Where Does Criminal Crypto Go?*

John M. Griffin† Kevin Mei‡ Zirui Wang§

March 19, 2025

Preliminary and Incomplete. Please do not circulate or post.

Abstract

To build a more comprehensive understanding of the criminal crypto ecosystem, we start with 190 thousand addresses from 300 thousand reports of scams, hacks, phishing, fake projects, impersonation, contract exploits, illicit actors, airdrops, and other nefarious blockchain activity on Ethereum, Bitcoin, and Tron blockchains. More sophisticated criminals stealing larger dollar amounts such as contract exploiters, hacks, and illicit actors use the Tornado Cash mixer. Among funds traceable to the Tornado Cash mixer, in some months, over 50% of the traceable funds are of criminal origin. Among Tornado Cash funds, players move the funds through a series of transactions, including through Uniswap, other decentralized exchanges (DeFi), or Wrapped ETH, before exiting through centralized exchanges. The ban on the mixer was at least partially effective. Mixers do not appear in the toolkit of most common investment scams, phishing, and fake projects despite these scams handling millions of smaller transactions on both Bitcoin and Ethereum. These less scrutinized operations with smaller dollar victims simply use multiple transactions, swaps on DeFi exchanges, and occasionally bridges and shadow exchanges to launder funds before exiting on centralized exchanges. Overall, although we study just a subset of all possible criminal activity, 5% to 20% of total inflow handled by some non-U.S. crypto exchanges originate from criminal networks.

keywords: Scams, Crypto Flows, DeFi, Ethereum, Bitcoin, Money Laundering

*We thank Integra FEC for 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
‡McCombs School of Business, University of Texas at Austin. KevinMei@utexas.edu
§McCombs School of Business, University of Texas at Austin. Zirui.Wang@utexas.edu

I. Introduction

As prices of Bitcoin and Ethereum increase, crypto has grown rapidly in use, acceptance, and features. The new crypto ecosystem allows for features with decentralized finance (DeFi) services such as various highly liquid decentralized swaps between crypto assets on the Ethereum network, multiple entry and exit points through various centralized crypto exchanges, wrapping of currencies, and even bridges across blockchains. We analyze how the dark side of crypto-criminal activity utilizes this ecosystem. In this paper, we gather a large compilation of transactions used in phishing attacks, romance scams, fake projects, contract exploits, impersonation, airdrop, fake returns, swim swaps, hacks, and ransomware and use these addresses to map the crypto money laundering ecosystem.

Cryptocurrency was envisioned as a decentralized financial system, but yet to the extent that it handles money, the organizations facilitating transactions must still conform to anti-money laundering laws. Since investors need trust in order to deploy capital and 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 entrepreneurial activity. However, the crypto industry also charges fees for crypto transactions regardless of their source, and monitoring services can be costly to operate. To conform to international law and interact with the global banking system, new users at exchanges must authenticate their identities through anti-money laundering and know your customer (AML/KYC) processes of these exchanges. Additionally, most exchanges purport to monitor transactions through know your transaction (KYT) policies to avoid receiving funds from known criminals. We analyze the effectiveness of these controls and how the crypto ecosystem launders criminal proceeds.

We uncover these activities through three main avenues. First, we *trace* the flows of addresses that have been reported to be involved in scams or hacks. This allows us to follow funds to destinations such as centralized exchanges, decentralized (DeFi) exchanges

(DEX), mixers, and bridges. Second, we focus on Tornado Cash, which was sanctioned by the U.S. Treasury. This allows us to examine how both decentralized and centralized exchanges interact with a service that is widely known to handle dirty crypto. Third, we examine how criminal flows directly interact with both decentralized and centralized exchanges.

We collect crypto addresses from a number of sources and gather a dataset of over 300,000 crypto addresses that have been reported to have been involved in some sort of scam or criminal activity. 190,000 addresses have some activity, because many online extortion scams use addresses that are never funded. Additionally, many addresses are reported multiple times, so after only using unique addresses and other checks on the data, we are left with over 62,000 addresses. More than 38 thousand addresses are in Bitcoin, 22 thousand on the Ethereum blockchain, and 1,200 on the Tron blockchain.

We turn to tracing analysis on Ethereum to gain a fuller understanding of how the criminal capital flows on the blockchain. Figure 1 shows how transactions on the Ethereum blockchain move through contract exploits, stolen funds, phishing, scams, illicit actors, and fake projects. Common obfuscation methods across all scams are the use of transactions in many intermediate nodes, funds moving through decentralized exchanges (DEXs) swap transactions, and funds move to centralized exchanges. Despite being infamous for laundering, we find that the main Ethereum mixing service, Tornado Cash, is used in only 2.6% of our total criminal activity. However, there are considerable differences in the nature of the flows across scams with contract exploit, stolen funds (hacks), and illicit actors interacting more often with the Tornado Cash and moving more funds through swaps on Uniswap. They also have considerable internal volume in both small, medium, and large nodes. Hacks, contract exploits, and illicit foreign actors are known to engage in more advanced criminal activity and have considerable scrutiny on their larger transactions, which can explain why they are more frequent users of Tornado cash, DEXs, and bridges across blockchains.

We next turn to an examination of Tornado Cash to understand how both centralized and decentralized exchanges handle flows from this known money-laundering entity. On August 8, 2022, the US Treasury Department sanctioned Tornado Cash but the ban was lifted on November 26, 2024 by the order of a U.S. court regarding the legality of banning computer code. We use these three different bans periods to examine how exchanges interface with Tornado Cash, pre-ban, during the ban, and post-ban. The crypto industry fought against the Tornado Cash ban. When the 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."[1]

Our findings show that Tornado Cash handles considerable criminal flows from more sophisticated cyber criminal gangs, with the Lazarus group from North Korea being the largest identified user. Despite the limitations of our data and the premise of attempting to detect funds purposefully hidden, in some months more than 50% of the funds entering the mixer are from a criminal actor. This makes one wonder why the crypto industry in the U.S. is proud to defend this service, especially when foreign actors like the Lazarus group specializing in defrauding Western entities and citizens that are the major customers of U.S. crypto exchanges. The ban was mostly effective in reducing the use of the mixer and the funds moving to large exchanges. After the sanction, the U.S.-based exchanges largely stopped receiving funds and the volume to Binance and Huobi dropped considerably. OKX continued to receive funds from Tornado Cash along with smaller exchanges. Post-sanction, the centralized exchanges still receive minimal flows.

DeFi exchanges appear to have less concern with taking funds from Tornado Cash than centralized exchanges. The most common DeFi destination of funds coming out of Tornado Cash is Uniswap, other DEXs, and bridges where the funds will move to

[1] https://news.bitcoin.com/historic-win-for-crypto-court-strikes-down-treasurys-overreach/

another blockchain. Most of the funds moving to one of these destinations occur directly after leaving Tornado, indicating that there is likely no monitoring for DEX swaps and no concern for DEXs to reject their transaction. Funds often move through DeFi swap transactions before centralized exchanges accept funds from Tornado Cash, even during the ban. Overall, the ban appears to have reduced the effectiveness of the mixer, although more time is required to understand the utilization of the mixer after the ban.

We now turn our attention to criminal flows more generally and their paths through decentralized and centralized exchanges. One of the largest sources of DeFi swap flows is Tokenlon, but this service seems to specialize in handling funds from romance and other related investment scams. Uniswap and 1inch are more commonly used by other tainted funds. Nearly 80% of funds from contract exploits move to Uniswap. More than half to 70% of the funds from phishing, fake projects, and illicit actors use Uniswap. 1inch is also popular for large scammers in the stolen funds, phishing, and fake project categories. Although these patterns have changed some over time, these services remain popular over the entire period.

Whether directly or, more commonly, after going through a DeFi swap, centralized exchanges are common frequent destinations for tainted funds. We find that more than 30% of all flows to exchanges such as WazirX and Bitkub are associated with tainted funds after the deposit address heuristic. Tainted flows account for between 3.4 to 7.6% of total funds to well-established exchanges like Binance, Bybit, Huobi, and OKX. Respectively, these exchanges have handled more than $58.2, $2.4, $19.1, $10.3 billion of funds tainted by criminals during our 2021 to 2024 period. U.S. crypto exchanges generally handle only a small percentage of tainted funds indicating their internal controls and monitoring are much more effective.

Institutions in the U.S. must file a Suspicious Activity Report (SAR) for any deposits above $10,000 to the Financial Crimes Enforcement Network. We examine the bunching of transactions around $10,000 and $100,000 thresholds across exchanges. Bunching on these

thresholds is more common on overseas crypto exchanges, and slightly more so among criminal inflows suggesting that criminals commonly move money at round number increments on these exchanges without much concern of detection. On U.S. exchanges there is some bunching slightly below $10,000 suggesting that criminals believe their transactions at $10,000 may be reported and seek to stay under the threshold.

Our findings suggest practical areas for industry improvement, enforcement, and policy to deter money laundering. First, more attention should be paid to DeFi swap transactions. Criminals do not appear to be concerned that these services will reject their transactions and criminals are much less cautious with money coming out of the swap transactions suggesting that they believe the money is viewed as clean money. Users who use DeFi pools as "investments" by providing liquidity to these automated marker makers inadvertently facilitate cheap liquidity for money laundering. There is a wide range of practices by crypto exchanges with some exchanges accepting close to zero percent of funds from criminal actors whereas other exchanges accept five to 30 %. The fact that criminal inflows are close to zero at some exchanges and that U.S. exchanges stopped receiving Tornado Cash funds after the ban suggest that monitoring procedures can be effective. Many large centralized exchanges need to do more monitoring of funds and have more rigorous KYC and KYT procedures, particularly for detecting dirty money coming through swap transactions.

Our paper relates to two main literatures. First, 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 (2021) find only $5 billion in dark-market activities, Bitcoin mixers, and other criminal activities in 2020. Cong, Harvey, Rabetti, and Wu

(2023b) show that 43 ransomware gangs carried out 2,690 attacks from May 2019 to July 2021. 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. Chainalysis (2024) also provides a survey and examples of various types of criminal activity and calculates a total of $24.2 billion in 2023 through wallets directly identified with various identified for illegal activity.[2] Griffin and Mei (2024) maps the flows of pig butchering scams by tracing the flows and showing how flows criminal flows are entering centralized exchanges and how these exchanges are allowing inducement payments to potential victims. This literature also relates to 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, 2018; Hamrick, Rouhi, Mukherjee, Feder, Gandal, Moore, and Vasek, 2021; Phua, Sang, Wei, and Yu, 2022), insider trading (Félez-Viñas, Johnson, and Putnins, 2022), and wash trading (Pennec, Fiedler, and Ante, 2021; Cong et al., 2023b) as briefly surveyed by Griffin and Kruger (2024). We extend the literature by using the most comprehensive database of all types of scamming and criminal activity to date and use this data to map a deeper understanding of the world of money laundering by examining common techniques such as swaps, mixers, and bridges utilized in isolation and in combination.

Second, we contribute to the literature on organized crime and money laundering. El Siwi (2018) notes that recognizing "money is the lifeblood of organized crime" led to the adoption of the anti-money laundering (AML) regime in Italy. Fracassi and Lee (2025) examine cross-country differences in anti-money laundering laws and their effectiveness. Agca, Slutzky, and Zeume (2020) studies how anti-money laundering enforcement impacts lending by U.S. banks. (Mirenda, Mocetti, and Rizzica, 2022) show how organized crime

[2]The report does not detail their methodology but note that the procedure undercounts. This appears to be because they mostly count illicit funds only into tagged addresses and not other closely related addresses that often receive criminal flows. Anderson (2021) notes that only three percent of financial scams are reported. Chainalysis also provides monitoring services to exchanges (such as Binance) and Tether, and generally does not detail specific entities nor specific stablecoins used for illicit flows. For example, the Binance blog discusses working with Chainalysis and Refintiv in 2018.

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.[3] 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. Levi (2015) surveys the literature on how organized crime is financed and notes that what is known has been primarily limited to prosecuted case records. Our paper focuses on how money laundering and criminal fund flows work in the crypto sphere where the vast majority of criminal flows are not detected. Such an understanding is necessary to understand why the traditional framework of laws is seemingly ineffective in the crypto sphere and whether additional policies are needed.

II. Data and Methodology

This paper develops a grouping of datasets into a unified framework to follow illicit funds. We do this by collecting data on transaction flows on Bitcoin, Ethereum, and Tron. Transaction-level data is then enriched with attribution labels to ascribe addresses and flows to specific actors. Tracing methodologies further organize these transactions such that we can consistently follow specific funds that start at an illicit address to track their flows to subsequent destinations. This section describes the process of developing our datasets and tracing methodology.

A. Data

We primarily use two types of data: blockchain transaction data and attribution data. Blockchain transaction data is sourced from the Bitcoin, Ethereum, and Tron blockchains. Importantly, the fields include the blockchain address of the sender and receiver, which allows us to construct paths of flows between addresses.

Beyond routine cryptocurrency transfers, transactions may also be invoked by spe-

[3] Draca and Machin (2015) survey a growing literature on the economic incentives for crime.

cialized functions. We process data emitted from common functions, which allows us to follow funds that are swapped or bridged. Swapping is typically when an address uses a service like a decentralized exchange to change one type of cryptocurrency into another type on the same blockchain. Bridging is when an address deposits tokens into a service on one blockchain and receives that amount on another blockchain, net of any fees. We process data on swaps and bridges to further follow relevant funds. We supplement transaction data with prices based on the closing price of the transaction date.

We use a rich set of sources of attribute data. First, we use data from online sources like blockchain.com, etherscan.io, and tronscan.org to label addresses that belong to known entities. We focus on service providers such as centralized exchanges, decentralized exchanges, bridges, or mixers.

Second, we used data on known illegal actors reported by various data collectors. These are mainly from victims or discovered by law enforcement or lawsuits. The single largest source of addresses is chainabuse.com, a leading reporting platform where victims and other users describe hacks and scams. We collect 311,997 submissions. Victims can choose the category that applies to their report or select "other." We use an OpenAI o3-mini model to classify victim reports.[4] After dropping reports of insufficient detail to categorize the type of scam, we use 227,745 reports. We also received data on 12,554 suspicious addresses collected as part of an online publication about pig butchering scams from the United States Institute of Peace (USIP).[5]

We drop 724 invalid cryptocurrency addresses, as determined by being clearly too short (e.g., user submitting website addresses) or of invalid format (e.g., all valid Ethereum addresses start with "0x"). We start with a total of 304,914 reports, or 303,778 after excluding contract exploit (discussed in more detail below), as presented in Table 1. The reports include 255,554 Bitcoin addresses, 39,903 Ethereum addresses, and 8,321 Tron

[4]We only keep model suggestions if the API returns a ranked probability of more than 99%. We follow the methodology from this notebook.

[5]We thank Jan Santiago (affiliated with PIDCO) and Raymond Hantho (Chainbrium) for sharing their data. This data was collected primarily from either interfacing with victims or probing scammer operations.

addresses. Many victim submissions include addresses without any transaction activity, which may be due to artifacts of how the data was collected. For example, the USIP project included collecting data by collecting addresses from "spoofed" websites of inauthentic trading platforms or baiting scammers and asking them for addresses to fund transfers. Similarly, many submissions are from victims who recognize email messages as fraudulent and subsequently report addresses without sending the scammer any funds. We remove 112,358 inactive addresses, the bulk of which were concentrated in extortion submissions with Bitcoin addresses. This leaves us with more than 192,000 addresses. Active addresses may have also been reported more than once and in more than one scam. In column 3, we remove duplicate addresses within the same scam and find that the vast majority of extortion reports occur with duplicated addresses. Before utilizing our transactions in any blockchain analysis we also remove any addresses that have been attributed to an identified exchange, service, or a destination with over 2,000 transactions. These may be inadvertently reported by victims if they follow their funds to their end destinations (e.g., reporting an exchange as the scammer). Lastly, to arrive at a unique number of addresses, we sort each address into one scam based on the scam that has the most reports for that address. This leaves us with over 38,000 Bitcoin addresses, 22,000 Ethereum addresses, and over 1,200 Tron addresses.

Figure IA.1 summarizes the total number of unique addresses and total dollar inflow. We define each scam in Table IA.I. Overall, we find that addresses reported as part of a contract exploit have the most dollar inflow. However, this is likely due to the nature of contract exploits where they may take out a large flash loan to drain a smaller amount and so the total loan amount is not the actual funds lost or stolen.[6] Therefore, we do not focus on the total inflows as meaningful for contract exploit. The next largest reports are stolen funds, pig butchering scams, and illicit actors. Extortion had the most reported addresses although only 5,000 active addresses. Nevertheless, it amounts to approximately $2 billion

[6] In this example, the attacker borrowed $150 million to steal $80 million by exploiting a bug.

in activity. Interestingly, extortions are nearly exclusively in Bitcoin, presumably because this is the easiest crypto for non-crypto actors to access. In Table 3, we present summary statistics for each scam and averages. We count the flows into these addresses from January 2020 to November 2024. The total inflow to these addresses is a total of $44.25 billion with $22 billion from Bitcoin and $21 Billion in Ethereum, and $1.2 Billion in Tron. These beginning nodes should not be used to scope the total amount of activity since these incoming amounts do not capture all the unreported scam addresses that are commonly gathered at collection points deeper in the networks.

Figure 2 shows a scatterplot of the average number of transactions on the x-axis and the total inflows into these reported addresses on Bitcoin, Ethereum, and Tron, on the y-axis. The size of the circles is based on the number of reported active addresses. After contract exploit, pig butchering or romance scams are the largest category with over $20 billion entering into these nodes. Notably, these accounts may be understated as there could be general scams or stolen funds with not enough information for our algorithm to classify as pig butchering. Fake projects, phishing, stolen funds, pig butchering, and scams have the highest proportion of addresses on the Ethereum network. Airdrop scams lead to nearly 200 transactions on average but appear to have netted very little activity.

In Figure 3, we plot the first active date of reported addresses and each subsequent transaction of more than $10,000. Panel A plots Bitcoin. It appears that many of the addresses that were identified in 2020 still appear active, however, many of the recent addresses have relatively sparse transaction activity. Further, the large jumps in the red line indicate that the largest inflows bunch together in single transactions. The majority of our sample was reported from 2021 to 2023. The decline of addresses in 2024 is largely a function of a delay in reporting and address collection. Victims may not immediately report addresses, and if reported, collection agents may require some time to verify the data.[7]

[7]Industry reports display this feature. For example, when calculating total cryptocurrency value received by illicit addresses in 2022, Chainalysis initially reported this as $20.6 billion in their 2023 report and updated

Panel B plots Ethereum transactions with Ethereum-based cryptocurrencies as different colored dots. Tether is the most common transaction type with 40% of flows and Ether, the native cryptocurrency of Ethereum has 30%. Here, the black line is more jagged due to large batches of submitted addresses by forensic researchers, but the red line is less jagged than Bitcoin, suggesting fewer large inflows. Panel C compares the number of years active based on the first year of activity. For most years, Bitcoin addresses are used for a shorter period of time, which is consistent with the practice of switching addresses more prevalently in Bitcoin. Bitcoin users switch addresses more frequently to the unspent transaction output (UTXO) model which encourages clearing the balance of an address with every transaction. Overall, across both blockchains, we find frequent address switching which highlights the need for continual monitoring and updating of attribution data. Nevertheless, the median transaction life for an an address in 2020 (2021) is 9.0 (5.8) months suggesting that criminals are not too concerned with their address being flagged, even though all of these addresses were at some point reported.

B. Methodology

Tracing organizes transaction-level data into a framework that delineates the path of transaction flows of subsequent addresses. We apply a suite of bulk tracing algorithms developed by Integra FEC and utilized and more fully described for pig butchering by Griffin and Mei (2024). When tracing a given address, the tracing algorithm first collects all inflows. If outflows exist, then the tracer follows outflows to the next address. The goal is to follow tainted outflows to their end destination. Importantly, if tainted outflow funds are commingled in a downstream address that contains flows from other sources, then the forensic researcher must choose how to follow subsequent outflows.[8] We follow

to $39.6 billion, a 92% increase, in 2024 (Chainalysis, 2023, 2024)

[8]For example, consider starting with a known criminal address at *address 0*. We follow their funds one hop to *address 1*. Suppose *address 1* also receives funds from another unknown source and it transfers all of its funds by splitting them between *address 2* and *address 3*. Both addresses are candidates for also having been tainted by the funds of *address 1*. A tracing methodology can delineate these based on the order of transactions. Therefore, tracing is more conservative than tainting all downstream addresses.

commingled funds on a "first-in-first-out" (FIFO) basis, a well-established and accurate process for following specific fund transfers in cryptocurrency transaction-level data (Anderson, Shumailov, and Ahmed, 2018). By using tracing, we seek to only follow flows that are highly likely to be controlled by reported criminal addresses, instead of implicating all downstream addresses.

We trace funds to their end destinations. Currently, our results on tracing are for the Ethereum network. A trace path is terminated if it triggers any of the following criteria: (i) the flows enter an identified service, such as an exchange; (ii) the flows enter an unidentified but large address with more than 2,000 transactions; (iii) the path reaches five hops; or, (iv) traced amounts diminish to be less than 0.00001 ETH or token quantities, which are known as *dusting* transactions.[9] The most commonly triggered criteria are (i) and (ii). In the case of (i), we present results on the most common end destinations. By halting at exchanges, services, or unidentified large addresses, we avoid incorporating flows from other unrelated entities that these large addresses may have received. The tracing algorithm also handles cases where tainted flows re-enter into another reported address without double counting the ultimate destinations.

For mixers, we trace flows that leave tainted services. For example, in the next section, we trace all Tornado Cash outflows. For services like Uniswap, Wrapped Eth, and bridge contracts, we only follow specific funds flowing through the transactions. Lastly, we *backtrace* or follow inflows to a tainted address back to their originating source.

III. How do Crypto Flows Differ by Scam?

We trace the reported addresses and follow the path of their flows to destinations for the various scams in Ethereum. We focus on differences in crypto transferring methods across scams. Here, we start with six graphs for each type of major scam. Centralized exchanges are on the left, DeFi exchanges (DEXs) are on the left bottom, and nodes that

[9] Dusting transactions may obfuscate tracing by creating many more paths for a researcher to follow.

transfer funds are in the middle and separated as to whether they have small, medium, or large dollar inflows. Tornado Cash is at the bottom of the graph, followed by bridges that move funds across the blockchain at the bottom right. Finally, flows moving to deposit addresses on centralized exchanges are displayed on the right of the graph. Flows in each graph are scaled by the total size of the scam so that inferences can be comparable across graphs regardless of the total network flows.

There are some similar patterns across most graphs. Obfuscation between intermediate nodes are common, funds, often interact with decentralized exchanges, and at least some funds move to centralized exchanges. However, there are considerable differences in the nature of the flows across scams. Contract Exploit, stolen funds (hacks), and illicit actors interact more often with the mixer Tornado Cash. These three also tend to move more money through Uniswap. They also have considerable internal volume in both small, medium, and large nodes. Contract exploits and stolen funds also seem to interact with various bridges to other blockchains. These types of hacks, contract exploits, and illicit foreign actors are known to engage in more advanced criminal activity and have considerable scrutiny on their transactions which can explain why they are more frequent users of Tornado Cash and DEXs.

Phishing activity has large flows in and out of the exchange Stake. They mainly transact in large nodes internally, and move some funds to Uniswap, though most move to centralized exchanges. The unclassified scam category shows large amounts of activity coming out of major exchanges, moving within the network considerably (consistent with obfuscating transactions), swapping funds through Tokenlon, and moving substantial funds to Binance. Since these are patterns most associated with pig butchering Griffin and Mei (2024), it seems that the general unclassified scam category may largely consist of romance or other related investment scams. For fake projects, these actors receive considerable flows from Robinhood investors, who do not show up as a player in any other scams. The fake projects make the most number of internal transactions, send money

through Uniswap, occasionally Tornado Cash, and commonly exit through Binance, OKX, or other smaller centralized exchanges.

IV. Tornado Cash

Since the mixing service Tornado Cash is the most well-known mixer on Ethereum and a well-known money laundering service commonly used by illicit actors and in hacks and contract exploits, we start with utilizing how other crypto actors interface with this service. We focus on flows entering and exiting Tornado Cash to more fully understand how centralized and decentralized exchanges handle flows from this known criminal service. On August 8, 2022, the US Treasury Department sanctioned Tornado Cash and thus prohibited the US financial system from accepting related funds. The ban was lifted on November 26, 2024 when a U.S. judge ruled that smart contracts or computer code cannot be blocked since they are not the property of a foreign national or entity. Additionally, we use these three different bans to examine how crypto activity interfaces with Tornado Cash, pre-ban, during the ban, and post-ban.

Panel A of Figure 4 shows the type of identifiable addresses that use Tornado Cash. To keep the exercise manageable, we sample the 2,500 largest nodes within the Tornado Cash network. To the left of the center Tornado Cash node, we notice that many of the addresses that remit funds to Tornado Cash are recognizable hacks and illicit organizations including the Lazarus Group. However, as might be expected from sophisticated actors, to the right of the center node most recipients do not appear in our attribution data. Among paths entering Tornado Cash, many are intertwined in more complicated networks, while outgoing paths are more discernibly clear. Users appear to funnel more money from decentralized exchanges (i.e., Uniswap, 1inch) than centralized exchanges. Further, Tornado Cash withdrawals are commonly funneled back to DeFi within one hop. Funds also move to centralized exchanges.

We note two peculiar common transaction paths. Many Tornado Cash users seem

to withdraw from Tornado Cash only to again deposit funds back into Tornado Cash. This is atypical because the intended use for Tornado Cash is to withdraw funds from a different account. These could be users concerned about probabilistic attribution if they are a large source of funds into the mixer. Additionally, withdrawn ETH is also obfuscated by depositing them in the Wrapped Ether and Ethereum Beacon contracts. These are very popular contracts and play a big role in the Ethereum ecosystem. Wrapped ETH allows users to deposit ETH and returns "WETH" that can be used in other token transactions. The Beacon contract serves as the cornerstone of the *proof-of-stake* mechanism and is the essential entry point for users seeking to participate as block validators in the blockchain consensus protocol. Here, we see Wrapped ETH and the Beacon both accept potentially tainted funds exiting Tornado Cash.

Figure 5 shows the time series of all flows to Tornado Cash, along with totals traced from our criminal flows. The August 2022 ban seems to have been effective in reducing volume to the mixer. Before the ban, Tornado Cash was handling more than $400 million per month, but after the ban by October 2022, volume is less than $50 million per month. Interestingly, the mixer becomes more attractive for criminals with the large volume as it is easier to plausibly deny that the outflows one receives are different from the input transactions. The volume in the mixer stays low until the ban is lifted. Nevertheless, the volume does not rise to pre-ban levels.

We also plot the time series of the scamming activity as a percent of the total activity. Despite the limited nature of our data and the fact that we are missing criminal activity, the totals vary widely by month but at times show a sizable fraction of the flows due to criminal activity. For example, in April 2022, approximately 28% of the flows are due to traced criminal flows to Tornado Cash. In July 2022 just prior to the ban approximately 45% of the funds are due to criminal flows. These totals are extremely high in March 2024. The drop-off in late 2024 is likely more of a by-product of our data reporting since reported criminal addresses are gathered with a considerable lag as previously discussed. Nevertheless,

the numbers are likely considerably understated since criminal flows are coming from sources which either cannot or which we have not previously traced including Tornado Cash itself, bridges, and the Wrapped Ether contract. When one examines the total flows into Tornado Cash as a fraction of the total flows for which there could be attribution, the percentage of the flows that is from criminal activity jumps considerably.

We next focus on the destinations of Tornado Cash by further tracing an additional step and reorganizing the data by type of destination. Figure 4 shows a sankey diagram of funds exiting Tornado Cash. Several interesting findings emerge. First, the most common destination is decentralized exchanges (DEX). If moving to a DEX most of the transactions go out of Tornado Cash to a node and then that node sends funds directly to Tornado Cash. Criminals do not appear concerned that a DEX will not accept their funds. Second, we retrace or continue to track funds coming out of decentralized exchanges. The most common destination of funds coming out of DEXs are Uniswap, other DEXs and bridges where the funds will move to another blockchain. Most of the funds going to one of these destinations move directly after one hop, indicating that there is no concern for being traced. The blue lines represent funds that move to centralized exchanges either directly or after a couple of transactions.

Some funds exit Tornado Cash and go directly into a centralized exchange in one hop, but most transactions take two or three hops. The fact that so many transactions move to exchanges from Hop two likely indicates that whatever monitoring services employed by exchanges only traces back one stop to see the source of the funds and that the criminals know that their accounts will not be frozen. The most common centralized exchanges where Tornado flows move to is Binance, OKX, fixed float, and various other smaller exchange. Exchanges that are known to follow strict KYC procedures such as Coinbase, and Kraken still receive some flows from Tornado Cash although they are relatively small. Additionally, considerable funds flow back to Tornado Cash again, or to Wrapped ETH. One possible explanation for the difference in pattern is that the large movement of funds

through Wrapped ETH, DeFi, back to DeFi, and bridges are criminals who are extremely concerned about protecting their identity, whereas others may prioritize speed or ease and thus move to decentralized or centralized exchanges.

Figure 6 further examines the funds that exit and enter Tornado Cash using details of the entity. Separate panels are for pre-sanction, during the sanction, and the post-sanction (after November 2024) period. Each graph is scaled relative to the total flows in the period. Pre-sanction Binance, OKX, Huobi, Coinbase, FTX, Kraken, and Kucoin were the largest exchanges to receive funds. Most of these flows were after two hops on the blockchain indicating not much concern about detection. After the sanction, the U.S.-based exchanges largely stopped receiving funds and the volume to Binance and Huobi dropped considerably. OKX dropped only slightly. Smaller exchanges continue to receive considerable flows. Post-sanction, the centralized exchanges receive minimal flows. During the sanction, and post-sanction, Uniswap, 1inch receive considerable flows. Bridges such as Thorchain and Arbtrium have grown in popularity.

Panel B shows inflows into Tornado Cash from a backtrace. The Lazarus group is a large contributor before the ban, but does not contribute after the ban (at least directly), perhaps because the volumes are too small to hide their highly scrutinized activities or they have found other lower costs effective measures. Contract exploits continue to use Tornado Cash during and after the ban. Wrapped ether, 1inch, and unidentified addresses tend to be the largest users of ETH post-ban. In Figure 7, we list the top 50 addresses that send the most absolute amounts to Tornado Cash. Overall, Tornado Cash is more commonly used by North Korean hackers, known as the Lazarus Group, and other contract exploits and hacks.

Overall, the study of Tornado Cash shows how various crypto players interact with a service known to handle dirty money; Our findings show that it handles considerable criminal flows from more sophisticated cyber criminal gangs. The ban was largely effective in reducing US-based crypto exchanges receiving funds from the mixer and also mostly

effective in reducing flows from other large crypto exchanges. DeFi exchanges regularly interact with the Tornado Cash mixer and appear to apply the cover for centralized exchanges to accept funds from Tornado Cash, even during the ban. Overall, the ban appears to have reduced the effectiveness of the mixer, although the post-ban volume is increasing, and only time will tell if the mixer recovers in popularity to levels before the ban.

V. Swaps, Centralized Exchanges, and Other Services

A. Swaps

Swaps are the cornerstone of DeFi. The most popular swaps are at decentralized exchanges, which are each a set of smart contracts that allow users to exchange one type of cryptocurrency for another on the same blockchain. Swaps are "decentralized" because no single authority will take ownership of customer funds. Therefore, this is an easy mechanism for illicit actors to change the type of crypto they use. This may be effective at obfuscating tainted flows because some commercial tracing software may not easily follow funds between different cryptocurrencies through swap transactions.

In Figure 8, we trace plot the outflows to DEXs. We find that pig butchering scams, impersonation, fake returns, and scam category most commonly send to Tokenlon. As discussed in Griffin and Mei (2024) , this may be a cohort of Southeast Asia based scammers with similar scans that launder funds through Tokenlon. Uniswap and 1inch are more commonly used by other tainted funds. These are popular DEXs within the broader Ethereum ecosystem. Of the $1 billion of contract exploit that can be traced to DEXs, nearly 80% go to Uniswap. Similarly, approximately 50% of the $1 billion of stolen funds, 60% of the $300 million traced from phishing, 60% of the $70 million from fake projects, and 70% of the $20 million from illicit actors use Uniswap. 1inch is also popular for large scammers in the stolen funds, phishiing, and fake project categories.

In Figure 8 Panel B, we plot the usage over time. We show that Tokenlon is consistently

used by scammers in this period. Uniswap is consistently the second largest destination for tainted funds, followed by 1inch. Scammers and exploiters also use well-known services like Curve.fi (used by contract exploits and stolen funds), CoW protocol (or Coincidence of Wants, used by contract exploit and illicit actors), and paraswap (used by contract exploit and airdrops). These DEXs correspond with many of the most popular DEXs of regular crypto users. Therefore, the liquidity provided here may be cheaper than alternative sources. The upshot is that users who want to use these pools as "investments" by providing liquidity for these automated marker makers may be providing laundering services for tainted funds.

B. Centralized Exchanges

The largest destination of tainted flows is centralized exchanges. These service providers are anecdotally the most convenient place for crypto funds to enter and exit the international financial system. We examine which exchanges interface with criminal flows.

B.1 Traced Funds to Centralized Exchanges

After tracing the funds to the exchanges, we count the total funds traced to each exchange and count the total. Panel A of Figure 9 shows the total by exchange and by scam. Of the $4 billion of pig butchering scams that are traced to a centralized exchange location, nearly 50% arrives at Binance. Similar patterns emerge for the more than $400 million traced from scam. Nearly all of the $100 million traced from impersonation can be traced to Binance. Stolen funds ($200 million), phishing ($150 million), fake projects ($100 million), and illicit actors ($70 million), and contract exploit ($20 million) have varying amounts that can be directly traced to centralized exchanges, but when possible, it seems like Binance, Huobi and OKX remain popular destinations. Coinbase, a U.S.-based exchange, is also a popular destination for scammers, fake project, and illicit actors, garnering more than 15% of each category. Of the $20 million traceable in airdrop that terminates at centralized exchanges, 40% arrives at Kucoin.

Panel B of Figure 9 shows how these dynamics change over time. Binance is consistently the largest destination for criminal funds, even after their historic $4 billion DOJ settlement in November 21, 2023. Huobi saw considerable flows in 2021 but the criminal flows are proportionally smaller in the latter half of 2023 and 2024. Gate.io and Kucoin are centralized exchanges with a considerable presence in 2024.

B.2 Flows after Deposit Address Clustering

We use the deposit address clustering heuristic described by Victor (2020). Funds remitted to deposit addresses at centralized exchanges can only be accessed by logging into the centralized exchange and thus these funds can only be accessed by the final user. Users can make new deposit addresses with no additional cost and sophisticated money launders can send money to multiple deposit addresses to avoid concentrated flows. Therefore, the rationale behind the clustering is that the two deposit addresses with a common sender are likely to be controlled by the same centralized exchange customer. To avoid clustering accounts where the entity is not controlled or involved in the scam but instead just making small inducement payments, we employ clustering only for addresses sending over $100,000.

Figure 10 shows the amount and percentage of funds in each exchange that are tainted. We find that more than 30% of all flows to exchanges like Aax, WazirX, and Bitkub are associated to tainted funds after the deposit address heuristic. Aax was a small exchange operated out of Hong Kong that went defunct in 2022. WazirX and Bitkub have both been implicated for harboring criminal funds.[10] Poloniex is an exchange with a long history and has approximately 14% of criminal flows. Additionally, we find that tainted flows account for between 3.4 to 7.6% of total funds to well-established exchanges like Binance, Bybit, Huobi, and OKX. Respectively, these exchanges have handled more than $58.2, $2.4, $19.1, $10.3 billion of funds tainted by criminals during our 2021 to 2024 period.

Other well-established exchanges are also common targets for tainted funds. Bybit,

[10] See sources on WazirX and Bitkub.

now the second largest exchange as of March 2025, has approximately 3.4% of total flows that are associated with tainted scams. We also follow $1.7 billion to Coinbase, the largest U.S.-based exchange. However, this is a small amount relative to the total flows to Coinbase.

B.3 Clustering Amounts

We consider whether KYC procedures influence customer deposits. To operate as a money service business, financial institutions in the U.S. must file a Suspicious Activity Report (SAR) for any deposits above $10,000 to the Financial Crimes Enforcement Network. We plot the histogram of transaction sizes around $10,000 and $100,000 in Figure 11 for all flows that enter eight centralized exchanges. We denote KYC-enforced exchanges as Coinbase, Crypto.com, Gemini, and Kraken because these are the largest U.S.-based exchanges. We label non-KYC exchanges as large international exchanges with weaker histories of enforcement: Binance, Huobi, OKX, and FTX.

Across all transactions, we see a large spike of deposits at round numbers. Customers seem to use cryptocurrency as transfers of value to send exactly $10,000 or $100,000, regardless of whether an exchange is U.S.-based or not. We also see more mass just to the left of the large spikes for all four figures. This suggests that payments just less than round numbers occur more often than payments just more than round numbers. Further, this exists even at $100,000, despite $10,000 being the more commonly monitored threshold.

Comparing the top left and top right panels, flows to international exchanges have more flows right at $10,000, suggesting that users at international exchanges (loose KYC) likely are using crypto to move funds and have little concern for round number thresholds. At strict KYC exchanges, illicit flows in red dots send even fewer transactions right at $10,000, and thus are even more likely to avoid $10,000 than regular users. Illicit flows also contain more transactions of $9,800 and $9,900 than other regular users. This suggests that illicit actors disproportionately hide funds below the limit at KYC exchanges. Overall, the reporting limits influence all customer behavior at KYC-enforced exchanges compared

to international exchanges. Illicit funds appear to hide with greater bunching at KYC exchanges.

In Figure 12, we plot the percentage of transactions between $9,500 and $10,500 that occur in four bins: exactly $10,000, $9,900 to less than $10,000, $9,00 to $9,910 and $9,800 to $9,810. These occur with descending probability such that $10,000 is the most common transaction size in this range. We evaluate whether recent historic settlements at Binance have influenced deposit behavior. First, Binance settled with the U.S. Department of Justice on November 21, 2023, pleading guilty to federal charges and violating the Bank Secrecy Act. The CEO stepped down under this historic settlement. Further, regulators have appointed a compliance monitorship at Binance as announced in May 17, 2024.[11] Customer deposit behavior does not seem to have been influenced by either of these two days. The proportion of customers that deposit exactly $10,000 appears to have declined slightly in mid-2024 but increased by the end of the year. The same fraction of customers still bunches just below the limit and at similar round numbers. This suggests that customers do not believe Binance will seize their funds after the settlement.

C. Bridges

Bridges are a set of contracts that can be used to intermediate transfers between different blockchains. For example, suppose a user on the Bitcoin blockchain wants to use their BTC to fund an Ethereum address. One option is for that user to deposit their BTC in a centralized exchange, swap it into ETH, and transfer that ETH to an Ethereum address. Another option is to transfer ownership of that BTC to the address of a bridging service called Wrapped Bitcoin on the Bitcoin blockchain. That service would then deliver "WBTC" to a user-specified address on the Ethereum blockchain that can be used like any other token. The trade-off for the user is that using the bridge publishes the transaction on the public blockchain; however, using the bridge circumvents any possibility that an exchange would flag this transaction for KYC or KYT review.

[11] As reported by the Wall Street Journal at this link.

Importantly, bridging tokens across blockchains is another potential channel to obfuscate dirty flows. The rationale is that conventional tracing software focuses on following flows from one blockchain at a time and it may be difficult for a researcher to maintain continuity if they need to switch blockchains. In contrast, a user may also have a legitimate need to move funds to different blockchains. Centralized exchanges and bridges may both provide this service although centralized exchanges are more expensive.[12]

In the traces, we find that flows to bridges amounts to $166M, a relatively small amount. This is dwarfed by the amount that enters centralized exchanges. There are a few potential interpretations of this disparity. Illicit actors appear not to be worried about the KYC review of their transactions. Further, if they had a legitimate need for different blockchain services, they appear to be satisfied with the slightly more expensive service provided by the centralized exchange.

The largest active bridge is Bitget. Among the total flows to the Bitget bridge, we find that nearly 40-50% of flows can be attributed to addresses downstream of our trace. This suggests that the Bitget bridge users are concentrated among addresses that are related to other reported scammers or hackers. Although the flows are small, they appear to be growing later in the period.

Overall, we find that bridges are less popular than centralized exchanges for tainted flows. However, among the bridges that are used, the most common users may be other related bad actors. This is suggestive evidence that criminals understand the value of bridge services. If centralized exchanges apply more strict KYC/KYT procedures, then researchers should monitor whether illicit flows to bridges continues to grow.

[12]To bridge crypto indirectly through a centralized exchange, a user would need to pay two transfer fees (inbound and outbound) and the swap's bid-ask spread. To bridge crypto directly, a user would pay one smart contract call. On the Ethereum blockchain, as of March 2025, the median transfer fees is approximately $0.10 each while bridging incurs $0.15, according to Etherscan. These prices are below the typical cost from the period we study.

D. Potential Shadow Exchanges

The last common destination of traced funds are large unidentified addresses. This occurs when we conservatively stop at a large address that is likely an exchange but we lack the data to attribute it to any specific entity. Over time, as forensic researchers continue to expose illicit flows, these entities may be unmasked. For example, Huione is a notable "shadow" exchange based in Southeast Asia that is commonly used by scammers. However, the broader crypto community has only recently uncovered the set of addresses used by this exchange.

We trace approximately $2.7 billion to large addresses that we cannot identify. In Figure IA.2, we note that the same large unidentified addresses appear in traced paths from different types of scams and hacks. This suggests that there are exist common services used by these scammers and hackers, such as shadow exchanges. We highlight these as one area where the forensic community should apply more scrutiny.

VI. Conclusion

We analyze the dark side of crypto activity and money laundering originating from a wide variety of scamming, hacks, and other criminal activity. DeFi services, such as swap contracts on decentralized exchanges, that are commonly used by regular users are also popular with scammers and hackers. Mixers like Tornado Cash, although infamous, are infrequently used as compared to DEXs or centralized exchanges. However, even though known for money laundering and even after the U.S. ban, we find that many Tornado Cash users also funnel their proceeds directly into DEXs indicating little fear of monitoring by DEXs.

Centralized exchanges are the largest destinations for tainted flows, likely because these are venues where users can offload cryptocurrency into fiat in the international financial system. In principle, these exchanges should enforce anti-money laundering laws. Recent regulatory enforcement actions against these have seemingly not deterred

such activities in most criminal crypto activities. However, the government's ban against Tornado Cash caused a marked decrease in large centralized exchanges handling funds from Tornado Cash. This indicates that future regulatory intervention or guidance for exchanges to not handle flows from identified sources of dirty money or utilize more effective monitoring could reduce the connections between criminals and centralized exchanges. Overall, cryptocurrency environments continue to be an active arena for dirty capital flows. Scammers, hackers, and other bad actors continue to find new avenues to launder their funds, yet most of the criminal flows are mostly detectable and traceable.

We hope our research will encourage more rigorous monitoring and enforcement. Our findings indicate that both centralized and decentralized exchanges could implement much more active monitoring but have seemingly chosen not to. Regulatory intervention or more active prosecution may be needed to reduce criminal flows in the space. We hope to see more forensic research to help more strictly understand, detect, monitor, and reduce dirty capital flows.

References

Agca, Senay, Pablo Slutzky, and Stefan Zeume, 2020, The Weight of Compliance: Anti-Money Laundering Enforcement, Bank Composition, and Lending, *Working Paper* .

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, Keith B., 2021, To Whom Do Victims of Mass-Market Consumer Fraud Complain?

Anderson, Ross, Ilia Shumailov, and Mansoor Ahmed, 2018, Making Bitcoin Legal, *Security Protocols XXVI* 11286, 243–253.

Chainalysis, 2023, The 2023 crypto crime report.

Chainalysis, 2024, The 2024 crypto crime report.

Cong, Lin, Kimberly Grauer, Daniel Rabetti, and Henry Updegrave, 2023a, Blockchain forensics and crypto-related cybercrimes.

Cong, Lin William, Campbell R. Harvey, Daniel Rabetti, and Zong-Yu Wu, 2023b, An anatomy of crypto-enabled cybercrimes.

Draca, Mirko, and Stephen Machin, 2015, Crime and Economic Incentives, *Annual Review of Economics* 7, 389–408.

El Siwi, Yara, 2018, Mafia, money-laundering and the battle against criminal capital: the italian case, *Journal of Money Laundering Control* 21, 124–133.

Foley, Sean, Jonathan R Karlsen, and Tālis J Putniņš, 2019, Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?, *The Review of Financial Studies* 32, 1798–1853.

Fracassi, Cezare, and Eric Lee, 2025, The (in-)effectiveness of anti-money laundering, *Working Paper* .

Félez-Viñas, Ester, Luke Johnson, and Talis J. Putnins, 2022, Insider trading in cryptocurrency markets, *SSRN Electronic Journal* .

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?

Griffin, John M., and Kevin Mei, 2024, How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering, *Working Paper* .

Griffin, John M., and Amin Shams, 2020, Is bitcoin really untethered?, *The Journal of Finance* 75, 1913–1964.

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.

Li, Tao, Donghwa Shin, and Baolian Wang, 2018, Cryptocurrency pump-and-dump schemes, Working Paper.

Makarov, Igor, and Antoinette Schoar, 2021, 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.

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, 2022, Don't trust, verify: The economics of scams in initial coin offerings.

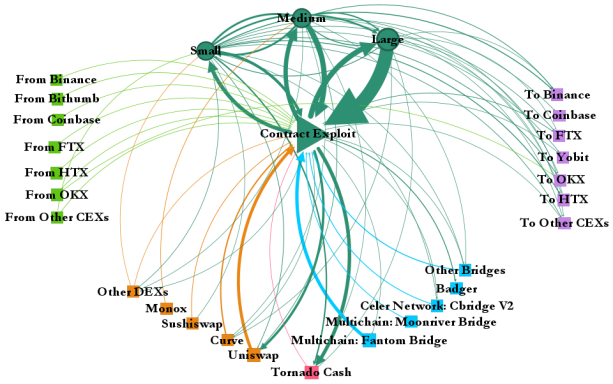
Sokolov, Konstantin, 2021, Ransomware activity and blockchain congestion, *Journal of Financial Economics* 141, 771–782.

Victor, Friedhelm, 2020, Address clustering heuristics for ethereum.

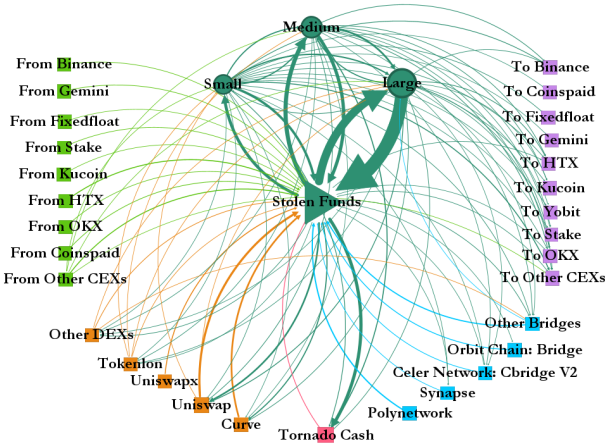
Figure 1: Network Graphs of Select Scams

This figure shows transaction flows for six distinct scam types, depicting representative fund movements across the crypto ecosystem. Each panel visualizes one specific scam, showing centralized exchange (CEX) inflows on the left-hand side, CEX outflows on the right-hand side, decentralized exchanges (DEX) in the lower left, blockchain bridges in the lower right, and the mixer Tornado Cash positioned at the bottom. The edges indicate the direction and relative magnitude of flows, with thicker edges representing larger transaction volumes. Edges concave upwards represent flows moving from left to right (e.g., from 9 o'clock to 3 o'clock), while edges concave downwards indicate flows moving from right to left (e.g., from 3 o'clock to 9 o'clock). The flows in each panel are individually scaled based on the total volume of activity specific to each scam.

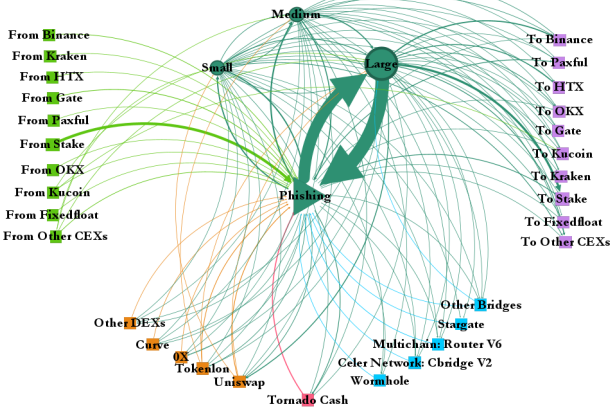
Panel A: Contract Exploit



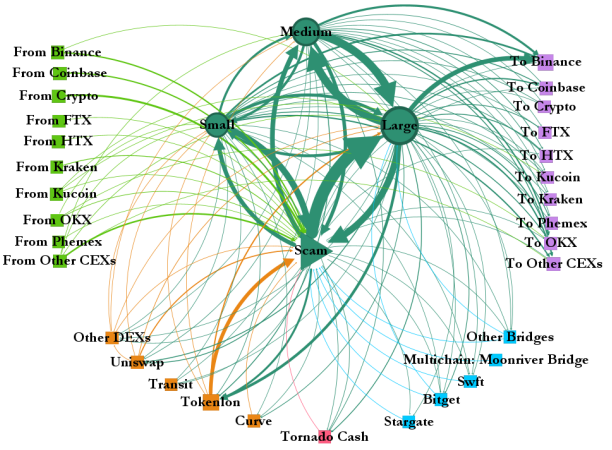
Panel B: Stolen Funds



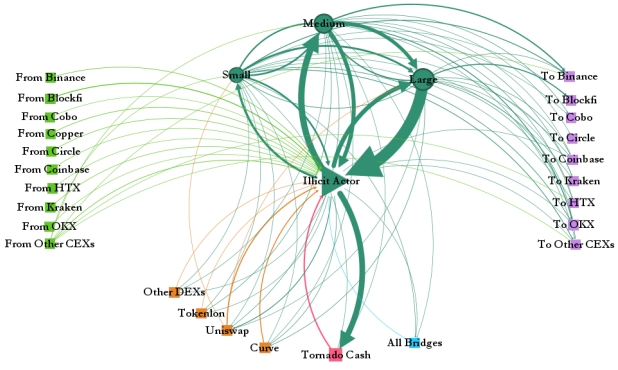
Panel C: Phishing



Panel D: Scam



Panel E: Illicit Actor



Panel F: Fake Project

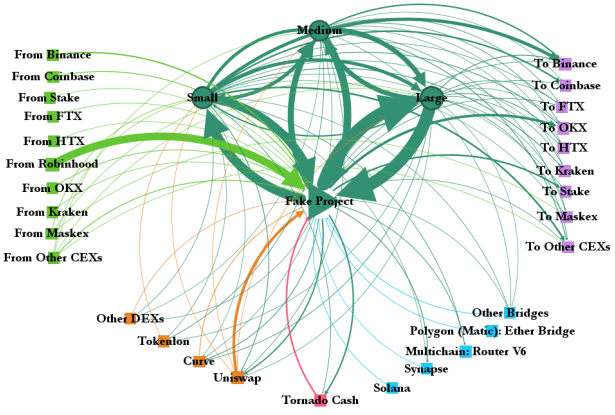


Figure 2: Inflows to Reported addresses

This figure shows inflows to reported addresses across different types of scams. Each point represents a specific type of scam. The vertical position (y-axis, logarithmic scale) indicates the total inflow value, and the horizontal position (x-axis) shows the average number of transactions per reported address. The size of each point corresponds to the total number of active reported addresses involved in that specific scam type. Each point contains a pie chart, which breaks down the blockchain composition of the addresses involved, specifically indicating fractions of Bitcoin (BTC), Ethereum (ETH), and TRON (TRX).

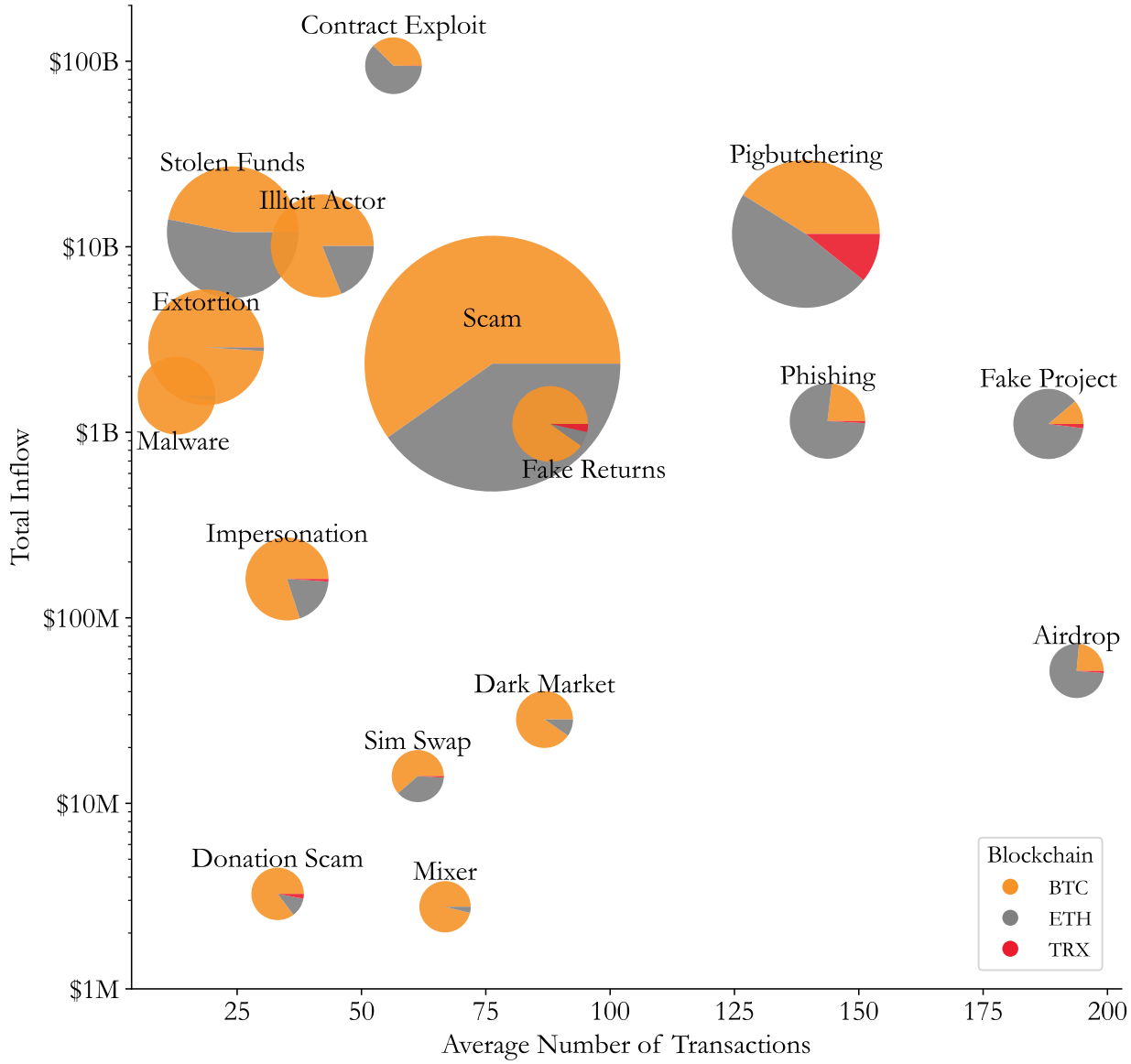
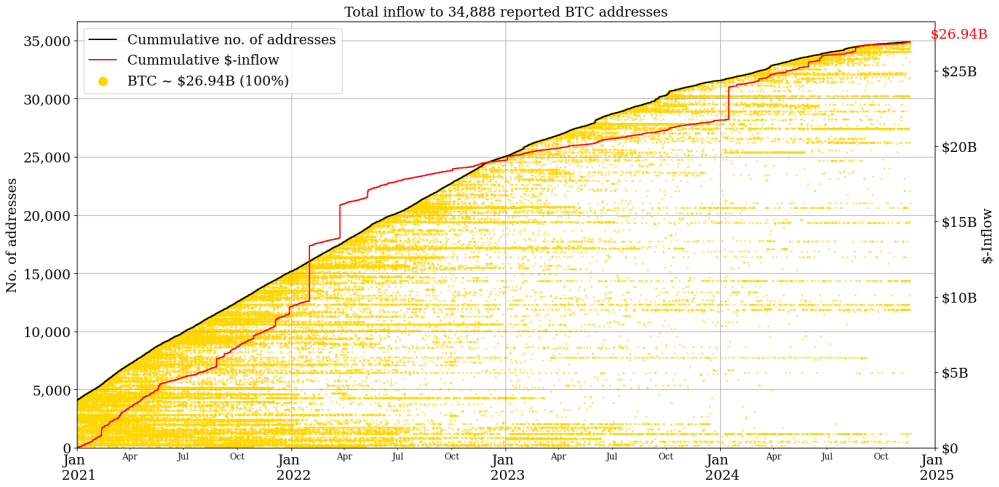


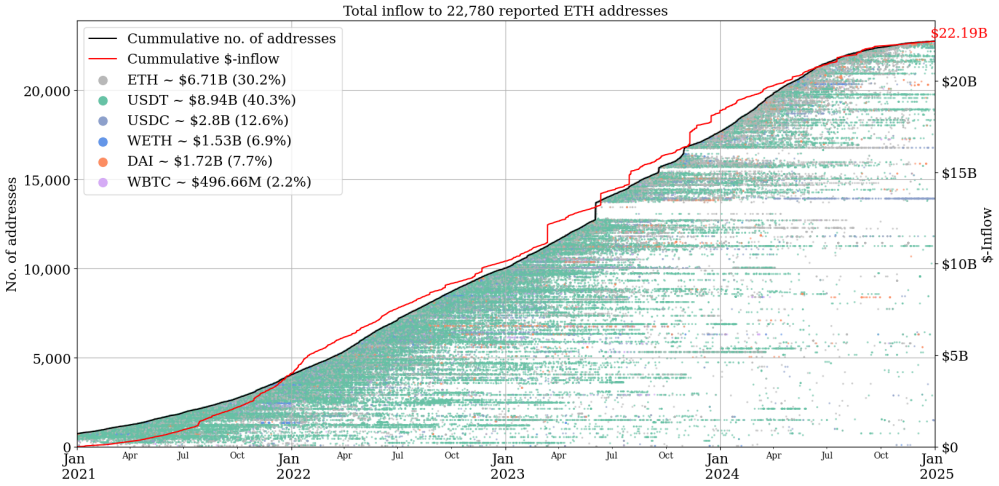
Figure 3: Transaction Timing and Address Activity

This figure shows the timing, inflow amounts, and activity duration of transactions to reported addresses. Panels A and B illustrate individual transactions sorted chronologically, with Panel A representing Bitcoin addresses and Panel B representing Ethereum addresses. Each horizontal line represents an address sorted by its first transaction date. The dots indicate transactions over $10,000, colored by the cryptocurrency or token type. The number of addresses, shown by the black line, is based on the date of the first transaction (left y-axis). The red line represents cumulative total inflows (right y-axis). Panel C illustrates the lifespan of addresses, showing how many years addresses remain active, grouped by their starting year.

Panel A: Bitcoin



Panel B: Ethereum



Panel C: Address Lifespan by Blockchain

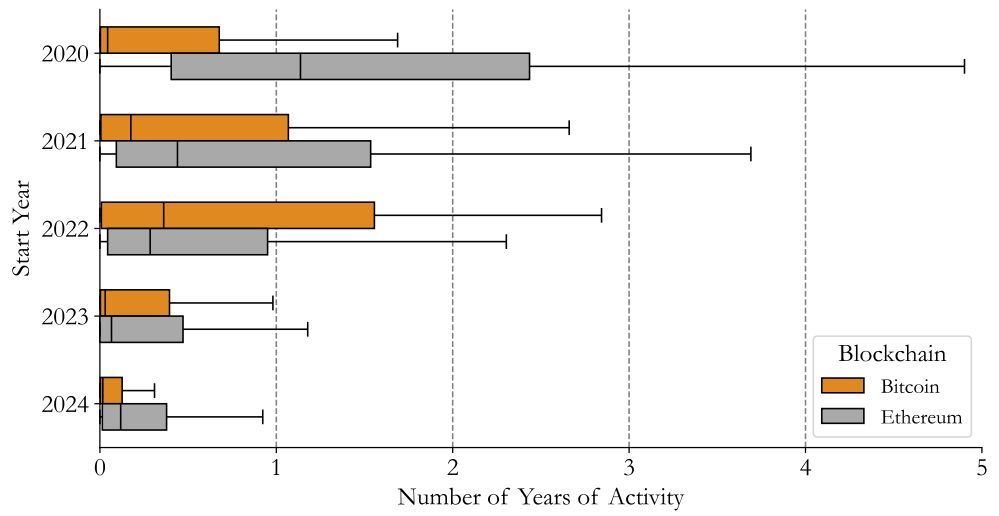
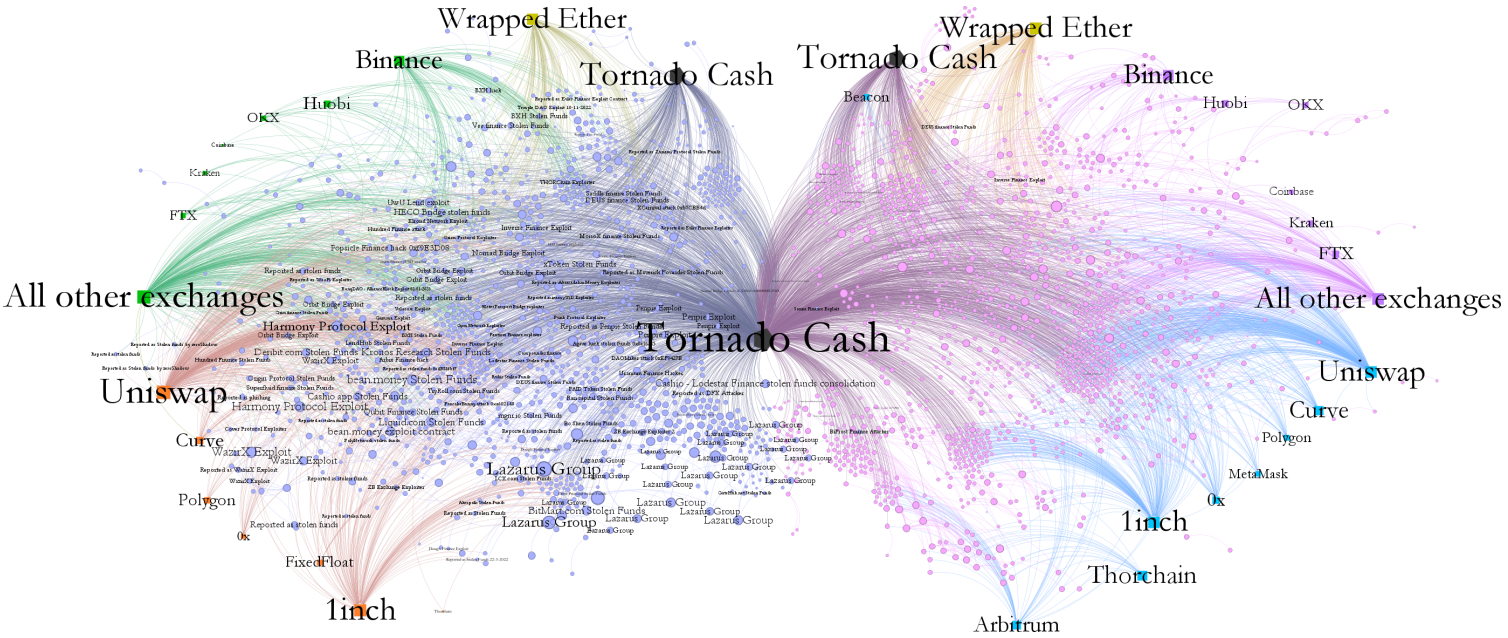


Figure 4: Tornado Cash Transaction Networks and Flows

This figure visualizes transaction flows involving Tornado Cash. Panel A illustrates the network of flows involving Tornado Cash, with senders positioned on the left and receivers on the right. Edges concave upwards 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 downwards indicate flows moving from right to left (e.g., from 3 o'clock to 9 o'clock). Panel B uses a Sankey diagram to depict the outflows from Tornado Cash across multiple transaction hops, where flows into centralized exchanges are shown in blue and flows into decentralized exchanges are shown in red.

Panel A: Network Graph



Panel B: Sankey Diagram

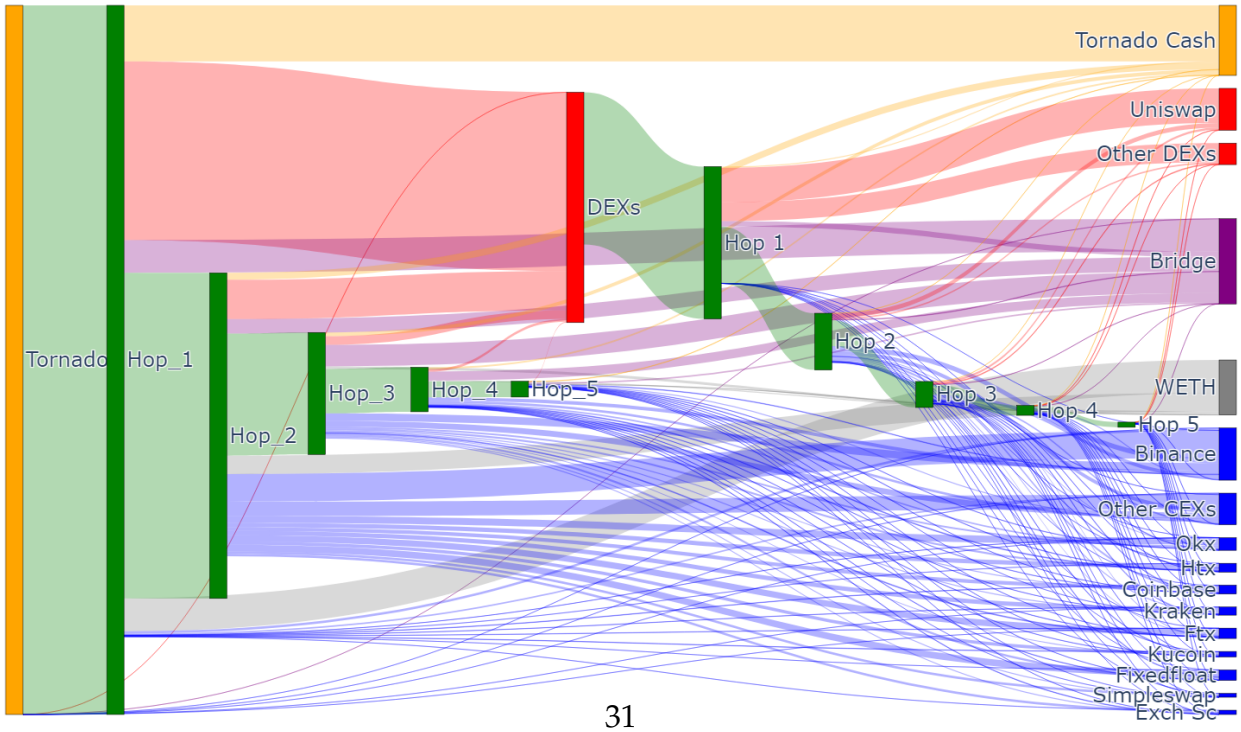


Figure 5: Inflows to Tornado Cash

This figure shows the total inflows and traced criminal inflows to Tornado Cash from 2021 to 2024. The blue line indicates the total monthly inflows to Tornado Cash. The red line represents traced monthly criminal inflows from all scam types. The dashed vertical lines indicate the period during which Tornado Cash was sanctioned by the U.S. Treasury, beginning on August 8, 2022, and lifted on November 26, 2024. The legend provides aggregate statistics for the entire period.

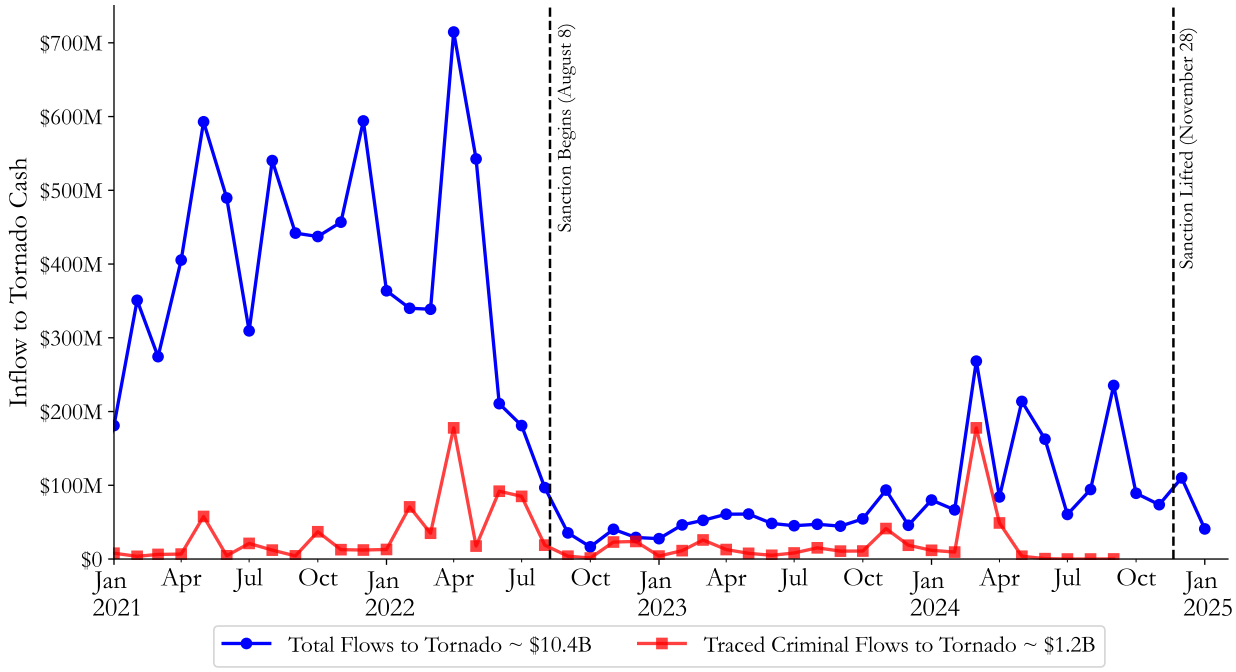
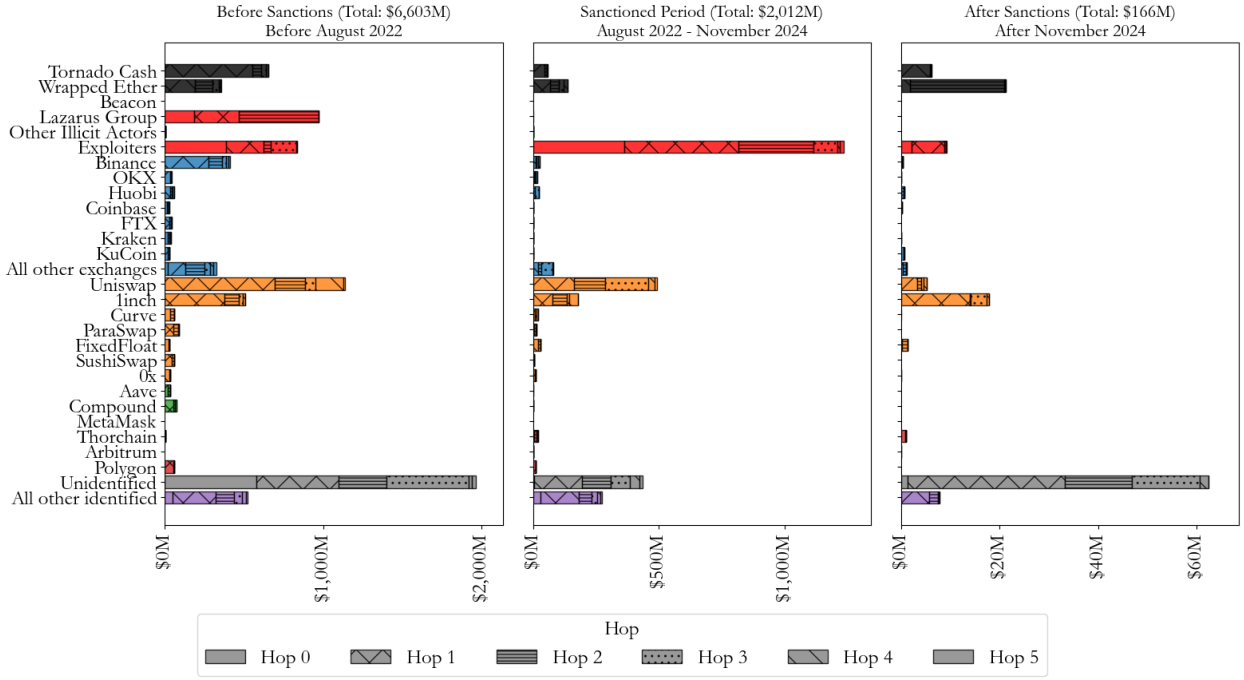


Figure 6: Destinations of Tornado Cash Outflows

This figure shows Tornado Cash inflows (Panel A) and outflows (Panel B) by hop. The y-axis lists the various entities found in each corresponding trace, and the hatches stand for the hops in each trace. The left panels are before the ban, the center panels are during the ban, and the right panels are after the ban was lifted. Hatches indicate hop distance from Tornado Cash.

Panel A: Tornado Cash Inflows



Panel B: Tornado Cash Outflows

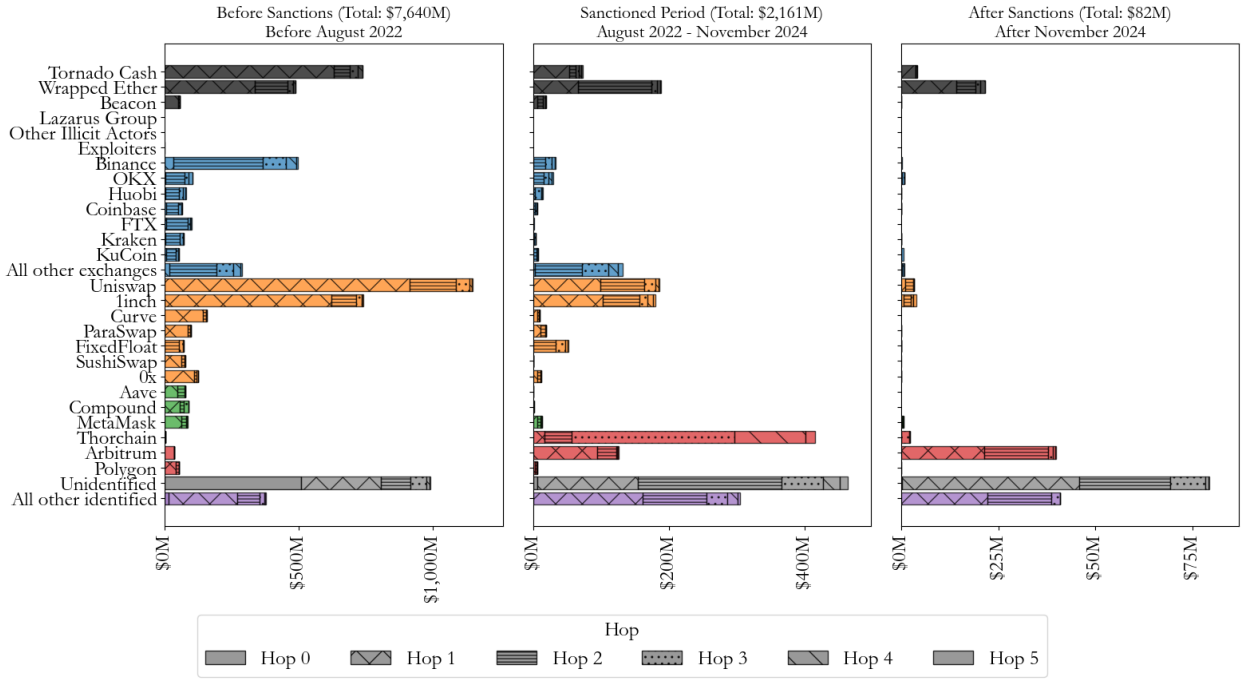


Figure 7: Top Tornado Cash Related Scams

This figure shows the total amounts deposited by the top 50 reported addresses into Tornado Cash. Each horizontal bar represents an individual reported Ethereum address, and is colored according to its scam category. Hatches indicate in which hop of the backward trace the reported addresses forwarded the funds for depositing to Tornado Cash.

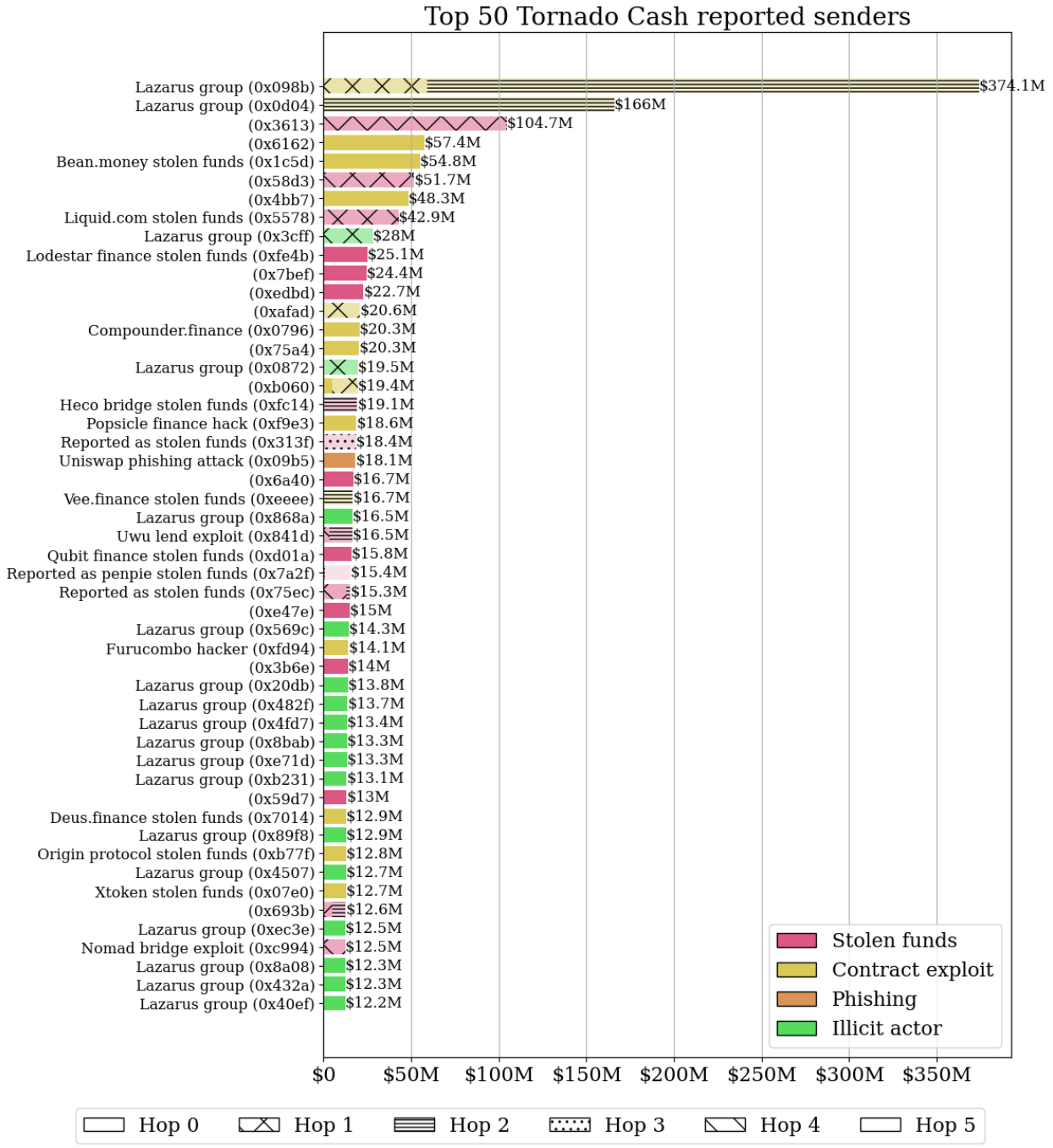
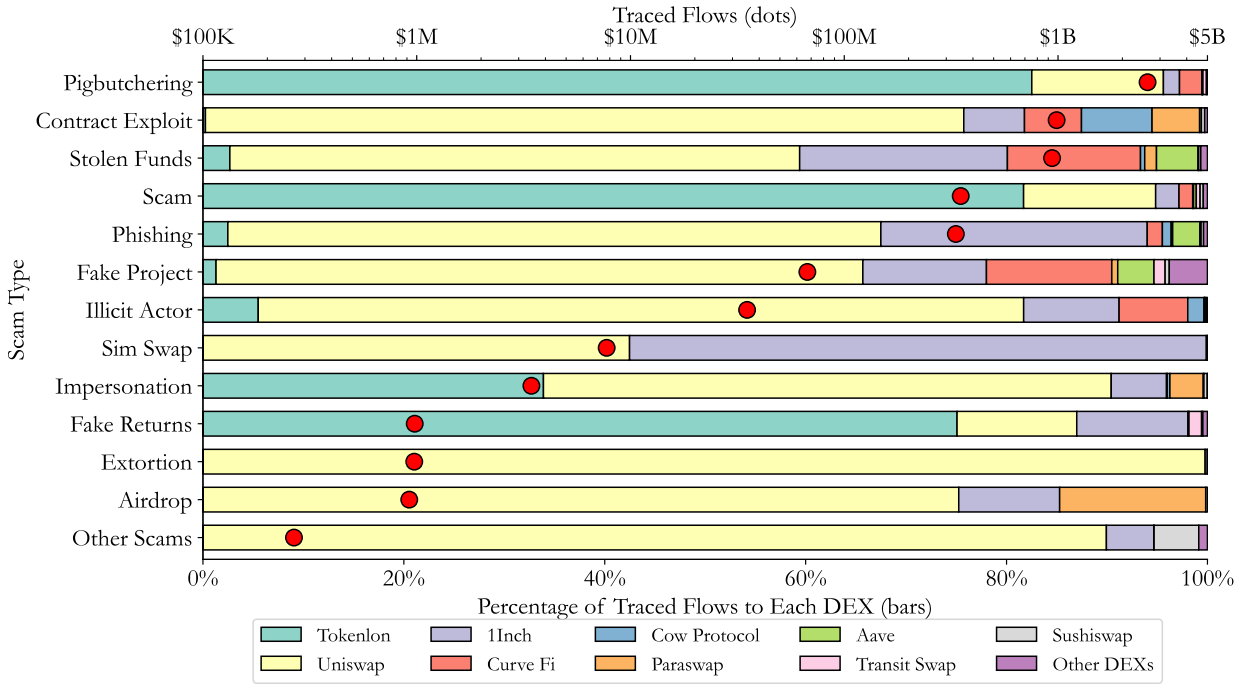


Figure 8: Traced Flows to Decentralized Exchanges (DEXs)

This figure shows the DEX destinations for each traced scam. Panel A shows the totals for each scam. Each horizontal bar is broken by the DEX percentage of the total amount traced to DEXs for each scam, which is reflected in the lower x-axis. The corresponding red dots to each bar indicate the total amount traced to DEXs for each scam, which are represented in the upper x-axis. Panel B shows the DEX flows as a percentage of the total monthly traced to DEXs.

Panel A: Traced Flows to DEXs by Scams



Panel B: Traced Flows to DEXs by Months

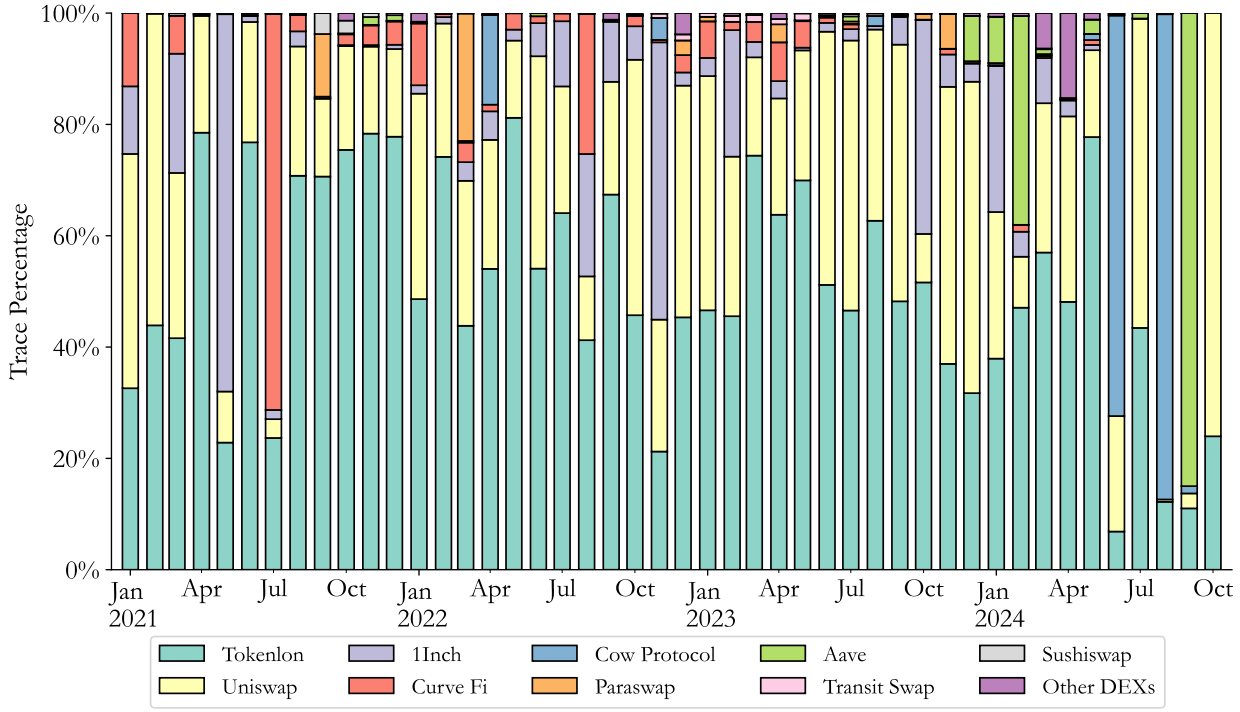
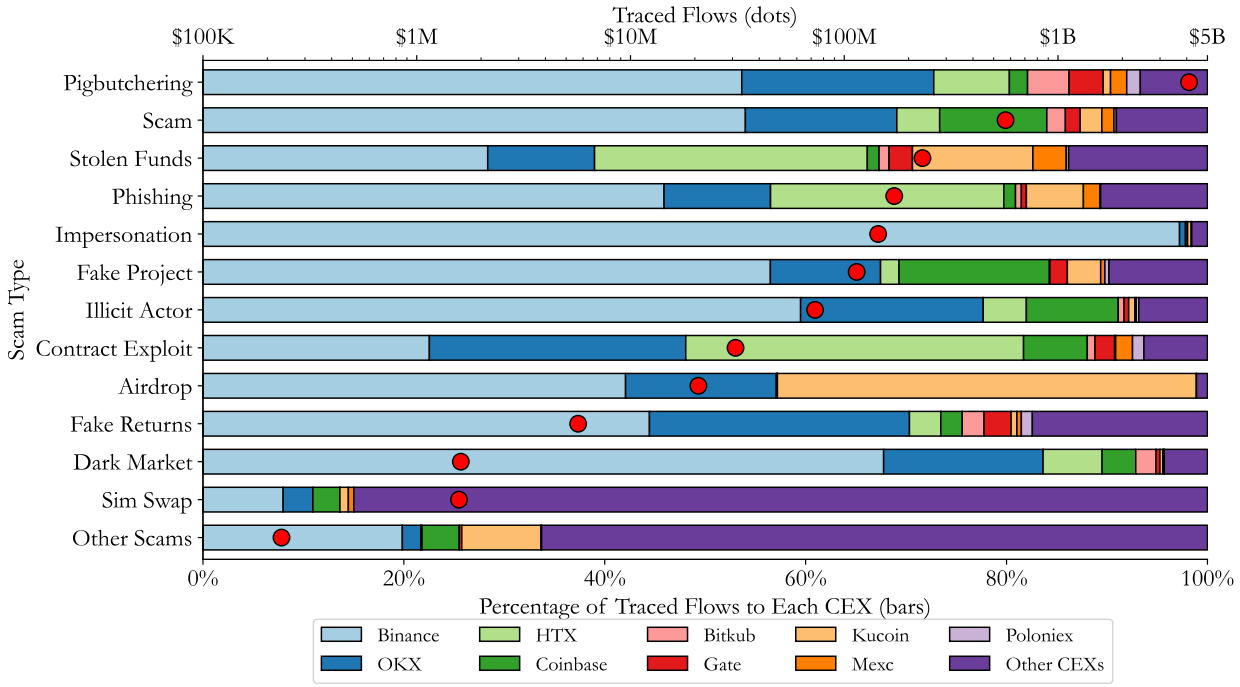


Figure 9: Traced Flows to Centralized Exchanges (CEXs)

This figure shows the CEX destinations for each traced scam. Panel A shows the totals for each scam. Each horizontal bar is broken by the CEX percentage of the total amount traced to CEXs for each scam, which is reflected in the lower x-axis. The corresponding red dots to each bar indicate the total amount traced to CEXs for each scam, which is represented in the upper x-axis. Panel B shows the CEX flows as a percentage of the total monthly traced to CEXs.

Panel A: Traced Flows to CEXs by Scams



Panel B: Traced Flows to CEXs by Months

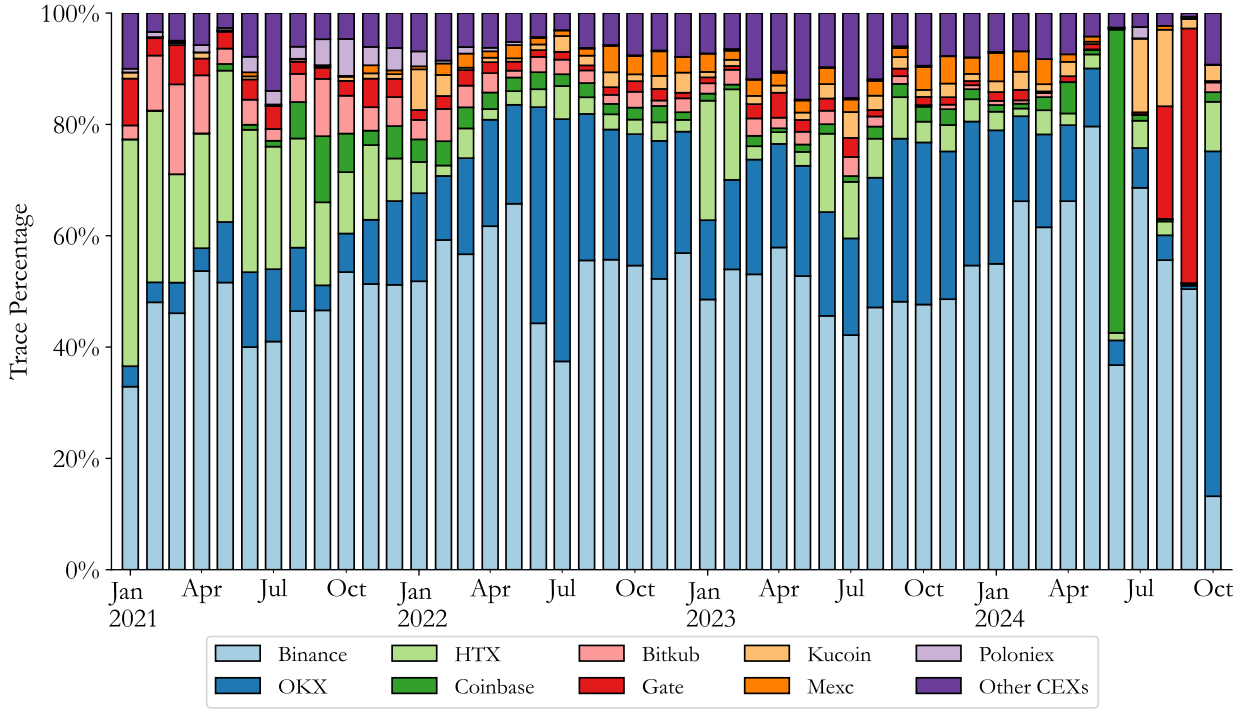


Figure 10: Fraudulent Activity per Exchange

This figure shows the proportion of total lifetime fraudulent activity relative to the total inflow for each exchange after the deposit clustering heuristic. The vertical axis lists individual exchanges. The horizontal axis at the top represents the percentage of total lifetime fraudulent inflows relative to the exchange's overall inflows, depicted by horizontal bars. The horizontal axis at the bottom displays the total lifetime fraudulent inflow in dollars, represented by red dots.

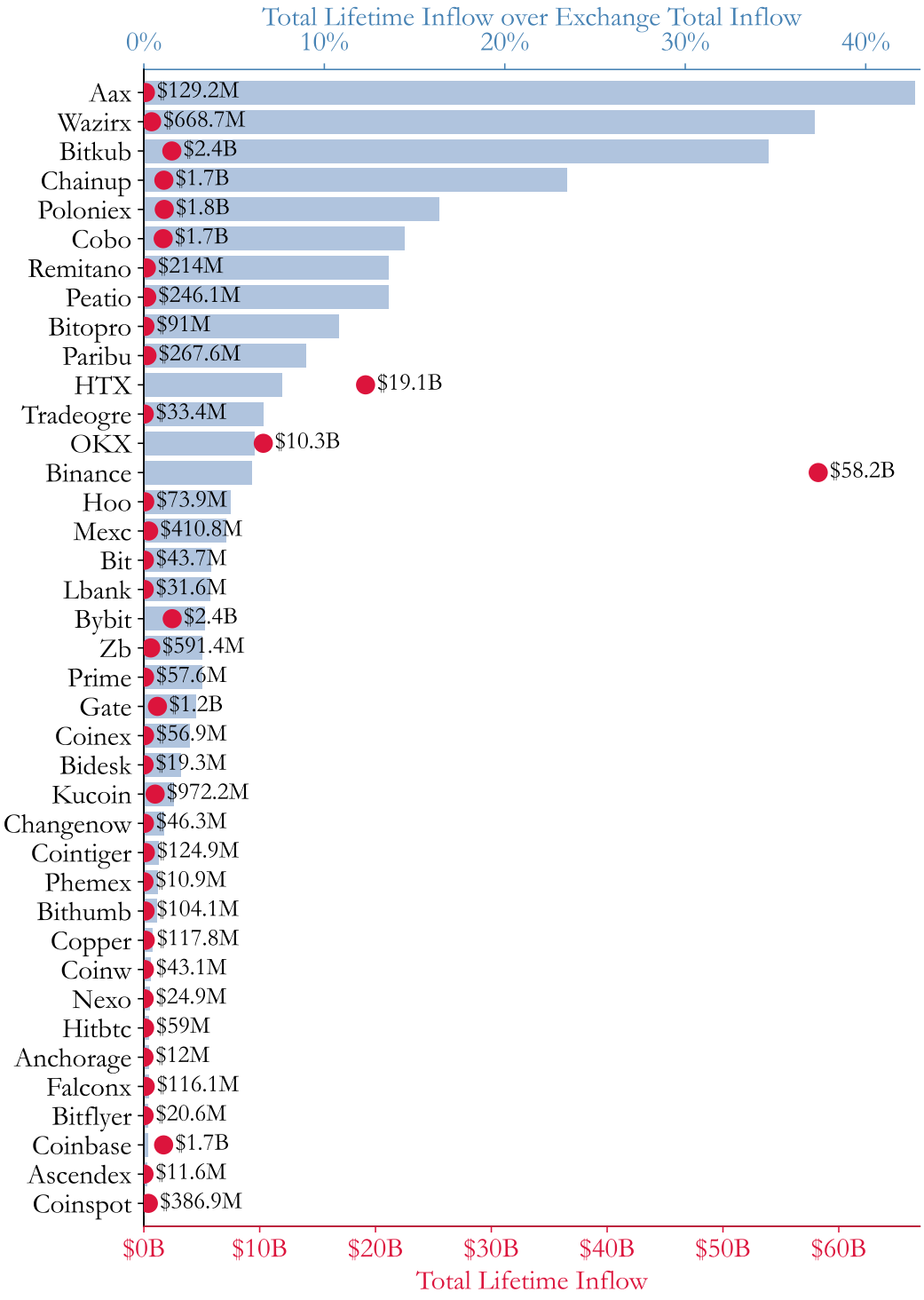


Figure 11: Evidence of Bunching

These histograms show the distribution of transaction size. The x-axes show the transaction size binned to intervals of $10. The y-axes show the number of transactions in that bin as a percentage of the total transactions shown within that range. The upper panels show percentage of transactions between $9,500 and $10,500 that fall in each bin and the bottom show the range between $99,500 and $100,500. Left panels split KYC-enforced exchanges (Coinbase, Crypto.com, Gemini, Kraken) and the right show other major exchanges with looser enforcement histories (Binance, Huobi, OKX, FTX). Red dots show the distribution of illicit flows and bars show all other transactions that occur to these exchanges. The center bin is exactly the round number of $10,000 (top panels) or $100,000 (bottom panels). The bins to the left of the center bin are left-inclusive (e.g., $9,990 to $9,999.99) and the rights to the right are right-inclusive (e.g., $10,000.01 to $10,010).

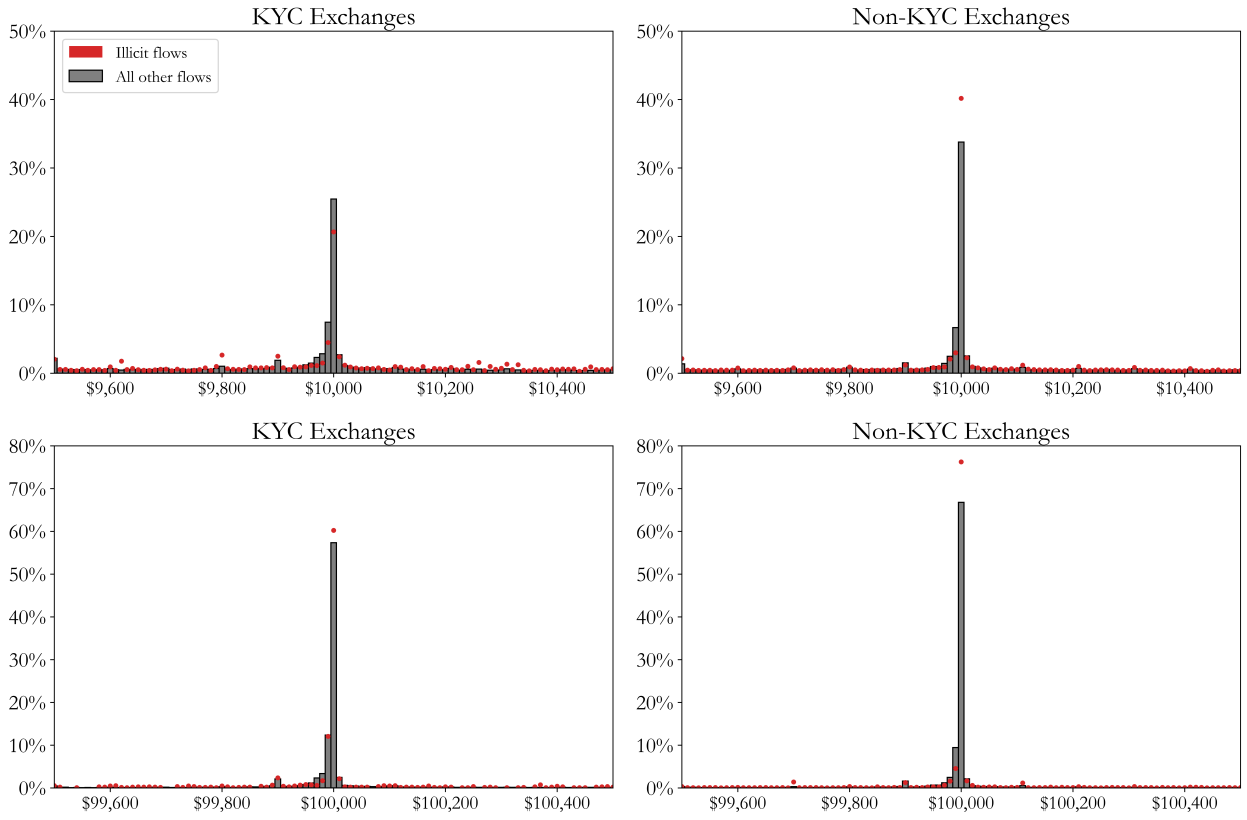


Figure 12: Monthly Distribution of Binance Deposits by Transaction Size Bins

This figure shows the monthly proportion of deposits to Binance that fall into specific transaction size bins around $10,000. The horizontal axis shows the timeline from 2020 to 2025, while the vertical axis displays the percentage of transactions within each bin. Four bins are shown: exactly $10,000 (red line), $9,900–$10,000 (green line), $9,900 (orange line), and $9,800 (blue line). Two vertical dashed lines indicate significant regulatory events at Binance: the DOJ settlement on November 21, 2023, and the announcement of compliance monitorship on May 17, 2024.

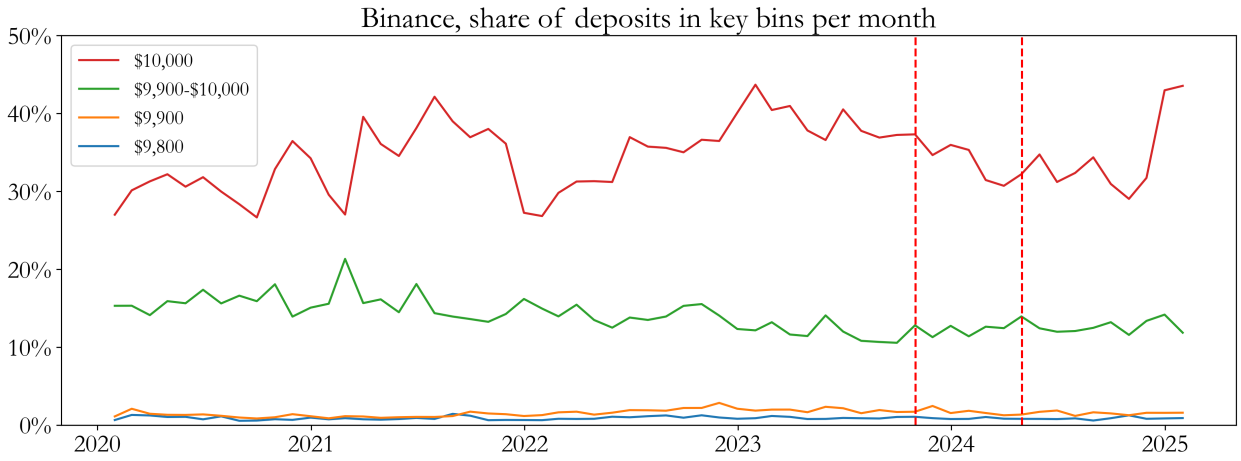
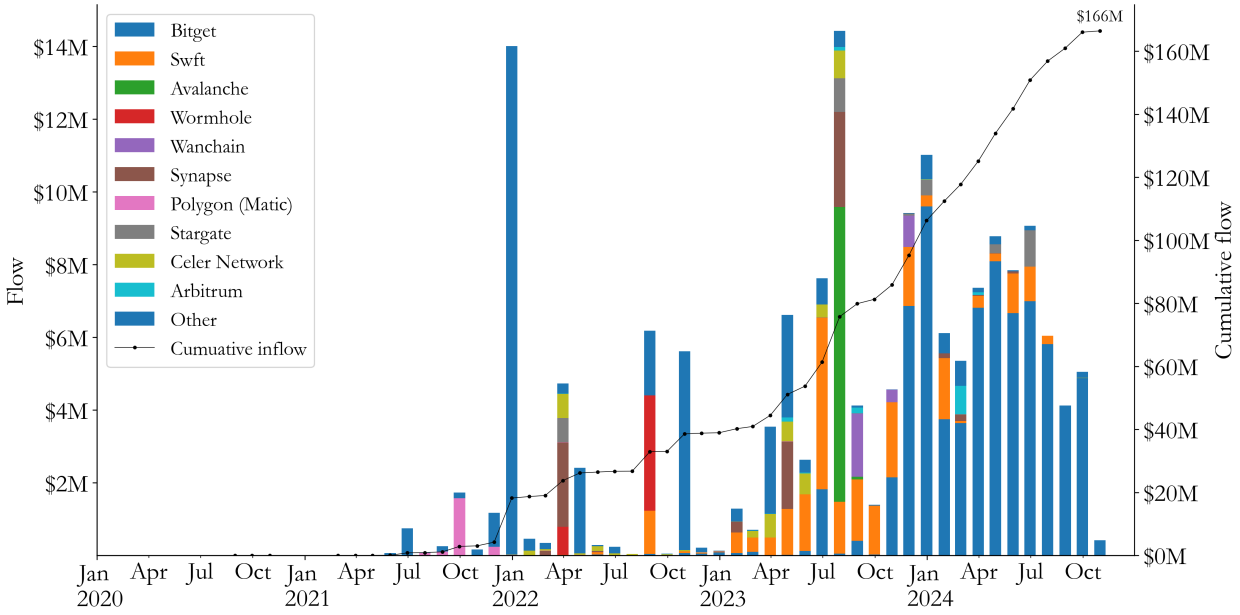


Figure 13: Flows to Bridges

This figure shows the flows to bridges over time. Panel A represents traced amounts to all bridges in the data. Panel B focuses on Bitget, the largest destination, and compares total Bitget flows to the traced flows.

Panel A: Flows to Bridges



Panel B: Flows to Bitget

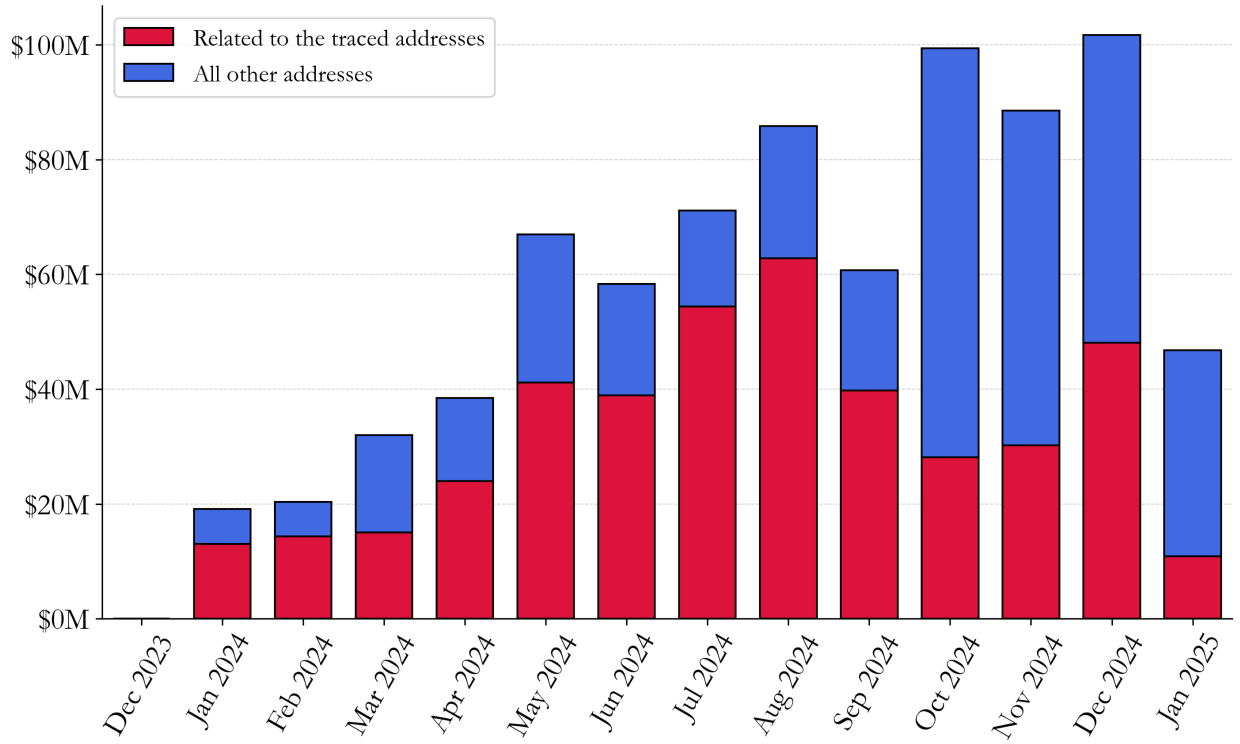


Table 1: Reports Summary

This table presents summary statistics of reports. The totals exclude contract exploit.

	Total Reports	Reports with active address	and remove duplicates within scams	and remove likely exchanges	and remove duplicates between scams	Total Inflow
Contract Exploit	1,136	1,088	730	557	504	$94.18B
Stolen Funds	9,264	9,136	9,136	7,980	7,943	$12.2B
Pigbutchering	25,809	21,056	13,172	10,095	8,880	$10.45B
Illicit Actor	6,882	6,872	6,872	5,158	5,061	$10.26B
Scam	30,056	29,872	29,872	22,167	21,466	$3.82B
Extortion	192,935	91,977	7,406	6,416	6,226	$2.82B
Malware	14,341	10,569	10,150	2,992	2,640	$1.62B
Phishing	5,699	5,227	3,606	2,670	2,196	$1.12B
Fake Project	4,101	3,854	2,546	1,911	1,815	$1.09B
Fake Returns	4,843	4,407	3,791	2,621	2,098	$1.06B
Impersonation	7,348	6,355	4,297	3,336	2,966	$157.62M
Airdrop	795	739	494	340	262	$37.79M
Dark Market	833	831	827	577	575	$28.32M
Sim Swap	192	170	152	122	105	$9.8M
Mixer	40	38	38	26	26	$2.77M
Donation Scam	640	365	224	163	125	$749.4K
Bitcoin (excl. CE)	255,554	147,671			38,727	$22.17B
Ethereum (excl. CE)	39,903	35,845			22,445	$21.32B
Tron (excl. CE)	8,321	7,952			1,212	$1.2B
Total (excl. CE)	303,778	191,468			62,384	$44.68B

Table 2: Address Total Inflow Summary

This table presents summary statistics by scam of the total dollar inflow into addresses. The total row excludes contract exploit.

Category	N	Total Inflow	Mean	Std	25%	50%	75%
Contract exploit	504	$94.18B	$186.86M	$2.8B	$19.47K	$133.01K	$377.69K
Stolen funds	7,943	$12.2B	$1.54M	$13.48M	$6.65K	$60.01K	$353.83K
Pigbutchering	8,880	$10.45B	$1.18M	$10.08M	$5.2K	$55.16K	$401.01K
Illicit actor	5,061	$10.26B	$2.03M	$61.88M	$145.03	$1.24K	$19.12K
Scam	21,466	$3.82B	$177.9K	$1.68M	$594.3	$5.31K	$33.92K
Extortion	6,226	$2.82B	$452.74K	$16.72M	$538.69	$1.36K	$3.33K
Malware	2,640	$1.62B	$613.87K	$2M	$4.61K	$98.33K	$400.3K
Phishing	2,196	$1.12B	$510.88K	$9.35M	$1.52K	$17.5K	$109.43K
Fake project	1,815	$1.09B	$599.47K	$4.53M	$22.87	$10.77K	$170.03K
Fake returns	2,098	$1.06B	$506.72K	$11.74M	$763.28	$6.26K	$35.36K
Impersonation	2,966	$157.62M	$53.14K	$321.75K	$913.69	$5.27K	$20.78K
Airdrop	262	$37.79M	$144.22K	$677.8K	$113.15	$5.21K	$51.11K
Dark market	575	$28.32M	$49.26K	$373.98K	$57.3	$236.02	$2.87K
Sim swap	105	$9.8M	$93.37K	$152.03K	$4.08K	$24.14K	$113.71K
Mixer	26	$2.77M	$106.57K	$519.04K	$64.09	$188.35	$5.76K
Donation scam	125	$749.4K	$6K	$20.91K	$44	$397.05	$2K
Total (excl. CE)	62,384	$44.68B	$716.20K	$19.64M	$846	$7.49K	$76.33K
Total	304,914	192,556			62,888	$138.86B	

Table 3: Address Number of Transactions Summary

This table contains summary statistics on the number of transactions by scam. The total row excludes contract exploit.

Category	N	Total No. Transactions	Mean	Std	25%	50%	75%
Scam	21,466	1,761,745	82	173	5	21	79
Pigbutchering	8,880	1,194,910	134	254	6	34	145
Fake project	1,815	335,267	184	347	8	32	177
Phishing	2,196	325,046	148	283	6	31	145
Illicit actor	5,061	214,310	42	138	2	3	17
Stolen funds	7,943	196,736	24	85	2	5	14
Fake returns	2,098	177,457	84	186	4	15	74
Extortion	6,226	107,647	17	85	2	3	7
Impersonation	2,966	102,453	34	109	2	6	17
Dark market	575	49,747	86	246	3	6	43
Airdrop	262	42,981	164	315	7	42	165
Malware	2,640	35,497	13	65	2	2	4
Contract exploit	504	19,552	38	138	2	4	17
Sim swap	105	6,586	62	128	2	8	58
Donation scam	125	3,559	28	64	2	4	15
Mixer	26	1,737	66	234	2	2	4
Total (excl. CE)	62,384	4,544,302	72	184	3	10	52

Table 4: Deposit Addresses Summary

This table contains summary statistics on the deposit addresses encountered at the end of trace paths. Large deposit addresses are addresses where we have followed more than $100,000 in traced amount, while small addresses are lower $100,000.

Panel A. Large deposit addresses ($\geq$ \$100K)	count	mean	std	min	25%	50%	75%	max
Transaction count	5,663	142	218	2	21	63	165	1,961
Total Inflow ($K)	5,663	8,731	50,298	100	517	1,697	5,590	2,801,075
Total Outflow ($K)	5,663	8,749	50,366	0	517	1,700	5,590	2,800,159
Average Transaction Size ($K)	5,663	152	678	1	30	67	139	41,371
Days Active	5,663	452	426	0	100	358	709	2,535
In Degree	5,663	17	27	1	4	9	20	521
Out Degree	5,663	3	3	1	2	3	4	106
Panel B. Small deposit addresses (< \$100K)	count	mean	std	min	25%	50%	75%	max
Transaction count	16,414	97	184	2	15	37	95	1,998
Total Inflow ($K)	16,414	4,905	26,471	100	343	926	2,916	1,589,760
Total Outflow ($K)	16,414	4,909	26,472	0	344	928	2,916	1,589,760
Average Transaction Size ($K)	16,414	139	537	0	27	57	122	39,598
Days Active	16,414	534	460	0	128	476	823	2,722
In Degree	16,414	14	22	1	4	8	15	620
Out Degree	16,414	3	11	1	2	3	4	1,423

For Online Publication

Internet Appendix for: "Where Does Criminal Crypto Go?"

Figure IA.1: Summary statistics on scam sizes

This figure shows the summary statistics of the reported addresses by types of scams.

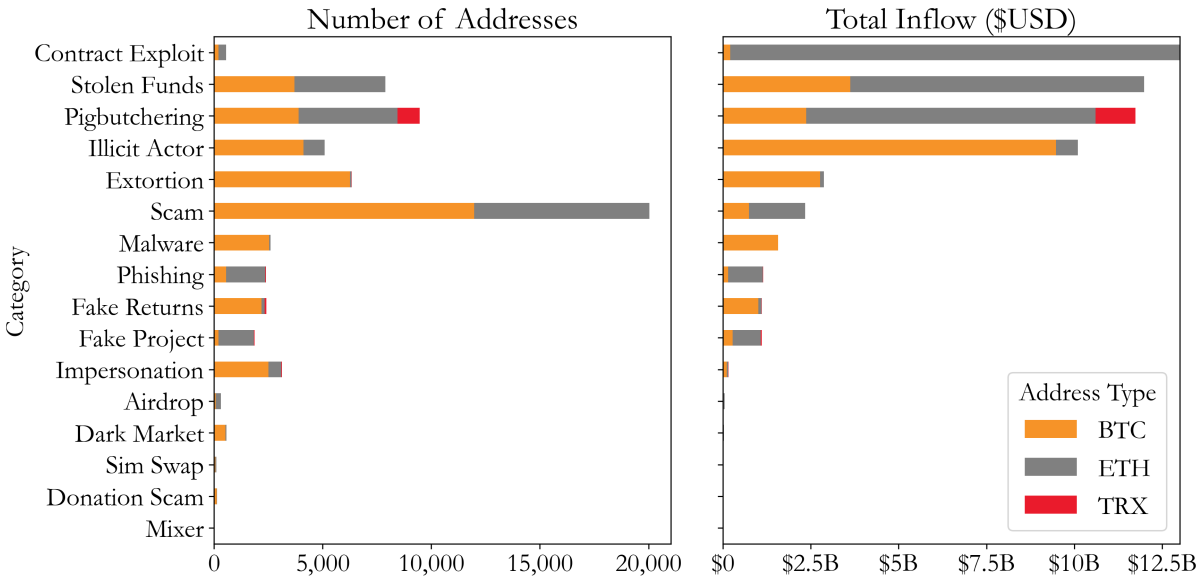


Figure IA.2: Unidentified destinations across scams

This figure shows the traced flows to unidentified addresses above the 2,000 transaction threshold.

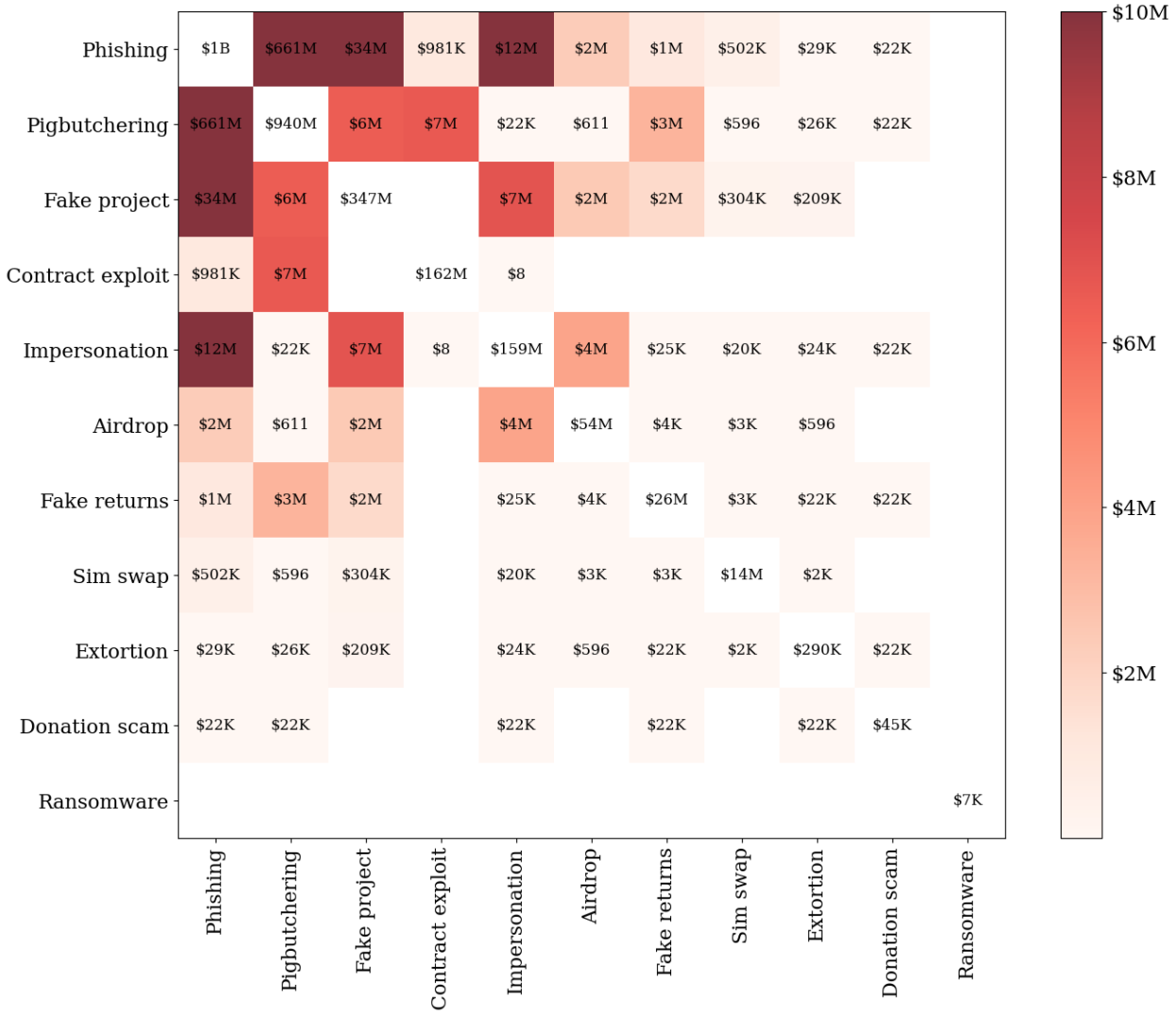
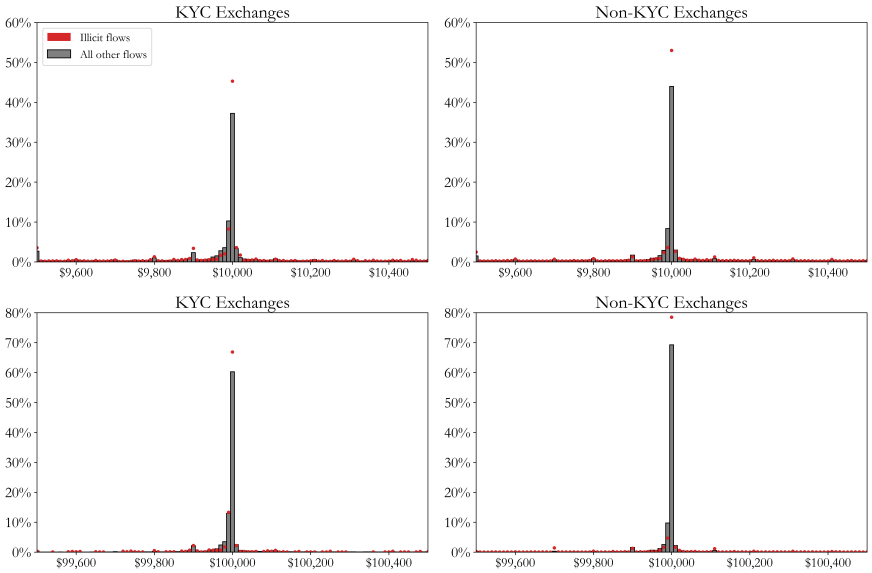


Figure IA.3: Deposit

These histograms show the distribution of transaction size. Panel A shows just stablecoins and Panel B shows other popular cryptocurrencies on Ethereum.

(a) Stablecoins: USDT, USDC, DAI



(b) Ether, Wrapped BTC, Wrapped ETH

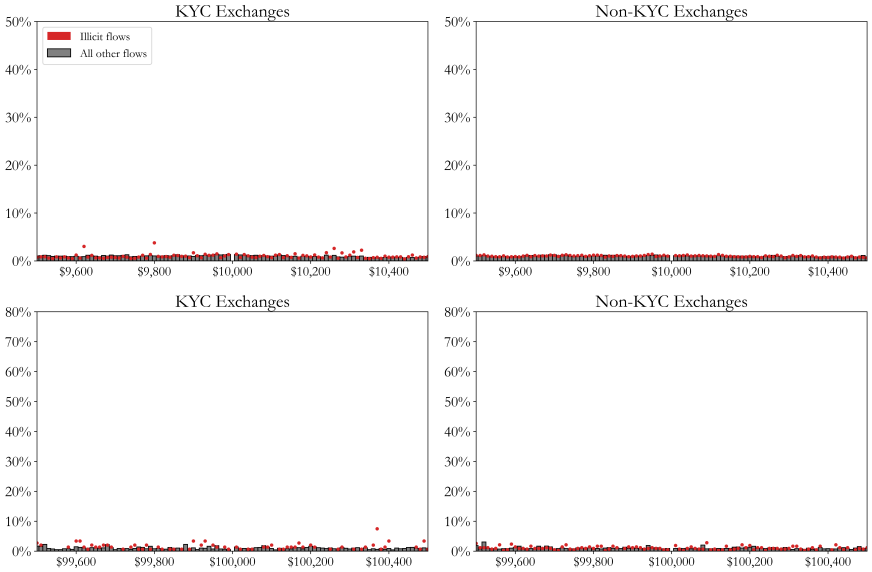


Figure IA.4: Tornado related scams

This figure shows the type of scams that send and receive flows from Tornado Cash.

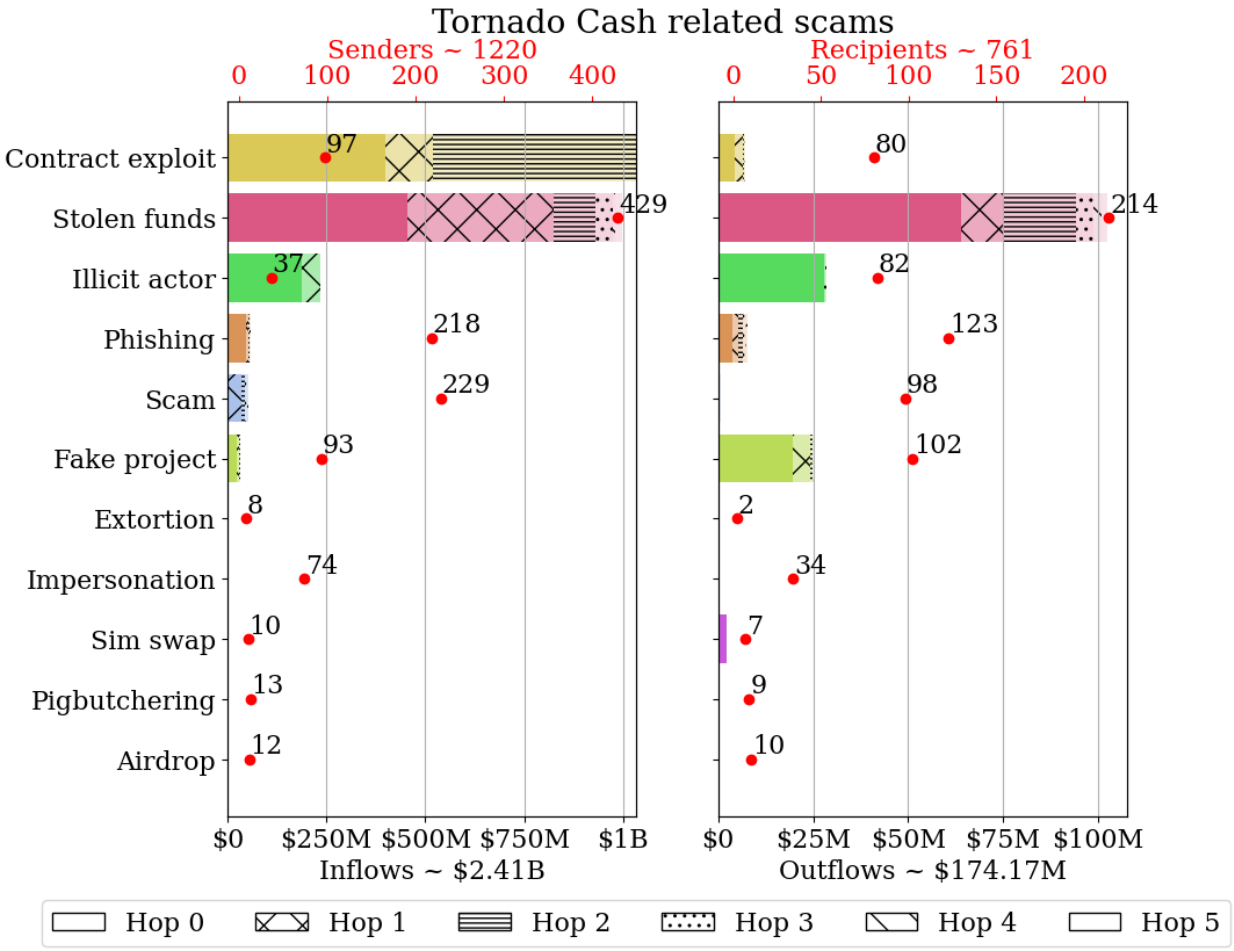


Table IA.I: Scam definitions

Type	Description
Extortion	Using intimidation to force someone to pay money under the threat of releasing sensitive information
Ransomware	Malware that encrypts the victim's files, or pretending to lock files, and demanding a ransom payment to decrypt them
Phishing	Tricking individuals to providing personal information, such as login information, often by driving traffic to a malicious website to gain access to wallets and secret keys
Impersonation	Imitating a famous person, brand, or organization for fraudulent purposes, often to ask for money or drive traffic to a fraudulent website to steal sensitive data, including "Nigerian Prince-type" scams where a rich foreigner promises to share the profits from a fake investment opportunity
Pig butchering	Confidence scam that lures victims into fabricated cryptocurrency investment schemes often by gaining a victim's affection, spoofing exchanges, and manipulating victims with fake returns or taxes
Donation scam	Posing as charities to exploit donors
Airdrop	Unsolicited mass distribution of a cryptocurrency token to direct investors to a malicious website
Fake returns	Promising fake returns to convince victims to invest through: promising fake payments - payout scam or load up scam faking returns by paying profits to earlier investors with funds from more recent investors - Ponzi scheme fraudulently and artificially inflating the price of a cryptocurrency, such as during a pump and dump scam - using misleading information or other techniques
Fake returns	Pretending to build a fake project only to abandon the project after attracting investors, such as rug pulls or exit scams
Sim swap	Convincing a mobile carrier to port a victim's phone number to their SIM card to gain access to sensitive accounts
Contract exploit	Exploiting vulnerabilities in a smart contract or other protocols to drain funds