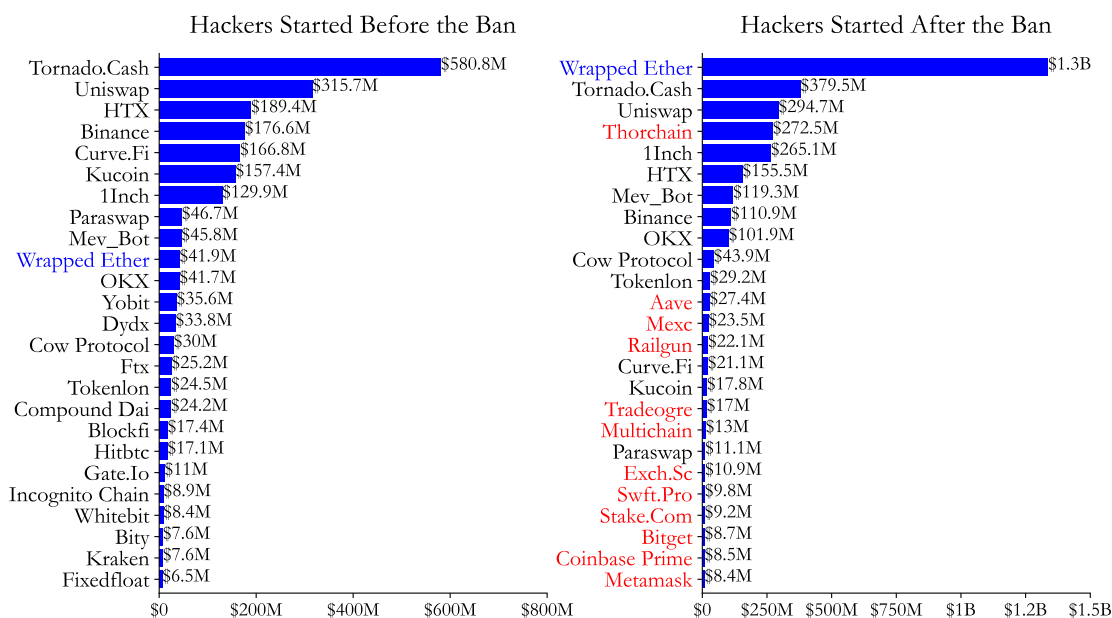


Figure 4. Tornado Cash Sanctions: Substitution Effects on Hacker Flow Destinations

This figure examines how hacker flow destinations change following the Tornado Cash ban and illustrates one prominent post-sanction laundering route using the 2025 Bybit hack. Panel A displays flows from reported hacker addresses to various destinations for two cohorts: hackers who started moving criminal funds before (left) and after (right) the ban. It highlights sizable shifts in blue and entirely new top destinations in red. Panel B shows the flows of proceeds of the \$1.4 billion theft from Bybit in February 2025. The left-hand side shows funds exiting Bybit and being forwarded through Ethereum by the hackers to the different services represented in the center. On the right-hand side of Thorchain are Bitcoin addresses, representing addresses downstream of bridge transactions. Concave down edges represent flows from a node on the left to another node on the right, and vice versa for concave up edges. Edges are colored by the flow amount in dollars, and nodes are colored by the corresponding types. Last updated August 2025.

Panel A: Hacker Destinations Before and After Sanctions



Panel B: Bybit Hack and Flows to Bridge

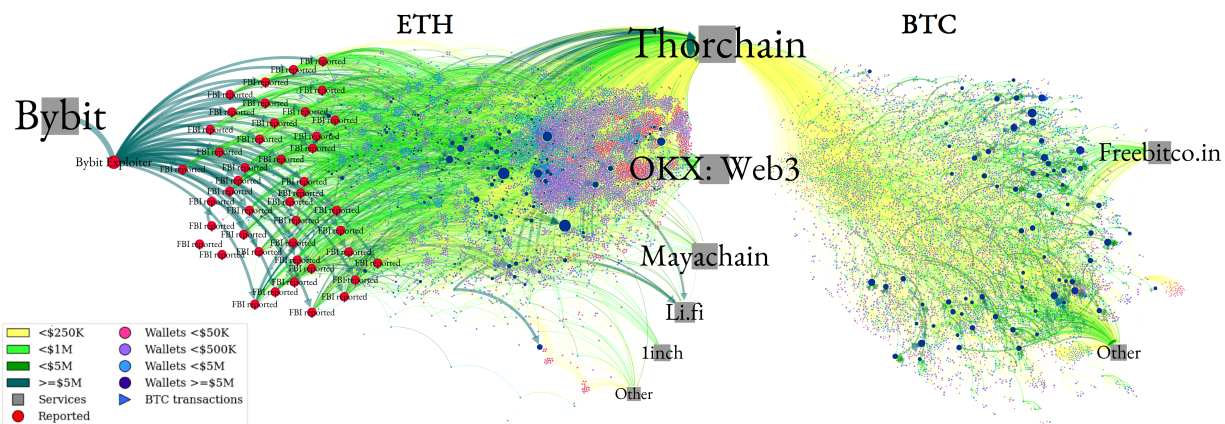
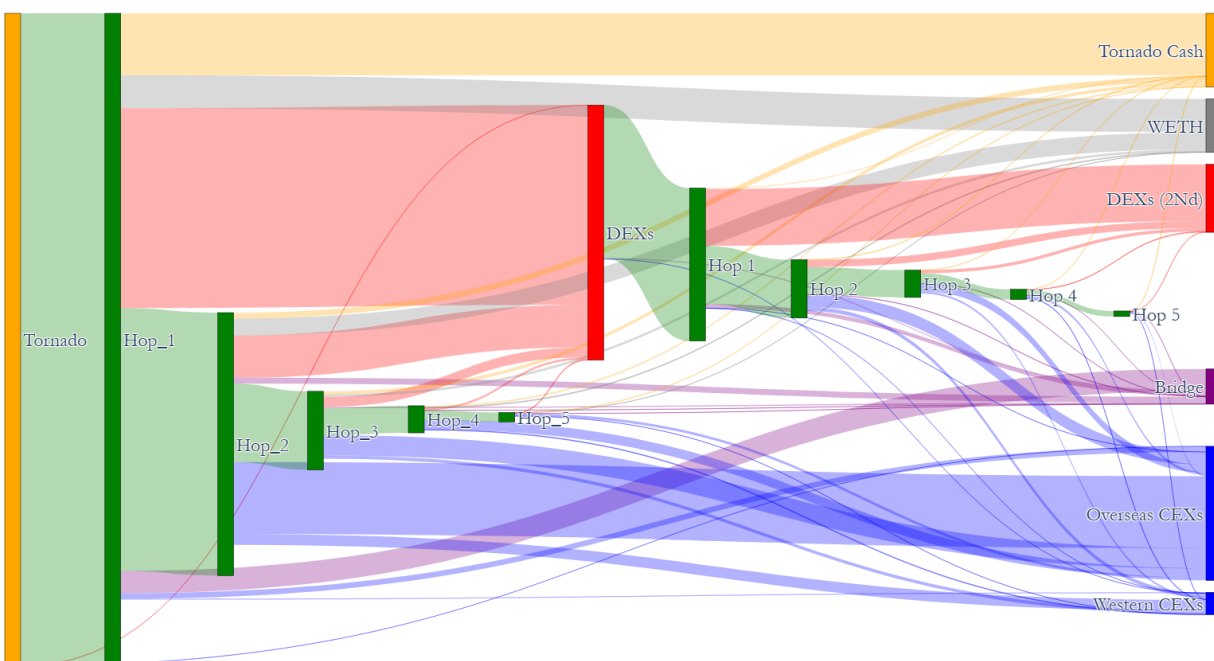


Figure 5. Tornado Cash Outflows to Destinations by Intermediate Hop

This figure visualizes Tornado Cash outflows and their destinations before and after the Tornado Cash ban on August 8, 2022, using Sankey diagrams. Panel A shows outflows before the ban, and Panel B shows outflows after the ban. In each diagram, flows originate from Tornado Cash on the left and proceed through intermediate hops (e.g., Hop 1, Hop 2, shown in green) before reaching final destinations on the right. Flows into centralized exchanges (CEXs) are shown in blue, decentralized exchanges (DEXs) in red, blockchain bridges in purple, and wrapped ETH (WETH) in gray. When flows arrive at a DEX, funds are traced through additional hops to identify their ultimate destinations after swaps. The width of each flow indicates the relative volume of funds moving along that path. Western exchanges are Coinbase, Crypto.com, Gemini, and Kraken, and all other exchanges are included as overseas exchanges.

Panel A: Before Tornado Cash Ban



Panel B: After Tornado Cash Ban

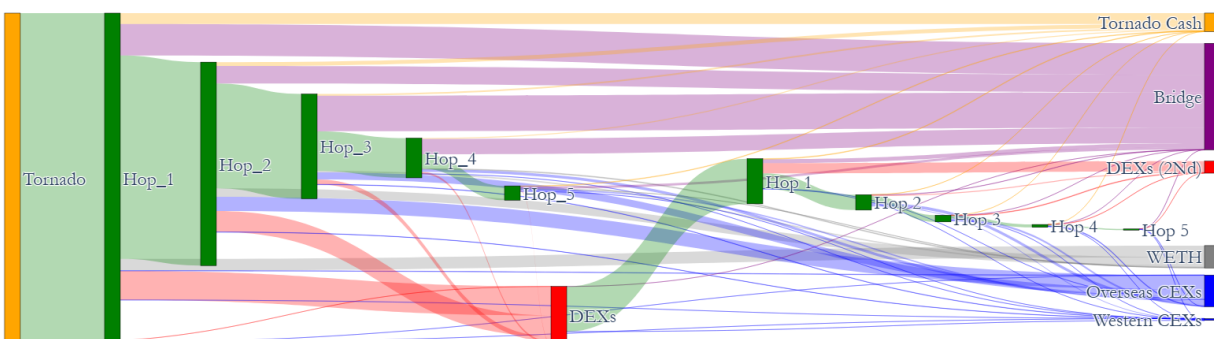
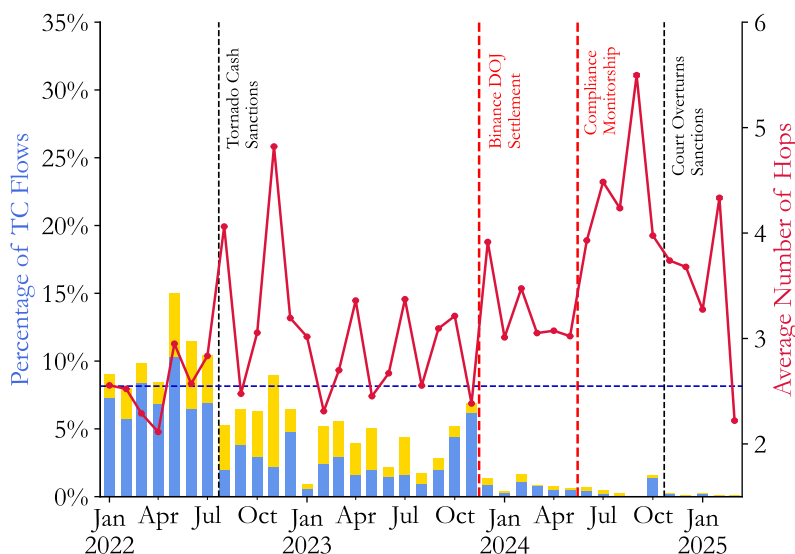


Figure 6. DOJ Settlement with Binance: Effects on Sanctioned Flows to Exchanges

This figure examines changes in sanctioned Tornado Cash flows reaching centralized exchanges around the Binance DOJ settlement and subsequent compliance monitorship. Panel A shows Tornado Cash outflows to Binance, and Panel B shows Tornado Cash outflows to other overseas exchanges. In both panels, bars represent the percent of monthly outflows to the respective destination. Blue bars represent flows that moved from Tornado Cash to the destination without passing through any decentralized exchanges (DEXs), while yellow bars represent flows that were first sent from Tornado Cash to DEXs, and then arrived at exchanges after being traced through DEXs. The red line shows the average number of hops before reaching the destination. The vertical dashed lines mark the August 8, 2022 Tornado Cash sanctions, the November 21, 2023 Binance DOJ settlement, the May 17, 2024 appointment of the compliance monitors, and the November 26, 2024 court ruling overturning the Tornado Cash sanctions.

Panel A: Tornado Cash Outflows to Binance



Panel B: Tornado Cash Outflows to Other Overseas Exchanges

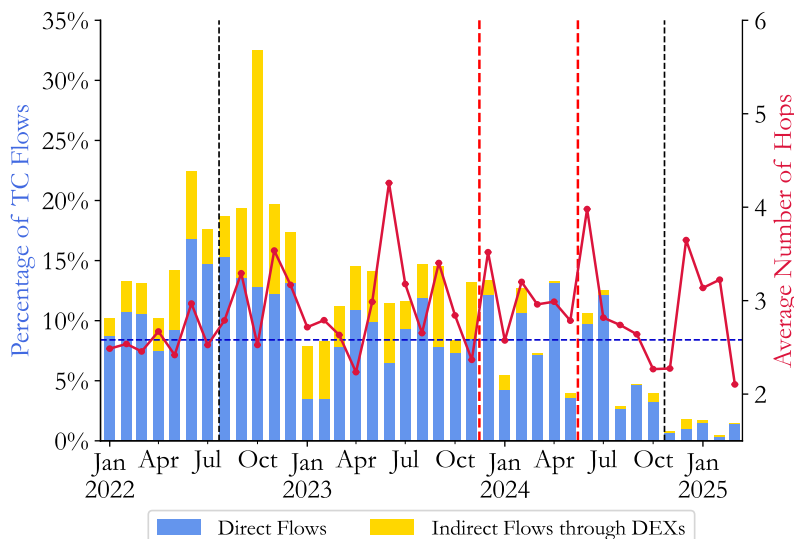
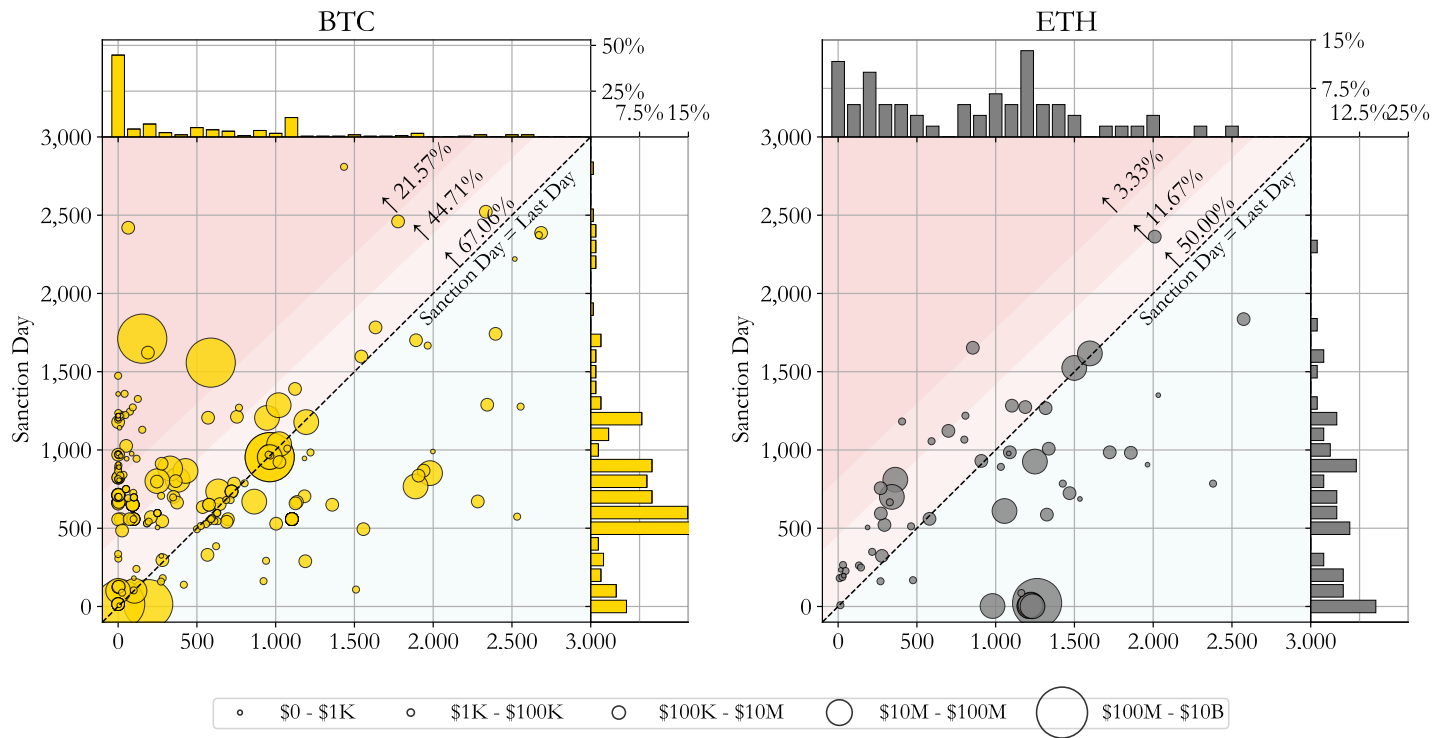


Figure 7. OFAC Sanctions against Users: Sanction Timing and Direct Effects on Fund Flows

This figure examines the timing of OFAC sanctions on individual wallets and the movement of funds associated with those wallets around designation. Panel A compares sanction timing with the transaction histories of sanctioned Bitcoin (left) and Ethereum (right) addresses. Each bubble represents a sanctioned address, with size proportional to total lifetime inflow in dollars. The x-axis reports the number of days between the first and last transaction, while the y-axis reports the number of days between the first transaction and the sanction date. Addresses on the 45-degree line last transact on the sanction date. The darker red regions identify addresses sanctioned more than one or two years after their last transaction. Histograms along the top and right margins show the distributions of the last-transaction and sanction dates, respectively. Panel B shows where funds associated with sanctioned wallets are located before and after the sanction date, including balances remaining in the sanctioned addresses, funds remaining elsewhere on-chain, and funds traced to crypto services. Each bar represents a monthly cross-section snapshot of destinations. “Unidentified” denotes addresses with more than 2,000 transactions, where tracing is stopped and no service or entity attribution is available. Hatched lines indicate services. The red line reports percentage of inflows transferred to services.

Panel A: Sanctioned Day versus Last Transaction Day



Panel B: Balance Traced from Sanctioned Addresses to End Destinations

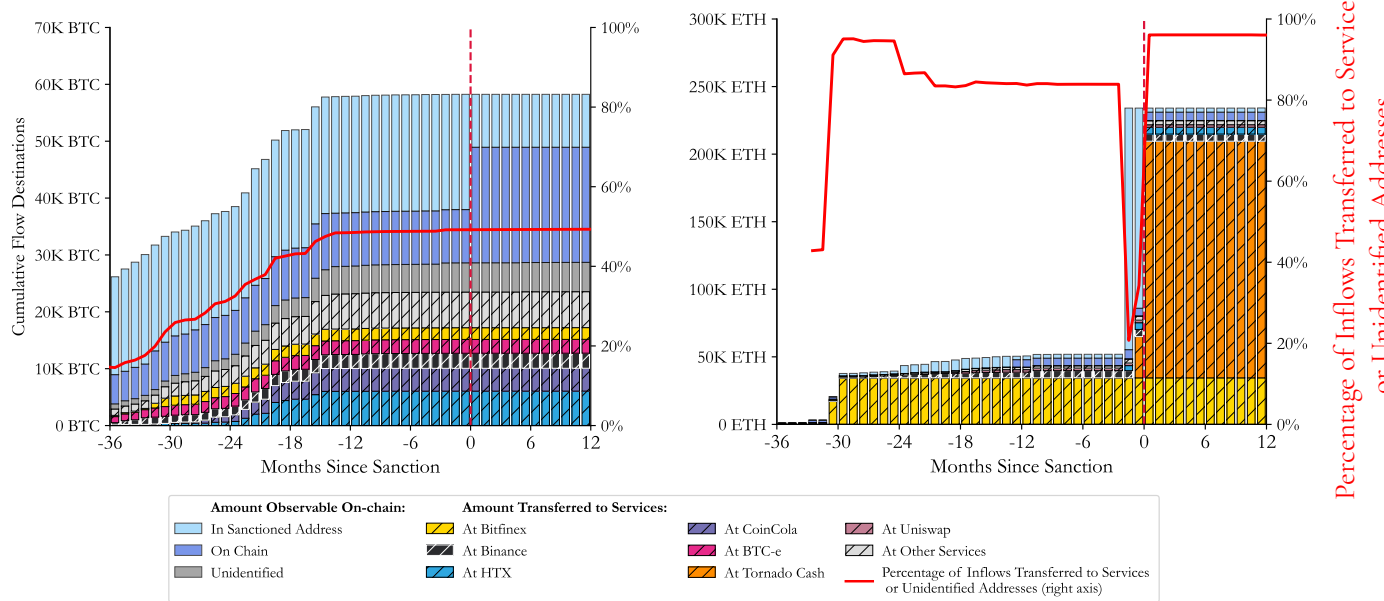


Figure 8. OFAC Sanctions against Users: Substitution Effects on Related Wallets

This figure studies whether activity shifts to non-designated addresses linked to sanctioned users following OFAC sanctions. Panel A plots dynamic difference-in-differences estimates of outflows from gas-clustered addresses related to sanctioned wallets. Panel B plots estimates of inflows to downstream deposit addresses tainted by funds from sanctioned wallets. Panel C plots estimates of inflows to additional deposit addresses clustered around those tainted deposit addresses. For all panels, the dependent variable is $\log(1 + \text{Flow}_{i,c,t})$, where $\text{Flow}_{i,c,t}$ is the panel-specific inflow or outflow for address i in sanction cohort c and week t . Flows are measured in U.S. dollars using closing prices on the day of the transaction. The regressions compare each set of related addresses with matched control addresses around the sanction date. A cohort is defined by an OFAC sanction date and includes all treated addresses assigned to that sanction event. Control candidates are drawn from addresses with activity in the year before the sanction event. The candidate pool is restricted to addresses matched to the treated addresses on transaction count and transaction volume and excludes known service addresses and treated addresses. 50 control addresses are then randomly drawn for each treated unit. The analysis is at the address by week level. Each regression includes cohort-address fixed effects and cohort-by-week fixed effects. The sample spans 52 weeks before and after the sanction date, the omitted period is the first event period, and standard errors are clustered by sanction cohort. The sample focuses on OFAC sanctions against individuals or organizations. This figure corresponds with Table 3.

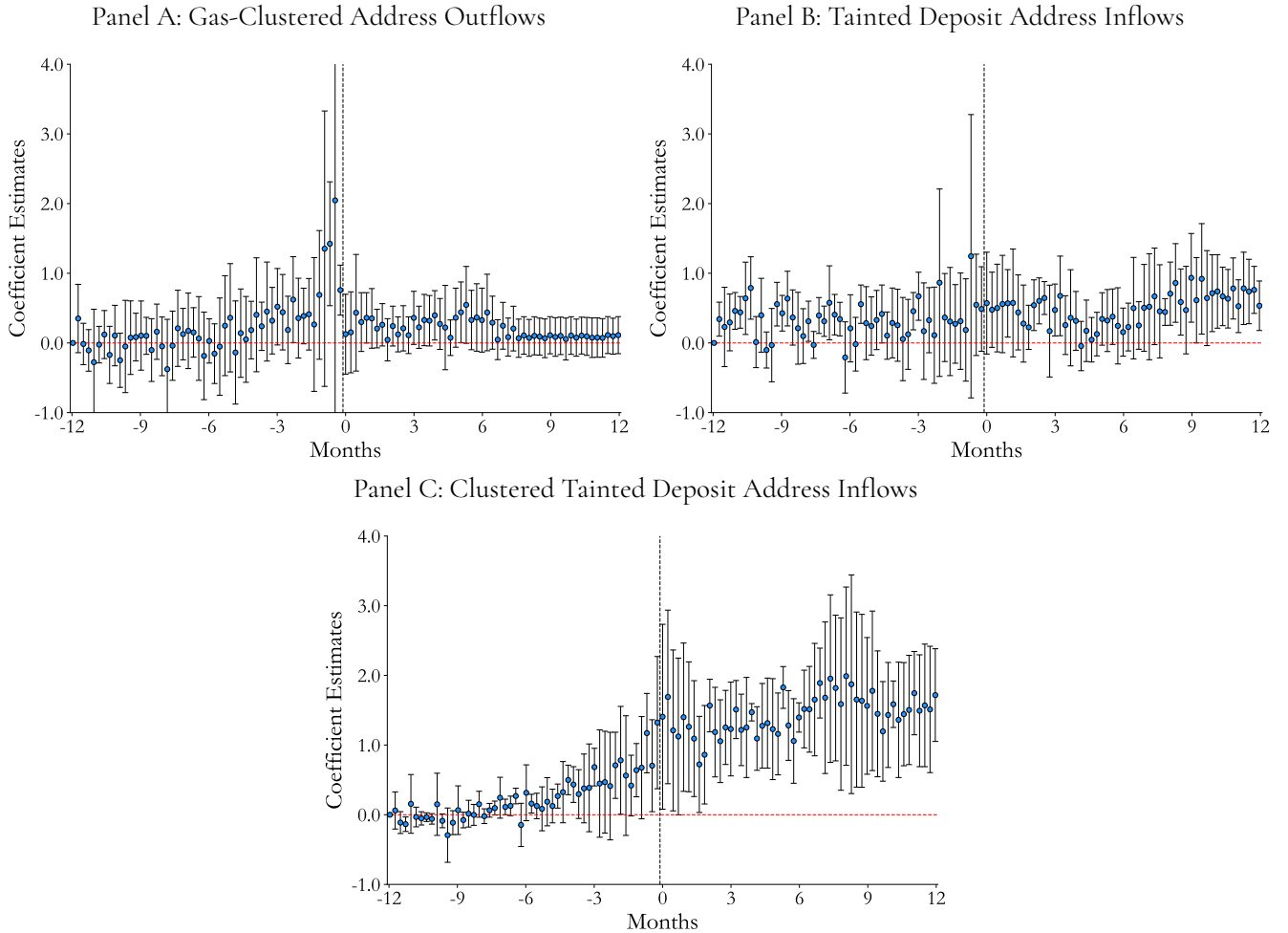
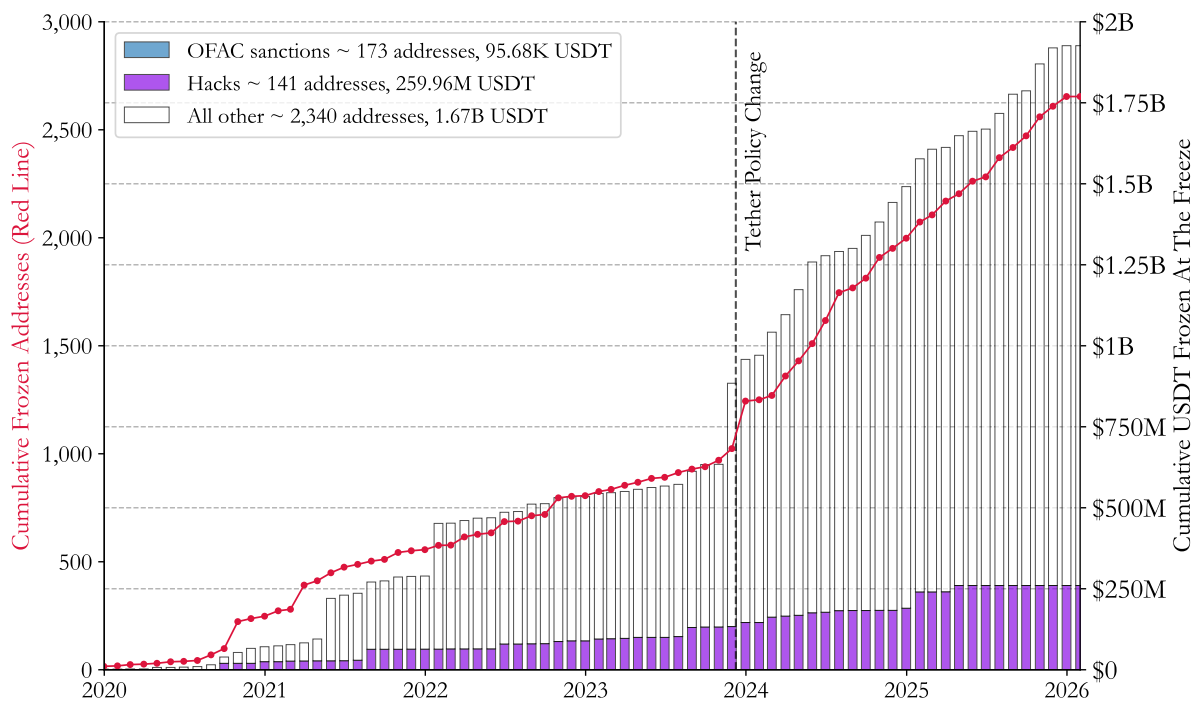


Figure 9. Tether Freezes: Aggregate Statistics

This figure presents the scope of Tether freezes and the pre-freeze activity of frozen addresses. Panel A summarizes enforcement scale over time: the red line (left axis) plots the cumulative number of frozen addresses, while the stacked bar (right axis) shows the cumulative dollar value of Tether frozen. Colored segments of each bar indicate frozen addresses appearing in the traced network of reported criminal flows and show the corresponding scam type, while white segments indicate addresses outside that network. Panel B illustrates inflow trajectories for addresses prior to being frozen. This panel plots a select sample of frozen addresses that have received more than \$10K in total inflows. The horizontal axis reports the number of days each address was active prior to being frozen, and the vertical axis (log scale) shows the total dollar inflow to that address. Each dot represents a transfer event, with dot size reflecting the cumulative inflow received by the address at that point in time. Multiple dots forming a line represent inflow trajectories for a single address. Red crosses mark the date each address was frozen.

Panel A: Cumulative Freezes Over Time



Panel B: Activity of Frozen Addresses Over Their Lifetimes

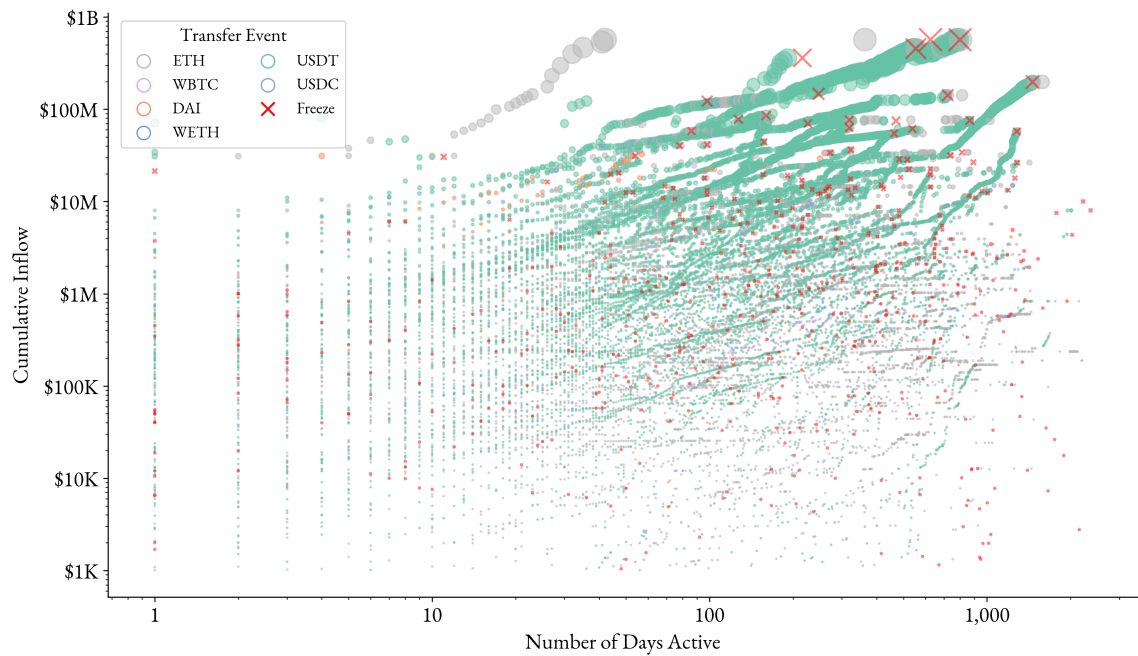


Figure 10. Tether Freezes: Swap Activity

This figure presents inflows and outflows indexed by the hours prior to and after the Tether freeze for the targeted addresses and the addresses clustered around them. For both panels, inflows and outflows are reflected in the left-hand y-axis, and these flows are broken into their corresponding cryptocurrency, denoted by the corresponding colors. Inflows are represented by upward-pointing bars, and outflows are likewise represented by downward-pointing bars. Hatched sections correspond to amounts swapped. Panel A shows the flows corresponding to the frozen addresses, which cannot transfer Tether after the freeze date, marked here by the dotted vertical line at the zero hour. Panel B shows the outflows of related addresses identified through the gas clustering heuristic.

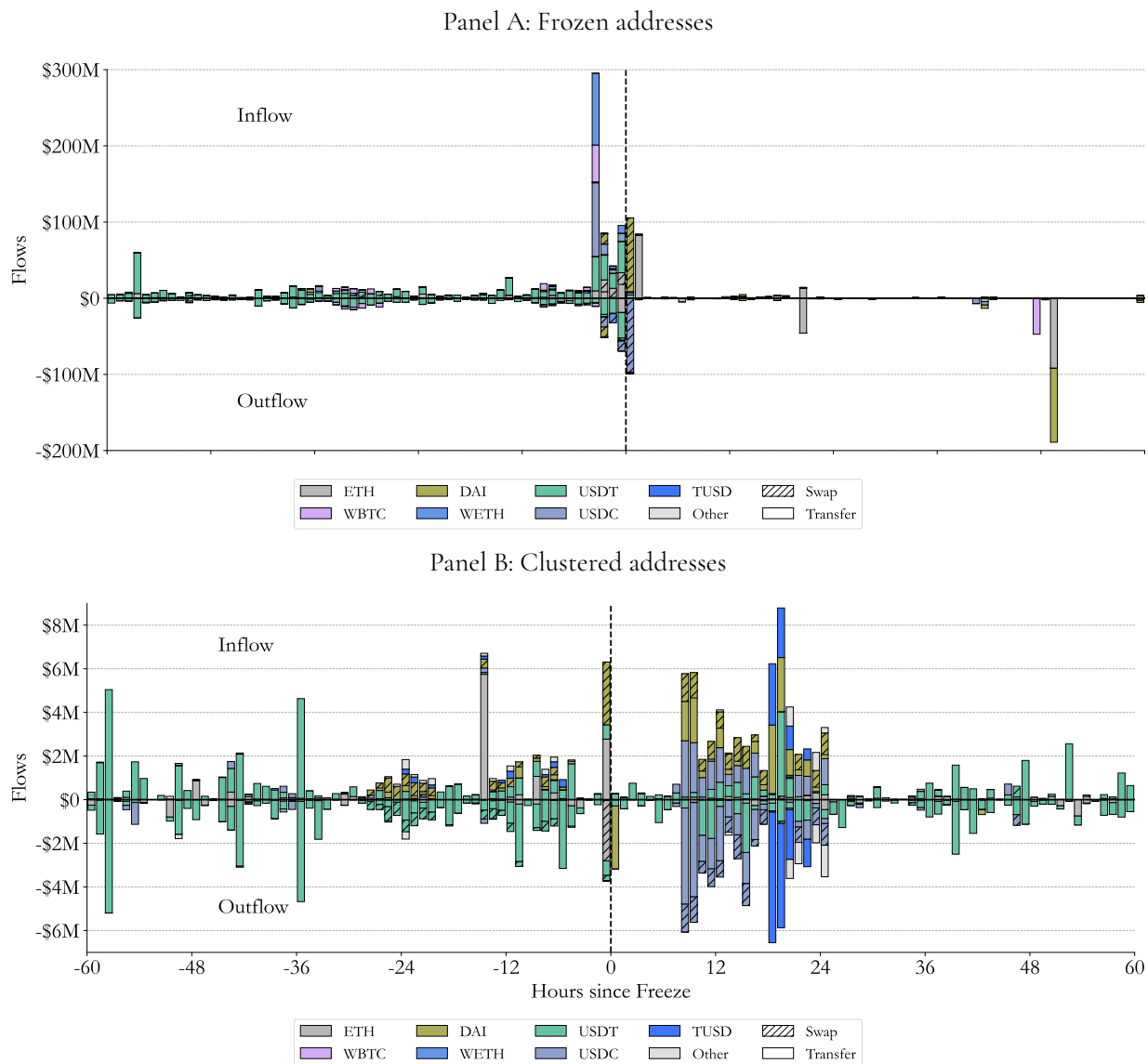


Figure 11. Tether Freezes: Substitution Effects on Related Wallets

This figure studies whether activity shifts to non-frozen addresses linked to targeted users following Tether freezes. Panel A plots dynamic difference-in-differences estimates of outflows from gas-clustered addresses related to frozen wallets. Panel B plots estimates of inflows to downstream deposit addresses tainted by funds from frozen wallets. Panel C plots estimates of inflows to additional deposit addresses clustered around those tainted deposit addresses. For all panels, the dependent variable is $\log(1 + Flow_{i,c,t})$, where $Flow_{i,c,t}$ is the panel-specific inflow or outflow for address i in freeze cohort c and day t . Flows are measured in U.S. dollars using closing prices on the day of the transaction. The regressions compare each set of related addresses with matched control addresses around the freeze date. A cohort is defined by a Tether freeze date and includes all treated addresses assigned to that freeze event. Control candidates are addresses with USDT activity in the 30 days before the freeze date, excluding known service addresses and treated addresses. 50 control addresses are then randomly drawn per treated address from candidates falling in the same transaction-count and volume bins as the cohort's average treated address. The analysis is at the address by day level. Each regression includes cohort-address fixed effects and cohort-by-day fixed effects. The sample spans 30 days before and after the freeze date, the omitted period is day -30 , and standard errors are clustered by freeze cohort. This figure corresponds to Table 4.

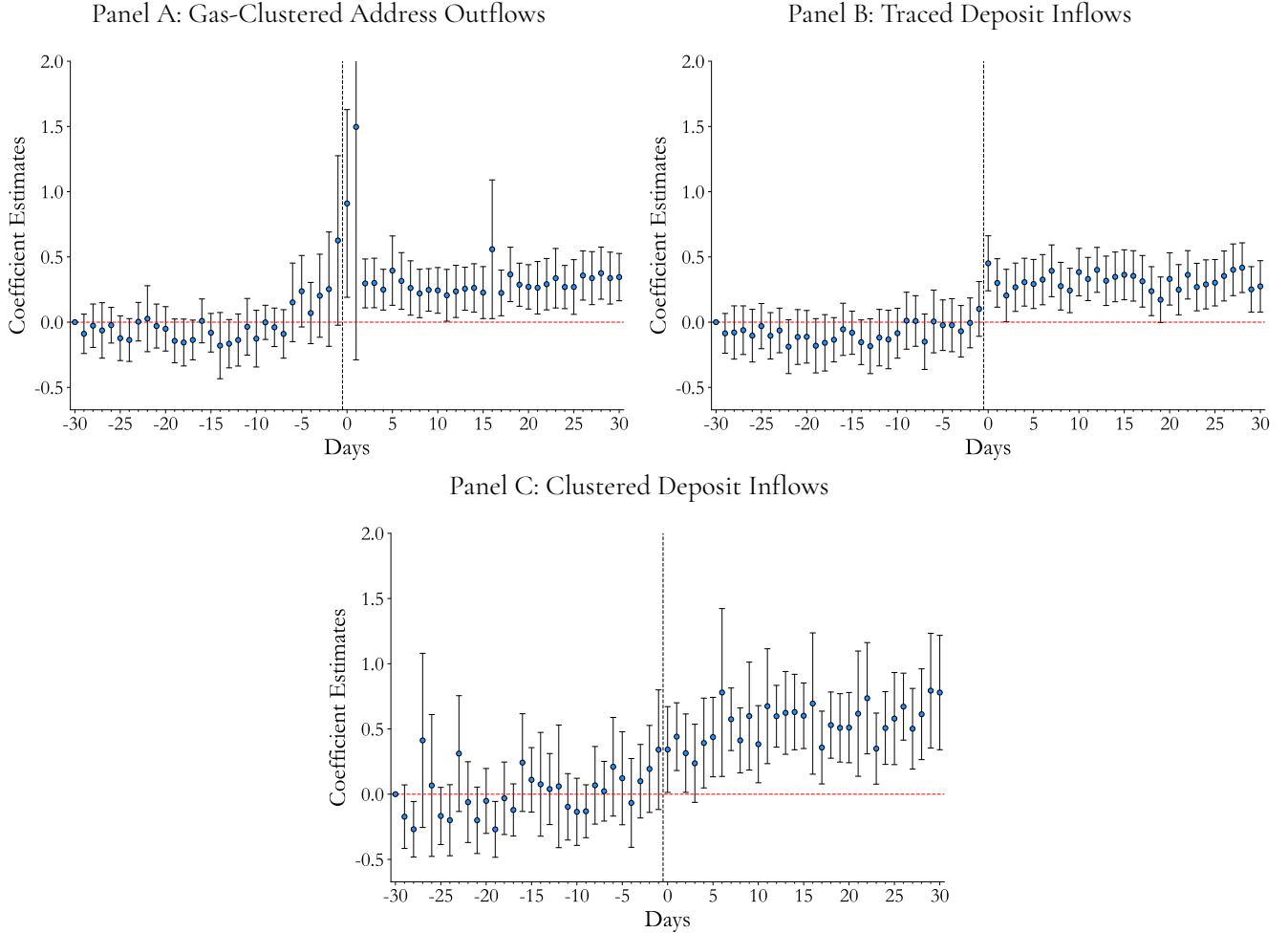


Table 1. Tornado Cash Sanctions: Effects on Privacy Coins and Hacker Flows

This table reports difference-in-differences estimates of the effect of the August 8, 2022 OFAC sanctions on Tornado Cash, first on transaction activity on privacy-focused blockchains (Panel A) and then on where hackers send funds (Panel B). In Panel A, Column (1) measures the aggregate change in all three privacy blockchains, while Columns (2)-(4) disaggregate to show each blockchain. It uses a blockchain-day panel spanning February 2022 through September 2023. The outcome is $\log(1 + Transactions)$, the daily number of transactions on a chain. Each column pairs the treated chain(s), named in the column header, with Bitcoin and Ethereum as controls. *Treat* equals one for the treated chain and *Post* equals one from the event week onward. Regressions include blockchain and date fixed effects, and standard errors are clustered by date. In Panel B, Columns (1)–(4) examine Tornado Cash, Wrapped ETH, swaps, and bridges, respectively. It uses a balanced hacker-address $\times$ destination $\times$ month panel spanning February 2022 through September 2023. The outcome is $\log(1 + TaintedFlows)$, the ETH traced from a reported hack to a given destination in a given month, winsorized at the 99th percentile of positive flows within each month. Each column takes one destination as the treated group: Tornado Cash, Wrapped ETH, decentralized exchange swaps, or bridges. Flows to overseas centralized exchanges are the comparison group, because those exchanges were not themselves targeted by the sanctions. *Post* equals one from August 2022 onward. The sample is hacker addresses that sent funds both to Tornado Cash and to at least one other attributed destination. Regressions include hacker-address and month fixed effects, and standard errors are double clustered by hacker address and month.

Panel A: Transaction Activity on Privacy-Focused Blockchains

	(1) Privacy coins	(2) Monero	(3) Dash	(4) Zcash
Treat $\times$ Post	-0.329*** (0.019)	-0.360*** (0.019)	-0.276*** (0.017)	-0.352*** (0.045)
Blockchain FE	✓	✓	✓	✓
Day FE	✓	✓	✓	✓
Observations	2,870	1,722	1,722	1,722
Adj. R-squared	0.986	0.986	0.988	0.986
Mean Dep. Var.	10.910	12.149	12.005	11.701
SD Dep. Var.	2.020	1.662	1.852	2.274
$\exp(\beta) - 1$	-28.0%	-30.2%	-24.1%	-29.7%

Panel B: Hacker Flows to Alternative Destinations

	(1) Tornado Cash	(2) Wrapped ETH	(3) Swaps	(4) Bridges
Treat $\times$ Post	-0.0834*** (0.0236)	0.0408* (0.0198)	0.0453** (0.0166)	0.0584*** (0.0178)
Hacker address FE	✓	✓	✓	✓
Month FE	✓	✓	✓	✓
Observations	8,440	8,440	8,440	8,440
Adjusted R^2	0.0192	0.0185	0.0406	0.0266
Mean Dep. Var.	0.0744	0.0227	0.0345	0.0252
SD Dep. Var.	0.6203	0.3050	0.3786	0.3254
$\exp(\beta) - 1$	-8.0%	4.2%	4.6%	6.0%

Standard errors in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 2. Effects of DOJ Settlement on Binance's Receipt of Sanctioned Flows

This table estimates how the DOJ enforcement actions against Binance affect the share of tainted flows reaching Binance. The analysis is at the exchange by month level. The dependent variable is each exchange's percentage share of all traced Tornado Cash outflows terminating in that month. Binance is the treated exchange; controls are other overseas exchanges. Columns (1) and (2) use the Binance DOJ settlement on November 21, 2023 as the event; Columns (3) and (4) use the Binance compliance monitorship announcement on May 17, 2024. For all columns, the pre-period is the six months before the Binance settlement. The post-period is the six months after the settlement in Columns (1) and (2), and the six months after the monitorship announcement in Columns (3) and (4). Columns (1) and (3) include year-month fixed effects only; Columns (2) and (4) add exchange fixed effects. Standard errors are two-way clustered by exchange and month.

	Binance Settlement		Binance Monitorship	
	(1)	(2)	(3)	(4)
Treat $\times$ Post	-1.572*** (0.122)	-1.572*** (0.123)	-2.925*** (0.068)	-2.925*** (0.069)
Treat	3.502*** (0.066)		3.502*** (0.066)	
Year-Month FE	✓	✓	✓	✓
Exchange FE		✓		✓
Observations	1,980	1,980	1,980	1,980
Adjusted R^2	0.208	0.564	0.292	0.496
Mean Dep. Var.	0.077	0.077	0.056	0.056
SD Dep. Var.	0.477	0.477	0.362	0.362

Standard errors in parentheses.

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

Table 3. OFAC Sanctions against Users: Effects on Targeted and Related Addresses

This table estimates how OFAC sanctions affect flows from sanctioned addresses and related addresses. The dependent variable is $\log(1 + Flow_{i,c,t})$, where $Flow_{i,c,t}$ is the panel-specific weekly inflow or outflow for address i in sanction cohort c and week t . Flows are measured in U.S. dollars using closing prices on the day of the transaction. Specifically, Column (1) focuses on outflows from sanctioned origin addresses, Column (2) focuses on outflows from clustered addresses identified through gas clustering, Column (3) focuses on inflows to tainted deposit addresses reached by traces from sanctioned addresses, and Column (4) focuses on inflows to clustered tainted deposit addresses. A cohort is defined by an OFAC sanction date and includes all treated addresses assigned to that sanction event. Control candidates are drawn from addresses with activity in the year before the sanction event. The candidate pool is restricted to addresses matched to the treated addresses on transaction count and transaction volume and excludes known service addresses and treated addresses. 50 control addresses are then randomly drawn for each treated unit. The analysis is at the address by week level. Each regression includes cohort-address fixed effects and cohort-by-week fixed effects. Standard errors are clustered by sanction cohort. The sample focuses on OFAC sanctions against individuals or organizations. This table corresponds to Figure 8.

	(1) OFAC Sanctioned Address Outflows	(2) Gas-Clustered Address Outflows	(3) Tainted Deposit Address Inflows	(4) Clustered Tainted Deposit Inflows
Treat $\times$ Post	0.009 (0.203)	-0.025 (0.061)	0.165* (0.095)	1.190*** (0.246)
Cohort-Address FE	✓	✓	✓	✓
Cohort-Time FE	✓	✓	✓	✓
Observations	150,410	153,413	162,181	326,374
Adjusted R^2	0.187	0.190	0.196	0.194
Mean Dep. Var.	0.458	0.447	0.437	0.789
SD Dep. Var.	1.922	1.894	1.928	2.828
$\exp(\beta) - 1$	0.9%	-2.5%	17.9%	228.7%

Standard errors in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 4. Tether Freezes: Effects on Targeted and Related Addresses

This table estimates how Tether freezes affect flows from frozen addresses and related addresses. The dependent variable is $\log(1 + Flow_{i,c,t})$, where $Flow_{i,c,t}$ is the panel-specific daily inflow or outflow for address i in freeze cohort c and day t . Flows are measured in U.S. dollars using closing prices on the day of the transaction. Specifically, Column (1) focuses on outflows from frozen addresses, Column (2) focuses on outflows from clustered addresses identified through gas clustering, Column (3) focuses on inflows to tainted deposit addresses reached by traces from frozen addresses, and Column (4) focuses on inflows to clustered deposit addresses. A cohort is defined by a Tether freeze date and includes all treated addresses assigned to that freeze event. Control candidates are addresses with USDT activity in the 30 days before the freeze date, excluding known service addresses and treated addresses. 50 control addresses are then randomly drawn per treated address from candidates falling in the same transaction-count and volume bins as the cohort's average treated address. The analysis is at the address by day level. Each regression includes cohort-address fixed effects and cohort-by-day fixed effects. Standard errors are clustered by freeze cohort. This table corresponds to Figure 11.

	(1) Frozen Address Outflows	(2) Gas-Clustered Address Outflows	(3) Tainted Deposit Address Inflows	(4) Clustered Tainted Deposit Inflows
Treat $\times$ Post	-0.114* (0.059)	0.364*** (0.032)	0.395*** (0.035)	0.528*** (0.050)
Cohort-Address FE	✓	✓	✓	✓
Cohort-Time FE	✓	✓	✓	✓
Observations	5,118,255	5,183,616	3,954,549	3,755,816
Adjusted R^2	0.164	0.161	0.153	0.155
Mean Dep. Var.	0.462	0.455	0.451	0.460
SD Dep. Var.	1.889	1.872	1.863	1.903
$\exp(\beta) - 1$	-10.8%	43.9%	48.4%	69.6%

Standard errors in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 5. Summary of Direct and Substitution Effects Across Policies

This table summarizes the key results across four enforcement actions, organized into policies targeting services and policies targeting users. The first column lists the enforcement actions. Tornado Cash sanctions and DOJ settlements with exchanges target services, while other OFAC sanctions and Tether freezes primarily target individuals or organizations. The second column describes effects on the targeted services and addresses, while the third column describes effects on substitute services and addresses. Sources are linked in superscripts. “F” indicates a Figure and “T” indicates a Table.

	Direct Effects	Substitution Effects
<i>Policies against services</i>		
1. Tornado Cash sanctions	- Decrease in Tornado Cash flows^{F2} - Decrease in hacker flows to Tornado Cash^{F2}	- Decrease in transactions on privacy-focused blockchains^{F3,T1} - Increase in hacker flows to bridges^{F3,F4,T1}
2. DOJ settlements with exchanges	Decrease in illicit flow to exchange^{F6,T2}	No detectable change in flow to other overseas exchanges^{F6,T2}
<i>Policies against users</i>		
3. OFAC sanctions on individuals and organizations	Little effect on sanctioned address flows because addresses are often inactive^{F7,F1A.16,T3}	- No change in clustered address flows^{F8,T3} - Increase in deposit flows^{F8,T3} - Increase in clustered deposit flows^{F8,T3} - Increase in flows to Tornado Cash^{F1A.15,T1A.4}
4. Stablecoin asset freezes	Decrease in frozen address flows^{F1A.20,T4}	- Increase in gas-clustered flows^{F11,T4} - Increase in deposit flows^{F11,T4} - Increase in clustered deposit flows^{F11,T4} - Increase in DeFi usage^{F1A.21,T1A.6}