Is Criminal Crypto a Sideshow? An Examination of Illicit Activity across Three Major Blockchains[*]

John M. Griffin[†] Zirui Wang[‡] Juan Antonio Artero Calvo[§]

March 16, 2026

Preliminary and incomplete. Some estimates may be updated. Please do not post, cite, quote, or redistribute without the authors' permission.

Abstract

Utilizing over 700 thousand addresses linked to various forms of criminal activity as a starting point, we partially map the criminal ecosystem of funds flowing into crypto exchanges on Bitcoin, Ethereum, and Tron from 2021 to 2025. After tracing tainted funds to crypto exchanges and clustering related deposit addresses, we find that a majority of crypto exchanges have between five to twenty percent, or more, of their inflows related to tagged criminal activity. The recently sanctioned HuionePay exhibits substantial similarities to other large offshore non-sanctioned crypto exchanges. Machine learning methods identify substantial additional criminal crypto activity. Taken together, these methods imply total estimates of criminal activity from 2021-2025 on these three blockchains alone of $1.02 trillion, with over $210 billion per year in 2024 and 2025. Overall, these findings challenge a common industry narrative that criminal crypto activity is de minimis and suggest many avenues for tighter regulation and monitoring.

JEL classification: G18, G23, G28, K24, K42
keywords: Bitcoin, Ethereum, Tron, Crypto Flows, Stablecoins

[*]We thank colleagues at the University of Texas at Austin for their helpful comments. We especially thank Kevin Mei and Alex Pettyjohn for guidance and helpful comments. 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. Artero Calvo is an Associate Researcher and Predoctoral Fellow at Integra FEC.

[†]McCombs School of Business, University of Texas at Austin.
[‡]McCombs School of Business, University of Texas at Austin.
[§]Integra FEC.

The crypto ecosystem has grown remarkably and changed considerably over the last seventeen years, particularly since 2020. As of March 2026, it features over eight thousand tracked coins and tokens, over 30 crypto ETFs worth over $100 billion in assets, hundreds of crypto venture and investment companies in the space, and a total crypto market cap close to $2.5 trillion.[1] Yet, there is evidence that crypto markets remain an active space for confidence scams, thefts, sanctioned and terrorist financing, phishing, and many other crimes. The crypto industry often argues that these activities also happen in the traditional finance markets, perhaps at even higher rates, but given the traceable nature of the activity, the crypto space receives greater scrutiny due to the traceable nature of the blockchain transactions. Industry reports estimate that crypto crime accounts for between 0.083% and well below one percent of all crypto transactions, but these estimates are substantially below academic Bitcoin estimates for earlier periods.[2] How prevalent is criminal crypto activity? How can it best be measured? Where does the activity take place and who are the major facilitators?

The biggest challenge to answering these questions is that most illicit activity is not reported, and criminal actors quickly take steps to hide their activity. To partially address these challenges, we take four distinctive approaches. First, we use an extremely large compilation of 734,443 identified criminal addresses from leading sources as a starting point to measure this activity. Second, we trace criminal activity across three major blockchains: Bitcoin, Ethereum, and Tron. Third, since criminals use many transactions to obfuscate funds and only a fraction of criminal addresses is reported, we trace tagged criminal funds to collection points or deposit addresses, and then measure all funds coming into these and closely related collection points. Fourth, we utilize machine learning methods to identify additional potentially tainted deposit addresses. In the process, our approach also uncovers distinct economic mechanisms at play across three blockchains.

We collect 734 thousand addresses reported for potential criminal activity from various public and private sources and examine the blockchain activity of these addresses from January 2020 to September

[1] As of March 11th 2026, the popular website CoinMarketCap tracks 8,651 individual cryptocurrency coins and tokens alongside 33 crypto-related ETFs worth over $100 billion. In addition, there are many hundreds of firms currently developing crypto-related projects. Coinbase Ventures has one of the largest portfolios of such firms, to this date they have invested in over 600 individual projects.

[2] We detail these numbers from industry reports and academic papers in the literature section.

2025. The largest categories are romance confidence scams (so-called "pig butchering" scams), thefts, sanctioned entities, phishing, illicit actors, rug pulls, impersonation, fake returns, fake projects, ransomware, extorsion, sim swap, airdrop, donation, and other scams. We find that Tether on Ethereum and ETH are more commonly utilized in romance scams, thefts, phishing, illicit actors, rug pulls, and fake projects, whereas Tether on Tron is more frequently utilized in miscellaneous scams and for sanctioned purposes such as terrorist financing. The frequency of Tron's use has grown over our sample period, and particularly so for illicit services laundering funds and attempting to bypass international sanctions.

We separately trace the flows across the three blockchains, stopping at identified services such as centralized exchanges (CEXes), decentralized exchanges (DEXes), other decentralized finance (DeFi) services, cryptocurrency mixers, and other less prominent services. We also stop at large unidentified entities which are likely services. Large, predominantly offshore CEXes, especially Binance and OKX, appear as major stopping points on all three blockchains. On Ethereum, DEXes such as Uniswap and Tokenlon appear as major hubs.

HuionePay is a Cambodian Fintech platform designated by FinCEN in May 2025 as a primary money laundering concern.[3] The firm's Cambodian banking license was revoked. We examine the traced activity to this firm as a benchmark for our subsequent analysis. We find that HuionePay interacts with itself as well as a host of other centralized crypto exchanges, including Binance, OKX, Maskex, ChainUp Custody, and HTX. Many flows from HuionePay move directly to these centralized exchanges within one or two blockchain hops, suggesting limited screening of those flows. This highlights how these smaller exchanges can facilitate a money laundering ecosystem.

We then take exchange deposit addresses that received at least $50,000 in tainted flows and examine all of their inflows. The rationale for imposing a filter of $50,000 is that Griffin and Mei (2025) show that these scammers commonly send small inducement payments, typically $1,000 or less to potential victims.[4] Additionally, once tracing to the deposit address, for Ethereum and Tron we use

[3]The following press release from May 1st 2025 explains that "Given the money laundering risk posed by Huione Group, FinCEN is proposing to prohibit U.S. financial institutions from opening or maintaining correspondent or payable-through accounts for or on behalf of Huione Group."

[4]A smaller threshold of $10,000 would probably be sufficiently conservative (and which we perform in robustness),

deposit address clustering to capture related inflows into the deposit address following Victor (2020) and Griffin and Mei (2025). Because of Bitcoin's UTXO structure and other differences in deposit-address architecture, we cannot apply the same procedure on Bitcoin. We then categorize all flows into centralized exchanges. Approximately 16.4% percent of HuionePay's deposit address dollar inflows on Tron are related to tagged illicit flows. Surprisingly, many large centralized exchanges are not far behind and approximate a similar percent for the total value of illicit inflow deposits. Binance receives 4.1% on Ethereum and 14.8% of flows on Tron. In total, tagged Binance deposit addresses have received $70.0 billion on Ethereum and $231.0 billion on Tron. HTX has similar fractions of illicit activity on Ethereum and Tron. Additionally, the crypto exchanges Kyrrex, BTSE, Bitkub, Poloniex, and Indodax all have higher percentages of tagged flows than HuionePay. Most exchanges having more than one percent activity on Ethereum or Tron are primarily located outside of the U.S. and Europe, which we label as non-Western. The largest Western crypto exchange, Coinbase, has tainted Ethereum deposits of less than 0.29%. Among Western exchanges with high amounts of tainted flows, we find Kraken and the non-defunct FTX with 2.4% and 5.1% respectively. Note that our totals for addresses tainted for illicit activity, are over 20 times the previous discussed self-reported estimates in the industry, even before applying any machine learning.

We also show the time series of the tainted flows. Since 2021, Tron has been gaining in popularity. By 2025, approximately 70% of clustered tainted exchange inflows are on Tron. Even though our captured totals reveal substantial illicit activity, it seems probable that these numbers could be undercounted, given that our starting point was only reported criminal flows and that low percentages of frauds are ever reported.[5] We use machine learning to assess this possibility as well as to characterize the features of criminal deposit-address activity.

From the Ethereum machine learning results, we learn that tainted deposit addresses exhibit a distinct transactional profile. They are more likely to act as short-lived collection points, receiving inflows from many hop-1 senders, receiving a smaller share of stablecoin inflows directly from centralized exchanges, and forwarding a larger fraction of inflows onward. Their hop-1 senders also tend

but we start with the requirement that the address receive at least $50,000 in tainted deposit inflows.

[5]Anderson (2021) finds that only three percent of consumer fraud victims report to a government agency.

to be newer wallets and more reliant on Tether rather than USDC. Tainted deposit addresses further display greater exposure to Tokenlon- and Tornado-traced flows, more round-number transfers, and fewer types of tokens transacted. On Tron, we find broadly similar patterns, with hop-1 sender characteristics dominating. In particular, tainted deposit addresses are associated with senders that have more 10,000-divisible transfers, and shorter address lifecycles also remain predictive.

We then build our criminal estimates from January 2021 to September 2025. On Ethereum, we follow $42.5 billion in direct flows, which increases by $150 billion with the incorporation of tracing to the deposit addresses and deposit address clustering. Additionally, the machine learning estimates an additional $218 billion in suspected criminal activity. For Tron we only start with $8.7 billion in tagged criminal activity, but an additional $400 billion of flows is tagged moving to deposit addresses receiving at least $50,000 of criminal activity and clustering those addresses with other likely candidates. Machine learning estimates an additional $163 billion in flows. Because of the differences in blockchain infrastructure, for Bitcoin we only cluster direct flows of $23.9 billion over the period. Overall, we calculate totals of criminal activity from all three blockchains and from different methods as $24 billion for Bitcoin, $371 billion from Ethereum, and $629 billion from Tron, for a total of $1.02 trillion, or an average of $210 billion per year in 2024 and 2025.

Despite the expansive nature of our analysis, our paper has limitations in measuring criminal activity. First, our methods may falsely tag addresses to the extent that people or services deal with criminals, but are not criminal. Second, our analysis undercounts activity to the extent that we do not measure activity: a) on privacy coins (such as Monero and Zcash), b) tokens other than the main ones we track on Ethereum and Tron, c) other blockchains (such as Solana), and d) criminal activity and addresses that are never reported or flagged.

Taken together, the results underscore the limitations of relying solely on inflows to reported fraudulent addresses when assessing the scale of illicit cryptocurrency activity. By combining transaction tracing, deposit address clustering, and machine learning, our approach progressively uncovers additional layers of deposit addresses used to collect and consolidate criminal proceeds. The resulting estimates indicate that the magnitude of criminal flows in cryptocurrency markets is substantially

larger than what surface-level metrics would suggest.

Overall, our findings have several important practical implications which should be of interest to industry participants and policy makers. First, many crypto exchanges have addresses that handle criminal activity that consist of between five and twenty percent of their total inflows. This is even before assessing additional activity from machine learning. This activity seems to represent a significant fraction of their business. Second, since many exchanges have similar or higher tainted flows (both as a percentage and in dollars) as the sanctioned HuionePay, more regulatory impact might be achieved by targeting exchanges exhibiting the highest quantitative tainted exposure. Third, machine learning estimates could be used by industry actors wishing to identify substantial activity that is likely to be criminal in nature. Given that most criminal activity is reported with a lag, the use of machine learning or other related AI-type algorithms could be accurate and useful at identifying and stopping criminal flows. Since our model yields considerable accuracy with off-the-shelf features, it seems probable that greater accuracy could be obtained utilizing more features and internal exchange information. Fourth, the predominant off-ramp for criminal crypto proceeds runs through regulated or semi-regulated platforms that operate know-your-customer and anti-money-laundering programs. The fact that some large CEXes, such as Coinbase, are destinations for relatively little criminal proceeds in comparison to their offshore counterparts, suggests that the surveillance policies at centralized exchanges vary considerably and that tougher policies potentially could significantly disrupt the criminal crypto flow ecosystem.

Related Literature This paper contributes to the growing literature examining cryptocurrency crimes. First, there are a few papers that try to quantify the extent of illicit activity on the Bitcoin blockchain in earlier periods. Foley, Karlsen, and Putniņš (2019) provides an examination of the total magnitude of potential illicit activity transacting in dark markets from January 2009 to April 2017. They find that 46% of non-exchange-related Bitcoin activity is associated with darknet websites known for illegal activities, though at the end of their sample in April 2017, this number decreased below 25%. Overall, they estimate that 27 million bitcoin market players conduct $76 billion in annual illegal activity, which is approximately three-fourths of the size of the U.S. illicit drug trade. In contrast,

Makarov and Schoar (2025) provide a general analysis of the players in the Bitcoin market and find that illegal activity, scams, and gambling account for less than 3% of Bitcoin volume from 2019 to 2025. Differences in their approach compared to Foley, Karlsen, and Putniņš (2019) are that their more comprehensive wallet attribution avoids possible overstatement of volume through recursive algorithmic identification, and they utilize a larger denominator by including exchange volume (which is over 75% of total volume).

Second, industry reports also discuss various trends and the size of total activity. Chainalysis (2025, 2026) produces interesting annual summary reports that track possible amounts of various types of criminal activity, show trends in various types of crime and produce interesting analysis of various types of activity including, stolen funds, scams, sanctions, dark markets, ransomware, cyber security, fraud shows, child abuse materials, terrorism finance, and malware. The 2025 Chainalysis crypto crime report places the total fraction of crypto transactions at only 0.14% of all transactions, whereas the 2026 report does not indicate an exact number, but says the number is well below 1%. The Chainalysis 2026 report places total activity at $59 billion in 2024, but that jumps to $154 billion in 2025, mostly due to a large increase in the categorization of sanctioned entities.[6] Binance claims that using data from top vendors in the field, only 0.018-0.023% of crypto activity is criminal in nature and that crime is less common in crypto than cash.[7] The 2025 TRM crime report (TRM Labs, 2025) estimated illicit activity at 0.42% of all transactions in 2024, and the 2026 report revised this estimate at 1.3% in 2024 and 1.2% in 2025 (TRM Labs, 2026). While these crime reports provide substantial information and are useful for understanding various trends in types of fraud, they do not detail methodologies or provide robustness on how they handle related transactions. Second, the reports may minimize activity to the extent that they are only analyzing tagged funds. The large jump in criminal activity in the 2025 to 2026 crime reports seem to be closely linked to the treasury classification of HuionePay and other individual actors (e.g. Lazarus Group, Iranian Revolutionary Guard Corps, etc.) as sanctioned entities, also indicating

[6]The bulk of total activity due to sanctioned entities is due to the ruble stablecoin known as A7A5. This Kyrgyzstan-based stablecoin was created early 2025, and to this day it has been used for transfers totaling $112.3 billion on the Tron blockchain.

[7]Even though Binance use Chainalysis attribution data, Chainalysis clarifies that there are potential limitations in those calculations, because Binance only accounts for direct deposits from illicit addresses and thereby fail to account for traced flows to deposit addresses.

that previous reports are missing much of this activity. The reports typically do not detail what percent of illicit flows is through exchanges or provide granular details on which centralized exchanges are receiving the most illicit flows.[8] Our approach focuses on illicit flows through centralized exchanges, as they are the common entry and exit points to the fiat banking system.

Third, there are interesting papers detailing illicit activity in various spaces. Cong, Grauer, Rabetti, and Updegrave (2023a) provide an overview of the concrete cryptocurrency scams with an emphasis on Ponzi schemes, rug pulls, darknet markets, ransomware attacks, hacks and stolen funds, and money laundering. Meiklejohn, Pomarole, Jordan, Levchenko, McCoy, Voelker, and Savage (2013a), details how clustering algorithms of Bitcoin activity can be used to identify transactions moving through the Silk Road, a darknet marketplace for illicit products and services operated between 2011 and 2013. Christin (2013), Janetos and Tilly (2017), and Goonetilleke, Knorre, and Kuriksha (2023) explore intertwined aspects such as vendor drug price and customer feedback in the Silk Road, Agora, and Hydra marketplaces respectively. These publications studied now defunct marketplaces using BTC for the purpose of payment settlement, but the use of BTC as a means of darkmarket payment appears much less common today.[9] Cong, Harvey, Rabetti, and Wu (2025) utilize criminal reports containing 21,650 wallet addresses and estimate $332 million of total inflows to Bitcoin cybercrime, while detail the economics and fee splitting activity of crypto-enabled ransomware gangs. Sokolov (2021) finds that Bitcoin transaction activity and fees increase around times of ransomware activity in 2014-2015. As briefly surveyed by Griffin and Kruger (2024), other types of nefarious trading activity in crypto, 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 Putnins (2022)), price manipulation (Gandal, Hamrick, Moore, and Ober-

[8] Chainalysis and TRM Labs sells tools to various law enforcement agencies, but also provides monitoring services to many industry participants. Most major exchanges and currencies purport to utilize one or both of these monitoring services, though it is up to those exchanges to decide what to do with the monitoring they receive.

[9] Citing the successful law enforcement shutdowns of Hydra and AlphaBay, Cong et al. (2023a) note that darknet marketplace activity has been on the decline. They note that that these have been decreasing in number and operating for shorter amounts of time throughout the years. Anecdotally Archetyp, one of the longest operating darknet marketplace (2020-2025) and once one of the most popular websites on Tor alsoused Monero for further anonymity. Data on these marketplaces is hard to parse because Monero is a privacy coin, as such, transaction level data is ambiguous and largely untraceable. Archetyp was shut down by German authorities.

man (2018); Griffin and Shams (2020)), and wash trading (Pennec, Fiedler, and Ante (2021); Cong, Li, Tang, and Yang (2023b)). Activity related to pump-and-dumps, insider trading, market manipulation, and wash trading are most likely not included in our analysis due to detection difficulty. Griffin and Mei (2025) show that most romance scams operate on Ethereum, send small inducement payments to Western crypto exchanges, and move from Western-based exchanges to non-Western-based exchanges. Utilizing the deposit address clustering algorithm of Victor (2020), they estimate $27.8 billion per year moving through tainted deposit addressesof clustered illicit flows in the Ethereum blockchain.[10,11]

Fourth, recent machine-learning research on illicit crypto activity primarily focuses on improving model detection performance using relatively small labeled samples of transactions or addresses.[12] A smaller literature leverages machine learning techniques to expand the observable set of tainted addresses. Li, Baldimtsi, Brandao, Kugler, Hulays, Showers, Ali, and Chang (2021) quantify illicit activity in Ethereum/DeFi by applying a smart local moving modularity clustering algorithm to expand the set of malicious Ethereum addresses from 2,628 to 23,638 addresses, although this large increase in addresses yields only a modest increase in aggregate ETH outflows. Wang, Pang, Chen, Zhao, Huang, Chen, and Han (2021) combine Bitcoin address clustering with multi-label classification to estimate the scale of Bitcoin ransomware, tracing more than $176 million in ransom payments from 41,424 victims.[13] Our paper contributes to this latter literature by starting with a scale of addresses over 18 times that of the literature and by focusing on labeling tainted deposit addresses collection points rather than the initial criminal address starting points. We use a tree-based LightGBM model within a positive-unlabeled learning framework to infer tainted exchange deposit addresses and aggregate

[10] Griffin, Mei, and Wang (2025) utilize similar tracing methods to evaluate the effectiveness of various types of sanctions. They find that sanctions directed towards money laundering facilitators (bans on mixers and fines on exchanges) are more effective than policies targeting individual addresses engaging in money laundering.

[11] A recent report from December 2025 by the International Consortium of Investigative Journalists (ICIJ) highlights the growing prevalence of pig butchering scams on the Tron blockchain. The report concentrates on cases where scammers have used HuionePay to launder large USDT amounts. Chapter Eighteen of Faux (2023) provides a detailed description of pig butchering scams.

[12] These papers compare alternative classifiers and focus on detection performance metrics, rather than quantifying the aggregate scale of illicit crypto activity citeweber2019anti; Chen, Peng, Liu, Li, Xie, and Zheng (2020); Li, Gou, Liu, Hou, Li, and Xiong (2022); Nicholls, Kuppa, and Le-Khac (2023); Ding, Shi, Li, and Cao (2024).

[13] Yin and Vatrapu (2017) use supervised machine learning techniques on a dataset of 854 bitcoin observations and find that the total number of addresses and bitcoins held by these entities are 5.79% and 10.02% according to Bagging, and 3.16% and 1.45% according to Gradient Boosting.

those predictions into blockchain-level estimates of illicit flows across Ethereum and Tron.

We contribute to this literature in four main ways. First, we utilize a set of over 700,000 tagged criminal addresses spanning over fifteen different types of criminal activities, giving a large starting point for measuring criminal addresses. Second, we provide an examination and comparison across three main blockchains: Bitcoin, Ethereum, and Tron. Third, we focus on funds flowing through crypto exchanges, as they are entry and exit points for the crypto ecosystem. Finally, we utilize machine learning methods to detect possible illicit deposit addresses in combination with these methods.

1. Background, Data, and Methodology

This paper arranges a group of data sets into a unified framework for following illicit funds. We do this by collecting data on transaction flows in Bitcoin, Ethereum, and Tron. Transaction-level data is then enriched with attribution labels to assign addresses and flows to specific actors. Tracing methodologies further organize these transactions so that we can consistently follow specific funds that originate from an illicit address and track their flows to subsequent destinations. In this section we present the essential blockchain background information necessary for understanding our dataset and methodology.

1.1 Blockchain Background

A blockchain is a form of distributed ledger technology that records data in sequentially linked blocks. Blockchain technology, coupled with the elliptic-curve cryptography, were first deployed towards clearing the first block of Bitcoin in January 2009. These techniques were then modified and employed in creating other decentralized blockchains such as Ethereum (launched in July 2015) and Tron (launched in May 2018). Each blockchain has its own consensus mechanism for deciding which transactions are included in a block and in what order. While the Bitcoin blockchain can only clear Bitcoin transactions, the Ethereum and Tron blockchains can move both the native token as well as other tokenized assets issued on the same blockchain. Once validated, these transactions are recorded into blocks which, as the blocks clear, provide a digital transaction ledger linking each transaction to the previous transaction. The differences in blockchain architecture ultimately influence how exchanges

appear on the blockchain. Centralized exchanges retain custody of users' assets while facilitating trading across multiple crypto assets and the conversion of crypto into fiat currency. Transactions executed internally within a centralized exchange are generally not recorded on the blockchain; only transfers into and out of the exchange appear on-chain.

Bitcoin The Bitcoin blockchain uses a proof-of-work consensus mechanism to verify transactions. This mechanism generally proves to be slower at building blocks and also results in higher transaction fees for miners from users. Transactions on Bitcoin consist of inputs and outputs from and to individual wallets, of which the inputs have to be signed using the cryptographic keys of each individual input wallet in order for the transaction to execute. These inputs are referred to as an "unspent transaction outputs" or UTXOs for short. When multiple addresses are used as inputs to a single transaction, the users of the inputs must have the private signing keys of all other inputs and are likely same individual (or entity). After finding connected components of this "same-input" relation throughout the entire Bitcoin blockchain, groups of wallets controlled by the same individual or entity can be assembled. To increase anonymity, some Bitcoin users engage in so-called "coinjoins" which deliberately serve to group many different wallet addresses controlled by different individuals.[14] As part of our tracing criteria, we do not trace through coinjoins.

On Bitcoin, large clusters of wallets can be linked to centralized exchanges, and often cluster as one "hot-wallet" executing most outbound transactions and containing a large balance of BTC. The wallets at the periphery of the cluster receiving BTC can act as deposit addresses to individual users that then flow directly to the exchange hot-wallet. However, deposits, but there is no certainty as to whether they correspond one-to-one with an individual exchange users.

Ethereum The Ethereum blockchain differs significantly from the Bitcoin blockchain. It employs a proof-of-stake consensus mechanism which is more energy efficient than proof-of-work, and also

[14] So-called cryptocurrency "mixers" or "tumblers" serve to obfuscate the provenance of crypto and thereby providing users additional anonymity and privacy. Mixers differ amongst themselves depending on the blockchain they operate in, with the largest of them being Tornado Cash on Ethereum. On Bitcoin coinjoins are mixers which combine many UTXOs from multiple users into a single transaction. The output of this transaction is the same value as the sum of all of inputs (minus fees), but the recipient addresses are different from those providing the UTXOs. A coinjoin appears on the blockchain as a large transaction with many inputs and many outputs. In this manner, the participants of a coinjoin are clustered together when using the common-input clustering heuristic. This transaction is an example of one such coinjoin.

results in faster block building and is substantially cheaper transaction fees for users. Furthermore, Ethereum is a programmable blockchain, which means that wallet addresses can run and execute code; these addresses are known as smart contracts. The smart contract function appeals greatly to developers for its flexibility and utility towards building decentralized finance (DeFi) services.

On Ethereum, both centralized and decentralized exchanges are prominent. Unlike a centralized exchange (CEX), a decentralized exchange (DEX) leverages the functionalities of smart contracts to execute trades on-chain without a third party retaining custody of the traded assets. Centralized exchanges on Ethereum have a clearer identifiable structure than in Bitcoin. Centralized exchanges in this blockchain typically appear as hot-wallet addresses with many deposit addresses attached to it, and the deposits correspond one-to-one with individual exchange users. The deposit addresses only send to the exchange hot-wallets.

Tron Tron is similar to Ethereum; it has a Delegated Proof-of-Stake mechanism and it is also a programmable blockchain with code and functionality similar to Ethereum. While Ethereum has a fairly developed DeFi ecosystem, DeFi exchanges are not frequently utilized on Tron. CEXes are the main service providers on Tron and the nature of the deposit addresses moving money to exchange hotwallets functions similar to their form on Ethereum.[15] This advantage may explain the generally higher transaction count per wallet addresses in the Tron blockchain.

1.2 Data

To delineate illicit networks and trace their financial flows, we primarily rely on two data sources: blockchain transaction data and attribution data. These datasets facilitate the identification of entities operating across the three blockchains and are essential for tracking the movement of tainted funds associated with the reported addresses.

[15] As of the time of March 13th of 2026, the website Token Terminal provides specific blockchain metrics and records a block time of 11.1 minutes alongside an average transaction fee of $0.4198 for Bitcoin, 12.1 seconds and $0.2259 for Ethereum, and 3.0 seconds with $0.623 for Tron. Historically, Tron fees have been cheaper than Ethereum but Ethereum fees have been dropping substantially. Transaction fees are subject to speculation and other specific details such as cryptocurrency type, and blockchain congestion.

Transaction data Blockchain transaction data is sourced from the Bitcoin, Ethereum, and Tron blockchains. The transaction record for each transfer includes the blockchain address of the sender and receiver, the amount transferred, and a timestamp, allowing us to construct complete paths of fund flows between addresses. We study BTC on Bitcoin; ETH, USDT, USDC, and DAI on Ethereum; and USDT on Tron—the dominant assets in the respective blockchain's criminal ecosystem. We store and access all blockchain data on Google Cloud's BigQuery, which includes transfers of native coins, ERC-20 tokens, and internal transaction events for complex Ethereum transactions. We use end-of-day cryptocurrency price data from CoinMarketCap to convert all values to US dollars; stablecoins are treated as equal to $1.

Attribution data To link pseudonymous blockchain addresses to real-world entities, we collect two types of attribution data: entity labels and criminal addresses. The first type consists of entity labels that identify the service provider operating each address. We focus on centralized exchanges (CEXes), decentralized exchanges (DEXes), bridges, mixers, darknet marketplaces, and individual actors known to facilitate illicit activity. These labels are essential for classifying the endpoints of traced fund flows.

The second type consists of victim-reported criminal addresses. This dataset extends and expands the victim report sample of Griffin and Mei (2025), which focused exclusively on pig butchering scams, to encompass a broader range of criminal activity. Because victim reports are submitted in free-text narrative form and may use inconsistent terminology, we classify each report into one of 12 scam categories based on the textual content of the victim's report using a fine-tuned GPT-4o-mini model.[16] The categories range from phishing, extortion, and impersonation to pig butchering, contract exploits, and ransomware; full definitions are provided in Table IA.1. After excluding inactive addresses, removing within-category duplicates, and filtering out addresses consistent with exchange service wallets, our final sample comprises approximately 734,443 reported criminal addresses. Table 1 presents summary statistics on the report and address sample by scam category and blockchain.

For entity labels, we draw on public online sources, including blockchain.com and etherscan.io, as well as proprietary attribution data. For criminal addresses, we collect victim reports from online

[16] Specifically, we use time-stamped model gpt-4o-mini-2024-07-18, fine-tuned on a labeled training set. The classification prompt is disclosed in the Internet Appendix.

reporting platforms.

1.3 Methodology

Our identification strategy progressively expands the set of tainted deposit addresses. We begin from victim-reported addresses and use tracing algorithms to follow tainted funds forward to deposit addresses. We then use clustering methods to identify additional deposit addresses likely controlled by the same actors. Finally, we use machine learning to infer tainted inflows for remaining unflagged deposit addresses. We apply this process on Bitcoin, Ethereum, and Tron and ensure that components are non-overlapping.

1.4 Crypto Tracing

Crypto tracing uses transaction-level blockchain data to follow specific funds from one address to the next as they move through intermediate wallets and eventually reach service endpoints. Tracing organizes these transactions into a directed flow map that follows funds across paths that branch or merge. When traced funds become commingled with other inflows in a downstream address, the tracing algorithm attributes subsequent outflows on a first-in-first-out (FIFO) basis, following established practice in the blockchain forensics literature. The purpose of tracing is to follow flows that are highly likely to be controlled by reported criminal addresses while avoiding the attribution of unrelated downstream activity.

Bitcoin We start from Bitcoin addresses reported by victims and first screen out addresses whose common-input clusters belong to identified services. We also remove reported addresses whose common-input clusters contain at least 500 wallets or are associated with at least 2,000 transactions, since such clusters are likely to correspond to services or other large entities rather than individual criminal wallets. For the remaining origins, we include all wallets in the qualifying common-input cluster so that tracing is conducted at the entity level. The tracing algorithm then gathers the UTXOs flowing into these origin clusters and follows tainted outflows forward using FIFO. Traces terminate when tainted UTXOs reach an identified service cluster or a suspected service cluster, again defined as a cluster with at least 500 wallets or at least 2,000 transactions. We follow tainted BTC UTXOs for up to eight hops.

Ethereum and Tron We start from victim-reported addresses and exclude addresses associated with more than 2,000 unique transactions, addresses that are smart contracts, and addresses that transact in more than five distinct cryptocurrencies. These screens are designed to remove misreported addresses and unidentified service-like entities. We then apply tracing algorithms following Anderson, Shumailov, and Ahmed (2018), Möser and Narayanan (2019), Tironsakkul, Maarek, Eross, and Just (2022), Griffin and Mei (2025). Similar to Bitcoin, when traced funds merge with other inflows in downstream addresses, outflows are assigned on a FIFO basis. To remain conservative, traces stop when they reach tagged service endpoints such as exchanges, bridges, mixers, and major DeFi routers, when they exceed five hops, when they reach high-activity addresses with more than 2,000 transactions, or when residual transfers fall to dust-level amounts.

1.5 Clustering

Following the identification of tainted fund flows to CEXes, we aggregate the relevant deposit transactions to conduct a clustering analysis. The primary objective is to uncover additional illicit flows to CEXes that evade standard tracing tools and are absent from our initial dataset of victim-reported addresses. Because transaction structure differs sharply between Bitcoin and the account-based chains, we use different clustering heuristics on Bitcoin and on Ethereum and Tron. Throughout, the clustering procedures are intentionally conservative. In particular, we require the seed depositor or deposit address to have received at least $50,000 in traced tainted inflows.[17]

Common-Input Clustering Heuristic on Bitcoin On Bitcoin, we begin with the set of traced depositor wallets that send funds into identified centralized exchange clusters. We then apply the common-input clustering heuristic to recover other wallets likely controlled by the same depositor, following Meiklejohn, Pomarole, Jordan, Levchenko, McCoy, Voelker, and Savage (2013b). The intuition is straightforward: if multiple Bitcoin addresses appear together as inputs to the same transaction, the spender must control the private keys for all of them, so those addresses are likely controlled by the

[17] This cutoff is motivated by Griffin and Mei (2025), who show that criminal networks frequently send small inducement payments, typically $1,000 or less, to exchanges; a much higher threshold reduces the risk that such small payments drive the clustering results. A smaller threshold such as $10,000 is likely still conservative, and we examine lower thresholds in robustness work.

same entity. We use this heuristic to move from an observed traced depositor wallet to the broader depositor cluster behind it. We then retain clusters with at least $50,000 in traced tainted inflows and exclude obvious outliers that appear to reflect "whales" rather than ordinary depositor entities.[18] Finally, we sum the outflows from these depositor clusters into centralized exchanges.

Deposit Address Clustering on Ethereum and Tron On Ethereum and Tron, we first use centralized exchange hot wallets to identify the customer-specific deposit addresses that feed into them. This structure allows us to apply deposit address clustering directly. We retain seed deposit addresses that receive at least $50,000 in traced tainted inflows and then collect the senders funding those deposits. We next apply the common-sender heuristic in Victor (2020): if the same sender funds multiple deposit addresses, those deposit addresses are likely linked to the same exchange customer. In implementation, we restrict attention to direct shared-sender links and exclude shared senders that appear to be services. Because this procedure is intentionally conservative and begins from seed deposit addresses with large traced tainted inflows, we measure total observed inflows to the clustered deposit addresses rather than only the traced component. On Tron, we additionally apply the same procedure around deposit addresses reached by tracing forward from identified HuionePay wallets, given HuionePay's central role in our traced Tron network.

1.6 Machine Learning on Unflagged Deposit Addresses

After tracing and clustering, some tainted deposit addresses could still be unflagged because they share no direct transactional link with the networks observed in victim reports. To capture this residual component, we use positive–unlabeled learning following Elkan and Noto (2008). Addresses identified from tracing and clustering are treated as positives; the remaining deposit-address universe is treated as unlabeled. We implement this classifier with a LightGBM base model, which is well suited to structured blockchain data.[19] The classifier estimates the probability that an unflagged deposit ad-

[18] This additional screen is designed to prevent a small number of extremely large, atypical entities from mechanically driving the Bitcoin clustering totals.

[19] The classifier is trained using 300 boosting rounds, a learning rate of 0.05, 64 leaves per tree, and 80% row and column subsampling. We hold out 10% of labeled positives for calibration and train on a 4:1 unlabeled-to-positive sample. A second LightGBM model estimates taint severity using 2,000 boosting rounds with early stopping and a learning rate of 0.02.

dress is tainted, and a second LightGBM model estimates taint severity, defined as the tainted share of inflows for addresses predicted to be tainted. For each unflagged deposit address, model-implied tainted inflow is computed as the product of (i) predicted tainted probability, (ii) predicted taint severity, and (iii) observed inflow.

We construct 270 features for each Ethereum deposit address and 219 features for each Tron deposit address from on-chain transaction data and local network structure. In the computer science literature, tree-based models remain competitive baselines for structured blockchain data and, in some settings, outperform graph-based approaches, especially when prediction are made at the address level and rely on rich behavioral features (Weber, Domeniconi, Chen, Weidele, Bellei, Robinson, and Leiserson (2019); Juvinski, Li, and Brini (2026)). Although our objective is not to benchmark alternative algorithms, the model achieves strong out-of-sample performance, with a ROC-AUC of 0.9498 and an F1 score of 0.8303, which is broadly in line with the computer science address-detection literature. In the current draft, this machine-learning step is implemented on Ethereum and Tron.

Our estimate adds four non-overlapping components: direct inflows to reported addresses, additional flows to deposit addresses with more than $50,000 traced flows, inflows to deposit addresses identified through clustering, and additional tainted inflows to unflagged deposit addresses inferred by machine learning.

2. Inflows to Reported Criminal Addresses

We begin by characterizing the breadth and direct scale of criminal activity in our sample. Our starting point is the set of 734,443 victim-reported addresses. This data allows us to measure what has actually been received by reported criminal addresses before any tracing, and to understand how criminal activity is distributed across different fraud categories and across the three blockchains.

2.1 Criminal Activity Across Scam Categories

Figure 1 plots the reported criminal addresses in our sample along two dimensions: the number of reported addresses in each scam category on the x-axis and the total inflow received by those addresses on the y-axis, both on logarithmic scales. The size of each bubble is proportional to the number of

transactions, and the pie chart within each bubble shows the cryptocurrency composition of inflows for Bitcoin, ETH, Tether , and USDC on Ethereum, and Tether on Tron.

Figure 1 reveals substantial heterogeneity across crime types, both in scale and structure. In terms of inflows the largest five categories are Pig Butchering ($22 billion), Stolen Funds ($13.7 billion), Sanctioned ($9.5 billion), Phishing ($7.4 billion), and Illicit Actor ($6.1 billion).[20] Panel A presents Ethereum, and Panel B presents Tron. The predominance of *Pig butchering* scams (i.e., scams in which victims are cultivated through fake romantic or investment relationships before being defrauded of large sums) is consistent with prior evidence of the outsized financial impact of these scams (Griffin and Mei, 2025). *Stolen Funds*, which encompasses attacks on smart contract vulnerabilities, rank second but involve far fewer addresses (approximately 4.2K) compared to Pig Butchering (approximately 75.2K), implying very high average receipts per address and reflecting the concentration of losses in a small number of large-scale protocol attacks.

The cryptocurrency composition of inflows, shown by the pie charts within each bubble, also varies meaningfully across categories. Bitcoin dominates in categories such as impersonation and fake returns, where the older, more established blockchain is commonly preferred. USDT on Ethereum or Tron, by contrast, accounts for the majority of pig butchering and sanctioned flows, consistent with the documented preference for stablecoins among organized criminal networks that seek to avoid exchange-rate volatility while maintaining liquidity. Stolen funds are largely centered on Ethereum, and show a higher share of native ETH. This conforms with the intuition that contract exploits attack developed DeFi infrastructure lending protocols in ETH, and/or liquidity reserves (usually in the native coin, ETH).

We next examine how these flows are distributed across the three blockchains and how they have evolved over time. Figure 2 presents two complementary views. The left panel shows the monthly inflow to reported criminal addresses, with the stacked colored areas indicating the cryptocurrency composition in each month and the red line tracking total monthly inflows. The right panel shows cumulative inflows over the full sample period by blockchain. Several patterns emerge. First, Ethereum

[20] Table 2 and 3 reports summary statistics for the total dollar inflows and the number of transactions of reported addresses by scam category.

accounts for the largest share of cumulative direct inflows at $42.1 billion, followed by Bitcoin at $23.9 billion and Tron at $8.7 billion. Second, the composition of criminal inflows has shifted markedly over time. In 2020 and early 2021, Bitcoin accounted for the substantial majority of monthly inflows. From mid-2021 onward, stablecoins—primarily USDT on Ethereum—grew rapidly in share, coinciding with the broader adoption of stablecoins in crypto markets. USDT on Tron, shown in the darker red-pink shading, began to appear as a meaningful component from 2022 onwards and has grown steadily since, reflecting Tron's increasing role as a low-cost conduit for criminal stablecoin flows in Southeast Asian fraud networks. Third, monthly inflows exhibit high volatility, with occasional sharp spikes corresponding to large individual events—such as exchange hacks, contract exploits, or coordinated scam campaigns—overlaid on a more persistent baseline of ongoing fraud.

The time-series evidence in Figure 2 suggests that criminal crypto activity has remained elevated over the sample period, while also diversifying its blockchain footprint, particularly through a shift toward stablecoins and Tron in recent years. Taken together, aggregating across categories yields an estimated $74.7 billion in direct inflows to reported addresses—a substantial figure that nonetheless likely understates true criminal volumes, since the victim report sample is far from comprehensive. The subsequent sections develop our methodological framework for pushing beyond these direct flows.

3. Where do Criminal Flows Go?

The direct inflows to reported addresses documented above capture only the first step of criminal fund movement. In practice, the operators behind fraud schemes do not simply accumulate funds at reported addresses—they move them onward through layered transactions designed to obscure the origin of proceeds. To understand how criminal funds travel from reported addresses to their eventual destinations, we apply the forward tracing methodology described in Section 1.3, following funds hop by hop from each reported address until they reach an identified service, an unidentified large address, or a terminal dust-level amount.

We trace 8 hops for Bitcoin, and 5 for both Ethereum and Tron wallet addresses. The reason for tracing more hops for Bitcoin is due to the UTXOs blockchain structure. Because of such structure,

users on Bitcoin are more prone to consolidate funds using more transactions and thereby funnel funds by employing more intermediate steps.

3.1 Mapping Criminal Fund Pathways

Figure 3 presents Sankey diagrams visualizing the traced fund pathways for Bitcoin in Panel A, Ethereum in Panel B, and Tron in Panel C. In each diagram, the leftmost node labeled "Origin" corresponds to the reported criminal addresses, and successive "Hop" nodes represent intermediate wallets through which funds pass before reaching identified services at the far right. Grey nodes at both ends represent unidentified terminal addresses, distinguished by whether they are large or small. Edge widths are proportional to the dollar value of traced flows.

The diagrams reveal several important patterns. A first notable observation is that Bitcoin funds travel through substantially more intermediate hops before reaching identified services. On Ethereum, funds more frequently reach services within one to three hops. Nonetheless, the leading Bitcoin recipients—Bit.com, Binance, and Coinbase—receive the majority of their inflows directly from origin addresses in a single hop.

A second consistent finding across all three blockchains is the prominent role of Binance as a destination. Binance appears among the top identified destination services in Bitcoin, Ethereum, and Tron. This prominence provides initial evidence suggesting its common use as an off-ramp through which launderers convert criminal proceeds into fiat currency across multiple blockchain ecosystems.

Third, the Sankey diagrams expose the presence of illicit or suspicious intermediary services that serve as waypoints in the laundering chain. On Ethereum, Tokenlon—an obscure decentralized exchange heavily used by pig butchering networks—appears as both an inflow source and an outflow destination, reflecting its use as a token swap intermediary that deliberately breaks the on-chain tracing trail. On Tron, HuionePay and Kyrrex emerge as prominent destination services alongside the major centralized exchanges. HuionePay, a Cambodian payment platform with documented ties to organized criminal compounds in Southeast Asia, receives a disproportionate share of Tron criminal outflows, consistent with the broader evidence of its role as a money laundering facilitator.

Fourth, on Tron, addresses linked to terrorist organizations appear among the prominent inflow sources to reported criminal addresses—alongside Binance as the top sender—suggesting that Tron serves as a convergence point for multiple categories of illicit finance. On Bitcoin, the leading identified sources include Binance, Genesis Trading, Kraken, and Coinbase; on Ethereum, Uniswap and Binance lead. Across all three blockchains, small unidentified wallets account for the majority of inflows, consistent with victims transferring funds directly from personal wallets after being scammed.

3.2 Destinations of Traced Flows Over Time

We next ask how the distribution of traced flows across destination service types has evolved over time. This temporal perspective reveals whether criminal networks have shifted their off-ramp strategies in response to market developments, enforcement actions, or changes in the availability of different services.

Figure 4 presents the monthly traced inflows to identified services from 2020 through late 2025. The left panel shows the service-type share as a stacked area chart—centralized exchanges (CEX) in blue, decentralized exchanges (DEX) in green, mixers in yellow, other DeFi in pink, and unidentified addresses in grey—with the red line tracking total monthly traced inflows. The right panel shows the cumulative totals by blockchain, with the hatched portion of each bar indicating the flows traced directly from origin addresses (before any clustering).

Centralized exchanges are the dominant destination throughout the sample period, consistently accounting for the largest share of traced outflows across all three blockchains. Decentralized exchanges on Ethereum represent a secondary but meaningful component. Their share exhibits notable variation over time, rising during periods of elevated DeFi activity in 2021–2022 and during specific events such as exchange hacks, where criminals exploited DEX infrastructure to rapidly swap stolen tokens before exchanges could freeze assets. Mixer usage, while small in aggregate share, is persistent and episodically elevated; its presence in traced flows reflects the ongoing use of privacy-enhancing tools by a subset of criminal actors, particularly those involved in hacks and contract exploits on Ethereum.

4. What Can We Learn from Recent Illicit Exchanges?

We now turn to examine recent money laundering services for two main reasons. First, we wish to understand how these exchanges operate and how they interact with the rest of the crypto ecosystem. Second, we wish to establish these exchanges as a benchmark for illicit activity for comparison purposes to other exchanges. Illicit crypto services take several forms, including darknet marketplaces that facilitate illegal trade and laundering venues that move, obscure, and off-ramp illicit proceeds. Figure 5 focuses on the principal services in our sample: Hydra Market, a major Bitcoin darknet marketplace; Nobitex.ir, the largest known Iranian crypto exchange; Garantex and Zedcex Exchange Ltd., service providers linked to illicit finance; and HuionePay.

HuionePay is a massive payment platform belonging to the larger Huione Group, a Cambodian conglomerate with links to the country's ruling Hun family.[21] In July 2024 the British blockchain analytics firm Elliptic Research (2024) reported that Huione was involved in the laundering scam proceeds for criminals worldwide. The firm highlighted Huione's role in laundering proceeds from pig butchering scams, primarily in USDT. A year later, in May 2025, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) identified Huione as a financial institution associated with illicit actors with little to no AML and KYC policies.[22] HuionePay operates similarly to a CEX, and our findings show a strong presence of HuionePay USDT activity on the Tron blockchain.

In Panel A of Figure 5, we plot illicit services active from 2020 till December 2025. These services are currently sanctioned by the U.S. Treasury. Throughout this period, we find Hydra's inflows amount for the largest share of illicit service activity, nevertheless this share decreases until Hydra's eventual shut down in April 2022. Throughout 2020 to 2022 we also see a rise of Nobitex.ir. It is not until 2022 that we find a meteoric rise of HuionePay as a share of the total illicit service space, and after mid-2022 HuionePay has comprised more than half of all illicit service activity and more than 60% throughout

[21] Reuters identified Cambodian businessman Hun To as one of the three directors of Huione. To is a cousin to the current Cambodian Prime Minister Hun Manet, and nephew to former Prime Minister Hun Sen (Manet's father).

[22] FinCEN notes that: "Of the $4 billion worth of illicit proceeds, FinCEN found that Huione Group laundered at least $37 million worth of CVC stemming from DPRK cyber heists, at least $36 million from CVC investment scams, and $300 million worth of CVC from other cyber scams."

the 2020 to December 2025 period. The overall inflows to these services show an increasing trend since 2020. Starting with monthly inflows ranging in the hundreds of millions in the period ranging from 2020-2023, in early 2023, these inflows rise steadily, reaching a billion per month early 2024. At the same time, the Elliptic report was released in the middle of 2024, when the inflows drop, and since then, the monthly inflows have remained in the high hundreds of millions albeit with a recent downturn in recent months. In Panel B, we plot the traced flows originating from HuionePay hot wallets. There are large recycled flows traced to HuionePay from HuionePay amounting to over $4.0 billion, and even larger flows traced to large unidentified addresses amounting to more than $44.9 billion. Flows to identified CEXes amount to $5.2 billion, with Binance being the chief recipient receiving $2.1 billion.

Figure 6 showcases the general trends and patterns of the traced HuionePay network. Panel A illustrates a network graph of the HuionePay ecosystem on the Tron blockchain, mapping the intricate flow of funds between central service nodes and peripheral exchanges such as Binance and OKX. Within this visualization, circular nodes represent individual wallets and square nodes denote service hot wallets, with node size corresponding to transaction degree and edge curvature indicating the directionality of the financial flows. Crucially, the dynamics of recycled capital are captured by the orange circular nodes, which are found in both the back and forward traces. These nodes denote individual wallets that emerge in both the backward tracing of origin deposits and the forward tracing of outgoing funds, thereby acting as bidirectional conduits. Visually constituting a dense, highly connected cluster in the upper-middle section of the graph, these orange nodes highlight a pronounced cyclical movement of capital, wherein substantial volumes of funds are continuously routed into and subsequently extracted from the central HuionePay infrastructure by the same participating entities.

Panel B of Figure 6 presents a dual-panel bar chart analyzing the aggregate sources and destinations of cryptocurrency transactions originating from and to HuionePay. The data is stratified by transaction proximity, denoted as "Hops" (ranging from Hop 0 to Hop 4), which quantifies the number of intermediary steps required to trace the funds between the respective entities. From CEXes to HuionePay the vast majority of the volume across the top exchanges occurs at Hops 3 and 4 (represented by

yellow and light orange). This suggests that funds are subjected to multiple transfers, potentially indicative of complex routing, mixing, or obfuscation techniques, before ultimately consolidating at HuionePay. Binance serves as the primary source of these inflows with an aggregate total of $460 million, followed by OKX ($323.6 million) and HTX ($243.1 million). In direct contrast to the inflow data, the outflow distributions are heavily concentrated at lower hop counts. A substantial proportion of the funds directed to Binance and OKX are classified as Hop 0 (red) and Hop 1 (dark orange). This indicates that transfers from HuionePay to these major trading platforms are executed directly or near-directly, with minimal intermediary steps. The total financial volume of outflows significantly dwarfs the inflows. Binance is overwhelmingly the dominant destination, receiving $2.1 billion, while OKX receives $1.6 billion. Maskex follows at a distant third with $455.1 million. The figure highlights a pronounced asymmetry in HuionePay's operational flow. Traced inflows from CEXs are smaller in aggregate volume and characterized by extended transaction chains (high hop counts). Conversely, outflows to CEXes are massively scaled and involve highly direct transfers (low hop counts), suggesting that HuionePay acts as a major consolidation point before directly offloading funds to top-tier CEXes.

5. What Is the Tainted Share of Exchange Flows?

The preceding sections establish that centralized exchanges are the most common exit point for tainted crypto flows, and that certain exchanges appear as particularly prominent destinations across blockchains. Reported criminal addresses certainly do not capture the full universe of criminal actors, and criminals may operate additional deposit addresses at these exchanges that our traces did not reach. To uncover these additional tainted flows and examine the cross-sectional distribution of tainted exposure more completely, we apply deposit address clustering.

The intuition for deposit address clustering is straightforward: because a centralized exchange assigns each customer a unique deposit address, two deposit addresses that receive funds from the same sender are almost certainly controlled by the same customer account. By identifying all deposit addresses that receive large flows from a common sender with a known tainted deposit address, we

can infer that those additional deposit addresses belong to the same tainted actor (as discussed in the Methodology section). On Bitcoin, we instead apply the common-input heuristic, which groups addresses that jointly appear as inputs to the same transaction, revealing shared key ownership, to identify additional tainted addresses belonging to the same entity.

In addition to clustering around deposit addresses identified through tracing reported addresses, we incorporate flows through HuionePay on Tron. As documented in Section 4., HuionePay is the single largest illicit service in our traced flows on Tron and was sanctioned by FinCEN in May 2025. We forward trace funds from HuionePay's known wallets to the exchange deposit addresses that received those flows, and then apply deposit address clustering around those deposit addresses as well.

5.1 Cross-Sectional Differences Across Exchanges

Figure 7 presents the results of this clustering exercise. Panel A plots each exchange as a bubble in three plots defined by two dimensions of tainted exposure: the horizontal axis measures the share of the exchange's total lifetime inflow that is tainted, and the vertical axis measures the total dollar amount of clustered tainted inflows received by the exchange. Bubble size is proportional to the number of tainted transactions. Each bubble is colored to indicate the blockchain and cryptocurrency: exchanges on Bitcoin are shown in gold on the left plot; exchanges on Tron appear in red on the right plot; and exchanges on Ethereum are shown on the center plot as pie charts subdivided by token, covering native ETH, USDT, and USDC. Western exchanges are marked with an asterisk. The red dashed vertical lines indicate the mean tainted inflow share across exchanges within each blockchain, and the blue dashed horizontal lines indicate the mean dollar amount of tainted inflows.

Several patterns stand out. First, there is a large dispersion both across and within blockchains. Bitcoin exchanges cluster in the lower left of the figure, reflecting both lower absolute tainted inflows and a lower tainted share of total volume compared to Ethereum and Tron. Some of the lower totals on Bitcoin could also reflect differences in blockchain structure and obfuscation methods. Across Ethereum and Tron exchanges, the tainted share varies widely, ranging from below 1% to above 20%, indicating that criminal actors are likely aware of the monitoring differences across exchanges.

Second, in terms of total tainted dollar volume, Binance is consistently the largest destination across all three blockchains, followed by other large exchanges such as HTX, Bybit, OKX, and FTX (prior to bankruptcy). On Ethereum, Binance receives $70.03 billion in clustered tainted inflows, $23.2 billion to HTX and $12.9 billion to OKX. On Tron, these figures reach $231.0, $34.9 and $35.5 billion respectively. It is interesting that the ordering of many of the exchanges is similar on both Ethereum and Tron.

Third, a notable and policy-relevant finding is that HuionePay, despite being formally sanctioned by FinCEN, is not the highest tainted inflow share in our sample and stands at 16.4%. Unsanctioned exchanges, including Kyrrex and BTSE on Tron and Bitkub on Ethereum, exhibit higher tainted inflow shares than HuionePay. With a share of 14.8%, Binance attracts a far greater tainted dollar volume and is very close to HuionePay's share of tainted inflows.

Fourth, Western exchanges, identifiable by the asterisk, sit in the lower tail of the tainted share distribution within their respective blockchains. Coinbase, for instance, exhibits tainted inflow shares well below the blockchain-level means. This pattern is consistent with stricter know-your-customer and anti-money-laundering compliance at regulated Western exchanges reducing their attractiveness as off-ramps for criminal proceeds.

5.2 Tainted Share and Blockchain Trends Over Time

Panel B of Figure 7 presents the monthly clustered tainted inflows over the full sample period from 2020 to September 2025, with the stacked colored areas indicating the cryptocurrency composition and the red line tracking total monthly tainted inflows. The bar chart at the right shows cumulative totals by blockchain.

The most striking pattern is the dramatic rise of Tron as the dominant blockchain for tainted flows. In 2020 and 2021, Tether on Ethereum accounted for the largest share of monthly tainted inflows. From 2022 onward, USDT on Tron grew steadily in relative share, eventually becoming the largest component of monthly tainted inflows and displacing Ethereum-based assets. This shift reflects Tron's low transaction fees and fast settlement, which facilitate the high-volume stablecoin transfers

characteristic of organized criminal networks.

The cumulative totals confirm this ordering: Tron accounts for $400 billion in clustered tainted inflows over the full period, surpassing Ethereum at $150 billion and Bitcoin at $24 billion. Using total inflows to exchange deposit addresses on each blockchain as the denominator, we estimate that tainted funds account for 11.5% of all Tron exchange inflows, 3.8% of Ethereum exchange inflows, and 0.25% of Bitcoin exchange inflows. These estimates suggest that roughly one in twenty Tether flowing into a Tron exchange account is associated with criminal activity. This level of taint points to the urgency of more systematic monitoring of stablecoin flows on this blockchain.

6. What does Machine Learning Indicate about the Nature of Criminal Activity?

While the tracing and deposit address clustering methodologies described above identify a substantial volume of tainted crypto flows, the set of reported criminal addresses from which we begin is inherently limited. Victim reports capture only a fraction of criminal activity, and even after tracing funds forward and applying deposit address clustering, there likely remain criminal deposit addresses that share no direct transactional link to our identified network. To move closer to the true scope of criminal activity in cryptocurrency markets, we turn to machine learning methods.

Deploying machine learning in this context offers two complementary benefits. First, by training a model on the behavioral features of known tainted deposit addresses, we can examine which address-level characteristics are most predictive of criminal involvement. This provides economic insight into how criminal deposit addresses differ from legitimate ones—effectively revealing the operational fingerprint of illicit crypto networks. Second, the trained model can be applied to the universe of unflagged deposit addresses to predict additional tainted addresses beyond those identified through tracing and clustering, thereby expanding our estimate of total criminal flows.

A key challenge in applying supervised learning to this setting is that our labeled data are inherently one-sided. We observe addresses that are *positively* identified as tainted through tracing and clustering, but we lack a verified set of addresses that are definitively clean. Any address not linked to our traced

network may be either a) non-criminal, or b) criminal but not unreported, either randomly or because the criminal activity uses different methods and the activity is particularly obfuscated. This asymmetry renders standard binary classification inappropriate, as treating all unlabeled addresses as negatives would contaminate the training signal with false negatives.

To address this, we adopt positive-unlabeled (PU) learning (Elkan and Noto, 2008), which requires only a set of confirmed positives and a set of unlabeled observations. We implement the Elkan and Noto (2008) estimator, which first trains a standard binary classifier on the positive-versus-unlabeled sample and then applies a calibration correction to recover the true posterior probability of being tainted. Specifically, let $s = 1$ denote that an address is labeled positive and $s = 0$ denote that it is unlabeled. The classifier estimates $\Pr(s = 1 \mid \mathbf{x})$, and the true positive probability is recovered as $\Pr(\text{tainted} \mid \mathbf{x}) = \Pr(s = 1 \mid \mathbf{x})/c$, where $c = \Pr(s = 1 \mid \text{tainted})$ is estimated from a held-out calibration set. We hold out 10% of labeled positives for this calibration step. As our base classifier, we use LightGBM, a gradient-boosted decision tree algorithm well suited to tabular data with heterogeneous feature types.[23] Our training sample consists of all positively labeled deposit addresses and a random sample of unlabeled addresses at a 4:1 ratio.

In addition to predicting whether an address is tainted, we require an estimate of the *severity* of taint—that is, what fraction of an address's total inflows are criminal. We therefore train a second model, a LightGBM regressor, exclusively on the set of known tainted addresses. The target variable is the ratio of traced tainted inflows to total inflows.[24]

We construct our feature set from on-chain transaction data for each deposit address. For Ethereum, the model incorporates 270 features. For Tron, the feature set comprises 219 features. Table 4 reports the summary statistics of select Ethereum deposit-address features, while Table 5 reports the statistics for Tron features.

The estimated tainted flow attributable to machine learning predictions is then computed as:

[23] The model is trained with 300 boosting rounds, a learning rate of 0.05, 64 leaves per tree, and 80% row and column subsampling.

[24] The target variable is transformed to logit space to accommodate the bounded support on $[0, 1]$. At prediction time, the inverse sigmoid is applied to recover the predicted tainted fraction, which we denote $\hat{p}_{\text{sev}}$. The severity model is trained with 2,000 boosting rounds (with early stopping), a learning rate of 0.02, and the same tree structure and subsampling parameters as the classification model.

$$\widehat{\text{Tainted Flow}}_{i,t} = \Pr(\text{tainted}_i \mid \mathbf{x}_i) \times \hat{p}_{\text{sev},i} \times \text{Inflow}_{i,t} \tag{1}$$

where $\Pr(\text{tainted}_i \mid \mathbf{x}_i)$ is the PU-corrected probability that address i is tainted, $\hat{p}_{\text{sev},i}$ is the predicted fraction of inflows that are criminal conditional on the address being tainted, and $\text{Inflow}_{i,t}$ is the observed dollar inflow to address i in month t. This decomposition allows the model to assign partial taint to addresses with intermediate predicted probabilities rather than imposing a binary classification threshold.

6.1 Feature Importance and the Anatomy of Criminal Deposit Addresses

To understand how each feature contributes to the model output, we use Shapley additive explanations (SHAP), a standard tool for interpreting machine learning models. For each address-feature pair, the SHAP value measures how much that feature shifts the model's predicted likelihood of taint relative to a baseline prediction. To assess global importance, the mean absolute SHAP value is typically computed for each feature across all observations. Because our model contains many high-dimensional features that are naturally correlated, individual feature importance can be unstable in the sense that the model may distribute predictive power across closely related variables. This is not problematic for prediction, but it can make interpretation at the individual-feature level less transparent. To obtain a clearer economic summary, we therefore group related features into economically meaningful families and rank feature families by the sum of the mean absolute SHAP values of the features within each family.

Figure 8 presents the SHAP summary plot for the top 20 feature families in the Ethereum tainted address prediction model. Each point represents an observation, with color indicating the underlying feature value and horizontal position reflecting that feature family's contribution to the model's predicted log-odds of being tainted. The most important feature family is *Hop-1 Sender In-Degree Distribution*, which captures the distributional statistics of the in-degree of hop-1 senders, where hop-1 senders are addresses that send funds directly to the deposit address, one transaction step upstream. Deposit addresses that receive funds from senders with low in-degree are more likely to be flagged as tainted, suggesting that the senders are transit wallets that do not transact with other counterparties

and serve primarily to relay funds along a laundering chain. The second-ranked family, *Unique Counterparty Count*, similarly reflects network structure: addresses receiving funds from a larger number of distinct counterparties are more likely to be tainted, consistent with criminal deposit addresses acting as collection points that aggregate flows from multiple intermediaries. *Inflows CEX Share*—the fraction of inbound value originating from centralized exchanges—ranks third. Deposit addresses with lower CEX inflow shares are more predictive of tainted status, consistent with the previous finding: criminal deposit addresses receive the bulk of their funds not directly from exchange withdrawals by end users but rather from transit wallets that relay funds off-chain. *Hop-1 Sender Active Days Distribution* and *Lifecycle* features further indicate that shorter-lived hop-1 senders and shorter-lived deposit addresses are more strongly associated with tainted status. *Hop-1 Sender Asset Usage Share*, *Source-Specific Trace Exposure*, *Total USD Value Level*, and *Hour-of-Day Pattern* each contribute additional explanatory power, implying that asset mix, service exposure, scale, and timing all matter. The remaining top-20 families capture transaction size distributions, round-amount structuring, and overall activity levels.

Figure 9 presents SHAP dependence plots for twelve individual features, complementing the family-level rankings by showing how specific features contribute to the model output across the support of the data. Several features indicate that tainted deposit addresses operate primarily as collection points rather than ordinary user wallets. Higher deposit-address in-degree is strongly associated with predicted taint (Panel A), consistent with addresses that aggregate inflows from many upstream senders. At the same time, a smaller share of stablecoin inflows originating from centralized exchanges is associated with higher predicted taint (Panel B), suggesting that these deposit addresses are funded less frequently from centralized exchanges. Deposit addresses with shorter histories contribute more positively to predicted taint (Panel C), and their hop-1 senders likewise tend to be short-lived (Panel D), indicating upstream activity concentrated in relatively brief operational windows. Upstream senders that predominantly transact in Tether align with higher predicted taint, while greater USDC usage among hop-1 senders contributes negatively to the prediction (Panels G and F). Direct usage of illicit DeFi services or mixers also matters: deposit addresses receiving flows linked to Tokenlon or Tornado Cash show discrete increases in SHAP contribution (Panels E and I). Round-number transfers divisi-

ble by 1,000 appear more frequently among tainted deposit addresses (Panel H). In addition, a larger fraction of stablecoin inflows is rapidly forwarded onward (Panel J), and outbound transactions are more heavily concentrated in stablecoins (Panel K). Lower token diversity also contributes positively to predicted taint (Panel L). Taken together, these feature-level patterns provide a more granular view of the behavioral differences highlighted in the feature-family rankings.

Figure 10 presents the analogous SHAP summary plot for the Tron blockchain, where the model incorporates 219 features organized into 27 families. Because our blockchain data on Tron only includes Tether transactions, the feature set is adapted accordingly, omitting multi-asset distinctions relevant only to Ethereum.

The feature importance ranking on Tron exhibits notable similarities to and some differences from the Ethereum model. Hop-1 sender characteristics again dominate, with *Hop-1 Sender Degree Distribution*, *Hop-1 Sender Tx Count Distribution*, and *Hop-1 Sender 10k-Divisible Tx Distribution* among the most influential families. Other important families include sender wallet age, total inflow, active days, deposit share, and average sent amount distributions, which together characterize upstream network behavior. *Lifecycle* features remain important, indicating that shorter-lived addresses are more associated with tainted activity across both blockchains.

6.2 Predicted Tainted Flows

We apply the trained models to the full universe of unlabeled deposit addresses on both Ethereum and Tron and compute the estimated tainted flows using Equation (1). Figure 11 presents monthly machine-learning-implied tainted flows for Ethereum in Panel A and Tron in Panel B in the red shaded area. For comparison and to provide a holistic view of total criminal activity, the figure also includes results from direct inflows in the grey shaded area and from deposit-address clustering in the coral shaded area from prior sections. The dashed red line shows cumulative flows over time.

Two notable patterns emerge in both blockchains. First, direct inflows to reported addresses—the measure that is more commonly available to regulators and researchers—constitute only a small fraction of total estimated criminal flows. These inflows are materially smaller than the additional

volumes uncovered through deposit address clustering and machine learning. Second, inflows to the reported address and to the clustered deposit address tend to decline in more recent periods. This pattern largely reflects reporting delay: fraudulent addresses typically enter victim-report databases only after victims discover the fraud and submit reports, which creates a lag between when transactions occur and when the associated addresses become observable to researchers. Viewed in isolation, this lag can give the misleading impression that criminal activity is declining over time. Machine learning helps mitigate this limitation by identifying additional deposit addresses based on their transactional behavior and network structure, allowing the analysis to capture criminal flows associated with more recent activity.

The cumulative totals shown on the right-hand side of Figure 11 further illustrate the contribution of each method. On Ethereum, direct inflows to reported addresses sum to approximately $40 billion, while deposit address clustering identifies an additional $120 billion in tainted inflows. Machine learning contributes a further $218 billion, bringing the total estimated tainted inflows on Ethereum to roughly $378 billion. On Tron, direct inflows account for about $8 billion, deposit address clustering contributes approximately $312 billion, and machine learning adds an additional $163 billion, resulting in total estimated tainted inflows of about $483 billion. These comparisons highlight how each successive layer of analysis expands the observable scope of criminal activity on-chain. Given that criminal activity is typically reported with a lag, our results also show how machine learning methods could be utilized by the crypto community to tag addresses acting in a suspicious manner. A limitation of our analysis is that our training dataset may be missing other types of criminal addresses. ML estimates should help to estimate missing addresses that follow a similar pattern as our current addresses, though it may not capture criminal addresses that use different patterns or obfuscation methods. For example, HuionePay was active from early 2022 to 2025, but only labeled as such in 2025. Thus, to the extent that HuionePay acted differently from other transaction centers, these transactions might not be detected until the activity was labeled as such. Similarly, sophisticated activity that is rarely labelled may have little data for training.

7. Conclusion

Given the evolving nature of the crypto landscape, it remains unclear to what extent the ecosystem facilitates criminal activity. We examine this question across three major blockchains. Overall, we find that between five and twenty percent of inflow volume at many exchanges is tainted. Given that such a large share of crypto exchange volume is associated with this activity, and the large cross-section of exchanges accepting criminal proceeds, crypto exchanges seem to have ample incentive to continue accepting illicit flows absent strong regulatory actions. Overall, we estimate that more than one trillion dollars in illicit activity has moved through crypto exchanges since 2021, but there are compelling reasons to believe that our estimates undercount the true scale of this activity. In the meantime, our research points to many tangible and implementable steps that regulators and industry actors can take to clamp down on criminal crypto activity.

We hope to see future research continue identifying and understanding the economic mechanisms underlying criminal activity. Given recent advancements in machine learning and AI, deeper crypto features and methods could be utilized to gain a fuller understanding of the crypto criminal ecosystem. Currently, many large crypto exchanges facilitate transactions both for individual crypto investors and for large criminal actors. This interaction seemingly facilitates low transaction costs for criminals and many opportunities for individuals to be defrauded. Because of the public nature of blockchain ledgers, the surveillance of criminal activity is much more feasible for researchers, industry participants, and law enforcement in the crypto landscape than in the traditional banking system. Thus, even though large parts of the current crypto ecosystem currently enable substantial criminal activity, there is nothing inherent in blockchain technology which makes this the only equilibrium. One could imagine a future in which such activity is largely segmented to a subset of the crypto ecosystem that has little interaction with reputable crypto exchanges and limited access to the fiat banking system. Such a world would make it harder for criminals to expropriate individuals and much more costly for criminals to exit into fiat currency. Reaching this equilibrium of segmented and low amounts of criminal activity will require awareness of the central role that crypto exchanges play in facilitating criminal activity

and substantially stronger enforcement by regulators.

References

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

Chainalysis, 2025, The 2025 crypto crime report, Report, Chainalysis.

Chainalysis, 2026, The 2026 crypto crime report, Report, Chainalysis.

Chen, Liang, Jiaying Peng, Yang Liu, Jintang Li, Fenfang Xie, and Zibin Zheng, 2020, Phishing scams detection in ethereum transaction network, *ACM Transactions on Internet Technology (TOIT)* 21, 1–16.

Christin, Nicolas, 2013, Traveling the silk road: A measurement analysis of a large anonymous online marketplace, in *Proceedings of the 22nd international conference on World Wide Web*, 213–224.

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.

Ding, Zhihao, Jieming Shi, Qing Li, and Jiannong Cao, 2024, Effective illicit account detection on large cryptocurrency multigraphs, in *Proceedings of the 33rd ACM International Conference on Information and Knowledge Management*, 457–466.

Elkan, Charles, and Keith Noto, 2008, Learning classifiers from only positive and unlabeled data, in *Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining*, 213–220.

Elliptic Research, 2024, Huione guarantee: The multi-billion dollar marketplace used by online scammers, Accessed: 2026-03-16.

Faux, Zeke, 2023, *Number Go Up* (Crown Currency).

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.

Félez-Viñas, Ester, Luke Johnson, and Talis J. Putnins, 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.

Goonetilleke, Priyanka, Alex Knorre, and Artem Kuriksha, 2023, Hydra: Lessons from the world's largest darknet market, *Criminology & Public Policy* 22, 735–777.

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, Kevin Mei, and Zirui Wang, 2025, Are crypto anti-money laundering policies effective?, *Available at SSRN* .

Griffin, John M., and Amin Shams, 2020, Is Bitcoin Really Untethered?, *Journal of Finance* 75, 1913–1964.

Hamrick, JT, 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 & Management* 58, 102506.

Janetos, N, and J Tilly, 2017, Reputation dynamics in a market for illicit drugs. arxiv, *Preprint posted online March* 6.

Juvinski, Luciano, Haochen Li, and Alessio Brini, 2026, Stableaml: Machine learning for behavioral wallet detection in stablecoin anti-money laundering on ethereum, *arXiv preprint arXiv:2602.17842* .

Li, Jiasun, Foteini Baldimtsi, Joao P Brandao, Maurice Kugler, Rafeh Hulays, Eric Showers, Zain Ali, and Joseph Chang, 2021, Measuring illicit activity in defi: The case of ethereum, in *International Conference on Financial Cryptography and Data Security*, 197–203, Springer.

Li, Sijia, Gaopeng Gou, Chang Liu, Chengshang Hou, Zhenzhen Li, and Gang Xiong, 2022, Ttagn: Temporal transaction aggregation graph network for ethereum phishing scams detection, in *Proceedings of the ACM web conference 2022*, 661–669.

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, 2013a, A fistful of bitcoins: Characterizing payments among men with no names, in *IMC 2013 - Proceedings of the 13th ACM Internet Measurement Conference*, Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC, 127–139, 13th ACM Internet Measurement Conference, IMC 2013 ; Conference date: 23-10-2013 Through 25-10-2013.

Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage, 2013b, A fistful of bitcoins: characterizing payments among men with no names, *Proceedings of the 2013 conference on Internet measurement conference* 127–140.

Möser, Malte, and Arvind Narayanan, 2019, Effective cryptocurrency regulation through blacklisting, Working Paper.

Nicholls, Jack, Aditya Kuppa, and Nhien-An Le-Khac, 2023, Fraudlens: Graph structural learning for bitcoin illicit activity identification, in *Proceedings of the 39th Annual Computer Security Applications Conference*, 324–336.

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.

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

Tironsakkul, Tin, Manuel Maarek, Andrea Eross, and Mike Just, 2022, Context matters: Methods for bitcoin tracking, *Forensic Science International: Digital Investigation* 42–43, 301475.

TRM Labs, 2025, 2025 crypto crime report, Report, TRM Labs.

TRM Labs, 2026, 2026 crypto crime report, Report, TRM Labs.

Victor, Friedhelm, 2020, Address Clustering Heuristics for Ethereum.

Wang, Kai, Jun Pang, Dingjie Chen, Yu Zhao, Dapeng Huang, Chen Chen, and Weili Han, 2021, A large-scale empirical analysis of ransomware activities in bitcoin, *ACM Transactions on the Web (TWEB)* 16, 1–29.

Weber, Mark, Giacomo Domeniconi, Jie Chen, Daniel Karl I Weidele, Claudio Bellei, Tom Robinson, and Charles E Leiserson, 2019, Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics, *arXiv preprint arXiv:1908.02591* .

Yin, Haohua Sun, and Ravi Vatrapu, 2017, A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning, in *2017 IEEE international conference on big data (Big Data)*, 3690–3699, IEEE.

Figure 1. Direct Inflows to Reported Addresses by Scam Category

This figure reports total inflows to reported addresses by scam category in our sample. Each bubble represents one scam category. The horizontal axis, shown on a logarithmic scale, reports the number of reported addresses in the category, and the vertical axis, also on a logarithmic scale, reports the total inflow to those reported addresses. Bubble size is proportional to the total number of transactions associated with the category, and the pie chart within each bubble shows the cryptocurrency composition of inflows. The cryptocurrencies shown are Bitcoin, ETH, USDT on Ethereum, USDC on Ethereum, DAI on Ethereum, and USDT on Tron. Scam definitions are reported in Table IA.1. Victim reports are classified into scam categories using `GPT-4o-mini` based on the prompt reproduced in Table IA.2.

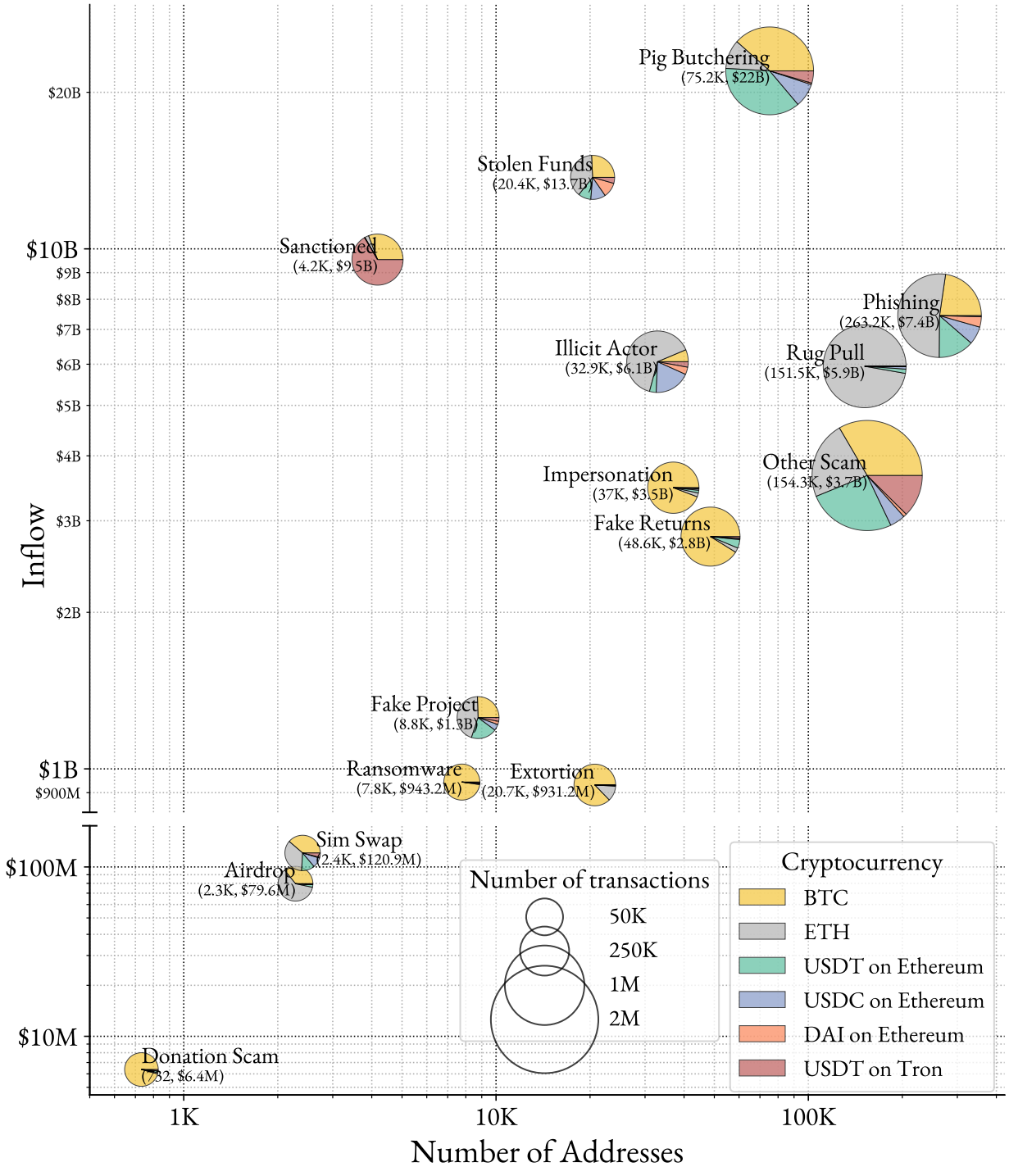


Figure 2. Direct Inflows to Reported Addresses by Blockchain

This figure reports direct inflows to reported addresses from 2020 through late 2025, broken down by blockchain and cryptocurrency. The left panel shows the monthly composition of inflows as a stacked area chart, with the left axis reporting cryptocurrency shares and the red line, read on the right axis, reporting total monthly inflows in dollars. The right panel shows cumulative inflows over the full sample period by blockchain, with each bar subdivided by cryptocurrency. The cryptocurrencies shown are Bitcoin, ETH, USDT on Ethereum, USDC on Ethereum, DAI on Ethereum, and USDT on Tron.

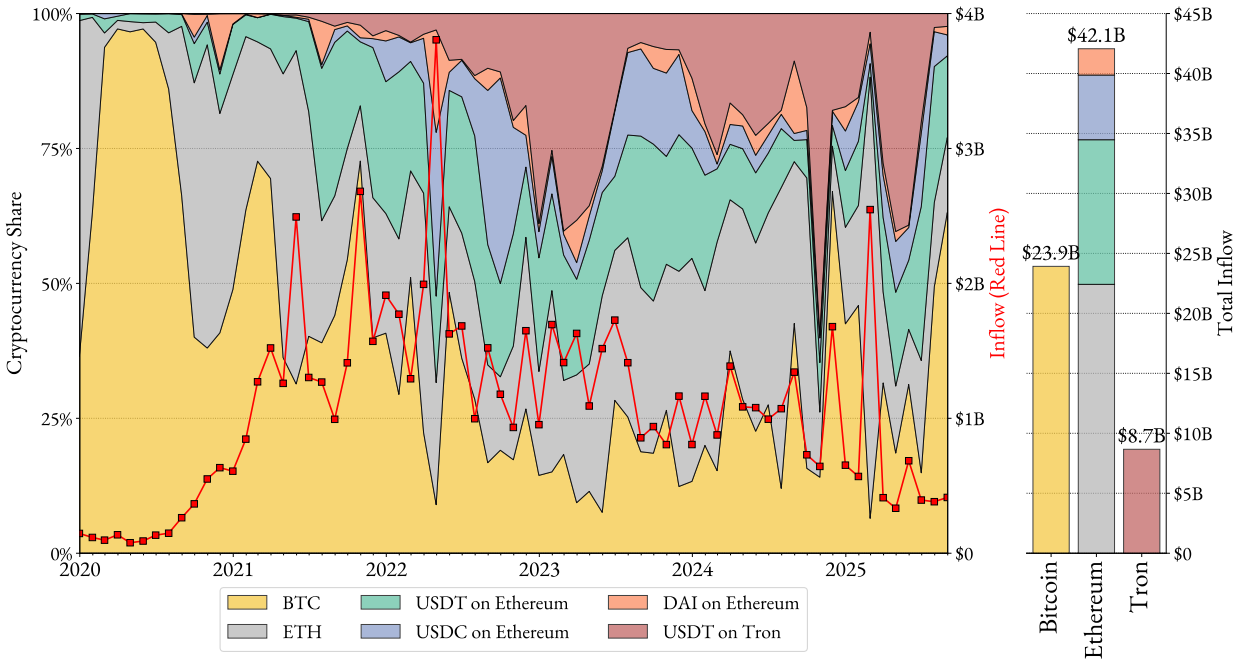


Figure 3. Traced Fund Pathways Across Blockchains

This figure presents Sankey diagrams of traced fund pathways from reported addresses on Bitcoin in Panel A, Ethereum in Panel B, and Tron in Panel C. In each panel, the node labeled "Origin" corresponds to the reported addresses, and successive "Hop" nodes denote intermediate wallets through which funds pass before reaching identified services or unidentified endpoints. Gray nodes represent identified services, with the five largest labeled individually and the remainder grouped as "Other." Dark purple nodes denote large and small unidentified trace endpoints. Edge widths are proportional to the dollar value of traced flows, and edge colors indicate the corresponding blockchain or token.

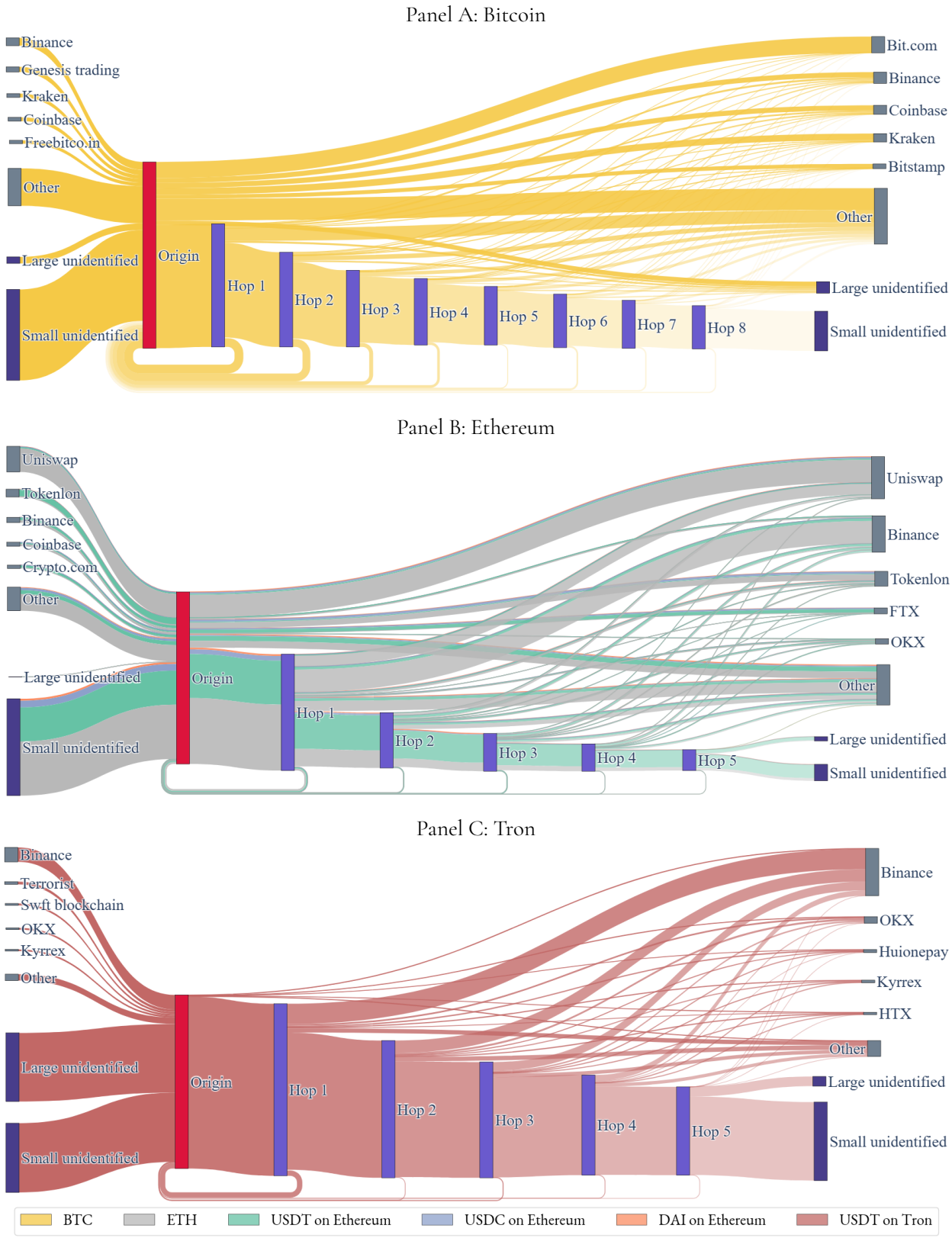


Figure 4. Traced Flows to Services Over Time

This figure reports monthly traced inflows from reported addresses to identified service destinations from 2020 through late 2025. In the left plot, the stacked area shows the share of monthly traced inflows accounted for by each service type, read on the left axis, and the red line, read on the right axis, shows total monthly traced inflows in dollars. Service types include centralized exchanges (CEX), decentralized exchanges (DEX), mixers, other DeFi services, other services, and unidentified addresses. The bar chart on the right reports cumulative traced inflows by blockchain over the full sample period. Within each bar, the hatched portion includes flows between reported addresses and balances remaining in intermediate wallets.

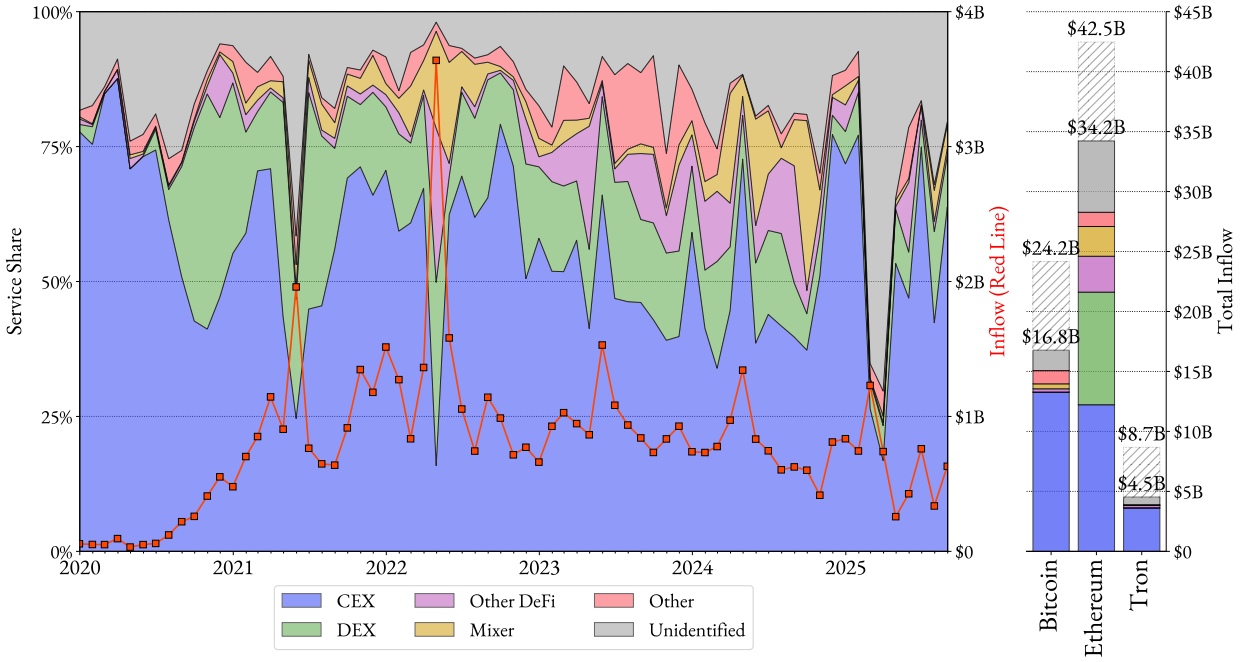
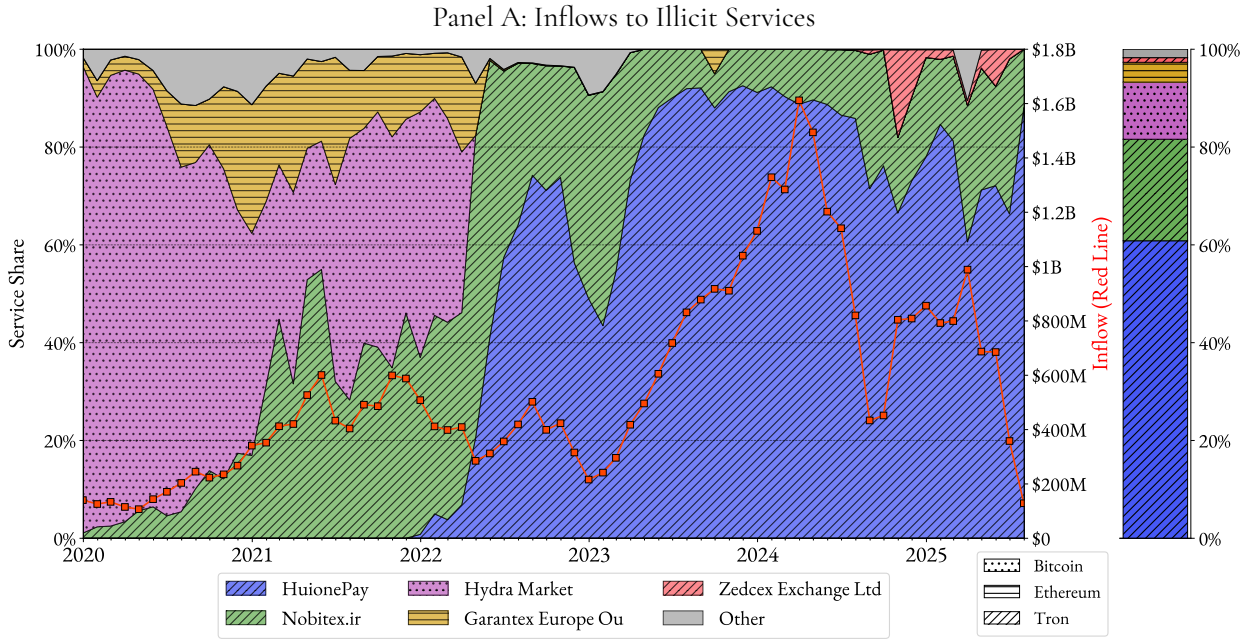


Figure 5. Inflows to Illicit Services and Traced HuionePay Exchange Flows

This figure reports inflows to identified illicit services and traced flows from HuionePay to centralized exchanges. Panel A shows monthly inflows to the major illicit services in our sample from 2020 through late 2025. In the left plot, the stacked area shows the share of total monthly inflows accounted for by each service, and the red line, read on the right axis, shows total monthly inflows in dollars. The bar on the right reports the aggregate service shares over the full sample period. Panel B shows traced flows from HuionePay hot wallets to major centralized exchanges from 2022 through late 2025. In the left plot, the stacked area shows inflows by destination exchange over time, and the red line, read on the right axis, shows cumulative traced inflows. The bar on the right reports the aggregate destination shares over the full sample period.



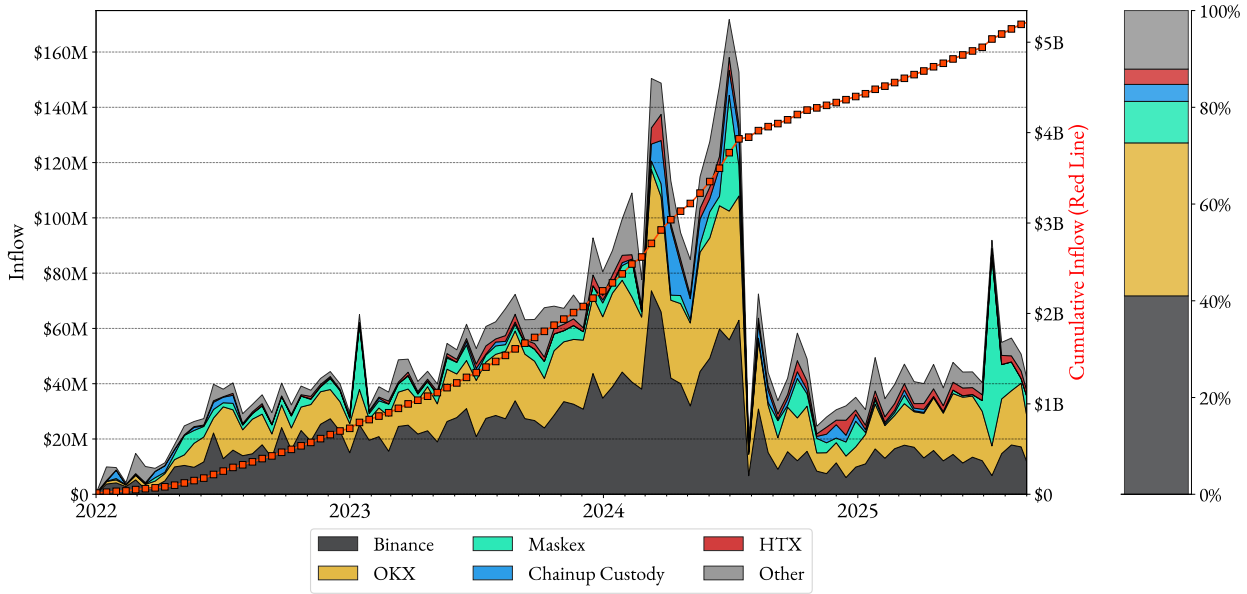
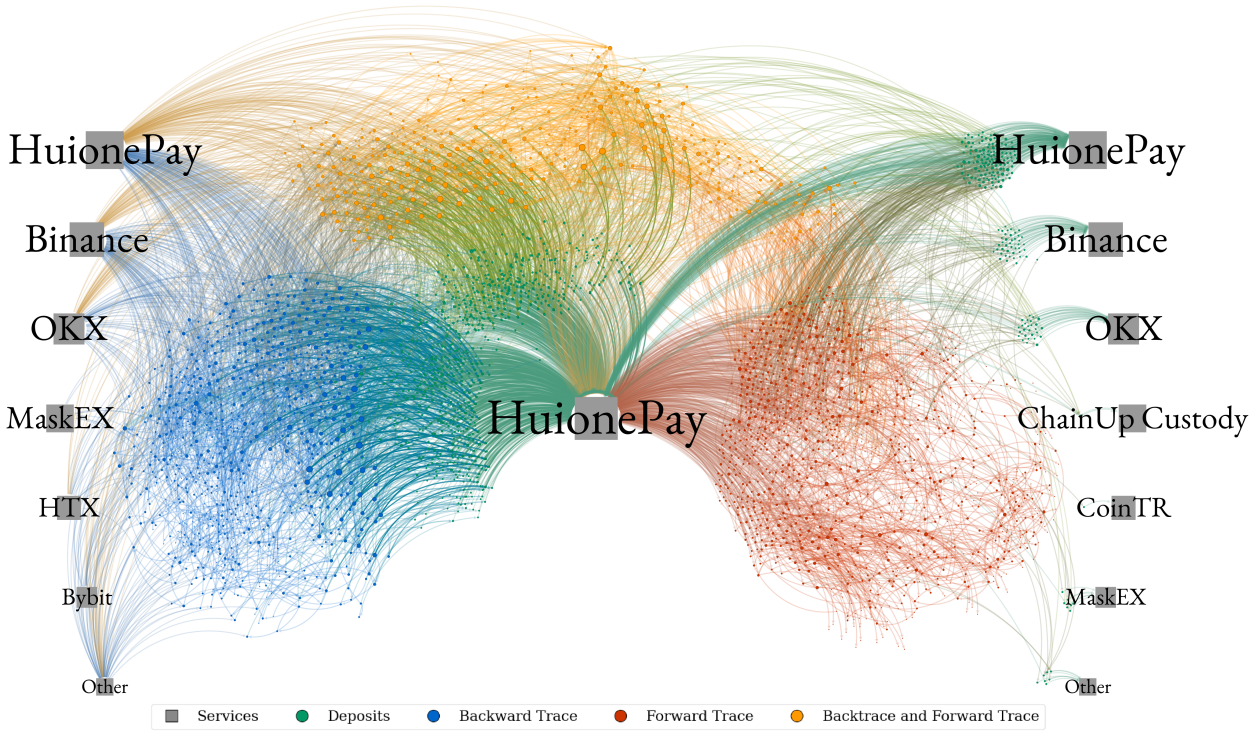


Figure 6. HuionePay Network and Traced Exchange Flows

This figure illustrates the structure of the traced HuionePay network on the Tron blockchain and the exchange flows associated with it. Panel A presents a network visualization constructed from random samples (around 0.5% of transactions) of the backtraced HuionePay deposit transactions and the forward-traced HuionePay hot-wallet transactions. Circular nodes represent individual wallets, square nodes represent service hot wallets, node size corresponds to degree, and node color indicates trace provenance. Concave-down edges represent flows moving from left to right, while concave-up edges represent flows moving from right to left. Panel B reports aggregate traced flows between HuionePay and major centralized exchanges. The left subpanel shows traced inflows from exchanges to HuionePay, and the right subpanel shows traced outflows from HuionePay to exchanges. In both subpanels, bars are decomposed by hop distance, from Hop 0 to Hop 4, indicating the number of intermediary steps in the traced path.

Panel A: Traced HuionePay Network



Panel B: Traced Flows Between HuionePay and Exchanges

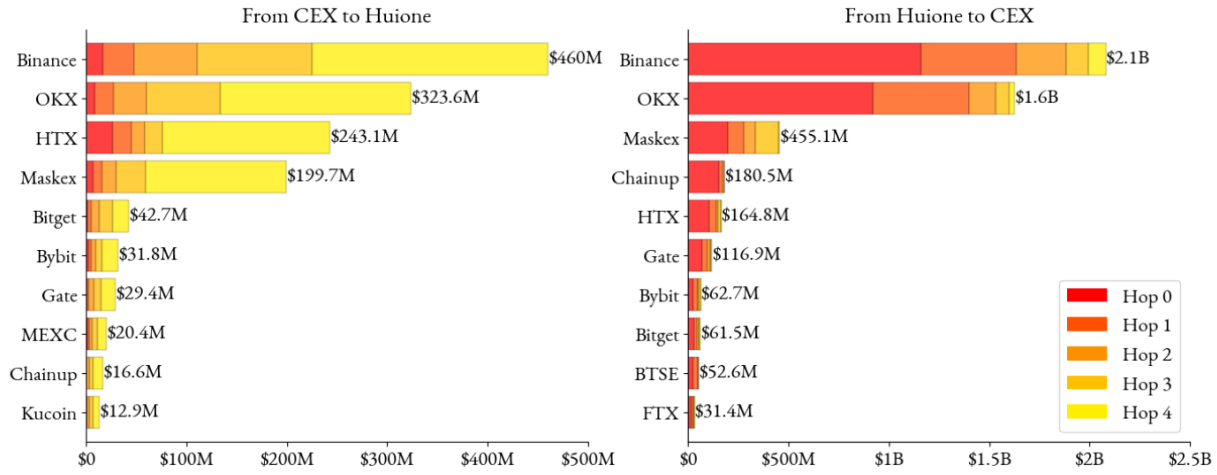


Figure 7. Clustered Tainted Inflows Across Blockchains

This figure reports clustered tainted inflows across Bitcoin, Ethereum, and Tron. Clusters are constructed using the common-input heuristic on Bitcoin and deposit-address clustering based on shared senders on Ethereum and Tron, starting from seed depositor or deposit addresses that receive at least $50,000 in traced tainted inflows. Panel A plots exchanges by two dimensions of tainted exposure: the share of lifetime inflows that are tainted on the horizontal axis and the total dollar amount of clustered tainted inflows on the vertical axis. Bubble size is proportional to the number of transactions. Bitcoin exchanges are shown in gold on the left plot, Tron exchanges in red on the right plot, and Ethereum exchanges as pie charts subdivided by token on the center plot. Exchanges marked with an asterisk are Western exchanges. Panel A is restricted to exchanges with more than $1 billion in clustered tainted inflows summed across the three blockchains. Panel B reports monthly clustered tainted inflows by cryptocurrency composition, with the red line showing total monthly inflows and the bars on the right reporting cumulative totals by blockchain.

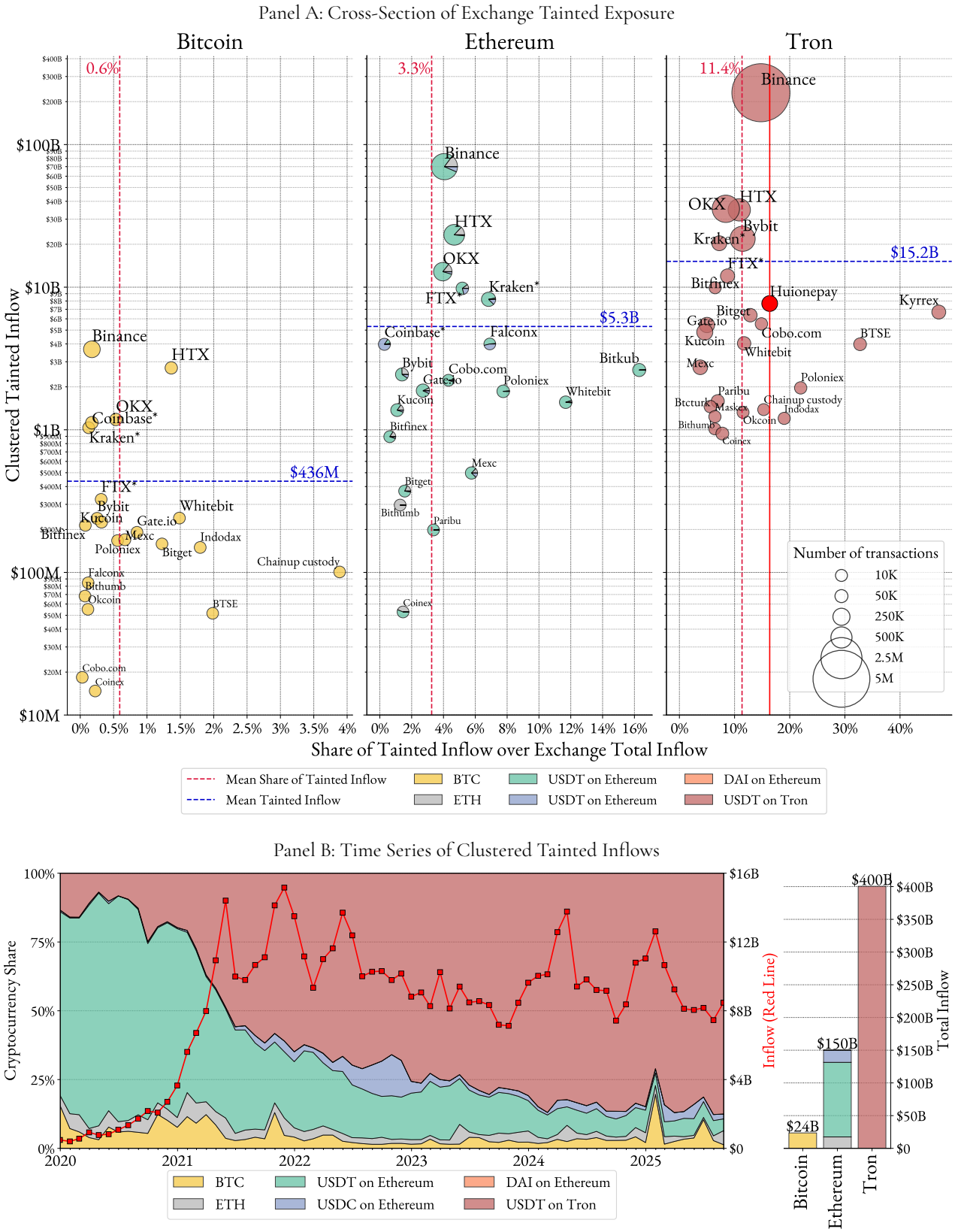


Figure 8. Top 20 Feature Families in Tainted Address Prediction on Ethereum

This figure shows the SHAP summary plot for the top 20 feature families in the Ethereum tainted-address prediction model. The model is trained on positively labeled deposit addresses identified through tracing and deposit-address clustering, where the clustering procedure begins from seed deposit addresses that receive at least $50,000 in traced tainted inflows. The model includes 270 features grouped into 28 families, and family importance is computed by summing the average absolute SHAP values of all features within each family. The families are ranked by this aggregate measure, with the final row combining the remaining eight lower-ranked families. SHAP values measure each feature family's contribution to the model output relative to the baseline, where positive SHAP values indicate that the feature increases the model-predicted likelihood that an address is flagged as tainted. Each point represents an observation. Color indicates the underlying feature value, with blue denoting low values and red denoting high values.



Figure 9. Individual Feature Effects in Tainted Address Prediction on Ethereum

This figure shows SHAP dependence plots for twelve important individual features in the Ethereum tainted-address prediction model. The model is trained on positively labeled deposit addresses identified through tracing and deposit-address clustering, where the clustering procedure begins from seed deposit addresses that receive at least $50,000 in traced tainted inflows. SHAP values quantify the contribution of a given feature to the model's prediction relative to the baseline prediction: positive SHAP values indicate that the feature increases the predicted outcome. Each panel is a scatter plot constructed from a random sample of 50,000 observations, where each dot represents one observation with its feature value on the x-axis and the corresponding SHAP value on the y-axis. The gray bars in the background show the distribution of the feature values. The panels are ordered by global feature importance.

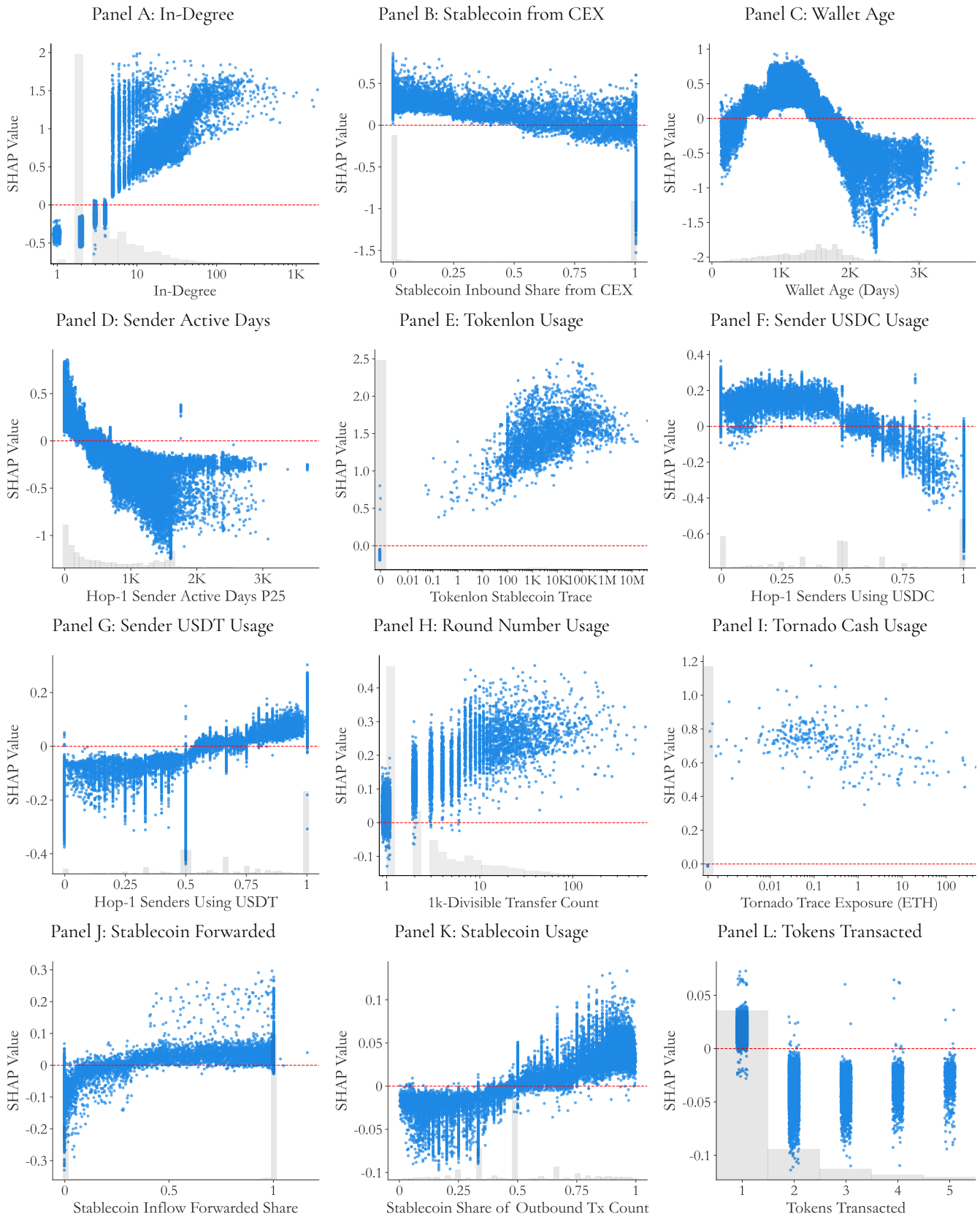


Figure 10. Top 20 Feature Families in Tainted Address Classification on Tron

This figure shows the SHAP summary plot for the top 20 feature families in the Tron tainted-address prediction model. The model is trained on positively labeled deposit addresses identified through tracing and deposit-address clustering, where the clustering procedure begins from seed deposit addresses that receive at least $50,000 in traced tainted inflows. The model includes 219 features grouped into 27 families, and family importance is computed by summing the average absolute SHAP values of all features within each family. The families are ranked by this aggregate measure, with the final row combining the remaining eight lower-ranked families. SHAP values measure each feature family's contribution to the model output relative to the baseline, where positive SHAP values indicate that the feature increases the model-predicted likelihood that an address is flagged as tainted. Each point represents an observation. Color indicates the underlying feature value, with blue denoting low values and red denoting high values.

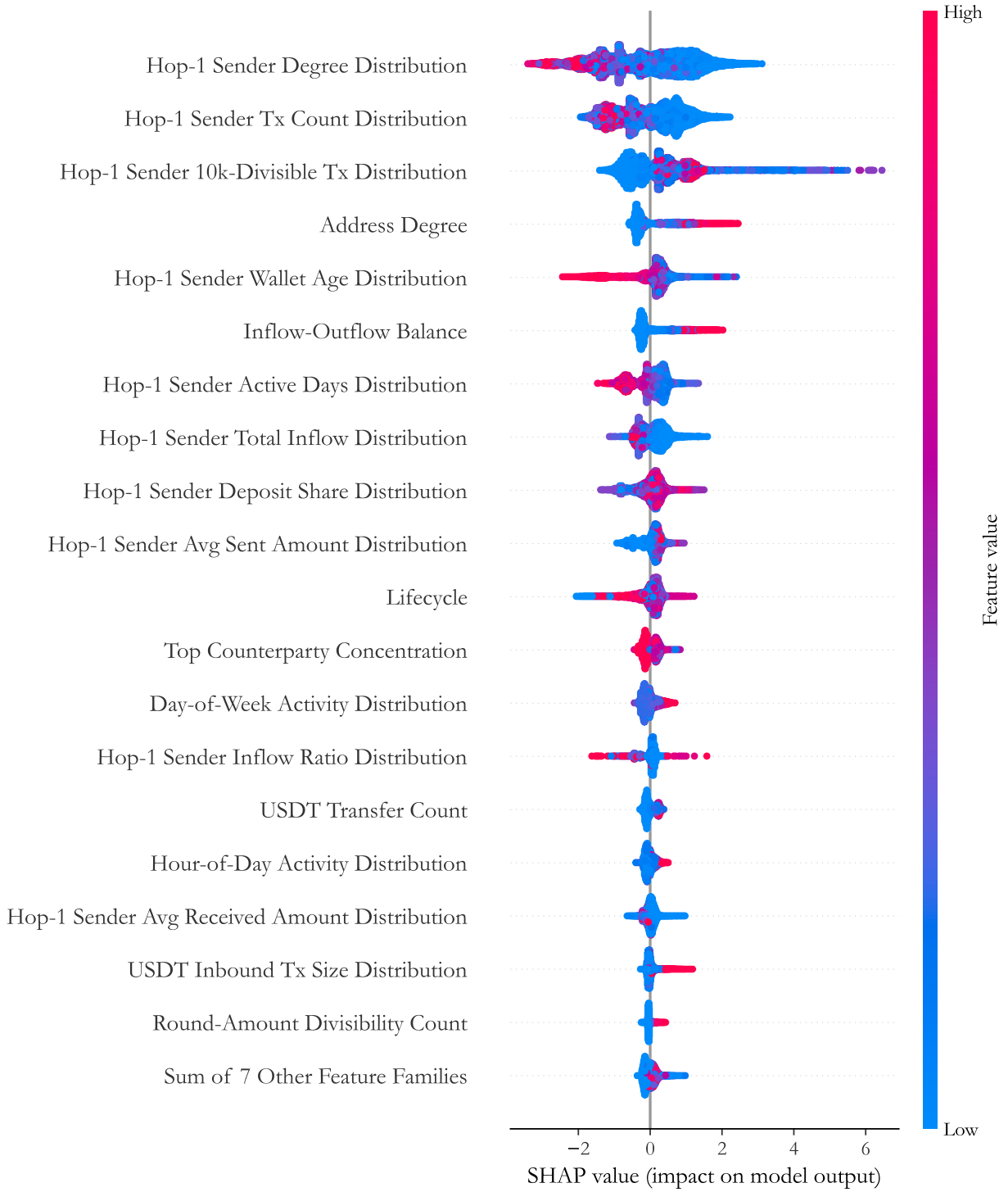


Figure 11. Tainted Flows by Identification Method

TThis figure presents monthly estimates of tainted crypto inflows identified by four methods: 1) direct inflows to victim-reported addresses, 2) additional inflows to deposit addresses with at least $50,000 in traced tainted inflows, 3) inflows to additional deposit addresses identified through deposit-address clustering, and 4) additional tainted inflows to unflagged deposit addresses identified by machine learning. Panel A reports estimates for Ethereum, and Panel B reports estimates for Tron. In each panel, the shaded areas plot monthly inflows attributable to each method, while the dashed red line traces cumulative tainted inflows over time. Deposit-address clustering begin from seed deposit addresses that receive at least $50,000 in traced tainted inflows, and the machine-learning model is trained on positive labels identified under the same threshold. Machine-learning-implied tainted flows are computed as the product of the predicted probability that a deposit address is tainted, the predicted fraction of inflows that are tainted conditional on taint, and the address's observed monthly inflows. The bars on the right side of each panel report cumulative totals by method and in aggregate over the full sample period.

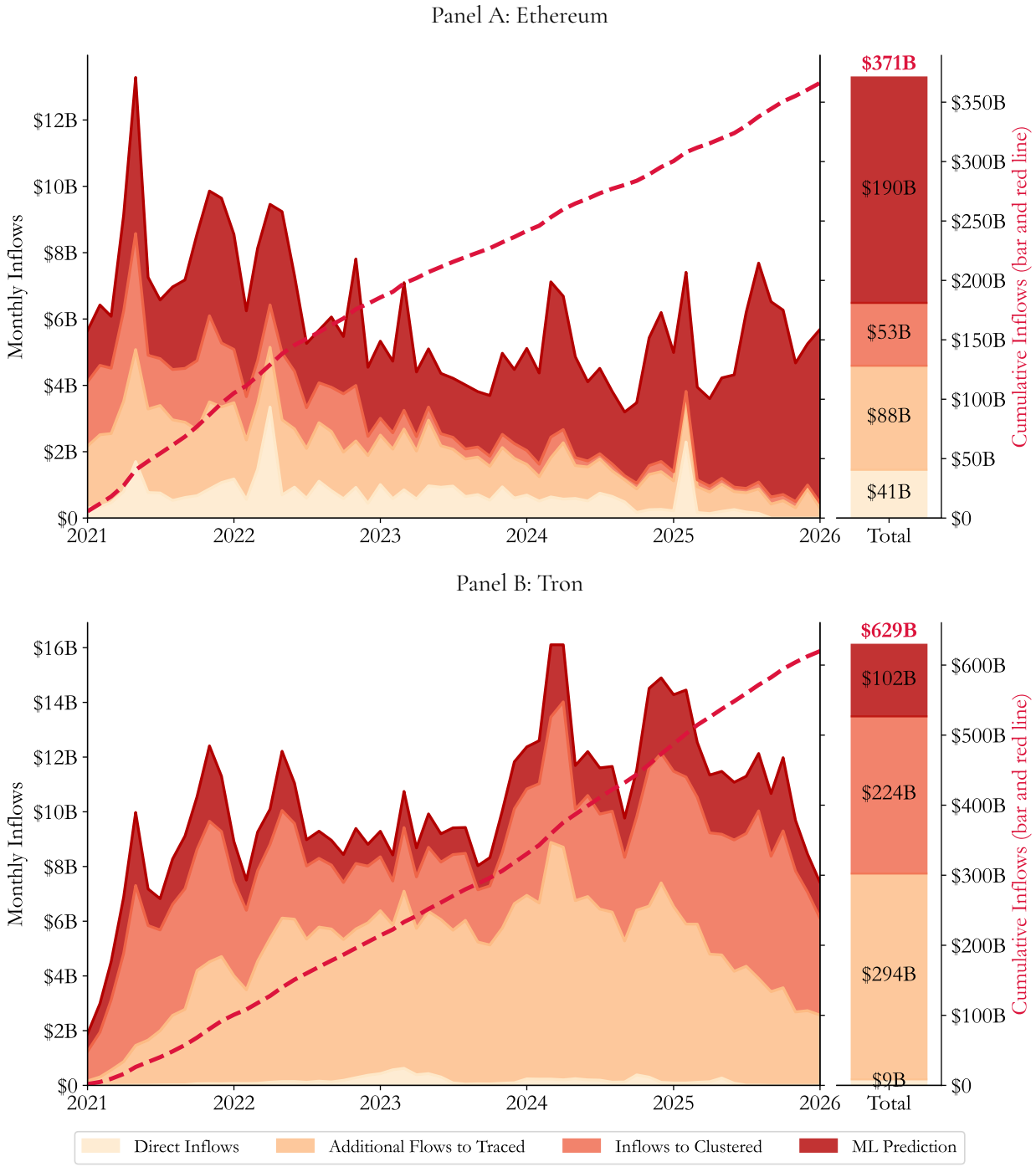


Table 1. Summary Statistics of Reports and Reported Addresses

This table reports summary statistics on the number of reports and addresses by scam category and by blockchain. The leftmost column first groups the data by scam type and then reports the corresponding totals by blockchain. Column (1) reports the total number of reports. Column (2) reports the total number of reported addresses after removing duplicate addresses, since the same address may appear in multiple categories. Column (3) reports the number of unique reported addresses that satisfy our tracing criteria. Column (4) adds Bitcoin addresses identified through common-input clustering for the Bitcoin addresses in Column (3). Column (5) reports the total inflows to the addresses in Column (4).

	(1)	(2)	(3)	(4)	(5)
Category	Total Reports	Reported Addresses	Addresses Meeting Tracing Criteria	Addresses Including Bitcoin Clusters	Total Inflow
Pig Butchering	32,819	25,667	14,279	67,364	$21.99B
Stolen Funds	12,376	11,596	9,478	18,718	$13.72B
Sanctioned	2,227	2,000	1,603	4,119	$9.54B
Phishing	250,392	219,940	171,703	191,743	$7.44B
Illicit Actor	10,371	9,361	6,939	32,228	$6.07B
Rug Pull	144,687	144,629	143,369	143,369	$5.95B
Impersonation	17,880	12,200	7,016	36,522	$3.47B
Fake Returns	15,995	10,360	5,970	48,084	$2.8B
Fake Project	7,196	5,512	2,492	8,085	$1.25B
Ransomware	12,778	12,333	1,814	7,685	$943.22M
Extortion	213,045	55,412	6,533	20,641	$931.18M
Sim Swap	1,766	1,234	663	2,162	$120.94M
Airdrop	8,402	1,847	969	2,227	$79.62M
Donation Scam	640	450	188	723	$6.37M
Other Scam	39,439	39,439	36,556	150,773	$3.67B
Bitcoin	323,362	145,296	65,160	390,031	$26.17B
Ethereum	434,650	395,826	337,802	337,802	$43.13B
Tron	12,001	10,858	6,610	6,610	$8.68B
Total	770,013	551,980	409,572	734,443	$77.97B

Table 2. Summary Statistics of Total Inflows to Reported Addresses

This table reports summary statistics for the total dollar inflows to reported addresses by scam category. Panel A presents Ethereum, and Panel B presents Tron. The address count N corresponds to Column (4) of Table 1, and total inflow corresponds to Column (5). For each category, the table reports total inflow, the mean, the standard deviation, and the 25th, 50th, and 75th percentiles. Categories are sorted by total inflow within each blockchain.

Panel A: Ethereum

Category	N	Total Inflow	Mean	Std	25%	50%	75%
Pig Butchering	7,058	$12.55B	$1.78M	$16.54M	$17.62K	$142.81K	$826.25K
Stolen Funds	4,780	$9.59B	$2.01M	$34.20M	$4.48K	$47.29K	$286.35K
Rug Pull	143,369	$5.95B	$41.47K	$246.67K	$5.58K	$9.32K	$22.4K
Phishing	168,560	$5.72B	$33.93K	$1.58M	$1.01	$3.01	$32.02
Illicit Actor	2,583	$5.51B	$2.13M	$21.24M	$2.05K	$26.88K	$421.77K
Fake Project	1,779	$899.97M	$505.89K	$3.48M	$540.17	$18.74K	$160.85K
Sanctioned	155	$265.99M	$1.72M	$4.33M	$1.98K	$112.39K	$724.87K
Fake Returns	1,121	$222.60M	$198.57K	$1.25M	$469.13	$4.09K	$41.85K
Impersonation	1,210	$191.74M	$158.46K	$1.67M	$389.31	$3.95K	$21.14K
Extortion	131	$118.51M	$904.63K	$7.69M	$1.03K	$7.98K	$45.63K
Sim Swap	398	$69.37M	$174.31K	$652.84K	$1.24K	$11.88K	$58.31K
Airdrop	139	$50.49M	$363.22K	$3.59M	$283.00	$2.15K	$14.04K
Ransomware	119	$12.98M	$109.04K	$269.64K	$1.77K	$15.70K	$95.50K
Donation Scam	23	$183.89K	$8.00K	$18.24K	$77.06	$352.66	$8.98K
Other Scam	6,377	$1.99B	$311.43K	$2.24M	$577.96	$5.30K	$49.69K
Total	337,802	$43.13B	$127.68K	$5.23M	$3.01	$2.92K	$11.29K

Panel B: Tron

Category	N	Total Inflow	Mean	Std	25%	50%	75%
Sanctioned	635	$6.34B	$9.98M	$54.55M	$11.45K	$98.34K	$1.76M
Pig Butchering	1,504	$992.63M	$659.99K	$10.00M	$12.29K	$62.96K	$217.42K
Stolen Funds	923	$599.53M	$649.55K	$2.92M	$17.96K	$109.16K	$272.05K
Illicit Actor	766	$173.20M	$226.11K	$637.39K	$15.68K	$52.53K	$182.27K
Fake Project	87	$35.6M	$409.19K	$917.35K	$2.73K	$6.17K	$93.25K
Phishing	80	$31.98M	$399.69K	$1.03M	$1.03K	$22.36K	$133.89K
Fake Returns	203	$24.61M	$121.25K	$602.59K	$1.26K	$8.02K	$36.36K
Impersonation	77	$9.27M	$120.45K	$449.07K	$646.11	$5.00K	$30.88K
Ransomware	12	$8.20M	$683.12K	$2.31M	$2.52K	$8.65K	$20.17K
Sim Swap	8	$4.76M	$595.57K	$1.12M	$16.04K	$67.28K	$495.68K
Airdrop	4	$647.07K	$161.77K	$315.2K	$3.38K	$6.26K	$164.65K
Extortion	9	$388.75K	$43.19K	$76.52K	$1.43K	$14.56K	$32.86K
Donation Scam	2	$85.63K	$42.82K	$60.17K	$21.54K	$42.82K	$64.09K
Other Scam	2,300	$455.01M	$197.83K	$1.94M	$3.03K	$13.02K	$57.36K
Total	6,610	$8.68B	$1.31M	$17.85M	$6.10K	$32.95K	$175.51K

Table 3. Summary Statistics of Transaction Counts for Reported Addresses

This table reports summary statistics for the number of transactions of reported addresses by scam category. Panel A presents Ethereum, and Panel B presents Tron. For each category, the table reports the number of addresses (N), the total number of transactions, the mean, the standard deviation, and the 25th, 50th, and 75th percentiles of address-level transaction counts. Categories are sorted by total number of transactions within each blockchain.

Panel A: Ethereum							
Category	N	Total Transactions	Mean	Std	25%	50%	75%
Rug Pull	143,369	1.10M	7.70	30.05	2.00	3.00	5.00
Phishing	168,560	955.38K	5.67	27.99	2.00	2.00	4.00
Pig Butchering	7,058	695.96K	98.61	180.77	8.00	31.00	108.00
Fake Project	1,779	78.00K	43.85	120.35	2.00	7.00	29.00
Illicit Actor	2,583	76.20K	29.50	167.57	1.00	2.00	9.00
Fake Returns	1,121	64.31K	57.36	178.48	2.00	7.00	33.00
Stolen Funds	4,780	57.44K	12.02	49.68	1.00	3.00	7.00
Impersonation	1,210	30.63K	25.32	78.81	2.00	4.00	14.00
Sim Swap	398	16.62K	41.77	109.21	2.00	7.00	28.00
Airdrop	139	4.95K	35.60	172.37	1.00	5.00	14.00
Extortion	131	3.77K	28.74	55.35	3.00	9.00	24.00
Ransomware	119	3.63K	30.50	74.59	2.50	10.00	22.50
Sanctioned	155	2.33K	15.00	42.95	2.00	5.00	7.00
Donation Scam	23	343.00	14.91	22.92	1.00	3.00	19.50
Other Scam	6,377	903.34K	141.66	5.90K	3.00	9.00	28.00
Total	337,802	4.00M	11.83	812.27	2.00	3.00	5.00
Panel B: Tron							
Category	N	Total Transactions	Mean	Std	25%	50%	75%
Sanctioned	635	268.31K	422.54	1.83K	6.00	35.00	184.50
Illicit Actor	766	191.81K	250.41	251.17	57.25	162.00	363.75
Pigbutchering	1,504	129.07K	85.82	134.41	7.00	32.00	104.25
Stolen Funds	923	19.19K	20.79	65.48	1.00	3.00	9.00
Fake Returns	203	14.49K	71.38	119.63	5.00	18.00	67.50
Impersonation	77	5.10K	66.18	164.14	3.00	11.00	43.00
Fake Project	87	4.69K	53.91	175.78	5.50	12.00	29.00
Phishing	80	4.46K	55.79	83.14	3.00	9.50	93.00
Sim Swap	8	716.00	89.50	93.67	12.25	71.00	124.50
Extortion	9	615.00	68.33	79.53	9.00	44.00	76.00
Ransomware	12	570.00	47.50	74.73	15.75	28.50	40.75
Airdrop	4	89.00	22.25	21.64	7.75	19.00	33.50
Donation Scam	2	47.00	23.50	31.82	12.25	23.50	34.75
Other Scam	2,300	153.61K	66.79	100.61	11.00	32.00	81.00
Total	6,610	792.77K	119.93	592.14	6.00	29.00	101.75

Table 4. Summary Statistics of Ethereum Deposit Address Features

This table reports summary statistics for selected Ethereum deposit-address features used in the machine-learning models. Panel A presents positively labeled deposit addresses identified through tracing and deposit-address clustering. To define the machine-learning sample, we restrict attention to deposit addresses that are not contracts, have fewer than 2,000 transactions, and transact in at most five tokens. Panel B presents unlabeled deposit addresses that satisfy the same sample restrictions but are not identified as tainted.

Panel A: Positively-labeled Deposit Addresses						
Feature Name	count	mean	std	25%	50%	75%
Transaction Count	357,422	37.61	106.92	3.00	6.00	27.00
Total Inflow ($)	357,422	1,038,100	26,971,532	505.00	4,299	51,926
Total Outflow ($)	357,422	1,046,331	27,008,789	487.00	4,260	51,865
Average Transaction Size ($)	357,422	14,418	239,898	96.00	523.00	2,859
Days Active	357,422	379.46	483.53	0.00	158.00	646.00
In Degree	357,422	8.32	26.05	1.00	2.00	7.00
Out Degree	357,422	2.68	4.10	1.00	2.00	3.00
Num 1k Divisible	357,422	2.22	12.43	0.00	0.00	0.00
Num 10k Divisible	357,422	1.12	8.16	0.00	0.00	0.00
Num 50k Divisible	357,422	0.53	5.31	0.00	0.00	0.00
Hop1 Senders Active Days Avg	357,422	714.73	536.76	229.80	700.50	1,095
Hop1 Frac Senders Use USDC	357,422	0.29	0.34	0.00	0.15	0.50
Hop1 Frac Senders Use Tether	357,422	0.58	0.40	0.14	0.67	1.00
Stablecoin Received Share from CEX	357,422	0.08	0.22	0.00	0.00	0.00
Stablecoin Sent Share from DEX	357,422	0.00	0.01	0.00	0.00	0.00
Tokenlon Stablecoin Trace ($)	357,422	10,055	200,236	0.00	0.00	0.00
Tornado Trace ETH	357,422	0.10	8.14	0.00	0.00	0.00
Panel B: Un-labeled Deposit Addresses						
Feature Name	count	mean	std	25%	50%	75%
Transaction Count	58,336,859	7.82	25.67	3.00	4.00	6.00
Total Inflow ($)	58,336,859	41,836	5,465,888	57.00	335.00	2,048
Total Outflow ($)	58,336,859	42,160	5,501,209	40.00	300.00	2,012
Average Transaction Size ($)	58,336,859	5,219	303,028	12.00	77.00	376.00
Days Active	58,336,859	301.53	471.32	0.00	83.00	398.00
In Degree	58,336,859	2.23	3.63	1.00	2.00	2.00
Out Degree	58,336,859	2.10	1.58	1.00	2.00	3.00
Num 1k Divisible	58,336,859	0.08	1.29	0.00	0.00	0.00
Num 10k Divisible	58,336,859	0.02	0.77	0.00	0.00	0.00
Num 50k Divisible	58,336,859	0.01	0.51	0.00	0.00	0.00
Hop1 Senders Active Days Avg	58,336,859	1,231	785.67	618.00	1,300	1,656
Hop1 Frac Senders Use USDC	58,336,859	0.42	0.42	0.00	0.50	1.00
Hop1 Frac Senders Use Tether	58,336,859	0.51	0.43	0.00	0.50	1.00
Stablecoin Received Share from CEX	58,336,859	0.42	0.48	0.00	0.00	1.00
Stablecoin Sent Share from DEX	58,336,859	0.00	0.01	0.00	0.00	0.00
Tokenlon Stablecoin Trace ($)	58,336,859	26.87	6,904	0.00	0.00	0.00
Tornado Trace ETH	58,336,859	0.01	3.18	0.00	0.00	0.00

Table 5. Summary Statistics of Tron Deposit Addresses Features

This table reports summary statistics for a subset of Tron deposit-address features used in the machine-learning models. Panel A presents positively labeled deposit addresses identified through tracing and deposit-address clustering. To define the machine-learning sample, we restrict attention to deposit addresses that have fewer than 2,000 transactions. Panel B presents unlabeled deposit addresses that satisfy the same sample restrictions but are not identified as tainted.

Panel A: Positively-labeled Deposit Addresses						
Feature Name	count	mean	std	25%	50%	75%
Transaction Count	852,344	122.22	235.01	8.00	33.00	120.00
Total Inflow ($)	852,344	937,846	113,945,771	2,503	22,480	161,632
Total Outflow ($)	852,344	933,019	109,531,931	2,500	22,510	161,819
Average Transaction Size ($)	852,344	7,523	284,111	159.00	526.00	2,116
Days Active	852,344	404.96	387.42	80.00	288.00	645.00
In Degree	852,344	19.26	41.94	2.00	7.00	19.00
Out Degree	852,344	1.99	1.62	1.00	1.00	2.00
Num 1k Divisible	852,344	14.27	53.41	0.00	1.00	8.00
Num 10k Divisible	852,344	5.09	29.94	0.00	0.00	0.00
Num 50k Divisible	852,344	1.61	16.53	0.00	0.00	0.00
Hop1 Senders Indegree Avg	852,344	259,036	403,064	220.00	61,704	373,407
Hop1 Senders Tx Count Avg	852,344	4,501,579	6,568,723	8,019	1,463,452	6,501,084
Hop1 Senders Wallet Age Days Avg	852,344	1,039	391.85	743.50	1,042	1,312
Hop1 Senders Total Inflow Avg ($B)	852,344	16.92	29.15	0.013	4.10	21.23
Hop1 Senders Active Days Avg	852,344	541.52	312.80	315.00	515.24	733.00
Hop1 Senders USDT Avg Sent Avg ($)	852,344	21,926	124,524	2,261	6,060	18,648
Panel B: Un-labeled Deposit Addresses						
Feature Name	count	mean	std	25%	50%	75%
Transaction Count	68,357,262	12.88	45.55	2.00	3.00	8.00
Total Inflow ($)	68,357,262	25,272	6,785,982	117.00	501.00	2,432
Total Outflow ($)	68,357,262	25,258	6,785,099	116.00	500.00	2,423
Average Transaction Size ($)	68,357,262	920.00	63,143	42.00	117.00	380.00
Days Active	68,357,262	166.67	272.75	0.00	27.00	233.00
In Degree	68,357,262	2.70	6.06	1.00	1.00	3.00
Out Degree	68,357,262	1.17	0.61	1.00	1.00	1.00
Num 1k Divisible	68,357,262	0.51	6.31	0.00	0.00	0.00
Num 10k Divisible	68,357,262	0.10	2.98	0.00	0.00	0.00
Num 50k Divisible	68,357,262	0.02	1.53	0.00	0.00	0.00
Hop1 Senders Indegree Avg	68,357,262	808,484	1,044,095	5,784	318,926	1,294,778
Hop1 Senders Tx Count Avg	68,357,262	12,432,686	14,493,667	188,948	5,923,496	20,416,895
Hop1 Senders Wallet Age Days Avg	68,357,262	1,392	546.55	964.50	1,437.50	1,818
Hop1 Senders Total Inflow Avg ($B)	68,357,262	55.83	76.24	122.89	21.88	88.73
Hop1 Senders Active Days Avg	68,357,262	935.71	582.26	479.50	874.50	1,322.67
Hop1 Senders USDT Avg Sent Avg ($)	68,357,262	21,933	187,019	1,377	3,295	9,266

For Online Publication

Internet Appendix for "Is Criminal Crypto a Sideshow?"

Table IA.1. Scam Definitions

This table reports the definitions of the scam categories used to classify victim reports in the paper.

Type	Description
Airdrop	Unsolicited mass distribution of a cryptocurrency token to direct investors to a malicious website
Donation Scam	Posing as charities to exploit donors
Extortion	Using intimidation to force someone to pay money under the threat of releasing sensitive information
Fake Project	Pretending to build a fake project only to abandon the project after attracting investors, such as exit scams
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
Illicit Actors	Wallets of known illicit entities, including state and non-state actors, for uses like money laundering or illegal drug sales
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
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
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
Ransomware	Malware that encrypts the victim's files, or pretending to lock files, and demanding a ransom payment to decrypt them
Rug Pull	An exit scam which explicitly utilizes the DeFi ecosystem to create a token only to later steal its liquidity
Sanctioned	Wallets of known sanctioned entities, including state and non-state actors, for uses like terrorism financing or software exploits
Sim Swap	Convincing a mobile carrier to port a victim's phone number to their SIM card to gain access to sensitive accounts
Stolen Funds	Wallets of known hackers targeting DeFi by performing contract exploits to steal crypto
Other Scam	Miscellaneous scams with little report information or fuzzy characteristics

Table IA.2. GPT Prompt for Classification of Victim Reports

This table reproduces the system prompt supplied to the fine-tuned GPT-4o-mini model (`gpt-4o-mini-2024-07-18`) used to classify each victim report into one of 12 scam categories. The model receives this system prompt together with the free-text victim report as the user message and is required to return a single letter (A–K or Z).

```
You are a US federal law enforcement agent investigating cryptocurrency scams. Read the
user's crime report and classify it into exactly ONE category below.

Output format rule (strict):
- Reply with EXACTLY ONE character: A,B,C,D,E,F,G,H,I,J,K, or Z.
- Do NOT output words, punctuation, explanations, or multiple characters.

Categories:
A - AIRDROP: [FRAUD] Unsolicited mass distribution of a cryptocurrency token to direct
    investors to a malicious website;
B - RANSOMWARE: [BLACKMAIL] Malware that encrypts the victim's files, or pretending to
    lock files, and demanding a ransom payment to decrypt them;
C - CONTRACT_EXPLOIT: [HACK] Exploiting vulnerabilities in a smart contract or other
    protocols to drain funds;
D - DONATION_SCAM: [FRAUD] Posing as charities to exploit donors;
E - EXTORTION: [BLACKMAIL] Using intimidation to force someone to pay money under the
    threat of releasing sensitive information;
F - FAKE_RETURNS: [FRAUD] 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;
G - PIGBUTCHERING: [FRAUD] 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;
H - PHISHING: [FRAUD] Tricking individuals into providing personal information, such as
    login information, often by driving traffic to a malicious website to gain access
    ↪ to
    wallets and secret keys;
I - IMPERSONATION: [FRAUD] 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;
J - SIM_SWAP: [HACK] Convincing a mobile carrier to port a victim's phone number to
    their SIM card to gain access to sensitive accounts;
K - FAKE_PROJECT: [FRAUD] Pretending to build a fake project only to abandon the
↪   project
    after attracting investors, such as rug pulls or exit scams;
Z - OTHER/UNCLEAR: Not enough info or doesn't fit.
```

Figure IA.1. Clustered Tainted Inflows: $10,000 Min Traced Tainted Inflow Threshold

This figure reports clustered tainted inflows across Bitcoin, Ethereum, and Tron. Clusters are constructed using the common-input heuristic on Bitcoin and deposit-address clustering based on shared senders on Ethereum and Tron, starting from seed depositor or deposit addresses that receive at least $10,000 in traced tainted inflows. It plots exchanges by two dimensions of tainted exposure: the share of lifetime inflows that are tainted on the horizontal axis and the total dollar amount of clustered tainted inflows on the vertical axis. Bubble size is proportional to the number of transactions. Bitcoin exchanges are shown in gold on the left plot, Tron exchanges in red on the right plot, and Ethereum exchanges as pie charts subdivided by token on the center plot. Exchanges marked with an asterisk are Western exchanges. Panel A is restricted to exchanges with more than $1 billion in clustered tainted inflows summed across the three blockchains.

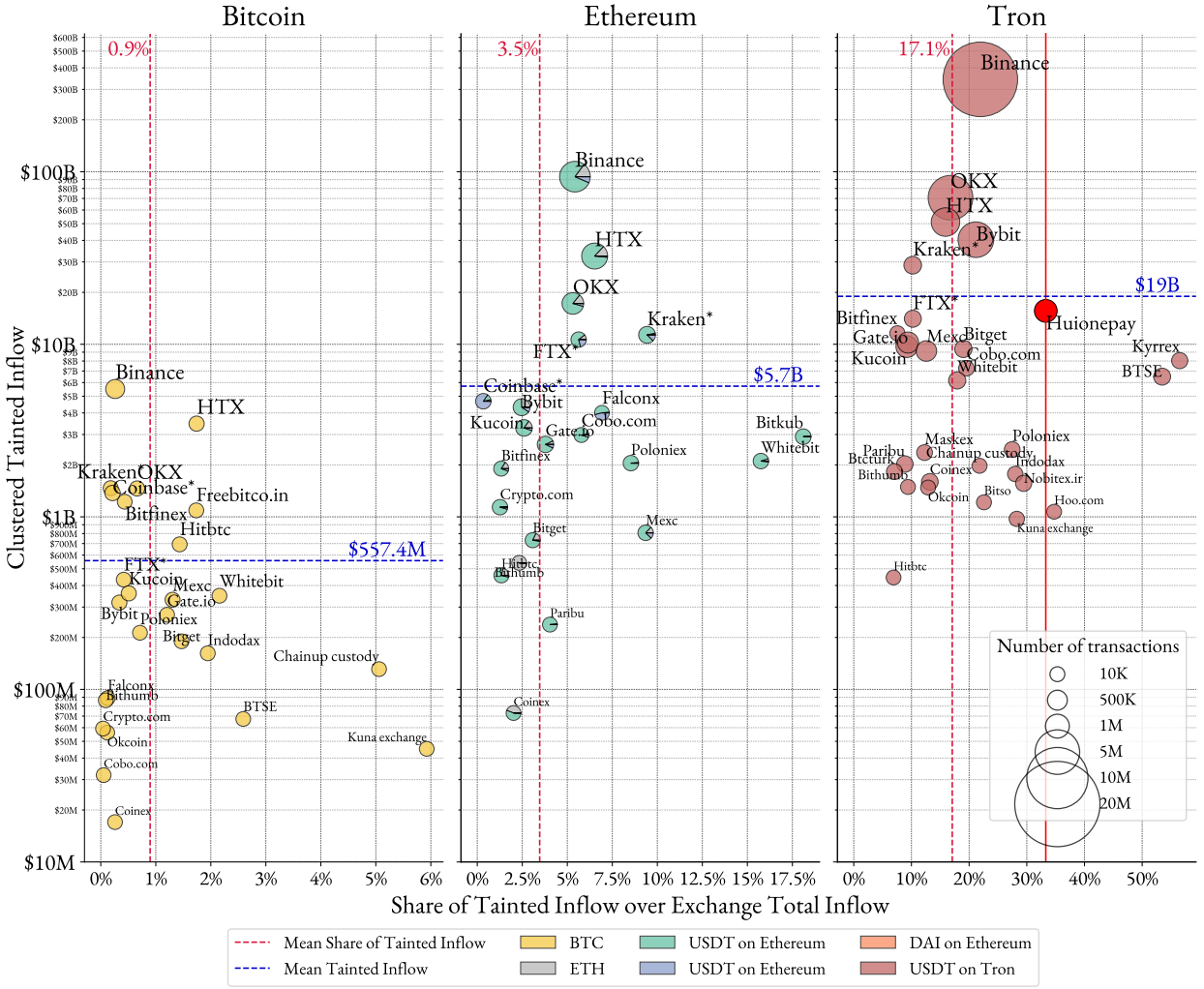


Figure IA.2. Clustered Tainted Inflows: $100,000 Min Traced Tainted Inflow Threshold

This figure reports clustered tainted inflows across Bitcoin, Ethereum, and Tron. Clusters are constructed using the common-input heuristic on Bitcoin and deposit-address clustering based on shared senders on Ethereum and Tron, starting from seed depositor or deposit addresses that receive at least $100,000 in traced tainted inflows. It plots exchanges by two dimensions of tainted exposure: the share of lifetime inflows that are tainted on the horizontal axis and the total dollar amount of clustered tainted inflows on the vertical axis. Bubble size is proportional to the number of transactions. Bitcoin exchanges are shown in gold on the left plot, Tron exchanges in red on the right plot, and Ethereum exchanges as pie charts subdivided by token on the center plot. Exchanges marked with an asterisk are Western exchanges. Panel A is restricted to exchanges with more than $1 billion in clustered tainted inflows summed across the three blockchains.

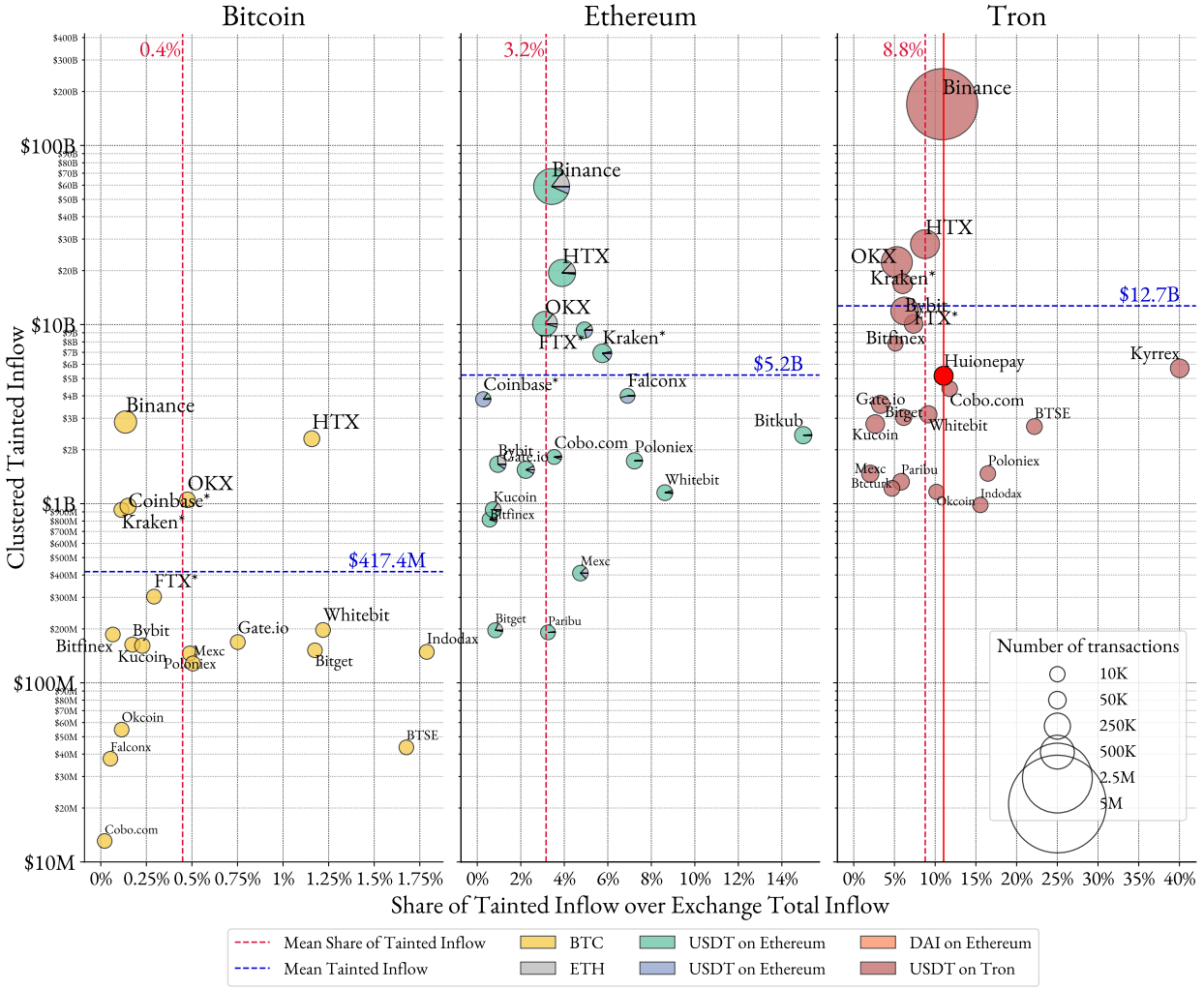


Figure IA.3. Top 20 Feature Families on Ethereum: $100,000 Clustering Threshold

This figure shows the SHAP summary plot for the top 20 feature families in the Ethereum tainted-address prediction model. The model is trained on positively labeled deposit addresses identified through tracing and deposit-address clustering, where the clustering procedure begins from seed deposit addresses that receive at least $100,000 in traced tainted inflows. The model includes 270 features grouped into 28 families, and family importance is computed by summing the average absolute SHAP values of all features within each family. The families are ranked by this aggregate measure, with the final row combining the remaining eight lower-ranked families. SHAP values measure each feature family's contribution to the model output relative to the baseline, where positive SHAP values indicate that the feature increases the model-predicted likelihood that an address is flagged as tainted. Each point represents an observation. Color indicates the underlying feature value, with blue denoting low values and red denoting high values.

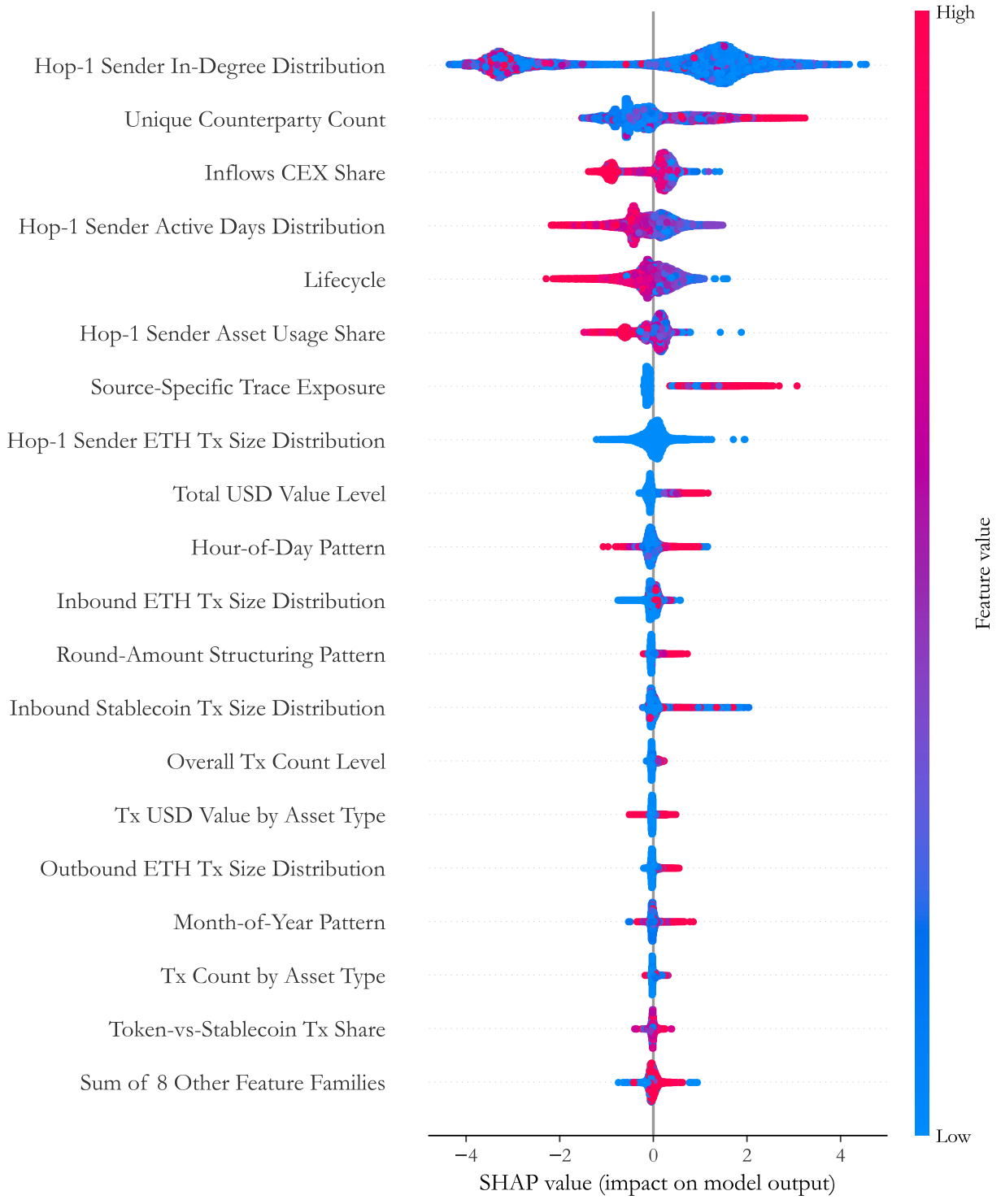


Figure IA.4. Individual Feature Effects on Ethereum: $100,000 Clustering Threshold

This figure shows SHAP dependence plots for twelve important individual features in the Ethereum tainted-address prediction model. The model is trained on positively labeled deposit addresses identified through tracing and deposit-address clustering, where the clustering procedure begins from seed deposit addresses that receive at least $100,000 in traced tainted inflows. SHAP values quantify the contribution of a given feature to the model's prediction relative to the baseline prediction: positive SHAP values indicate that the feature increases the predicted outcome. Each panel is a scatter plot constructed from a random sample of 50,000 observations, where each dot represents one observation with its feature value on the x-axis and the corresponding SHAP value on the y-axis. The gray bars in the background show the distribution of the feature values. The panels are ordered by global feature importance.

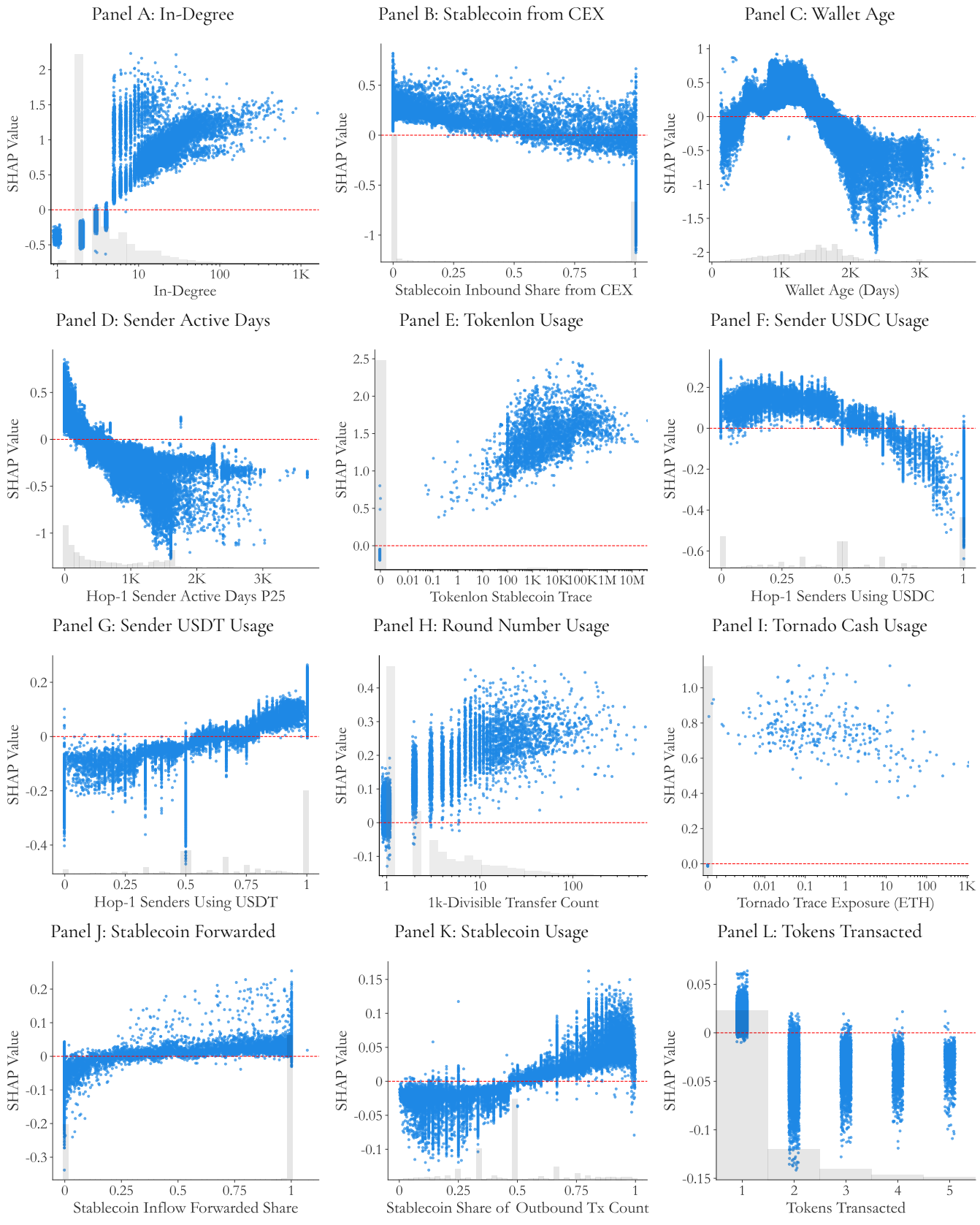


Figure IA.5. Tainted Flows by Identification Method: $100,000 Clustering Threshold

This figure presents monthly estimates of tainted crypto inflows identified by four methods: 1) direct inflows to victim-reported addresses, 2) additional inflows to deposit addresses with at least $100,000 in traced tainted inflows, 3) inflows to additional deposit addresses identified through deposit-address clustering, and 4) additional tainted inflows to unflagged deposit addresses identified by machine learning. Panel A reports estimates for Ethereum, and Panel B reports estimates for Tron. In each panel, the shaded areas plot monthly inflows attributable to each method, while the dashed red line traces cumulative tainted inflows over time. Deposit-address clustering begin from seed deposit addresses that receive at least $100,000 in traced tainted inflows, and the machine-learning model is trained on positive labels identified under the same threshold. Machine-learning-implied tainted flows are computed as the product of the predicted probability that a deposit address is tainted, the predicted fraction of inflows that are tainted conditional on taint, and the address's observed monthly inflows. The bars on the right side of each panel report cumulative totals by method and in aggregate over the full sample period.

