How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering*

John M. Griffin†, Kevin Mei‡

Abstract

Through blockchain addresses, we trace crypto flows and uncover methods commonly used by scammers to obfuscate their activities. The perpetrators interact freely with major crypto exchanges, sending over 98,000 small trust-building inducement payments annually to exchanges commonly used by U.S. and European investors. Funds exit the Ethereum network in large quantities, mostly in Tether, through less transparent but large exchanges. Criminal enterprises pay approximately 33 basis points in transaction fees and moved $27.8 billion annually into suspicious exchange deposit accounts between 2021-2023, including $5.6 billion annually sent from Western exchanges. Our findings highlight how many actors in the "reputable" crypto industry facilitate criminal capital flows.

JEL classification: G23, G28, G59
Keywords: Crypto, Money laundering, Illicit financial flows

*This paper is dedicated to all pig butchering victims, those defrauded and those enslaved, and especially the victim who provided the impetus to write this paper. We are thankful for helpful comments from Will Cong, David Dicks, Gleb Domnenko, Cesare Fracassi, Campbell Harvey, Zhiguo He, Sophia Hu, Brandon Kirst, Samuel Kruger, Katya Malinova (discussant), Alex Pettyjohn, Alex Priest, Marius Ring, Amin Shams, Michael Sockin, Josh White, Chishen Wei, Qinxi Wu, and seminar participants at Baylor University, the Crypto and Blockchain Economics and Research forum, Integra FEC, the University of Rochester, the University of Texas-Austin, and the University of Texas-Dallas. We thank Juan Antonio Artero Calvo, other research assistants, and especially Joseph Newcomer for excellent programming assistance. We thank Jan Santiago, Raymond Hantho, Chainbrium, and the United States Institute of Peace (USIP) for providing addresses collected as part of a USIP whitepaper. We further thank Integra FEC for use of their tracing tools and for substantial crypto-research support. Griffin is an owner of Integra FEC and Integra Research Group, which engage in financial consulting, research, and recovery on a variety of issues related to the investigation of financial fraud including crypto-related activities.

†McCombs School of Business, University of Texas at Austin. Email: John.Griffin@utexas.edu.
‡McCombs School of Business, University of Texas at Austin. Email: KevinMei@utexas.edu

How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering

Abstract

Through blockchain addresses, we trace crypto flows and uncover methods commonly used by scammers to obfuscate their activities. The perpetrators interact freely with major crypto exchanges, sending over 98,000 small trust-building inducement payments annually to exchanges commonly used by U.S. and European investors. Funds exit the Ethereum network in large quantities, mostly in Tether, through less transparent but large exchanges. Criminal enterprises pay approximately 33 basis points in transaction fees and moved $27.8 billion annually into suspicious exchange deposit accounts between 2021-2023, including $5.6 billion annually sent from Western exchanges. Our findings highlight how many actors in the "reputable" crypto industry facilitate criminal capital flows.

Random social media or text messages attempting to develop an online relationship are now commonplace. In a subset of cases, friendly online relationships slowly transition into "pig butchering scams" or *sha zhu pan*, which often bleed lonely, sick, and distressed victims into the loss of their life savings. Though varied in nature, the origin of these scams is often even darker, as an estimated 220,000 individuals are forcibly held in compounds in Southeast Asia to operate these scams, constituting modern-day slavery. Many investigative reports, government briefs, and documentaries describe how this scheme lures victims globally with elaborate schemes of friendship or romance orchestrated by individuals confined in Southeast Asian compounds run by Chinese criminal gangs.[1] This paper examines how these criminal organizations are financed through cryptocurrencies. How do criminal networks use crypto to move victim funds? Where does capital enter? Where do the funds exit? What obfuscation methods are employed? How pervasive is this activity? How can it be stopped?

Money flows are the lifeblood of organized crime by financing both current and future illegal activity. The international financial system has developed a framework, including anti-money laundering (AML) and know your customer (KYC) laws, to combat the financing of transnational organized crime. However, with the emergence of Bitcoin and other cryptocurrencies specifically designed to create an anonymous alternative financial system, criminal networks now have new avenues to avoid detection and seizure of funds. Nevertheless, crypto is rarely used as a medium of exchange to purchase goods and services, and typically needs to be converted to and from fiat currencies. The entry and exit points into the crypto ecosystem are typically crypto exchanges, which also purport to conform to international laws designed to mitigate illicit financial flows. Further, although cryptocurrencies are designed to be anonymous, the blockchain provides a ledger that tracks the movement of funds. Thus, the transactions are quasi-anonymous in that, by applying algorithms and substantial effort, it is often possible to determine how funds enter, transit, swap into different crypto, and exit the crypto ecosystem.

We use data from pig butchering victim reports to determine the cryptocurrency addresses where victims were directed to send their funds by scammers. We start with 4,512 Ethereum addresses, 4,394 Bitcoin addresses, and 993 Tron addresses. Of these initial sets, addresses on the

[1] Section 1 provides a brief summary of this evidence and describes the nature of the schemes.

Ethereum blockchain received $8.3 billion in funds, compared to $2.7 billion on Bitcoin and $884 million on Tron. Given that the Ethereum addresses represent approximately 70% of the total funds and a large share of traced Bitcoin is swapped to Ethereum, we focus on transactions on the Ethereum blockchain.

Based on blockchain information personally provided from an unfortunate U.S. victim who lost their retirement and life savings of approximately $465,000, we first show how their funds left their exchange's wallet in the form of ETH, USDC, and Bitcoin, were forwarded to another address, and subsequently swapped to other tokens using a relatively obscure decentralized exchange called Tokenlon. The pattern of this victim's funds is strikingly similar to many other adjacent nodes.

We then trace the funds of all reported addresses and follow their paths to centralized exchange deposit addresses from January 2020 to December 2024. Figure 1 plots the resulting networks for a two percent sample of nodes and features a few relevant patterns. First, the figure shows how flows often enter pig butchering networks from large exchanges where investors commonly have accounts (Coinbase, Crypto.com, and Binance). Second, funds are often swapped for Tether, denoted as USDT, through Tokenlon. Third, after circulating through various addresses in the networks, crypto exits the system through centralized exchange deposit addresses. Fourth, transactions in amounts above $100,000 and in particular $1 million commonly transfer funds to deposit addresses on Binance, Huobi, and OKX.

Across all exchanges, scammer networks initiated 98,682 small deposits per year between 2021-2023 to centralized exchanges for amounts below $10,000. The most common clustering is in small amounts at round numbers, such as $100, $200, or $500. The transaction patterns mirror the characteristics of *inducement payments* in pig butchering scams, which are small payments from scammers to victims used to build trust. Of these, 32,685 transactions per year were sent to Western exchange deposit addresses, including Coinbase (16,852), Crypto.com (14,183), and Kraken (1,102), while the remainder is concentrated in Asian exchanges such as Binance (20,391), Huobi (18,449), and OKX (12,069).[2] We find 78% of potential inducement payments are sent from addresses used in more than ten transactions, suggesting limited monitoring by crypto exchanges.

[2]Throughout this paper, we include Coinbase, Crypto.com, Kraken, Gemini, and FTX as Western exchanges because these historically can be accessed by U.S.-based users. We refer to Binance, Huobi, and OKX as Asian exchanges because they were founded in Asia and have historically been more focused on Asia-based users.

We consider deposit addresses that receive more than $100,000 as more likely to be scammer deposit addresses, since scammers are unlikely to transfer large sums to victims. These addresses are rarely associated with Western exchanges, but are common within Binance, Huobi, and OKX, as well as exchanges such as Kucoin, Bitkub, and MXC. The common feature of these exchanges is that they are perceived by some to have loose KYC procedures and at least partially outside of U.S. jurisdiction.[3] To more fully understand the scope of the networks, we apply *deposit address clustering* (Victor, 2020) by tracking addresses that send funds into user deposit addresses and finding other recipient deposit addresses likely associated with the same user. To avoid capturing payments made by criminals for things like inducement payments, we exclude all connections below $100,000 and only consider direct connections. Using this method to link additional deposit accounts likely controlled by scammers, we find an average of $27.8 billion per year between 2021-2023 of Ethereum-based inflow to these addresses.[4] Portions of this total could capture funds associated with other activity by these criminal networks or other closely-related networks.

After analyzing the networks unveiled from tracing scammed funds forward, we also trace backwards from all large deposit addresses to find the largest sources of fund flows. We then collect the set of all nodes in the forward trace and backward trace and find an average of $5.6 billion annually between 2021-2023 that originate from five Western exchanges, from over 450,000 transactions from potential victims, averaging over $12,000 per transaction. Because our tracing is overly conservative to avoid potential false trace paths, this likely understates the scope of funds originating from Western crypto exchanges.

Within the trace paths, we observe many distinct features of the network that shed light on how romance scams and money launderers operate. Scammers extensively recirculate and swap funds across different addresses and cryptocurrencies. These transactions incur costs but impede tracing tools and help obfuscate the true source of their funds. We estimate that transaction costs total to 33 basis points as a portion of outflows to exchange deposit addresses. This estimate only includes the direct on-chain transaction costs and excludes any expenses required to enter or exit at exchanges. In contrast, Soudijn and Reuter (2016) find costs of 7-16% to move physical Euro bills from Europe

[3]Most notably, the DOJ announced on November 21, 2023 that Binance pled guilty to disregarding anti-money laundering laws, had the CEO step down, and agreed to pay a penalty of more than $4 billion.

[4]Because of lags in detection and collection of addresses, 2024 calculations typically undercount true activity.

to Colombia and money laundering commission estimates range from 4-12% (US Department of the Treasury, 2002) and 10-20% (US Department of the Treasury, 2007). Cryptocurrencies thus appear to be a more cost-effective channel for moving illicit funds across borders. In total, scammer swap transactions may constitute more than 57% of Tokenlon transactions in the 2022-2023 sample. Overall, in the set of addresses touched by the criminals, we find $1.7 trillion in volume, 78% of which is in Tether. Further, we emphasize the global scale of this criminal network. We observe large inflows from potential Chinese victims in 2020 from Asia-based exchanges; however, after the Chinese financial authorities banned cryptocurrency trading in late 2021, there appears to be a decrease in Chinese victims and a shift to U.S. and European victims.

We evaluate the robustness of the parameters on the tracing algorithms by varying three different tracing criteria (hops, deposit size, and transaction count). The amounts vary from $16.9 billion of average annual activity between 2021-2023 with the most restrictive criteria to $33.8 billion with the least restrictive of activity, indicating possible ranges for these criminal activities and showing that results are not extremely sensitive to tracing thresholds. Note that our criteria only calculates amounts moving through exchanges, not the total amount scammed, that the totals can include other related activity through the same addresses, and that our criteria undercounts to the extent that addresses are not identified. In addition to our main results from tracing flows on Ethereum, we also trace 4,394 Bitcoin pig butchering addresses with a total inflow of $2,666 million and find that the Bitcoin scam networks funnel scammed funds into Binance ($228 million), Huobi ($187 million), and Tokenlon ($150 million).

We hope that this research, along with those of other researchers and practitioners, will expose the finances of these dark activities.[5] Banks and other traditional financial institutions have established anti-money laundering processes through internal controls and partnerships with law enforcement. Cryptocurrency monitoring, however, remains nascent. Unlike banks' proprietary

[5] "One of the most effective ways to deter criminals and to stem the harms that flow from their actions–including harm to American citizens and our financial systems–is to follow the criminals' money, expose their activity, and prevent their networks from benefiting from the enormous power of our economy and financial system." From M. Kendall Day while acting Deputy Assistant Attorney General for the Criminal Division of the U.S. Department of Justice. He is now a Partner at Gibson Dunn and has represented Binance. He also states: "More broadly, money laundering undermines the rule of law and our democracy because it supports and rewards corruption and organized crime, allowing it to grow and fester" (U.S. Senate, 2018). A recent hearing by the House Committee on Financial Services introduced H.R.9480, entitled "Empowering Law Enforcement to Combat Financial Fraud Act," to combat these investment schemes.

fraud detection data, the blockchain's public ledger enables academics and other parties to conduct large-scale studies of illicit activity. This project presents a roadmap on how large-scale tracing of tainted funds can help researchers expose and understand criminal financial activity and other illicit crypto flows. Our findings suggest that more robust monitoring could detect such activities.

There are several other practical implications of our study. First, organized or "legitimate" crypto exchanges serve as the on- and off-ramps for billions of dollars in criminal proceeds. Users with a crypto exchange account should realize that crypto exchange users are frequent targets of scams, and their funds are just a quick transfer away from being irreversibly lost—a risk that is far less prevalent for traditional investment accounts. Second, our findings indicate that the large players in the crypto space are likely not sufficiently protecting their customers from scams, and could provide substantially more transaction monitoring activity. Third, the Ethereum networks appear to reduce barriers for illicit financial flows of transnational organized crime. Fourth, romance scammers prefer the stablecoin Tether over other cryptocurrencies and the Ethereum blockchain over Bitcoin. Fifth, decentralized exchanges also serve as large swapping points to exchange crypto and obfuscate funds. Crypto hedge funds and users (many based in the U.S. and Europe) who might purport to engage in "arbitrage" or "liquidity trading" (PWC, 2023) may simply be making profits by facilitating low-cost money laundering. Finally, the large centralized crypto exchanges located in jurisdictions with opaque regulatory environments (Binance, Huobi, OKX, and others) seem to be preferential potential exit points that can further finance extremely large amounts of criminal activities. Such activity has continued as of the end of 2024, despite recent crackdowns and U.S. government settlements.

Our paper relates to three main literatures. First, there is a literature examining dark market activity in the crypto space. Foley et al. (2019) find that 46% of non-exchange-related Bitcoin activity from January 3, 2009 to April 2017 is associated with darknet websites from 27 million Bitcoin users. However, Makarov and Schoar (2021) use more conservative assumptions that account for potential double-counting and find that illegal activity, scams, and gambling account for less than 3% of Bitcoin volume over a more recent period from 2015 to 2021. In 2020, they estimated over $5 billion in dark market activities, online gambling, association with Bitcoin mixers, and scams. Cong et al. (2023b) examine 21,650 addresses involved in sextortion, blackmail

scams, and ransomware. Though ransomware is underreported, they show that 43 ransomware gangs carried out 2,690 attacks from May 2019 to July 2021. Cong et al. (2023a) provide a useful overview of various crypto investment scams, Ponzi schemes, ransomware, money laundering, and dark markets. Chainalysis (2024) calculates $4.6 billion through wallets directly identified with various crypto scams in 2023 among a total of $24.2 billion in wallets identified for illegal activity. Although the Chainalysis annual report does not detail its methodology, they mostly count illicit funds only into tagged addresses and not necessarily into other related addresses.[6] Chainalysis also provides monitoring services to exchanges (such as Binance) and Tether, which may influence why their report generally does not detail specific exchange destinations nor specific stablecoins used for illicit flows.[7] Reiter and Bitrace (2024) examines blockchain addresses associated with two U.S. and two Chinese pig butchering victims and shows overlap in the addresses where funds are sent. Meiklejohn et al. (2013), Sokolov (2021), and Amiran et al. (2022) examine the role of Bitcoin in the Silk Road (2011-2013), ransomware, and terrorism financing. Whereas the academic literature mainly focuses on dark market activity in Bitcoin, we analyze activity on Ethereum. Though focusing only on one type of scamming, the funds we track are multiples larger than the dark market estimates for Bitcoin in 2020 (Makarov and Schoar, 2021), indicating that the amount of criminal activity on Ethereum may be many times larger than previously estimated in Bitcoin. Our paper comprehensively maps the specific pig butchering criminal networks, which are an urgent public threat to ordinary people.

Second, there is a growing literature related to other types of nefarious trading activity in crypto, including price manipulation (Gandal et al., 2018; Griffin and Shams, 2020), pump-and-dump schemes (Li et al., 2018; Hamrick et al., 2021; Phua et al., 2022), and wash trading (Pennec et al., 2021; Cong et al., 2023b).[8] Capponi et al. (2022) study the economics that sustain widespread systematic and costly frontrunning on the Ethereum blockchain. Cong et al. (2023a) examine common crypto scams including those of investment, ICO, rug pulls, phishing, blackmail, and Ponzi schemes and reports over $10 billion of scam activity in 2021. We make a methodological

[6] They note that this procedure undercounts. The 2024 report (pages 104-112) lists scam categories of charity, giveaway, impersonation, investment NFT, phishing and extortion, romance (pig butchering), and rug pulls for a total of $4.6 billion in 2023 but does not give a dollar breakdown among the types. We further discuss these differences in Section 7.5.

[7] For example, the Binance blog discusses working with Chainalysis and Refintiv in 2018.

[8] Griffin and Kruger (2024) briefly survey forensic crypto research.

contribution by showing how bulk tracing can be applied to mapping multiple streams of funds moving through the Ethereum network. From studying the network structure we show how low transactions costs, simple obfuscation, and inducement payments can perpetuate scamming and highlight opportunities for institutions to take preventative actions.

Third, we contribute to the literature on organized crime. In a survey of the literature, Levi (2015) notes that the lack of access to capital and little overlap between the licit and illicit economy makes criminal enterprises rely on the re-investment of profits for growth. El Siwi (2018) notes that recognizing "money is the lifeblood of organized crime" led to the adoption of the anti-money laundering (AML) regime in Italy.[9] Moore et al. (2009) survey the economic structure of online crime and recommend more private data sharing and police enforcement focused on online gangs—recommendations that our findings also echo. Conrad and Meyer (1958) show how the strong economic incentives of slavery meant that the activity would have likely persisted if not for political intervention. Similar economic incentives and outcomes may exist for pig butchering. Examination of criminal fund flows has been primarily limited to prosecuted case records, which leads Levi (2015) to state: "we have little information about the mechanisms of financing." This paper seeks to partially fill this void.

1 Pig Butchering and Crypto Background

1.1 Background on pig butchering

Romance and related friendship scams appear in various forms. In this section, we describe common variants discussed by documentaries, investigative reporting, and online blogs.[10] Romance scams often begin with seemingly random messages through WhatsApp, social media, dating platforms, or standard text messages.[11] The scammers are looking for a victim who is lonely, going through tough times (such as a medical condition or divorce), and has sufficient cash.[12] First, there

[9] Draca and Machin (2015) survey a growing literature on the economic incentives for crime. Leukfeldt et al. (2019) find that technological knowledge for cybercrime in the Netherlands is often gained through a smaller set of technically skilled enablers in online marketplaces. (Mirenda et al., 2022) show how organized crime utilize cash and various shell companies to obfuscate transactions moving into the banking system.

[10] In-depth descriptions by investigative reporters and documentarians include sources such as ProPublica, the BBC (via YouTube), and Faux (2023).

[11] The UN (2023) notes that contact in the forms of "Boo, Facebook, Grindr, Hinge, Instagram, Lazada, Line, LinkedIn, Meet Me, Muslima, OkCupid, Omi, Shopee, Skout, Telegram, TikTok, Tinder, WeChat, WhatsApp, and Wink."

[12] Victims typically range between 30 to 60 years old, are often well-educated, and include similar proportions of both men and women (Global Anti-Scam Organization, 2022).

is a friendship or trust-winning stage, often spanning multiple months, which can also include the illusion of romantic potential (Wang and Topalli, 2022).

After the scammer has earned the victim's trust, the topic of investments will arise. Victims, often with little or no crypto exposure, will be encouraged to open an account at a legitimate, well-known crypto exchange that victims can verify, trust, and easily transfer funds to that account. Scammers will claim to have an edge at another seemingly professional platform and encourage victims to transfer crypto funds to a provided crypto address; however, this second platform is fake or spoofed, and the crypto address is owned by the scammer. On the fake platform, it will appear as if the victim has quickly generated significant returns. Often the person is encouraged to withdraw small profits from the platform back to the original account at the legitimate crypto exchange to build trust. This is known as an inducement payment because it induces the victim to send more funds. Through this process, the scammer can capitalize on both cryptocurrencies' reputation as a viable new technology, as well as the infrastructure connecting the traditional financial system and the cryptocurrency ecosystem to easily onboard funds.

Upon feeling more certain that the investment opportunity is legitimate, victims often make larger deposits. Some victims have drained their savings and investment accounts, borrowed up to their credit card limit, paid penalties to convert their retirement funds, borrowed from friends and family, or placed another mortgage on their home. In the final stage where a victim seeks to withdraw funds, they are often asked to pay "taxes" on the fictitious profits before the funds can be withdrawn.[13] Ultimately, the scam does not end until the victim cuts contact, or the scammer is sure that the victim is bled dry of funds. The scammers sometimes counsel the victim through the financial loss, which may dissuade victims from reporting the scam to law enforcement (Goffman, 1952; Wang and Topalli, 2022).

Pig butchering is a scam with global reach and large numbers of reported victims across many countries. The Federal Trade Commission indicates nearly 70,000 *reported* romance scam victims in the U.S. with reported losses at $1.3 billion in 2022.[14] Globally, since most consumer fraud

[13] A survey of 550 victims as of 2022 found an average loss for U.S. victims of $210,760 with a median of $100,000. 77% emptied their savings accounts and 33% were driven into debt by scammers (Global Anti-Scam Organization, 2022).

[14] FTC (2023) also finds that 34% of these funds are in cryptocurrencies, and the median loss is $4,400. In China, romance fraud or *sha zhu pan* cases comprise around 60 percent of all reported instances of fraud, and a $598

victims do not report to law enforcement, cases are likely severely underreported and the varying degrees of global estimates highlight the uncertainty in the magnitude of these activities.[15]

Pig butchering relies on an even darker crime. Many of the ground-level perpetrators are themselves victims of human trafficking and modern-day slavery. Lured by the potential of a high-paying job, people travel to countries such as Cambodia, Laos, Myanmar, Thailand, and the Philippines (UN, 2023). Their passports are taken, and they are forced to work twelve or more hours a day in walled compounds. Higher-level workers are often not enslaved, although they can also be at risk of physical abuse. It is unclear how many people are being held in these types of conditions but some estimates place 220,000 in Cambodia and Myanmar and other estimates at up to 500,000 in Southeast Asia.[16] Many perpetrators are thought to have ties to local political and military groups.[17] Variants of scamming operations are seemingly growing in popularity worldwide. In Nigeria, for example, reports range of up to "hundreds of thousands" of young men, known as "Yahoo boys," engaged in romance scamming (Barragan, 2023).

1.2 Background on cryptocurrency flows and key definitions

First-time cryptocurrency users typically access the ecosystem through a *centralized exchange*, which functions like a typical retail brokerage. Popular exchanges available to U.S. customers include Coinbase and Crypto.com. Other popular exchanges, historically focused on Asia, include Binance, Huobi, and OKX. Users can fund their accounts using the traditional financial infrastructure that links cryptocurrency exchanges to the banking system. New users must authenticate their identities through anti-money laundering and know your customer (AML/KYC) processes of these exchanges, then fund their accounts (Harvey et al., 2022). Most exchanges at least purport to monitor transactions through know your customer (KYC) or know your transaction (KYT) policies

million loss in 2019 (Wang and Zhou, 2023). However, China also claims to have blocked $51.6 billion in suspicious transactions in 2022 (Solomon, 2023), a number that dwarfs the reported estimates indicating that one of the two estimates, or both, are likely severely mistaken.

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

[16] United Nations Human Rights Office of the High Commissioner estimates at least 120,000 people in Myanmar and 100,000 people in Cambodia are enslaved in such scams (UN, 2023). Chinese anti-fraud organizations estimated 300,000 Chinese scammers in 2019, as reported on Weixin. 500,000 in Southeast Asia is estimated by the Global Anti-Scam Organization as reported by the BBC.

[17] In Cambodia, one large compound sits near a police station and the owner of the compound is one of the wealthiest businessmen in the country with political ties to the prime minister of Cambodia, as reported by the NYT. Other groups have ties to the United Wa State Army, "the most powerful drug trafficking organization in Southeast Asia," and a recent target of Chinese authorities (Solomon, 2023).

to avoid receiving funds from known criminals. The exchanges credit user accounts with the new funds, but continue to store the funds in centralized *exchange wallets*.

When exchange users send cryptocurrencies to another entity that is outside of their exchange, they must provide the receiving address, similar to a traditional bank transfer. Users can also transfer tokens from their account to an externally owned address. Transactions between addresses are recorded on the blockchain. Externally owned addresses can transfer crypto to other addresses including smart contracts. One of the most common types of contracts is a *swap*, where users exchange one type of ERC-20 token for another ERC-20 token, through services like Uniswap. Cong and He (2019), Harvey et al. (2022), Makarov and Schoar (2022), and Capponi et al. (2023) describe various aspects of smart contracts and decentralized finance.

If a cryptocurrency user intends to spend their cryptocurrency in the real-world fiat economy, the tokens typically need to leave the blockchain through a centralized exchange. For example, to convert Ether into dollars at Binance, a user would need to create a Binance account, verify their identity, and generate an Ethereum-blockchain deposit address that is uniquely tied to their Binance account.[18] Any money sent to that address would then be credited to their Binance account. Importantly, flows enter exchanges through deposit wallets and can be tied to a customer deposit address; however, flows leave exchanges from public exchange "hot wallets" and cannot be tied to a specific customer using data on the public blockchain.

2 Data and Methodology

In this section, we first discuss the data used to identify the scammer addresses. We then describe the methodology for following their funds, discuss relevant blockchain details, and provide rationale for our approach. The third subsection describes a trace of two scammer addresses from a single victim report and the fourth subsection provides summary statistics for all reported scammer addresses.

2.1 Data

Our understanding of the networks relies on three main types of data: data on victim reports of pig butchering, blockchain transaction-level data, and blockchain address identity data. From

[18] Users may generate multiple deposit addresses. Deposit addresses are controlled by the exchange at the direction of the user.

online message boards, dedicated crypto-scam reporting websites, and personal accounts directly from victims, we collect 6,281 addresses. Since the online message board also has many addresses simply tagged as "Other," we trained an OpenAI o3-mini model to read through reports and it identified 590 victim accounts that are highly likely to be romance scams for a total of 6,871.[19] Additionally, the United States Institute of Peace (USIP) shared a set of 12,554 addresses used in pig butchering scams.[20] After removing duplicate addresses, our starting sample contains 18,165 addresses. Many addresses have no transactions either because the address was reported or collected from a known spoofed website without any funds lost, or because a victim made a typographical error when reporting. Our sample contains 10,200 addresses after removing inactive addresses.[21]

One limitation is that reports of scammer addresses may be imprecise. We rely on the verification processes of independent organizations that collect victim reports. We mitigate the chance of capturing activities unrelated to pig butchering by removing any addresses of potential exchanges and other services based on criteria described in the next section. Imposing this filter removes 301 addresses, and the resulting dataset has 9,899 addresses (4,512 on Ethereum, 4,394 on Bitcoin, and 993 on Tron) addresses reported to be associated with pig butchering scammers.[22]

We use transaction-level data to identify the movement of funds on the Bitcoin and Ethereum blockchains. Data fields for each transaction include the transaction hash (or unique identifier), sending address, receiving address, the token being transacted, time stamp, and amount of tokens transferred. We collect data on cryptocurrency identities for address hashes and token hashes primarily from Etherscan.com and other web searches.[23] We also use end-of-day prices from CoinMarketCap.com to convert quantities to dollar values.[24]

2.2 Tracing methodology

Our first analysis *traces* flows by following the movement of funds between different addresses. This procedure begins by identifying all funds that have entered or exited reported scammer ad-

[19] In robustness analysis, we show that the inclusion of these reports are immaterial to our main results.

[20] As part of Chainbrium's contribution to a broader project on transnational crime in Southeast Asia, spearheaded by the United States Institute of Peace (USIP), they collected crypto addresses from a variety of sources. These include private victim groups, victim reports, and direct contact with scammers, as displayed in Figure IA.1. We thank USIP for sharing this data and Jan Santiago (affiliated with PICDO) and Raymond Hantho (Chainbrium).

[21] The Internet Appendix Section A describes the data from victim reports in more detail.

[22] In Figure IA.2, we plot the use of addresses over time across different blockchains and find that Ethereum is the most active within our sample.

[23] A common source of exchange addresses within the crypto community is the hildobby Dune list.

[24] For simplicity, we assume stablecoins (Tether, USDC, and DAI) always have a price of $1.

dresses, which are the addresses where victims were directed to send their funds, and then following the subsequent paths. We use Ether (ETH, the native cryptocurrency on Ethereum), ERC-20 token, and Bitcoin tracing algorithms developed by Integra FEC and apply additional filters.[25] One primary contribution is the ability to simultaneously follow multiple paths at scale while maintaining conservative assumptions that are highly unlikely to aggregate unrelated accounts. Our approach by design is not to capture all flows, but to focus on capturing flows that are extremely likely to be controlled by a scammer.

We trace all Ether and tokens that enter scammer addresses and follow the traced paths until any of the following termination criteria are met: (i) the path meets an identified service, such as an exchange; (ii) the path meets an unidentified but large address that has more than 2,000 transactions; (iii) the path reaches five hops; (iv) the path reaches an address that appears to be involved in any other type of activities unrelated to scams, such as yield farming or NFT trading; or, (v) traced amounts diminish to be less than 0.00001 ETH or token quantities, which are known as *dusting* transactions designed to obfuscate tracing. The most often binding and most important criteria is (i) meeting an identified service. As a result, we do not follow large addresses that may incorporate flows from unrelated entities such as mixers. These criteria and potential limitations are described in more detail in Internet Appendix Section B.

We also trace Bitcoin sent to the Ethereum blockchain using the Wrapped Bitcoin (WBTC) cross-blockchain bridging mechanism.[26] Each WBTC minted is pegged one-for-one to a BTC on the Bitcoin blockchain. This process generates logs that include the corresponding Bitcoin transaction hash and stores them on the Ethereum blockchain. We use this fact to link, one-for-one, the WBTC entering the Ethereum blockchain and trace these tokens to deposit addresses.

We focus on Ethereum paths that start from exchange wallets sending funds to scammer addresses and end at user deposit addresses. Because the trace path expands rapidly as transactions branch off, we do not follow funds that enter large unidentified entities. Our approach allows us to

[25] This tool has been developed over time and verified over time in various investigative contexts. We also apply additional filters for our specific contexts as discussed below. When tainted funds are co-mingled within an address with a balance that includes other funds, the path of the tainted funds is traced on a "first-in-first-out" (FIFO) basis. FIFO is a well-established and accurate process for following specific fund transfers in cryptocurrency transaction-level data (Anderson et al., 2018).

[26] WBTC is an intermediation mechanism that allows users to exchange BTC on the Bitcoin blockchain for WBTC tokens on the Ethereum blockchain.

manage the complexity as paths grow with each hop and conservatively find likely scammer-owned deposit addresses used to offboard cryptocurrencies. We focus on the inputs into our traced networks in Section 3 and the outputs in Section 4. We reverse the steps and trace backward from potential scammer deposit addresses in Section 5, such that summing the total lifetime flow to these deposit addresses indicates the size of the pig butchering networks. We further collect all nodes that have appeared in both the trace and back-trace and study features of the networks in Section 6. A diagram summarizing our approach is presented in Figure IA.3.

2.3 An example of a victim-reported scammer address and network

We first examine the crypto flows associated with a victim who gave us their story and crypto information in the hopes that this could benefit others. The victim is an approximately 60-year-old male. After developing an online relationship, the scammer coached him through the investment process that involved transferring approximately $70,000 in Bitcoin, $25,000 in Ether, and $370,000 in USDC from Coinbase to a spoofed exchange. All told, this middle-class victim, a diligent saver, who had taken an early lump-sum pension payout, lost his retirement and life savings of approximately $465,000.

Figure 2 reports the details of the crypto flows around the victim-reported addresses on the Ethereum blockchain. The red and dark red nodes are the addresses reported by the victim. The blue and grey lines leaving Coinbase indicate that the victim sent funds in USDC and Ether. The funds were then swapped at Tokenlon. Tokenlon is a relatively obscure decentralized exchange based in Singapore that serves as a wrapper for other swap services. To further understand this network, we trace the scammer addresses and follow their paths. We find many other fund paths that exit Coinbase and Crypto.com are quickly directed to the dark red node, often within twelve hours. Each transfer also requires paying a transaction cost in ETH, known as a *gas fee*. The dark red node appears to provide the ETH to the upstream nodes that is later used to pay gas fees. Most trace paths also lead to Tokenlon, where the USDC or Ether is often swapped for Tether or DAI. DAI has an interesting property in that it is thought to be outside of the reach of law enforcement.[27] Scammed funds often cycle through many nodes. Ultimately, most funds enter Binance as Tether,

[27] Crypto users make this claim because DAI is managed as a decentralized stablecoin through a series of smart contracts. In contrast, USDC and Tether are issued by Circle and Bitfinex respectively, which are both registered as money service businesses with the U.S. Financial Crimes Enforcement Network and thus must freeze funds in response to the U.S. justice system.

with large transactions also entering OKX and Huobi. As we will see later, most of the small payments to Coinbase and Crypto.com fit the characteristics of inducement payments.

2.4 Reported scammer addresses

Figure 3 shows the 4,512 Ethereum, 4,394 Tron, and 993 Bitcoin active addresses reported by the victims.[28] Notably, victims may include multiple addresses within the same report, such as in cases when scammers provide different addresses to victims.[29] The horizontal axis is the number of total transactions by the node and the vertical axis is the total dollar inflow. Most addresses received between $10,000 and $10 million in total lifetime inflow.

Of all possible cryptocurrencies, our investigation of the reported scammer addresses suggests that activity is concentrated in Ether and a few ERC-20 tokens within Ethereum, including Tether, USDC, DAI, and Wrapped Bitcoin.[30] Other tokens are occasionally transacted, but our focus is on these major cryptocurrencies, unless otherwise noted.[31] Some Ethereum addresses are used less than ten times, whereas most of the addresses are used more than twenty times. Bitcoin addresses generally have less total funds flowing through them and slightly fewer transactions. Tron addresses appear in a greater number of transactions than Bitcoin addresses, although with lower dollars per transaction. Exchanges will cease outflows to addresses that are known to be associated with criminal activity, but some customers may also not want exchanges monitoring their activity. Scammers might choose to use fresh addresses if exchanges monitor inflows and outflows. The fact that addresses are used so frequently suggests that scammers are not too concerned about the exchange prohibiting such activity. The combined total amount is $8,275 million in Ethereum, $2,666 million in Bitcoin and $884 million in Tron.

Table 1 displays summary statistics on Ethereum scammer addresses. These addresses vary in size, with an interquartile range of 23 to 224 transactions and $55,000 to $1.4 million in total inflow. Across all reported Ethereum addresses, the mean (median) inflow is $1.9 million ($325,000).

[28] Some victim reports suggest their funds were sent to large nodes. As we describe in the IA, to avoid falsely attributing nodes, we only report addresses with fewer than 2,000 transactions and that only transact with included functions.

[29] It is also possible that the victim provides the address where they sent their funds and the next address where the funds went after. In this case, both Ethereum addresses would enter our trace without being double counted, if they were non-exchange address with below 2,000 transactions.

[30] Although victims often send funds in USDC, the most common primary token across addresses is Tether because addresses have many other within-network Tether transactions.

[31] Another common occurrence is non-ERC-20 tokens, or "spoofed" Tether contracts that imitate Tether, which often have zero market value and may be part of a separate scam. We screen out these tokens.

Outflows tightly match inflows, due to the common practice of forwarding funds and periodically switching addresses. The median address is active for 79 days.

3 Tracing the Network

Figure 1 presents a sample of Ethereum trace paths that illustrate many of the features we find in the scammer networks.[32] The boxes represent exchanges and are sized proportionally to the amount of funds exiting exchanges on the left side and entering the exchange on the right side of the graph. Edges representing transactions exiting exchanges are shades of green, with the darkest shades representing large transaction amounts and lighter colors representing smaller transactions. The red triangles are reported scammer addresses. All other circular nodes are other addresses encountered in the trace. Pink indicates non-exchange addresses and shades of blue indicate exchange-controlled deposit addresses. Each scammer node is sized proportionally to the amount received and is positioned closest to the nodes they transact with the most; shorter edge lengths indicate large transaction amounts. The figure shows many clusters of non-identified nodes surrounding reported scammer addresses. Edges within the network and into Tokenlon are colored light purple, and transactions out of Tokenlon are fuchsia. Edges entering exchanges are colored shades of blue. Extremely light colors are small transactions (possibly inducement payments) below $10,000, light blue is between $10,000 and $100,000, blue is between $100,000 and $1 million, and black is greater than or equal to $1 million.

The figure shows how crypto enters the networks from large crypto exchanges, such as Coinbase, Crypto.com, and Binance, in small and medium sized transactions. Related nodes often transact with each other and swap through with Tokenlon. Funds in amounts above $100,000 and in particular $1 million commonly flow to deposit addresses on Binance, Huobi, and OKX. Coinbase, Crypto.com, and Binance also receive a large amount of small transactions.

Figure 4 presents an aggregate view of the entire tracing results of the 4,512 scammer addresses. In Panel A, edge thickness is proportional to transaction amounts and edge colors correspond to cryptocurrency used. $504 million from Crypto.com enters scammer addresses, $589 million from Coinbase, and $309 million from Binance, followed by smaller amounts from other exchanges. These

[32] To reduce complexity, we show only a two percent sample. The sample was generated by picking a random set of about 200 scammer nodes in the Ethereum blockchain, and then randomly selecting related paths that start from and end at exchanges. The total sample contains 5,758 nodes and 16,431 edges.

funds are primarily in Tether, though Coinbase and Crypto.com send out Ether and USDC. Panel B summarizes this inflow and outflow of transactions with exchanges by hop and shows the combined breakdown of the $3.2 billion entering these addresses from all exchanges (as shown in Figure IA.4). Yet, the reported addresses interact with over $8 billion in funds. Many of these funds may be other funds moving through the system, as funds are recirculated through multiple hops and swapped at Tokenlon. This extensive recirculation is one way to obfuscate funds. Tokenlon plays a large role in the networks as shown by the crypto swapping in Panel A and totals in Panel B with large flows entering as USDC and Ether, only to return as DAI and Tether. Ultimately, 80% of flows re-entering exchanges are Tether.

We trace $4.4 billion to exchanges while the remainder met the halting criteria before reaching an exchange. Important exit points include $1.2 billion sent to Binance, $505 million to OKX, $175 million to Huobi. Only $83 million (or 1.8%) was sent to Coinbase and Crypto.com. Panel B indicates that over $1 billion enters exchanges within two hops. Transactions to OKX appear to move mostly within three hops, while transactions to Binance continue to occur even five or more hops away.[33] For early hops the funds appear in ETH, USDC, and Wrapped BTC, but in later stages the funds are almost exclusively in Tether with some DAI.[34] Overall, crypto typically moves from U.S.-based Crypto.com and Coinbase to Binance, Huobi, and OKX, which are Asia-focused exchanges.

We also examine whether exchange sources have changed over time from January 2021 to December 2024. Most of the funds enter the networks from Binance, Huobi, and OKX in early 2021 (as shown in Panel A of Figure IA.4). In May 2021, flows from Coinbase begin to appear, and by 2022, the majority of funds appear to enter the networks from Western exchanges. The Tokenlon funds entering the networks also appear larger in 2021, but one should interpret this as funds from other victims that have already been swapped through Tokenlon. Tether (USDT) consistently appears to be the dominant crypto entering reported scammer addresses throughout the period. ETH and USDC were popular in late 2021 and 2022. Wrapped Bitcoin appears in 2022 and DAI in 2023.

[33] The tracing procedure counts hops starting after the first outbound transaction of any starting addresses. Therefore, the trace shows a sixth node when programmed to terminate at five hops.

[34] While our previous analysis has focused on transactions with exchanges, Figure IA.5 shows all transactions with any address by hop.

The growth of scammer activity in 2021 coincides with a boom in crypto enthusiasm. While scammer activity has declined with overall crypto activity, we are also cautious to read too much into a slowdown of inflows in 2024 due to data and clustering. Given that scammers may frequently use new addresses that we may not have access to, we expect a natural decline in more recent flows. We also expect a lag in reporting data, as victims may not immediately report addresses, and if reported, collection agents may require some time to verify the data.[35] Industry reports also increase their reported crime for a given period substantially after a year or two. For example, when calculating total cryptocurrency value received by illicit addresses in 2022, Chainalysis initially reported this as $20.6 billion in their 2023 report and updated to $39.6 billion, a 92% increase, in 2024 (Chainalysis, 2023, 2024).

In total, the pattern from exchanges suggests a shift from Asian exchanges to Western exchanges in late 2021. Because our victim addresses are primarily from 2021 and beyond, this analysis likely understates the extent to which victim funds are entering the system through Asia-focused exchanges before 2021. Exchanges are only a proxy for victim location. Because the addresses were collected from a variety of sources and the country composition could have shifted over time, this proxy could affect our inferences over time. We examine this and other features in more detail in Section 6.

4 Outflows from the Networks

We now focus on outflows from these scammer networks to deposit addresses. We interpret these results with the context that centralized exchanges typically must adopt know your customer protocols, implying that each deposit address is linked to an authenticated exchange customer. Some customer addresses are likely linked to pig butchering victims, and we examine whether exchanges had opportunities to mitigate this scam. Other customer addresses are likely scammer accounts used to "cash out" to fiat, providing an avenue to size total transaction costs and proceeds of the scam operation.

[35] Indeed, in earlier work our data stopped in October 20, 2023 and our analysis showed decreasing flows by July 2023. After running our analysis with a newer set of victim addresses we received after December 2023, we saw substantial increases in funds in the second-half of 2023.

4.1 Deposit addresses

We follow the trace path to 89,583 user deposit addresses. Figure 5 splits deposit addresses into four groups based on the amount of funds received in the trace path. There are more than 73,000 deposit addresses that receive less than $10,000 for a combined $102 million. These small payments are consistent with the characteristics of inducement payments, which we discuss in more detail in the next subsection. Overall, Coinbase and Crypto.com receive small inflows, typically below $10,000, but almost always below $100,000. In contrast, deposit addresses that received more than $100,000 tend to be non-Western exchanges such as Binance, Huobi, OKX, and Bitkub, which are thought of as more anonymous. We interpret these larger flows as likely scammer-owned deposit addresses.[36]

Figure IA.7 summarizes by the average transaction sizes exiting and entering exchanges. While funds exiting Coinbase and Crypto.com have a mean (median) transaction size of approximately $14,000 ($1,661) and $12,000 ($1,985) respectively, funds entering these exchanges average between $3,000 ($589) and $7,000 ($525). We interpret these as large transactions where U.S. victims are defrauded, followed by potential inducement payments, as discussed in the next subsection. In contrast, transactions leaving Binance, Huobi and OKX average approximately $9,000 (median of $1,276, $1,475, $1,000), while amounts entering exchanges average $152,000 ($15,455), $45,000 ($4,314), and $36,000 ($7,678), respectively. We view the small outbound transactions as small transactions of non-Western victims from these exchanges, while large inbound transactions are interpreted as the final deposits after scammers have aggregated and laundered their collections and prepare to trade into fiat currencies.

4.2 Potential inducement payments

Inducement payments may help scammers gain the trust of their victims. We consider a transaction of less than $10,000 as a potential inducement payment.[37] To understand the full scale of these payments, we collect a list of all inducement payment senders within the traced networks and expand our data to consider any transaction up to $10,000 from these inducement payment senders to any exchange deposit address. Figure 6 examines the sizes of potential inducement pay-

[36] In terms of large inflows, Binance ($1,283 million) is the largest exchange, followed by OKX ($493 million), and Huobi ($136 million) (as shown in Panel B of Figure IA.6). Additional statistics about deposit addresses are presented in Table 2.

[37] The $10,000 threshold is also the limit above which banks must file a Suspicious Activity Report.

ments and finds that most are $1,000 or less. We find 318,081 payments for $500 or less and these payments are more weighted towards Coinbase and Crypto.com. There are also small payments to Binance, Huobi, and OKX, indicating that there are likely many victims on these platforms as well. Interestingly, these payments seem to cluster at round numbers, which may be a function of the scammers sending fake gains as round numbers or encouraging victims to withdraw funds.

Figure 7 plots the cumulative number of transactions for each sending address. We produce these graphs for the four largest exchanges: Coinbase, Crypto.com, Binance, and Huobi. Addresses that send multiple successive transactions will be visible as right-ward leaning columns of dots. Interestingly, addresses with more than 10 transactions have a median active span of 113 days and a 75th percentile of 228 days, or 3-8 months, as presented in Table IA.1, which can be interpreted as the duration before scammers switch addresses.

During the focal period of 2021 to 2023, we observe 98,682 potential inducement payments per year, including 20,391 to Binance, 18,449 to Huobi, 12,069 to OKX, and 32,685 to five Western exchanges, the bulk of which is concentrated in Coinbase (16,852) and Crypto.com (14,183). In some cases, a *clean*, or previously unused, address sent potential inducement payments, such as 3,302 addresses that sent only once to Coinbase and 2,190 addresses that sent only once to Crypto.com. However, as few as 214 addresses were responsible for over 24,781 transactions to Coinbase and 220 addresses for 27,394 to Crypto.com. We find that 69% of potential inducement payments are sent from addresses used in more than ten transactions, suggesting limited monitoring by crypto exchanges.

We document 180,072 total (49,351 annually between 2021-2023) unique exchange deposit addresses that receive transactions of up to $10,000 from potential inducement payment senders (as shown in Figure IA.8). These include 36,147 (10,441) Binance, 29,150 (7,574) Huobi, 18,428 (5,070) OKX, 48,167 (13,802) Coinbase, and 38,043 (10,199) Crypto.com, which we interpret as a lower bound of the total number of addresses that receive inducement payments. Potential Western-based exchange addresses that receive inducement payments total 92,529, or an average of 25,181 addresses per year between 2021-2023. Most new deposit addresses are concentrated in Binance and Huobi in 2020 to 2021, while OKX, Coinbase, and Crypto.com appear more commonly in late 2021 through 2024.

4.3 Transaction costs

We calculate the aggregate transaction costs incurred within this trace, also known as gas fees in Ethereum, and present summary statistics in Table 3. Within our sample, we see an average gas fee of $5.56 and a median of $2.46 per transaction. As a percentage of the amount transferred, the median is ten basis points, and the mean is 5.93%.

Swaps were associated with higher gas fees with a median of $17.36 per transaction, or 27 basis points of the final amount. Swaps also have the opportunity of gaining or losing money due to the spread. The median loss was 19 basis points. In Figure 8, we plot the fees for token swaps in four parts: gas fees as dollars and as a percentage, and swap losses or gains as dollars and as a percentage.[38]

Gas fees for transfers of ETH and ERC-20 tokens do not typically change with the amount transferred, which provide an incentive to aggregate payments and move larger amounts at once. For example, transactions below $10,000 have a mean gas fee of 9.48% of the transferred amount, whereas amounts above one million paid 0.0005% in gas fees.

Altogether, these networks include $7.8 million in ETH and token gas fees, $2.1 million in swap gas fees, and an aggregate loss of $3.2 million in swaps, for a total of $13.1 million in transaction costs. This represents the total fees used to move hundreds of millions of dollars across multiple hops. If we conservatively consider $13.1 million as the total transaction cost needed to transfer the $4 billion into the largest deposit addresses with more than $100,000 inflow, then transaction costs amount to 0.33% of flows to scammer deposit addresses.[39] Note that this is the direct cost of transferring funds and does not account for any payments to potential service providers such as professional money launderers, potential losses due to asset seizure, nor transaction costs incurred from converting funds to fiat at exchanges.

5 Sizing the Scamming Networks

We now examine the total flow into likely scammer deposit addresses.

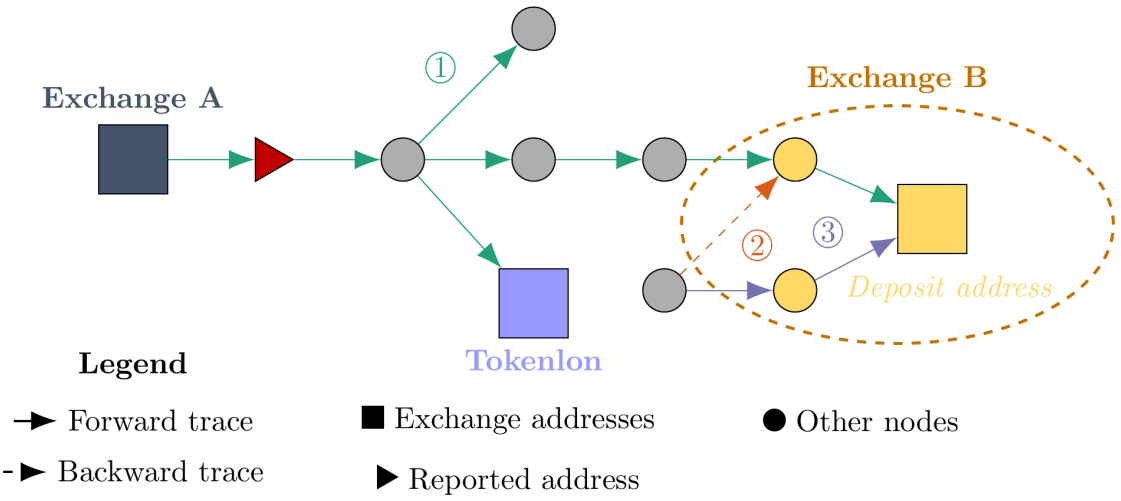
[38] The percentages are based on ETH prices as of midnight on the transaction date and stablecoins are assumed to be $1.

[39] The denominator in this calculation, $4 billion, is the sum of all flows to deposit addresses that received more than $100,000 in Figure 5. Other valid denominators include the total volume moved or the total amount inflow, both of which are larger denominators; thus, we use 0.33% as a conservative estimate.

5.1 Sizing methodology

We next collect all Ethereum deposit addresses that have received more than $100,000 in total across four tracing steps: (i) initial paths found from reported scammer addresses; (ii) *retraces* by finding post-swap paths for tokens that interact with Tokenlon; (iii) Bitcoin paths that can be traced across the WBTC bridge (as discussed in Section 2.2); and (iv) a second retrace of (ii) and (iii). We focus on a total of 4,479 potential scammer deposit addresses (as shown in Figure IA.9). $31.3 billion flows into these deposit addresses over time (as shown in Figure IA.10). Most of the funds are flowing into Binance, followed by much smaller amounts into Huobi, and OKX. This group of paths is denoted as Path 1 in Exhibit 1 below.

Exhibit 1 Diagram of trace paths



We follow Victor (2020) to identify additional related addresses using a method called *deposit address clustering*. Each deposit address is assigned to a single user, and users can create many deposit addresses without incurring any costs. If any address sends funds to a deposit address, then that money can only be accessed again using a user account on the exchange platform. Thus, if an address sends funds to two deposit addresses, then these are likely both controlled by the same user.[40] The heuristic associates any given address that deposits to the same deposit address and then considers other related deposit addresses. We find these by following Path 2 and Path 3 in Exhibit 1 and sum the total inflow to determine the total revenue of the scammer networks.

[40] Victor (2020) compares three heuristics for identifying ownership and finds deposit address clustering "is currently the most effective approach."

5.2 Sizing results

Figure 9 plots the results of these findings over time from January 2020 to December 2024 and highlights two results. The sum all inflows to these addresses and find $94.6 billion, most of which is concentrated in exchanges typically considered outside of U.S. jurisdiction. Of these exchanges, Binance is the overall largest destination. The second largest exchange was Huobi in 2020-2021 and OKX in 2021-2023. This amounts to $27.8 billion per year between 2021-2023, which are the focal years of our sample.[41]

This result seeks to capture the most likely scammer-controlled addresses and avoid capturing other activities. While our research design choices are conservative, some factors may influence the interpretation of our results. If a given network recirculates funds across different exchanges, such as if a scammer sends scam proceeds from their OKX account to one of their Binance deposit addresses, then it would lead to double counting of funds. Deposit addresses may also be owned by other service providers, such as website providers (Xia et al., 2020). Additionally, the funds received may be due to activities other than pig butchering scams. For example, the pig butchering networks also collect proceeds from ransoms, human trafficking, and other illicit activities (UN, 2023). Although crypto addresses related to human trafficking addresses are difficult to obtain, we obtained one Ethereum address personally verified by a large non-profit working to stop human trafficking. They believe the address physically traces to the KK Park compound in Myanmar. This address was in our traced pig butchering network and shows some of the connection between pig butchering and human trafficking.

5.3 Backtracing

To learn more about the source of funds, we conduct a *backtrace* of five steps to find all paths that enter these deposit addresses similarly to how a forward trace described in Section 2. We examine the sources of funds that later enter into these potential scammer deposit addresses and find that $62.5 of the $94.6 billion come from exchanges.[42,43]

[41] As a robustness analysis, in Section 7 we vary our criteria and discuss potential ranges. We also decompose our steps into deposit addresses from the original trace and those incrementally from deposit address clustering and find that the heuristic effectively captures more activity in 2021 (as shown in Figure IA.11).

[42] See Figure IA.12. The remainder did not reach a source within five hops, or the path reached a large address with more than 2,000 addresses and terminated.

[43] Since large movements are more likely to reflect criminals shifting large funds, we focus only on initial transactions leaving these exchanges in amounts less than $500,000. We exclude larger transactions to reduce the risk of capturing large "recycling" of funds that may exit Binance only to return to one of our deposit addresses. This is likely an

Identifying flows exiting exchanges provides an avenue to assess the magnitude of pig butchering's financial harm to victims. We consider all addresses that have been found in both the forward and backward traces, apply the consistent set of screens as Section 2.2, and examine all direct movements out of an exchange to these nodes, which are likely controlled by a scammer or an affiliate. In Figure 10, we plot the flow of funds exiting each major exchange and entering the scammer networks, with splits by transaction size. Since we are interested in understanding the potential magnitudes of funds stolen from Western victims, we examine all crypto movements out of exchanges for less than $500,000. We interpret this as more likely to be new funds from victims, especially because victims who may have lost larger amounts still transacted in multiple batches. Scamming networks may send amounts less than $500,000 from exchanges, but as shown in Figure 1, large transactions by scammers into Western exchanges are rare. Across all addresses, the scammer networks received $19 billion, or $5.6 billion per year between 2021-2023, from Western exchanges in transactions of less than $500,000. We interpret $5.6 billion annually as a lower bound of the amount defrauded from victims using Western exchanges. We find an average of 453,771 transactions per year of less than $500,000 from Western exchanges, with a mean of over $12,000 per transaction. The total (mean 2021-2023) includes $4.1 (1.4) billion from Coinbase, $6.0 (2.0) billion from Crypto.com, and $7.1 (2.4) billion from Kraken.

The prior analyses primarily depicted flows from exchanges to the network, or from the network to exchanges. Another perspective is to sum all transaction volume within the network. Total volume within the network totals to $1,706 billion, as shown in Figure IA.13 split by cryptocurrencies. We find that 78% is in Tether. Inflows from Western exchanges are relatively more commonly in USDC and Ether, but are often swapped into Tether when sent to potential scammer deposit addresses in non-Western exchanges.

6 Features of the Network

The networks we identify help shed light on how transnational organized crime operates. Some prominent features are evident in Figure 2, such as the extensive mixing and forwarding of tokens. Funds often circulate through the network and connect in loops. Within the network graph, we also see examples of "dusting" transactions or sending small amounts of tokens to many addresses and

overly conservative estimate because the backtrace paths stop at large nodes and thus does not include all paths from exchanges.

thus creating more paths for any potential investigator to follow (Figure IA.14 shows over 500,000 transactions of less than $5 from the forward trace). These efforts are potentially costly to the criminals: each transaction incurs transaction fees and dusting tokens are essentially lost revenue. We examine the shift in sources of inflows after a government crackdown and the extensive use of token swaps.

6.1 Impact of crypto crackdowns

On June 21, 2021, the Chinese financial authorities asked banks and payment firms to cut ties to crypto channels and on September 24, 2021 banned all crypto trading.[44] To examine the flow of funds prior to 2021 and the potential shift in fund source, Figure 11 Panel A plots the flow from exchanges to addresses from January 2020 through December 2024, grouped by the active hour of the day and by month. The size of each square is proportional to total volume and colors indicate of the percentage of exchange flows into the network originating from Western exchanges. The red line corresponds to China's crypto ban. Prior to this line, activity seemed to be concentrated during Chinese waking hours and non-U.S. exchanges. After this announcement, however, activity begins to wane, and by December 2021, we see an increase in activity from U.S. waking hours. This provides corroborating evidence of a shift in the victim base from Asia-based victims to Western-based victims.

We are interested in whether scammer deposits were impacted by law enforcement operations. Panel B of Figure 11 plots weekly flow into deposit addresses in the three largest exchanges (Binance, Huobi, and OKX) over time. Vertical red lines denote six key dates of crypto bans, police raids, and arrests and charges related to crypto scams in Asia. Foremost, we interpret this with a backdrop that our sample is incomplete and may lag total scam activity due to the data collection and verification process. Some events appear effective, such as the Chinese ban on crypto coinciding with a decline in Huobi deposits. However, for most subsequent events, scammer activity persists even after these raids, arrests, and charges. This matches anecdotal evidence that scammers remain active despite international pressure.[45]

[44] News reports of these decisions are presented in Table IA.2.
[45] As reported by news organizations such as the BBC.

6.2 Use of Tokenlon swaps

The scammer networks use decentralized exchanges such as Uniswap and Tokenlon to swap between different cryptocurrencies. To someone who may be looking for money laundering channels, fees on a decentralized exchange may be cheaper than swapping in a centralized exchange. Popular tracing tools often stop at swap transactions. While Uniswap is arguably the most popular decentralized exchange, Tokenlon is relatively obscure and may be a distinctive trait of pig butchering scams.[46]

In Figure 12 Panel A, we plot the number of Tokenlon transactions over time as found in either the forward or backward trace. This suggests thousands of transactions per month where funds were converted from ETH, USDC, WBTC, and DAI to Tether before depositing Tether to various deposit addresses. More strikingly, these transactions with a scammer on one side of the transaction constitute more than 60% of all Tokenlon swap transactions per month. This suggests that if a given crypto user chooses to swap with Tokenlon, their trading helps scammers obfuscate the flow of funds. Our numbers are also likely undercounted as we are only tracing those scamming funds we can identify. As shown earlier in Figure 4, a common feature is that most of the flows move to Tokenlon relatively quickly.

We also plot a transition matrix on the most common swaps seen in our four main traced avenues (Figure 12 Panel B). We see that Tether (USDT) is the main destination for all token pairs. For example, the most common pair is swapping ETH into Tether. USDC is the preferred stablecoin on Coinbase, but we see most USDC be swapped into Tether or DAI. DAI may be a popular token because it is believed to be beyond seizure by law enforcement authorities. Interestingly, very little volume is ever swapped into USDC. Lastly, we also see a substantial amount of WBTC swapped for Tether and DAI. The "Other" to WBTC pair includes Bitcoin that we traced into the Ethereum blockchain as WBTC as explained below in Section 7.4.

7 Additional Analyses and Discussion

Because of the size and complexity of our identified scammer networks, we undertake additional analyses to further evaluate our findings on Ethereum and present some related findings on Bitcoin

[46] Uniswap is a consistently top 3 decentralized exchange with more than 20% market share while Tokenlon was ranked in the 30-50 range with 0.1-0.2% market share according to CoinMarketCap in early 2024.

and swaps.

7.1 Sensitivity analysis

We evaluate whether our findings are sensitive to the criteria used to exclude addresses in the trace or the deposit address heuristic. The three tested dimensions are number of hops, deposit size, and transaction count. Number of hops refers to steps we followed funds, or depth of tracing. Terminating the trace earlier is more conservative because it decreases the number of potential end destinations, such as deposit addresses. Earlier analysis indicates that, although the network recirculates funds through multiple interconnected addresses, 53% of funds reach a termination criteria within the base case of five hops. Deposit size refers to the minimum threshold we use to determine that a deposit address is potentially related to the criminal network. We emphasize large addresses with more than $100,000 of total inflow to mitigate the risk of following potential inducement payments. Increasing this threshold is more conservative. Lastly, transaction count is used as a heuristic to determine whether an address has too many transactions to plausibly belong to a regular Ethereum user. Decreasing this threshold is more conservative because addresses with a high number of transactions are more likely to be an unidentified service or vendor.

Figure IA.15 presents a sensitivity analysis table calculating the average annual inflow in the three years between 2021-2023. In Panel A, we find that varying number of hops considered in the base case leads to an estimate of between $23-30 billion. Varying the deposit size cutoff has a large influence on the number of deposit addresses that remain in scope. Using $50,000 of lifetime inflow as an aggressive cutoff leads to a larger estimate of $33 billion, while a more conservative criteria of $250,000 leads to $17 billion.[47] Similarly, in Panel B, we display a similar matrix varying the transaction count cutoff and find that these estimates are not as sensitive compared to the deposit size criteria.

Overall, while the calculated amount varies as expected, our primary findings remain unchanged. We estimate that this network deposited more than $20 billion per year between 2021-2023. One insight for forensic researchers is that transaction counts are not a sensitive criterion and more effort should be focused on accurately increasing the depth of traces and identifying wallets with large dollar amounts.

[47] These sensitivity assumption choices were informed by the deposit address summary statistics Table 2. For example, the median inflow of addresses with less than $100,000 is $45,000.

7.2 False positive testing

We wish to understand how pig butchering networks differ from other scamming activity on Ethereum. We gather data on 27,868 Ethereum addresses from 14 different scam categories from chainabuse.com (as shown in Table IA.3). The largest categories are phishing, impersonation, hacks, and fake projects. Among 1.18 million addresses in our networks from forward or backward tracing activity, we find only 648 as reported in other scams, or 2.3% of reports. The second largest category is fake returns, which can plausibly be due to victims misclassifying a romance confidence scheme as an illegitimate investment scheme. Although pig butchering networks have been reported to engage in other illicit activities (UN, 2023), these findings suggest that pig butchering organizations focus on this crime and that our methods have a relatively low incidence of capturing other scams such as phishing, hacks, or ransomware.

Lastly, the sample includes a large portion of victim stories that are categorized as "Other" scams. We used the reports labeled as "Pig Butchering" or "Romance" scams to fine-tune an OpenAI o3-mini model to recognize romance scams within the "Other" category. The model classified 590 of these stories as likely pig butchering reports.[48] In Figure IA.18, we plot the same graph as Panel A of Figure IA.4 excluding these 590 addresses. The message of these graphs is qualitatively similar.

7.3 Connectedness and deposit addresses sensitivity

We find that more than 99% of nodes are connected within one large, interconnected network (as shown in Figure IA.16). The fact that such a large part of the pig butchering touches this broader network indicates that the network is (a) several criminal networks using the same common front-end service, such as services to spoof exchange platforms, (b) several criminal networks using the same group of front-end services, or (c) mainly one criminal network. Given the reporting that scamming operations are located in several countries, we believe (b) is the most likely.

As a robustness analysis, we examine if our results are driven by a few errant deposit addresses. We plot deposit addresses based on the number of reported scammer addresses that lead to each deposit address. We find that our largest addresses are connected to multiple victim reports, which

[48] We only used the model output if the Chat Completion API returned a ranked probability of more than 99% as described in this documentation.

reduces concerns that they are only loosely connected to victims (as shown in Figure 13). We have also manually examined the large address fund paths to see if there are any unusual nodes on the path. Further, to consider the influence of large deposit addresses, we rank deposit addresses by total inflow and find two addresses that havereceived over $1 billion, but the vast majority receive substantially less (as shown in Figure IA.17). The top 100 of our 89,583 deposit addresses account for $19.6 billion of the estimated $94.6 billion in lifetime inflow to likely scammer deposit addresses.

7.4 Bitcoin tracing and swaps

We trace Bitcoin using a similar framework, though tailored to its specific blockchain transaction architecture. Bitcoin tracing is more straightforward because transactions follow the common input heuristic: any two addresses that jointly send money in a transaction can be confidently grouped into a *cluster* controlled by the same entity. Following this methodology, we expand our scope to include addresses within the same cluster as the originally reported scammer address. Details of the tracing methodology are provided in the Internet Appendix C.

Transactions on Bitcoin frequently originate from Coinbase or Square Cash App (as shown in Figure IA.19). These transactions generally go to an address that is then forwarded through multiple transactions into the scammer's collection point. The collection network also uses dusting transactions which consist of small Bitcoin transactions meant to confuse standard tracing algorithms by creating more paths for the researcher to follow. These trace paths lead to similar destinations: $228 million to Binance, $187 million to Huobi, $158 million to Kraken, and $150 million to Tokenlon (Figure IA.20). Given that these are two different blockchains, we cannot ascertain whether these Binance and Huobi addresses are related to the deposit addresses found in Ethereum. However, the prominence of Tokenlon remains a distinct finding and offers a chance for linking funds to the Ethereum blockchain.

Tokenlon is a non-custodial decentralized exchange and thus does not directly store any user funds. When users send Bitcoin to the Tokenlon storage account, they are receive a Tokenlon-affiliated Ethereum token called imBTC, which can then be traded for the third-party Wrapped Bitcoin. Interestingly, of the 15,290 transactions of this type, corresponding to 2,582 unique Ethereum addresses, 774 of these addresses already appeared in our original Ethereum trace. These findings highlight that scammers move considerable proceeds to Ethereum and that the scamming on

Bitcoin appears to be conducted by the same actors as on Ethereum.

7.5 Discussion

Here we clarify what our paper does and does not show. Our methods capture the amount of funds flowing through exchanges controlled by persons or entities likely engaged in pig butchering activity. There are reasons to believe these totals may be either more or less than the sum of all global pig butchering dollar activity. Let us first discuss the reasons our numbers may overcount criminal funds. First, our totals capture funds flowing through exchanges and will include double counting if criminals move funds through more than one exchange. Since our results show that few criminal funds flow to Western-based exchanges, the amount of funds coming out of Western-based exchanges in our backtrace of $5.6 billion per year represents a lower bound on the amount from Western-based victims. Second, our methods will overestimate if we trace through deposit addresses controlled by other service providers. To avoid this possibility of aggregating funds through service providers we stop at any node that receives more than 2,000 transactions and demonstrate in robustness tests that our results are not highly sensitive to reducing this threshold to 1,000. Decreasing the number of hops under consideration in the trace path would also decrease the likelihood of following funds to an unrelated entity. In robustness tests, we show that our results have low sensitivity to the number of hops. This reduces but does not eliminate the risk that some funds could belong to unrelated parties. Furthermore, when following money leaving a given address, tracing the specific funds sent is more conservative than counting all potential paths downstream of an address. The latter method would implicate any address that is within a certain degree of separation downstream from the original address. Our approach only follows amounts using first-in first-out attribution, up to the original address outflows. We also perform robustness checks on large deposit addresses. Our results are not driven by a few large deposit addresses. Third, our methods include any financial activity occurring in the criminal network in a similar manner and not just pig butchering. For example, we found ransom payments paid by victims in our transactions that overlapped with pig butchering activity. Thus, the totals will represent not just romance scams but any other type of crypto activity that flows through related networks.

There are also other reasons why our numbers may understate flows related to pig butchering networks. First, our beginning point is only known nodes which we collect from a variety of sources,

yet this is likely only a small set of total criminal activity. As an example, our Figure 2 shows that around each reported node there are multiples of unreported nodes that engage in similar behavior forwarding to collection points. This aligns with the norm that only a small subset of financial crimes are reported.[49] The extent of unreported addresses in 2024 is likely large, particularly given the delay in reporting and the stop in some collection activity from USIP in late 2023. Thus, we focus on activity up to 2023. Second, our main results emphasize activity on Ethereum. However, we also show substantial reported activity in Bitcoin and Tron.[50] Third, and most importantly, our numbers are understated to the extent that we stop tracing funds at large unidentified nodes. These large, unidentified addresses could be shadow exchanges and could aggregate many other criminal funds.[51] We also do not trace through mixers, although relatively small amounts of pig butchering funds go to mixers. One reason scammers may avoid mixers like Tornado Cash is because mixing can taint funds such that KYC compliant exchanges may no longer accept their funds for uses like inducement payments. Overall, there are good reasons why our totals may be under or over counted. Our personal opinion is that given the conservative nature of the tracing criteria stopping at unknown nodes and not capturing activity on Tron, our totals of funds flowing through crypto exchanges are more likely to be undercounted than overcounted.

We think the range of the estimated scamming activity of $16.9 to $33.8 billion per year, while noisy, is instructive. We highlight a few differences and similarities to industry reports. Chainalysis (2024) estimates $4.6 billion of scamming activity in 2023. Although Chainalysis does not provide methodology details, their brief descriptions seem to indicate that they primarily focus on funds flowing to reported addresses. Notably, when discussing romance scams, they acknowledge: "this figure is likely just the tip of a much larger iceberg. Romance scams are notoriously underreported, and our analysis began from a limited set of reported instances" (Chainalysis (2024) page 108).[52]

[49] Anderson (2021) notes that only three percent of financial scams are reported.

[50] Anecdotal evidence suggest that Tron is popular in Southeast Asia and that scammers may prefer this for Asian victims. Our tracing methods can also be employed on the Tron blockchain but drawing inferences would likely be difficult given that there exists substantially less data that attributes Tron addresses to specific entities.

[51] If these funds reach another deposit address that we directly trace, then the funds would be captured. However, if the funds that we stopped tracing later enter a deposit address that is not included in the deposit address heuristic, then the funds would not be included in our base estimates. They may be included in sensitivity analysis.

[52] The size, scope, and sources of addresses used in Chainalyis reports remains unclear. For example, even if someone reported their data to the FBI at IC3, this data would not be distributed more broadly unless someone also reported the data directly to Chainalysis. To our knowledge, it is not the FBI's current policy to make this data public or available for commercial use, although our work shows that such distribution could be useful.

We agree that relying solely on reported addresses limits the completeness of any analysis, as can be seen from our tracing-based analysis. Finally, we also compare our results to the estimates of average U.S. victim loss of $210,760 (Global Anti-Scam Organization, 2022).[53] If estimates of 220,000 to 500,000 people engaged in scamming activity are accurate, then potential annual scamming volume could plausibly range from $46.4 to $105 billion if each worker scams even one person per year.[54]

Our paper also presents economic forces within the network structure. We highlight transaction costs and the usage of DeFi swap transactions, which typically include liquidity provided by U.S. based speculators. More importantly, we expose the systematic usage of inducement payments. These small profits returned to Western-based exchanges strengthen victim beliefs in the investment scheme and persuade them to liquidate their retirement accounts or go into debt (Global Anti-Scam Organization, 2022). The tracing procedure we introduce is critical in exposing inducement payments since these payments can only be found from tracing to deposit addresses.

Overall, we believe our paper's primary contribution is demonstrating how bulk tracing and blockchain forensics can be used to detect, monitor, and disrupt crypto activities on the Ethereum network. While other papers have examined these issues on Bitcoin (Foley et al., 2019; Makarov and Schoar, 2021), and some analysis has occurred on Ethereum (Cong et al., 2023a,b; Victor, 2020), our paper is the first (to our knowledge) to detail how bulk tracing and blockchain analytics can be used to analyze criminal activity on Ethereum. Our paper highlights the importance of such an approach. We conclude with practical implications from our analysis.

8 Conclusion and Implications

Our paper provides the first comprehensive examination of pig butchering scamming activity and shows many previously unknown facets about transnational organized crime networks. There are several practical implications of our study for enforcement agencies, policy makers, potential victims, the crypto industry, and academics. First, large crypto exchanges that purport to con-

[53] This average per victim from a survey of 550 victims is comparable to our numbers of $5.6 billion per year leaving Western exchanges (Section 5.6) divided by the 25,181 addresses receiving inducement payments at Western exchanges (Section 4.2), which yields an average of $223,568.

[54] Assuming an average of $210,760 per victim, the annual victim loss would be between $46.4 and $105 billion. If one used the median U.S. victim loss of $100,000 reported in the survey, this would be between $22 and $50 billion per year. These calculations are only illustrative as we do not know how often they ensnare a victim.

form to AML/KYC and KYT procedures like Binance, Huobi, OKX and others have acted as potential exit points for an average of $27.8 billion annually in criminal flows. Second, perhaps because of its relative stability and opacity, Tether serves as the crypto of choice for exiting the system, and decentralized exchanges also serve as large swapping points to obfuscate funds. Third, users who provide liquidity to these DeFi platforms (some of whom are U.S. and European-based crypto "hedge funds") and the prior listed exchanges with weaker AML/KYC provisions may be profiting simply by facilitating money laundering. Fourth, the consistent patterns and substantial cross-pollination across addresses indicate that these scams should thus not be treated simply as individual crimes, which is often the norm for law enforcement. Fifth, Western-based exchanges like Coinbase and Crypto.com provide common entry points for victims into the scam network. Users should be aware their funds in crypto exchange accounts can quickly disappear. Sixth, since these scamming networks also send thousands of small inducement payments back to these major exchanges, it is likely that most crypto exchanges are not adequately monitoring and protecting their customers from these networks. Similar to credit card companies flagging fraudulent transactions based on location and other transaction details, crypto exchanges could circumvent ongoing scams. We propose that better monitoring of inducement payments from pig butchering networks can safeguard clients from transferring additional funds to scammers.

More generally, our analysis shows that the "legitimate" crypto space commonly serves as the entry and exit point to the illegitimate space and thus facilitates the lifeblood that enables pig butchering and modern-day slavery. Our findings suggest that criminal networks move substantial funds easily, cheaply, and without much fear of detection. There is much that can be done to tighten capital controls on the funds feeding these large criminal networks. The public nature of the blockchain also offers future academic research a substantial role in building upon our approach to monitor and understand the economic forces of other criminal and non-criminal crypto activity.

References

Amiran, D., B. N. Jørgensen, and D. Rabetti. 2022. Coins for Bombs: The Predictive Ability of On-Chain Transfers for Terrorist Attacks. *Journal of Accounting Research* 60:427–466. URL https://onlinelibrary.wiley.com/doi/abs/10.1111/1475-679X.12430.

Anderson, K. B. 2021. To Whom Do Victims of Mass-Market Consumer Fraud Complain? URL http://dx.doi.org/10.2139/ssrn.3852323.

Anderson, R., I. Shumailov, and M. Ahmed. 2018. Making Bitcoin Legal. *Security Protocols XXVI* 11286:243–253. URL http://link.springer.com/10.1007/978-3-030-03251-7_29.

Barragan, C. 2023. The Romance Scammer On My Sofa. Atavis. URL https://magazine.atavist.com/the-romance-scammer-on-my-sofa-nigeria-yahoo-boys.

Capponi, A., G. Iyengar, and J. Sethuraman. 2023. Decentralized Finance: Protocols, Risks, and Governance. *Foundations and Trends® in Privacy and Security* 5:144–188. URL http://dx.doi.org/10.1561/3300000036.

Capponi, A., R. JIA, and Y. Wang. 2022. Maximal Extractable Value and Allocative Inefficiencies in Public Blockchains. *SSRN Electronic Journal* URL http://dx.doi.org/10.2139/ssrn.3997796.

Chainalysis. 2023. The 2023 Crypto Crime Report.

Chainalysis. 2024. The 2024 Crypto Crime Report.

Cong, L., K. Grauer, D. Rabetti, and H. Updegrave. 2023a. Blockchain Forensics and Crypto-Related Cybercrimes. URL http://dx.doi.org/10.2139/ssrn.4358561.

Cong, L. W., C. R. Harvey, D. Rabetti, and Z.-Y. Wu. 2023b. An anatomy of crypto-enabled cybercrimes.

Cong, L. W., and Z. He. 2019. Blockchain Disruption and Smart Contracts. *The Review of Financial Studies* 32:1754–1797. URL http://dx.doi.org/10.1093/rfs/hhz007.

Conrad, A. H., and J. R. Meyer. 1958. The Economics of Slavery in the Ante Bellum South. *Journal of Political Economy* 66:95–130. URL http://dx.doi.org/10.1086/258020.

Draca, M., and S. Machin. 2015. Crime and Economic Incentives. *Annual Review of Economics* 7:389–408. URL http://dx.doi.org/10.1146/annurev-economics-080614-115808.

El Siwi, Y. 2018. Mafia, money-laundering and the battle against criminal capital: the Italian case. *Journal of Money Laundering Control* 21:124–133. URL http://dx.doi.org/10.1108/JMLC-02-2017-0009.

Faux, Z. 2023. *Number Go Up*. Crown Currency.

Foley, S., J. R. Karlsen, and T. J. Putniņš. 2019. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? *The Review of Financial Studies* 32:1798–1853. URL https://doi.org/10.1093/rfs/hhz015.

FTC. 2023. Romance scammers' favorite lies exposed. Online Report. URL https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed#ft2.

Gandal, N., J. Hamrick, T. Moore, and T. Oberman. 2018. Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics* 95:86–96. URL https://www.sciencedirect.com/science/article/pii/S0304393217301666.

Global Anti-Scam Organization. 2022. Statistics of crypto-romance / pig-butchering scam. https://www.globalantiscam.org/post/statistics-of-crypto-romance-pig-butchering-scam.

Goffman, E. 1952. On Cooling the Mark Out: Some Aspects of Adaptation to Failure. *Psychiatry* 15:451–463. URL http://dx.doi.org/10.1080/00332747.1952.11022896.

Griffin, J. M., and S. Kruger. 2024. What is Forensic Finance? University of Texas, Working Paper. URL http://dx.doi.org/10.2139/ssrn.4490028.

Griffin, J. M., and A. Shams. 2020. Is Bitcoin Really Untethered? *The Journal of Finance* 75:1913–1964. URL https://onlinelibrary.wiley.com/doi/abs/10.1111/jofi.12903.

Hamrick, J., F. Rouhi, A. Mukherjee, A. Feder, N. Gandal, T. Moore, and M. Vasek. 2021. An examination of the cryptocurrency pump-and-dump ecosystem. *Information Processing and Management* 58:102506. URL https://www.sciencedirect.com/science/article/pii/S0306457321000169.

Harvey, C. R., T. Abou Zeid, T. Draaisma, M. Luk, H. Neville, A. Rzym, and O. van Hemert. 2022. An Investor's Guide to Crypto. URL http://dx.doi.org/10.2139/ssrn.4124576.

Leukfeldt, E. R., E. R. Kleemans, E. W. Kruisbergen, and R. A. Roks. 2019. Criminal networks in a digitised world: on the nexus of borderless opportunities and local embeddedness. *Trends in Organized Crime* 22:324–345. URL http://dx.doi.org/10.1007/s12117-019-09366-7.

Levi, M. 2015. Money for Crime and Money from Crime: Financing Crime and Laundering Crime Proceeds. *European Journal on Criminal Policy and Research* 21:275–297. URL http://dx.doi.org/10.1007/s10610-015-9269-7.

Li, T., D. Shin, and B. Wang. 2018. Cryptocurrency Pump-and-Dump Schemes. Working Paper.

Makarov, I., and A. Schoar. 2021. Blockchain Analysis of the Bitcoin Market. Working Paper. URL http://dx.doi.org/10.3386/w29396.

Makarov, I., and A. Schoar. 2022. Cryptocurrencies and Decentralized Finance (DeFi). Working Paper. URL http://dx.doi.org/10.3386/w30006.

Meiklejohn, S., M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage. 2013. A fistful of bitcoins: characterizing payments among men with no names. *Proceedings of the 2013 conference on Internet measurement conference* pp. 127–140.

Mirenda, L., S. Mocetti, and L. Rizzica. 2022. The Economic Effects of Mafia: Firm Level Evidence. *American Economic Review* 112:2748–2773. URL http://dx.doi.org/10.1257/aer.20201015.

Moore, T., R. Clayton, and R. Anderson. 2009. The Economics of Online Crime. *Journal of Economic Perspectives* 23:3–20. URL http://dx.doi.org/10.1257/jep.23.3.3.

Pennec, G. L., I. Fiedler, and L. Ante. 2021. Wash trading at cryptocurrency exchanges. *Finance Research Letters* 43:101982. URL https://www.sciencedirect.com/science/article/pii/S1544612321000635.

Phua, K., B. Sang, C. Wei, and G. Y. Yu. 2022. Don't trust, verify: The economics of scams in initial coin offerings.

PWC. 2023. 5th Annual Global Crypto Hedge Fund Report. URL https://www.pwc.com/gx/en/new-ventures/cryptocurrency-assets/5th-annual-global-crypto-hedge-fund-report-july-2023.pdf.

Reiter, J., and Bitrace. 2024. Connecting Chinese and American Scam Victims. Working Paper.

Sokolov, K. 2021. Ransomware activity and blockchain congestion. *Journal of Financial Economics* 141:771–782. URL https://www.sciencedirect.com/science/article/pii/S0304405X21001422.

Solomon, F. 2023. China Unleashes Crackdown on 'Pig Butchering.' (It Isn't What You Think.). Wall Street Journal. URL https://www.wsj.com/world/asia/china-unleashes-crackdown-on-pig-butchering-it-isnt-what-you-think-d623ada3.

Soudijn, M., and P. Reuter. 2016. Cash and carry: the high cost of currency smuggling in the drug trade. *Crime, Law and Social Change* 66:271–290. URL http://dx.doi.org/10.1007/s10611-016-9626-6.

UN. 2023. Online Scam Operations and Trafficking Into Forced Criminality In Southeast Asia: Recommendations For A Human Rights Response.

US Department of the Treasury. 2002. 2002 National Money Laundering Strategy.

US Department of the Treasury. 2007. 2007 National Money Laundering Strategy.

U.S. Senate. 2018. Combating Money Laundering and Other Forms of Illicit Finance. Online Transcript: https://www.govinfo.gov/content/pkg/CHRG-115shrg29913/html/CHRG-115shrg29913.htm.

Victor, F. 2020. *Address Clustering Heuristics for Ethereum*, p. 617–633. Springer International Publishing. URL http://dx.doi.org/10.1007/978-3-030-51280-4_33.

Wang, F., and V. Topalli. 2022. Understanding Romance Scammers Through the Lens of Their Victims: Qualitative Modeling of Risk and Protective Factors in the Online Context. *American Journal of Criminal Justice* 49:145–181. URL http://dx.doi.org/10.1007/s12103-022-09706-4.

Wang, F., and X. Zhou. 2023. Persuasive Schemes for Financial Exploitation in Online Romance Scam: An Anatomy on *Sha Zhu Pan in* China. *Victims & Offenders* 18:915–942. URL https://www.tandfonline.com/doi/full/10.1080/15564886.2022.2051109.

Xia, P., H. Wang, B. Zhang, R. Ji, B. Gao, L. Wu, X. Luo, and G. Xu. 2020. Characterizing cryptocurrency exchange scams. *Computers & Security* 98:101993. URL http://dx.doi.org/10.1016/j.cose.2020.101993.

9 Figures and Tables

Figure 1. Network graph of reported addresses and traced funds

This figure shows the flow of funds following the movement from a subset of reported scammer addresses. Edges that are concave up represent flows moving from left to right (e.g., the curve moves as if going from 9 o'clock to 3 o'clock). Similarly, edges that are concave down represent flows moving from right to left (e.g., from 3 o'clock to 9 o'clock). Nodes are colored by identity, as described in the legend below, and their size is proportional to the total amount transacted. Edges are colored by transaction size and identity. Green edges are transactions from exchanges, while blue and purple are transactions to exchanges. Edges entering or exiting exchanges with darker colors represent larger transactions. Except for exchanges, any given node is positioned closest to any other nodes it transacts with the most. For simplicity, the nodes are a 2% sample of the total number of traced nodes.

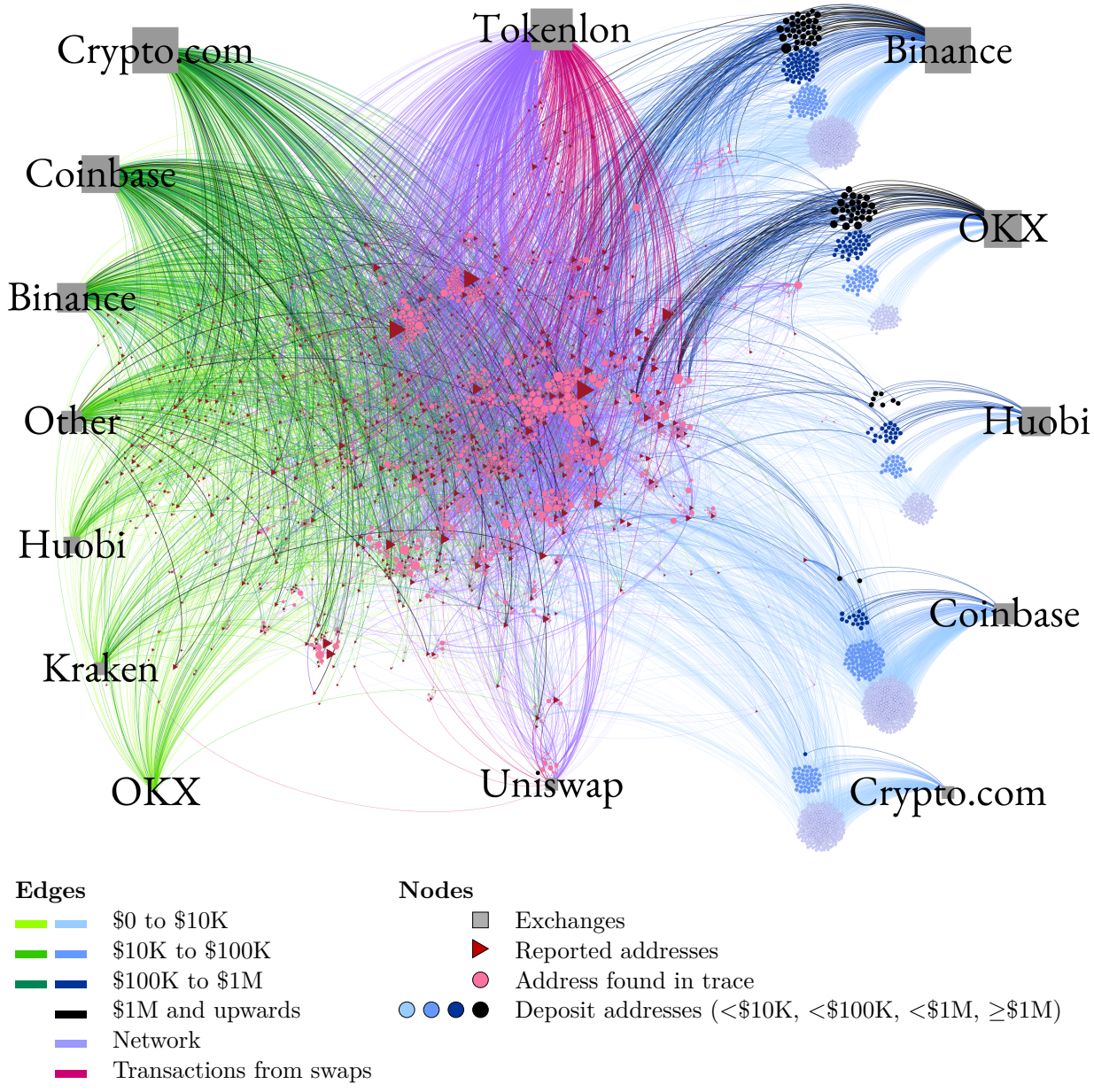
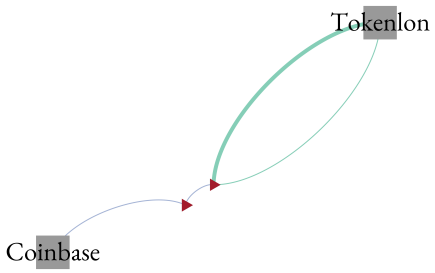
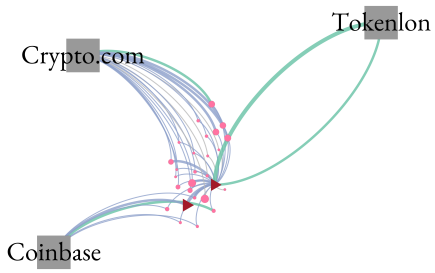


Figure 2. Network trace of two scammer addresses from one victim report
This figure shows the flow of funds that can be attributed to a victim report. The report includes two addresses plotted in dark red in Panel A. The victim sent funds to the left red node and were later transferred to the right red node, which swapped the funds into Tether. Panel B and C plot the trace originating from the right red address or collection node, with Panel B plotting the other inflows into the collection node (i.e., right red node), and Panel C plotting the trace of the swapped funds leaving the collection node. Edge colors correspond to the most commonly transacted token between nodes (see bottom left legend). All other conventions follow Figure 1.

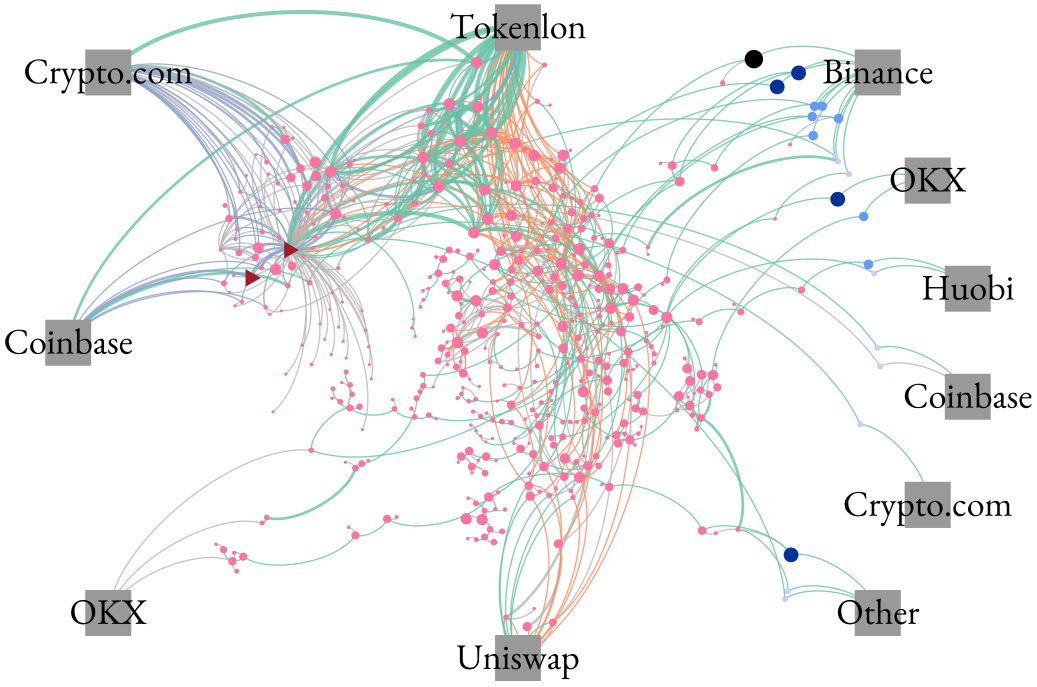
(a) Trace part of the first reported address



(b) Other flow into the reported collection point



(c) Trace paths from the reported collection point



Edges
ETH
USDT
USDC
DAI

Nodes
Reported addresses
Address found in trace
Deposit addresses (<$10K, <$100K, <$1M, ≥$1M)

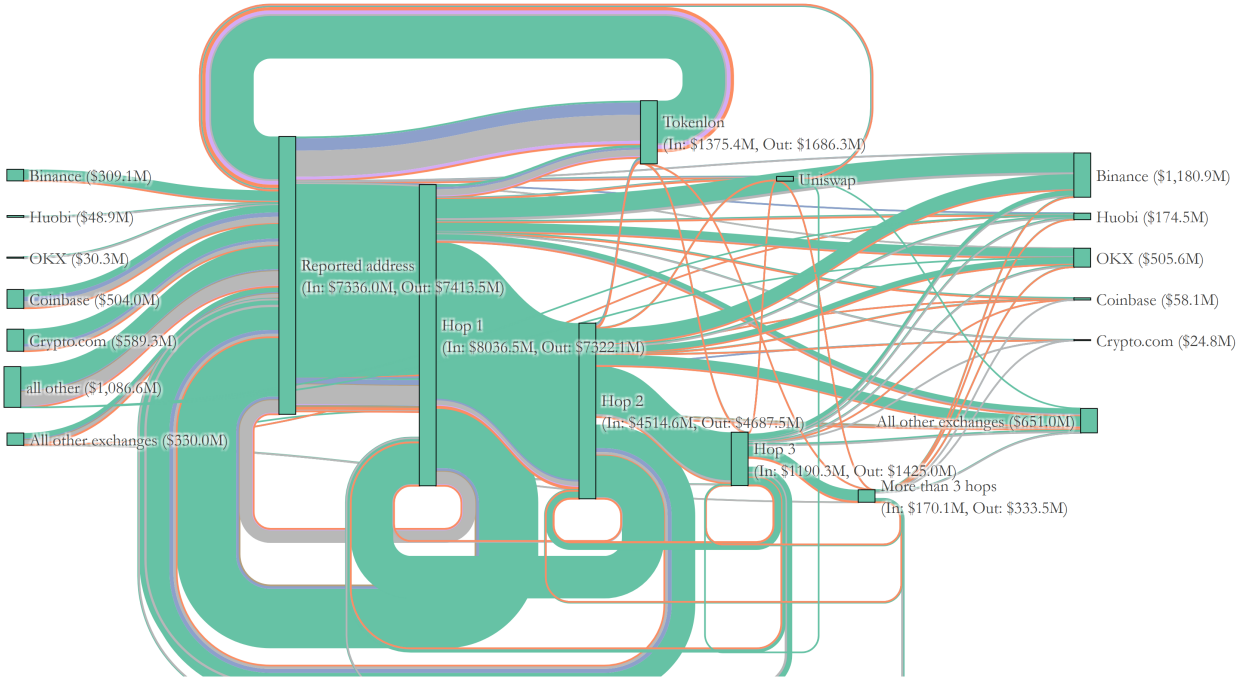
Figure 3. Overview of reported scammer addresses
This figure shows the distribution of the size of reported addresses. The horizontal axis plots the number of all transactions in log scale, based on the number of unique transaction hashes. The vertical axis plots the total amount traced to each address in log scale, which is the same as the total inflow for these addresses. The colors indicate the most commonly transacted token for each address as described in the legend.



Figure 4. Total flow of traced funds

This figure shows the flow of funds traced through reported scammer addresses. Traced funds include those received by scammers and later sent to other addresses. In Panel A, addresses are grouped into nodes based on the number of hops within the trace we encounter each address. Exchange addresses are identified using Etherscan and large exchanges are displayed as their own node. Nodes are sized based on the total combined inflow and outflow. Edges are displayed for each cryptocurrency type tracked, with colors displayed in the legend below. Totals in net transactions within each node (e.g., excludes transactions between two reported addresses). Panel B plots the exchange-related inflows and outflows of the network, such that transactions between non-exchange addresses are excluded. The columns of outflows in hops 1-6 sum to the total outflow in the right.

(a) Sankey diagram of all flows



(b) Exchange-related flows

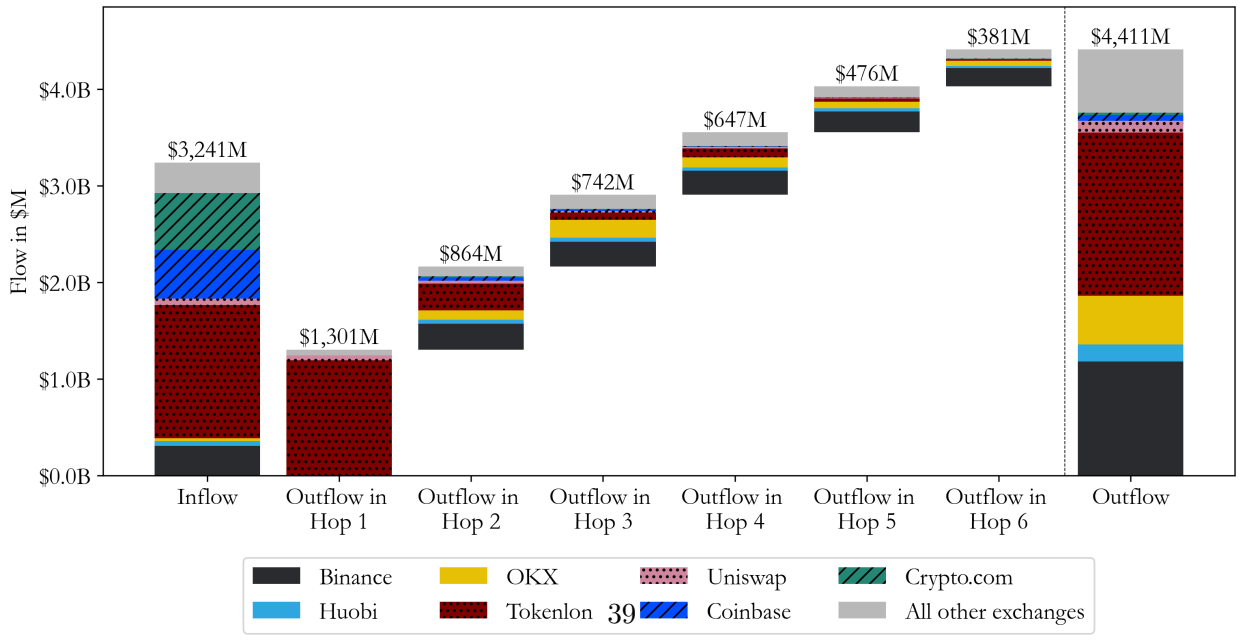


Figure 5. Distribution of deposit addresses

This figure shows the distribution of traced deposit addresses, decomposed by exchange and by size of each deposit address. Deposit addresses are grouped based on the total amount traced to each address, with the breakdown displayed in the horizontal axis as grouped bins. The total of each group is then split by exchange, with colors indicated in the legend. The total number of addresses in each bin is presented at the top of each bar. The left vertical axis indicates the share of each bin. The right vertical axis indicates the total amount traced to each bar.

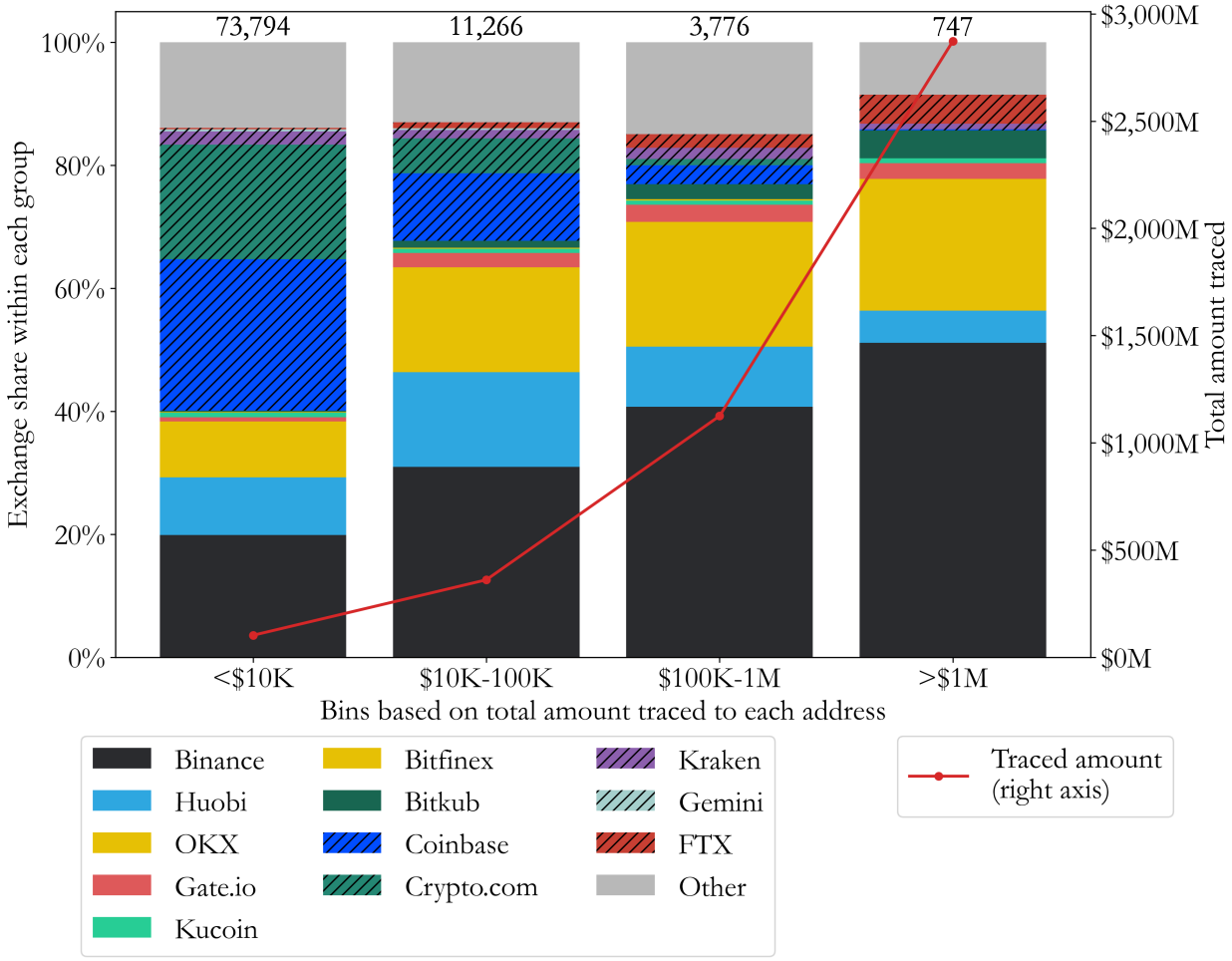
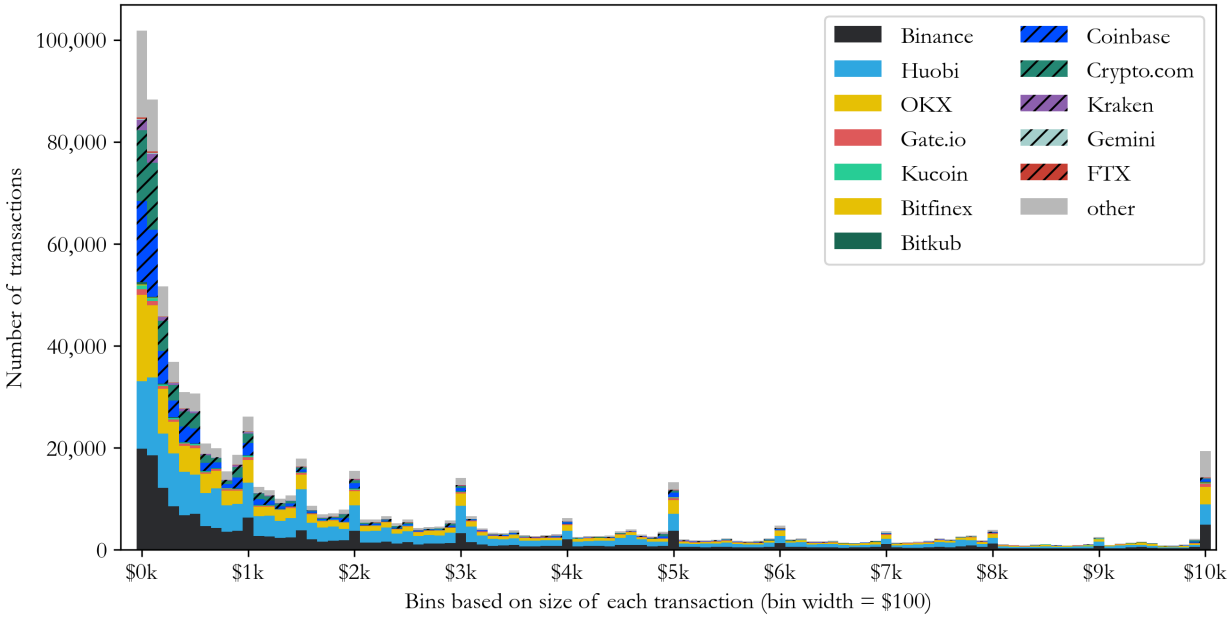


Figure 6. Payments to small deposit accounts
This figure shows the distribution of transaction sizes for accounts that received less than $100,000. The horizontal axis plots the size of the transaction and the vertical axis plots the corresponding number of transactions for each size. Exchanges are colored based on the legend.

(a) Transactions to small addresses



(b) Transactions to small addresses, magnified to those under $2,000

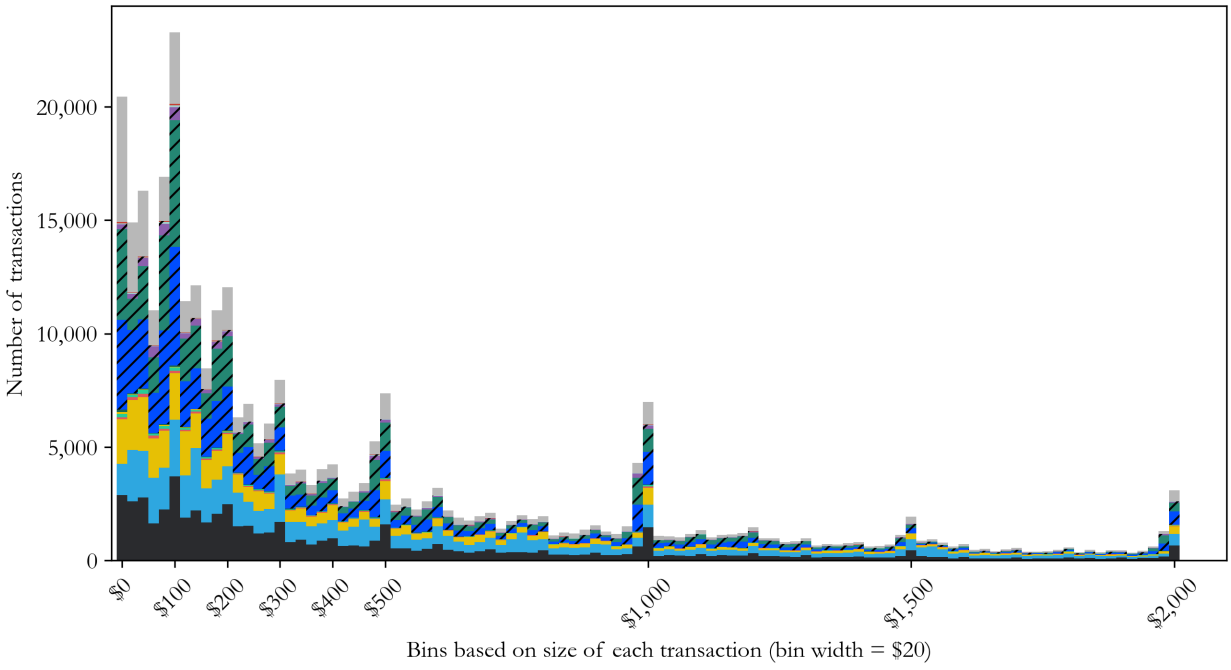
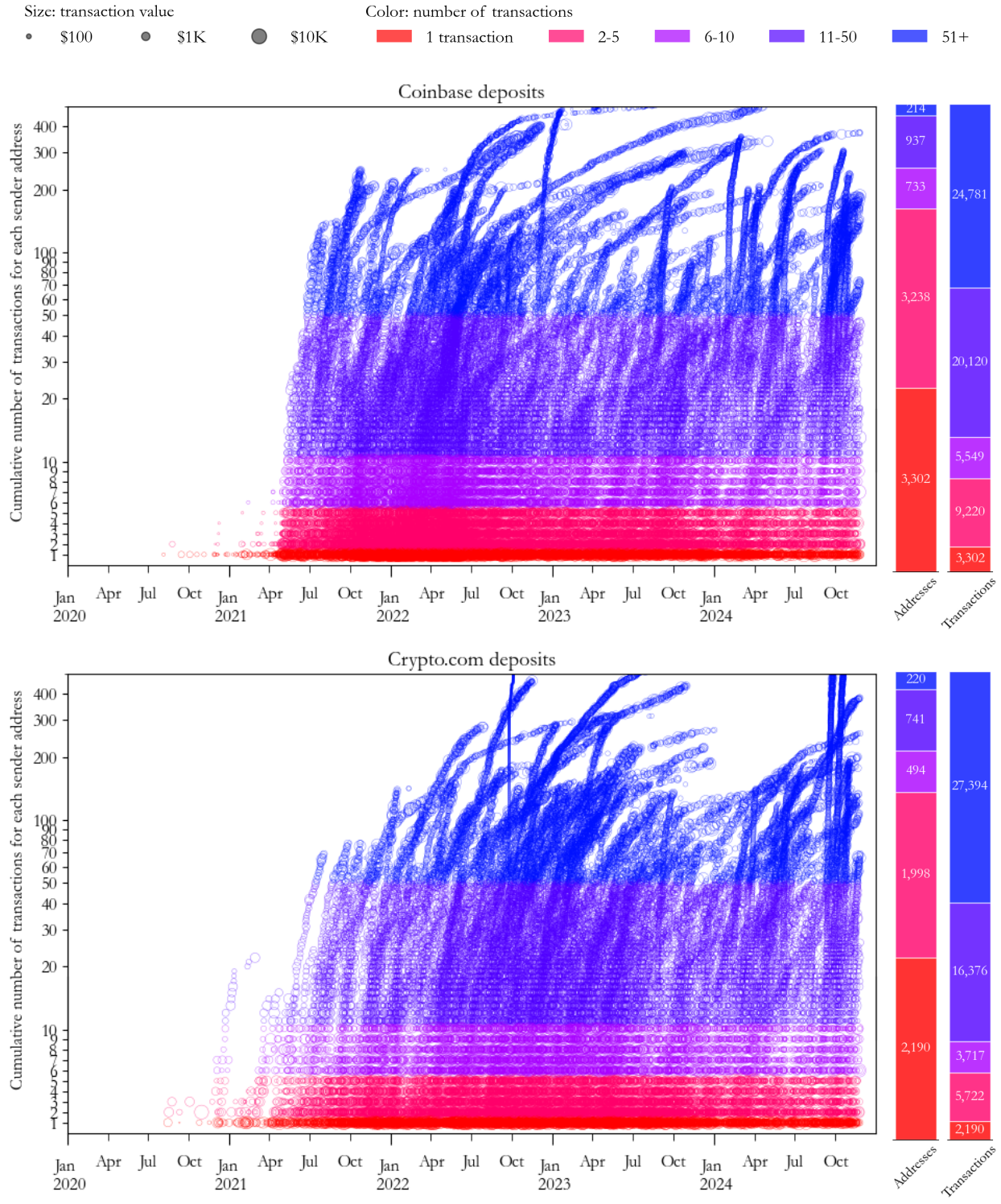
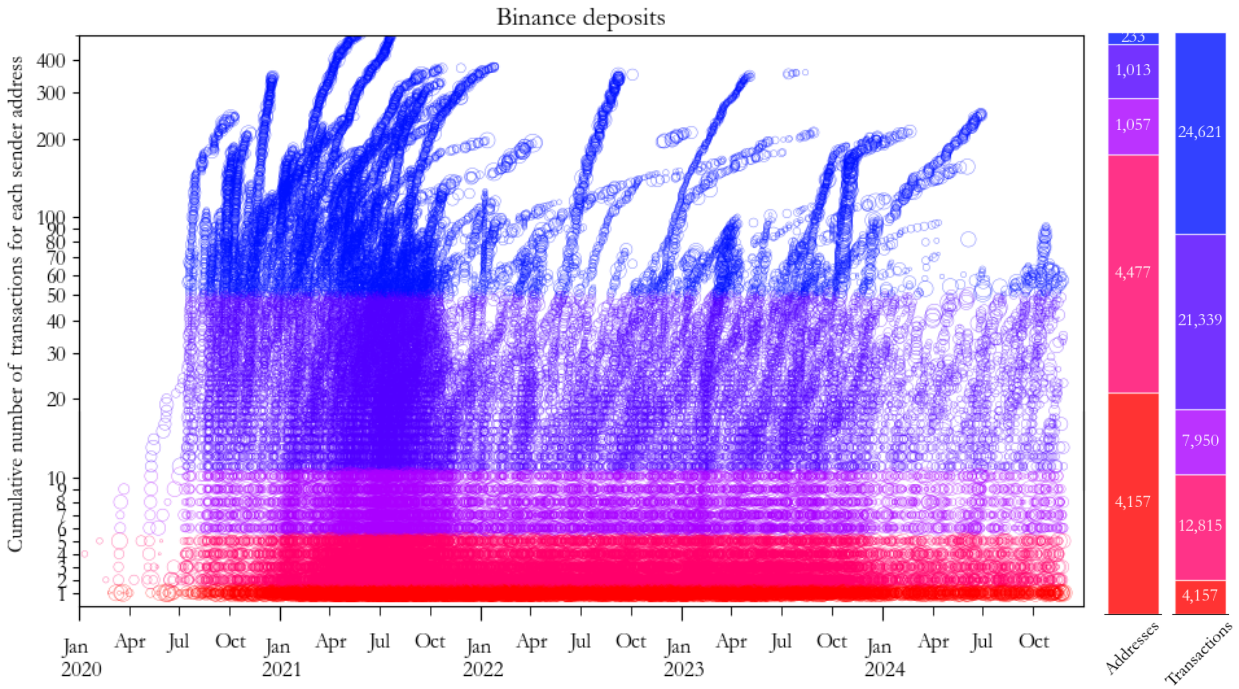


Figure 7. Transactions sent to exchanges

This figure shows the activity of individual addresses that send transactions to Coinbase (Panel A), Crypto.com (Panel B), Binance (Panel C), and Huobi (Panel D). Each dot is a single transaction. The horizontal axis plots time. The vertical axis plots the cumulative number of transactions initiated by each sender to a given exchange as of that date. Colors encode the number of transactions by each sender-exchange relationship. Dot size indicates transaction size. Bars on the right-hand side show the distribution of addresses and values across the color groups. This sample is restricted




Binance deposits
Cumulative number of transactions for each sender address
400
300
200
100
90
80
70
60
50
40
30
20
10
9
8
7
6
5
4
3
2
1
Jan 2020
Apr
Jul
Oct
Jan 2021
Apr
Jul
Oct
Jan 2022
Apr
Jul
Oct
Jan 2023
Apr
Jul
Oct
Jan 2024
Apr
Jul
Oct
235
1,013
1,057
4,477
4,157
24,621
21,339
7,950
12,815
4,157
Addresses
Transactions

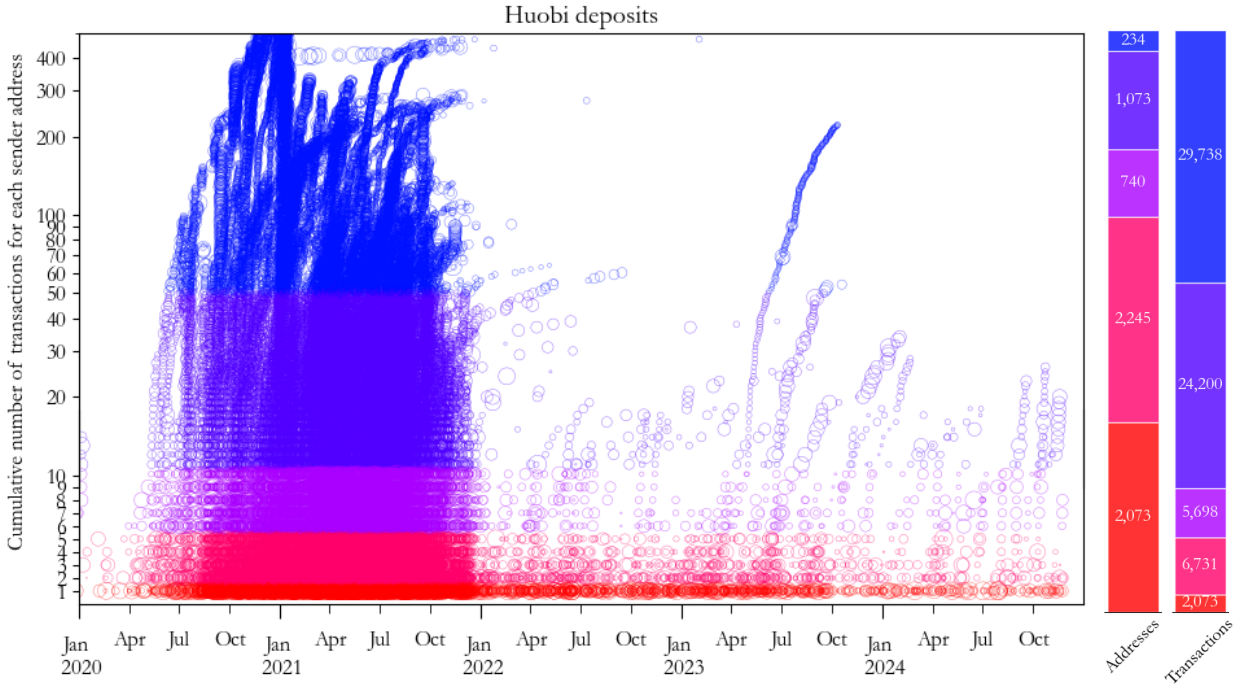
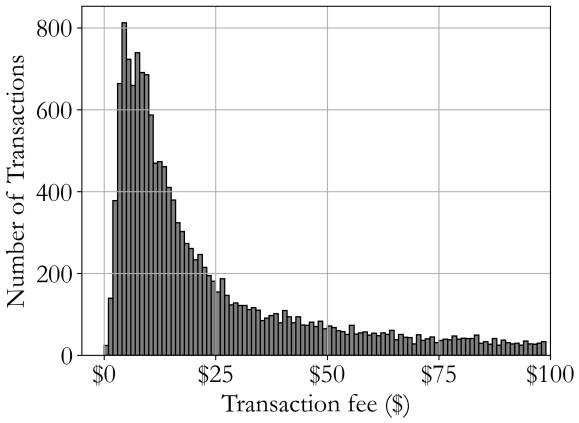

Huobi deposits
Cumulative number of transactions for each sender address
400
300
200
100
90
80
70
60
50
40
30
20
10
9
8
7
6
5
4
3
2
1
Jan 2020
Apr
Jul
Oct
Jan 2021
Apr
Jul
Oct
Jan 2022
Apr
Jul
Oct
Jan 2023
Apr
Jul
Oct
Jan 2024
Apr
Jul
Oct
234
1,073
740
2,245
2,073
29,738
24,200
5,698
6,731
2,073
Addresses
Transactions

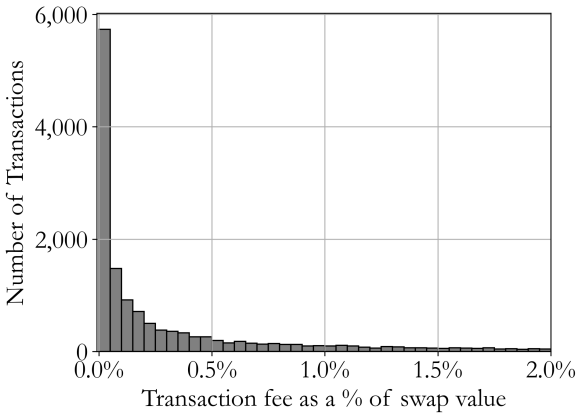
Figure 8. Transaction fees for swaps

This figure shows the distribution of fees paid for token swaps. Panel A plots the gas fees paid per swap transaction in dollars and truncates the data at $100 to improve visual clarity. This is also similar to gas fees paid for simple Ether (ETH) and token transfers, which are not included in this figure. Panel B plots gas fees as a percent of the total transaction amount and truncates data at 2%. Panel C plots swap net profit and truncates values between -$2,000 and +$500. Panel D plots swap net profits as a percentage of total outgoing value from the swap and truncates values between -10% and +10%.

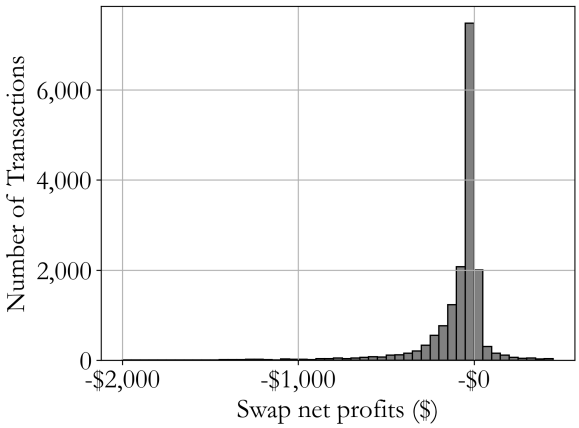
(a) Gas fees in dollars



(b) Gas fees as a % of total transferred amount



(c) Swap net profit in dollars



(d) Swap net profit as a % of total outgoing value

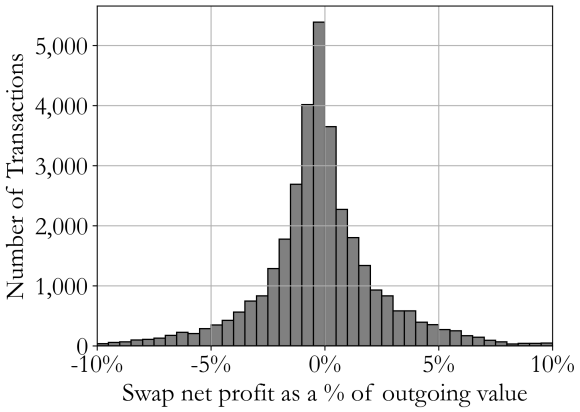


Figure 9. Total inflow to associated deposit addresses
This figure plots the total inflow to associated deposit addresses over time, sorted by the controlling exchange, with the corresponding total amounts in the legend.

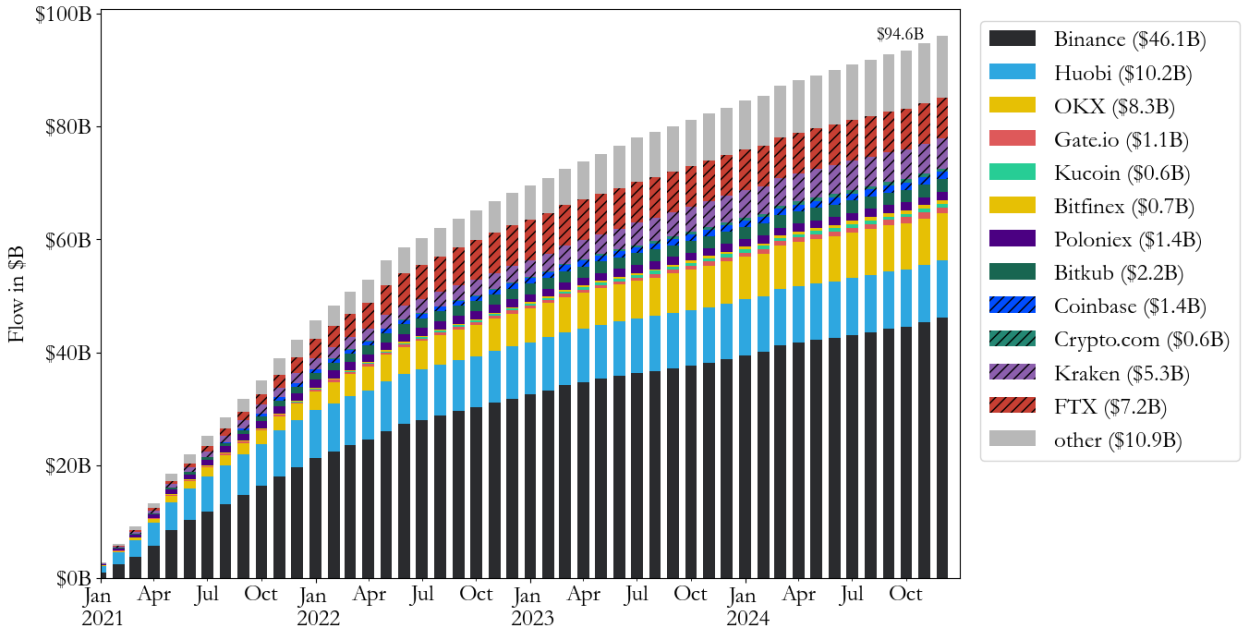


Figure 10. Sources of flows to scammer networks
This figure plots the originating exchange of funds that later flow into our traced scammer network addresses, with the horizontal axis representing the total flow for each exchange on the vertical axis. This considers any addresses found within the forward or backward trace that had less than 2,000 transactions, transacts with less than five tokens, only uses included functions, and is not an otherwise already identified exchange. Transaction flows are grouped according to whether the transactions are less than $100,000, between $100,000 and $500,000, or greater than $500,000; respectively these groups are represented by lighter and darker shades of the corresponding exchange color. We present the sum of each at the top of each bar, and the sum of transactions less than $500,000 is presented in parentheses.

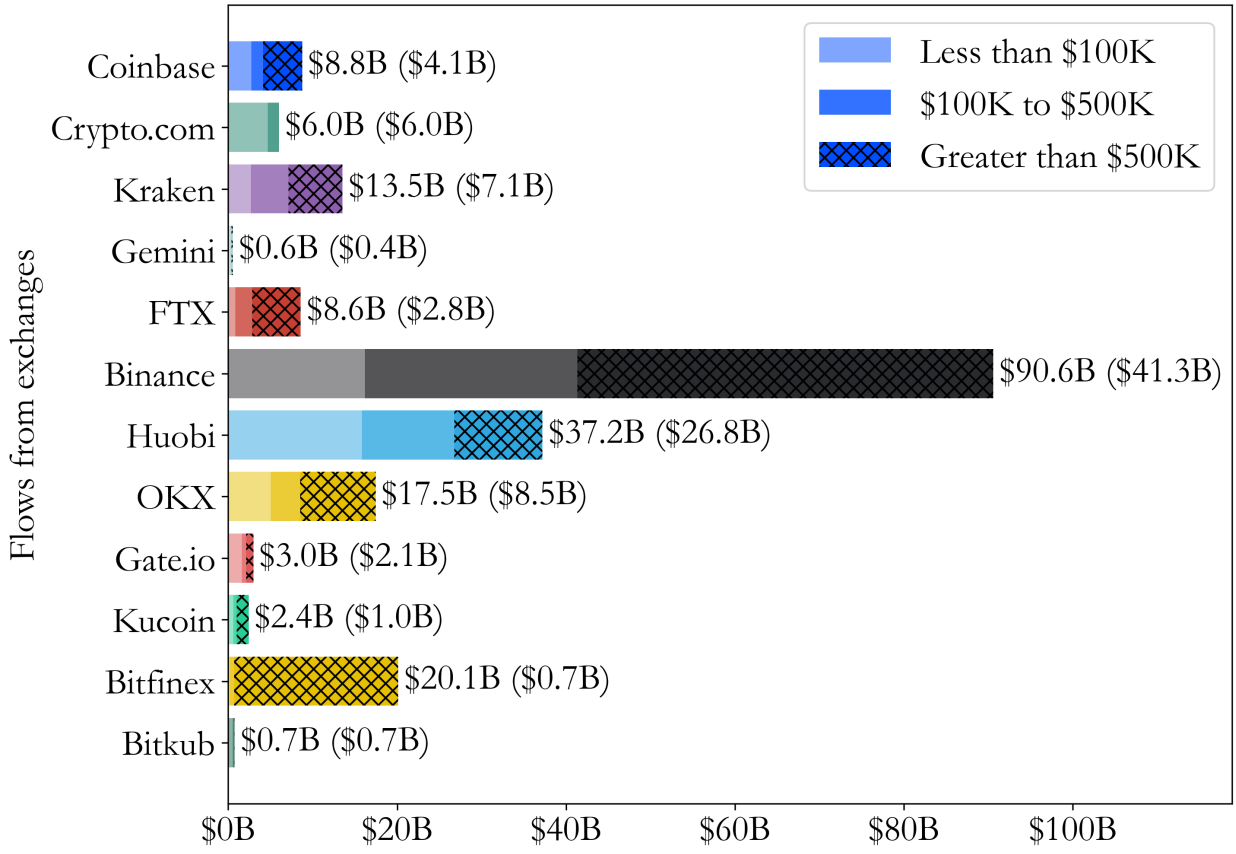


Figure 11. Inflow to associated deposit addresses

This figure shows inflows over time, decomposed by hour of inflow. The horizontal axis represents monthly activity. In Panel A, the vertical axis represents the time-of-day of activities in UTC, with each square proportional to the number of transactions that occurred in that hour. Squares are colored by prevalence of U.S.-based exchanges as a share of the total number of transactions. U.S.-based exchanges are defined as Coinbase, Crypto.com, Kraken, Gemini, and FTX. The vertical dotted red line demarcates the date that Chinese authorities banned crypto trading. Panel B plots the weekly flow into deposit addresses of Binance, Huobi and OKX. Major law enforcement operations are shown here as vertical dotted red lines. Sources are in Table IA.2.

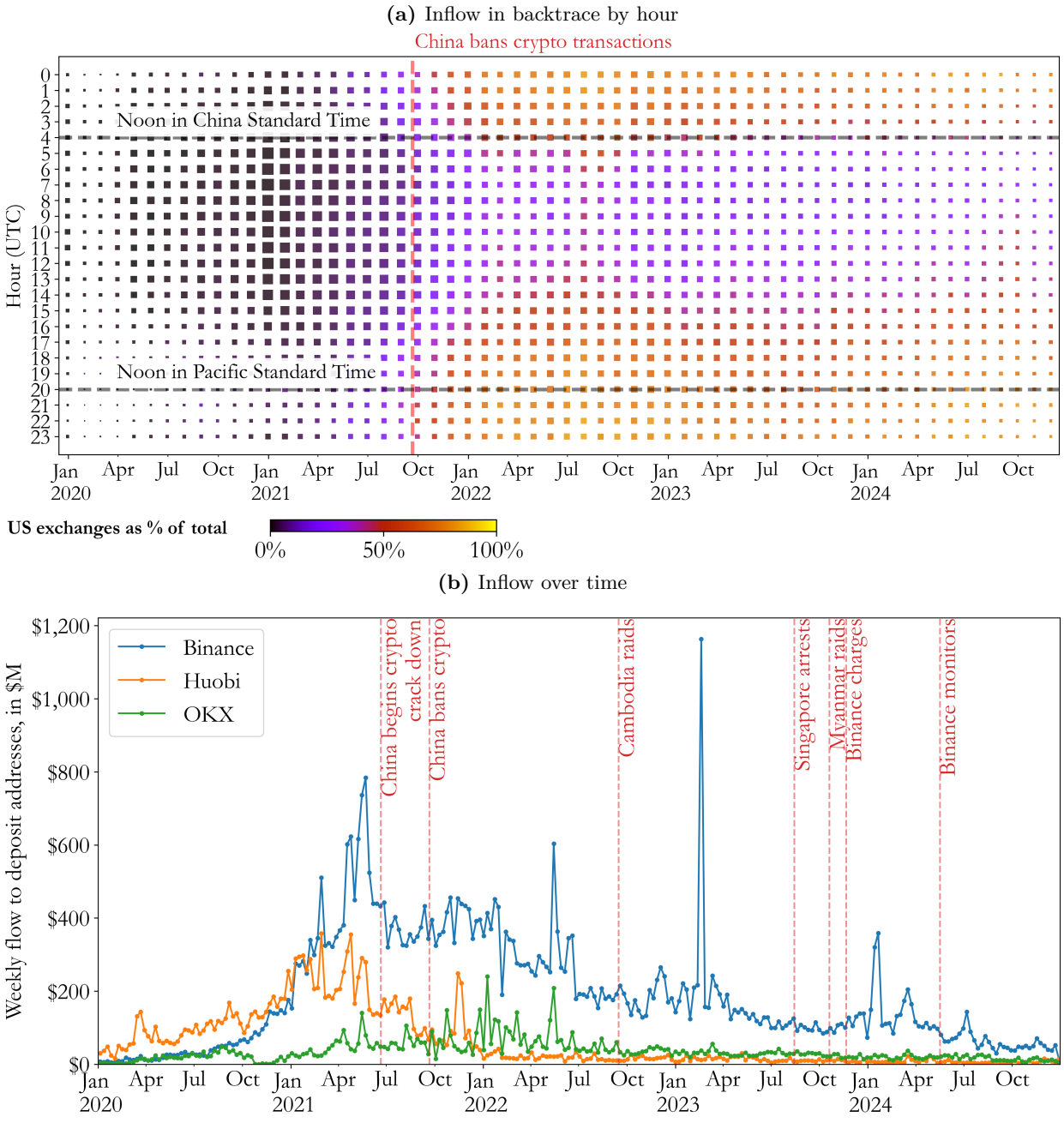
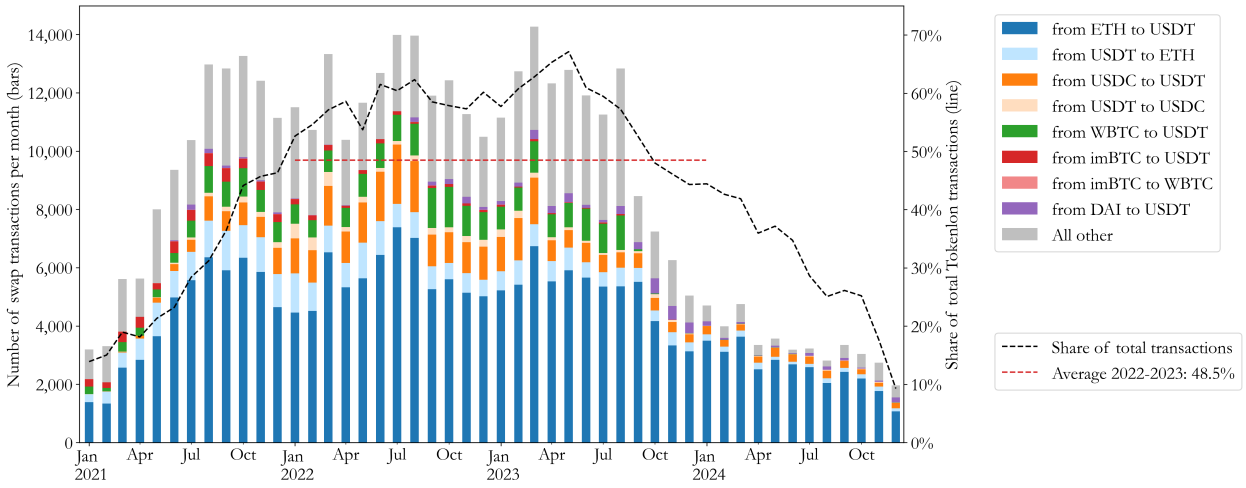


Figure 12. Tokenlon swaps

This figure shows all Tokenlon swaps transacted within either the forward or backward trace. Panel A shows the total number of transactions over time, with counts plotted on the left-hand vertical axis and colors indicating the swapped currencies, as displayed in the legend. The right-hand vertical axis describes these bars as a percent of the total Tokenlon number of transactions. Panel B plots a transition matrix of the most common swaps. The left-hand-side rows label outgoing currencies and the top columns label incoming currencies from each swap. The numbers represent the counted number of times each swap occurs in the trace, and square size is proportional to the numbers.

(a) Tokenlon swaps over time



(b) Tokenlon swaps transition matrix

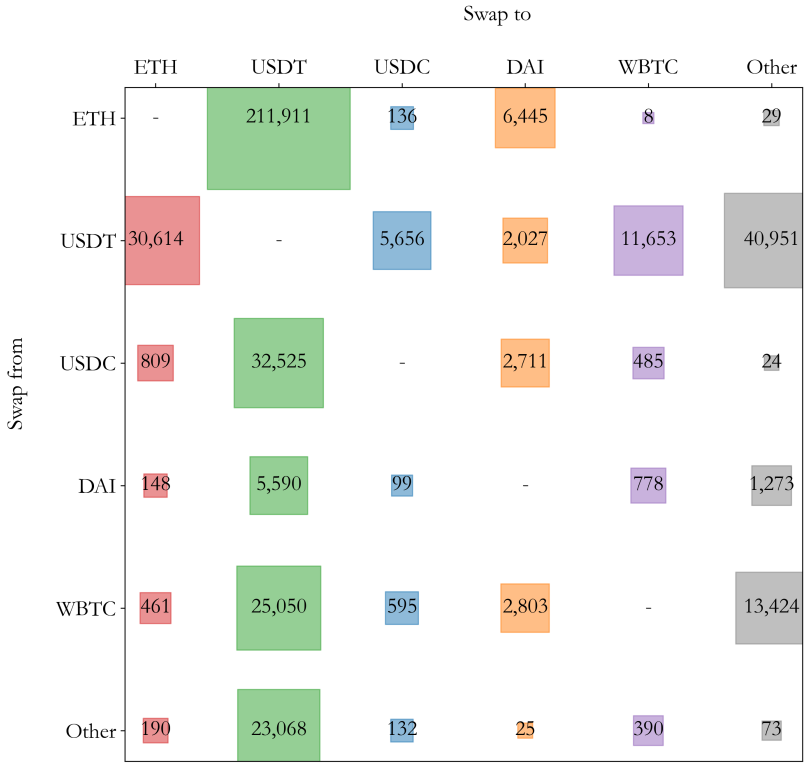
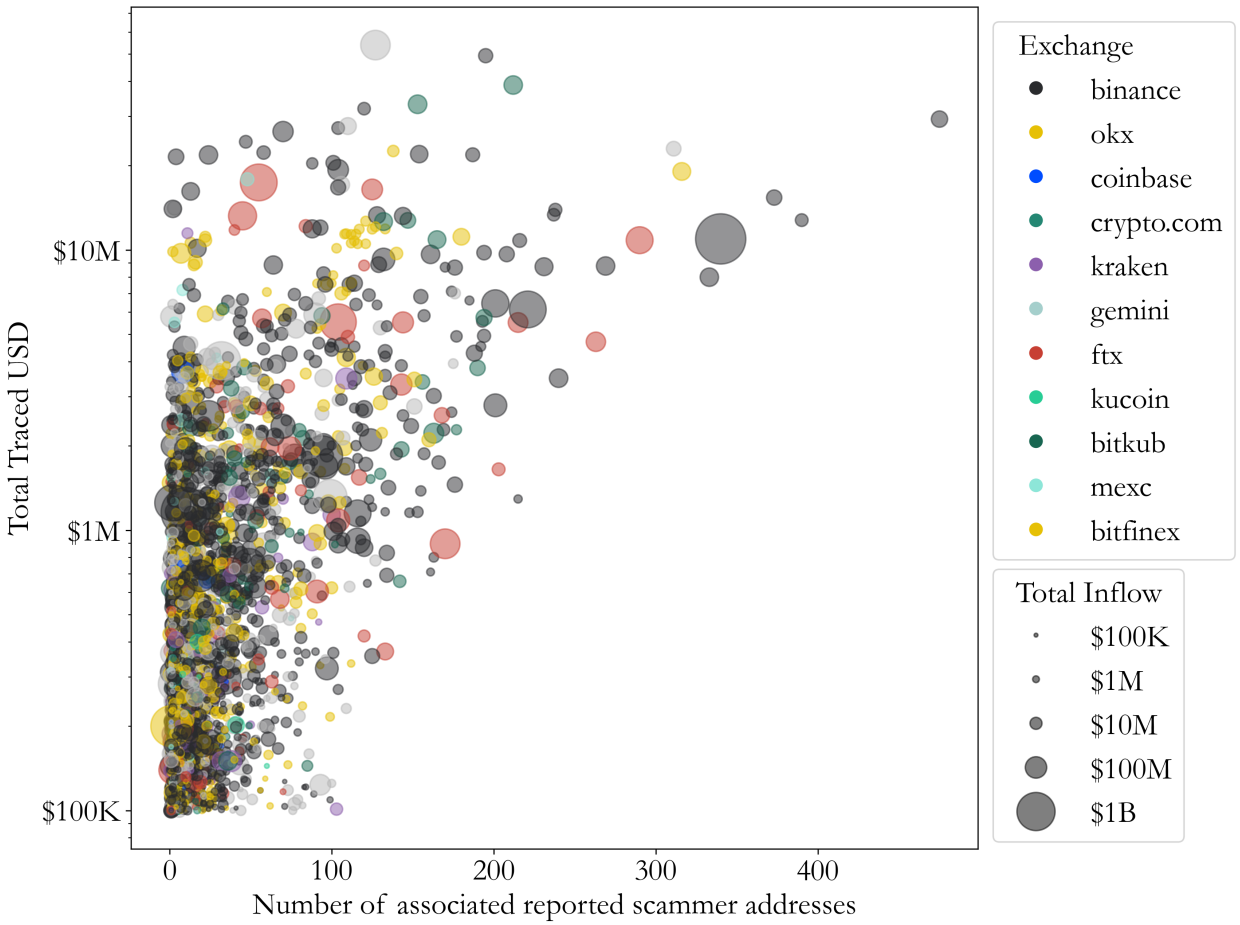


Figure 13. Sources for large deposit addresses
Panel A plots the number of different seed addresses that correspond to the largest deposit addresses. The horizontal axis plots the number of corresponding originally reported scammer addresses related to each deposit address, and the vertical axis plots the total amount traced to each deposit address. The histogram in Panel B shows the distribution of associated reported addresses in comparison to their associated deposit address.

(a) Sources by traced amount



(b) Distribution of associated reported to deposit addresses

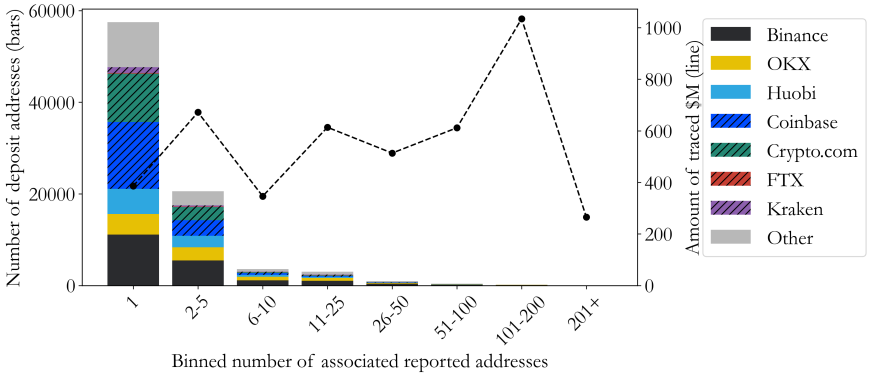


Table 1. Ethereum victim-reported scammer address summary statistics
This table presents summary statistics on victim-reported addresses on the Ethereum blockchain. The transaction count is the number of traced transactions, and the total inflow and outflow are the respective sums of all transacted funds into and from the reported scammer addresses. The average transaction size is the sum of transacted amounts divided by the transaction count. Days active is the number of days between the first and last transaction of each address. In and out degree respectively correspond to the number of distinct addresses sending in and receiving from the reported scammer addresses.

	count	mean	std	min	25%	50%	75%	max
Transaction Count	4,512	188	292	1	23	78	224	1,992
Total Inflow ($K)	4,512	1,898	8,034	0	55	325	1,359	251,247
Total Outflow ($K)	4,512	1,868	7,825	0	54	322	1,325	250,941
Average Transaction Size ($K)	4,512	20	51	0	3	8	20	2,006
Days Active	4,512	168	224	0	26	79	218	2,499
In Degree	4,512	33	67	1	5	14	33	1,456
Out Degree	4,512	25	55	0	4	9	25	1,289

Table 2. Deposit address summary statistics

This table presents summary statistics on deposit addresses. The transaction count is the number of traced transactions, and the total inflow and outflow are the respective sums of all transacted funds to and from the deposit addresses. The average transaction size is the sum of transacted amounts divided by the transaction count. Days active is the number of days between the first and last transaction of each address. In and out degree respectively correspond to the number of distinct addresses sending in and receiving from the reported scammer addresses. Panel A is a subsample for large deposit addresses receiving greater than or equal to $100,000 from the traced network; Panel B is a subsample for the remaining deposit addresses with less than $100,000 traced.

Panel A. Large deposit addresses ($\geq$ \$100K)	count	mean	std	min	25%	50%	75%	max
Transaction Count	3,476	158	223	2	30	81	188	1,961
Total Inflow (\$K)	3,476	10,643	64,411	100	729	2,193	6,770	2,801,075
Total Outflow (\$K)	3,476	10,614	63,741	100	729	2,195	6,770	2,748,749
Average Transaction Size (\$K)	3,476	139	419	1	30	62	129	16,071
Days Active	3,476	463	400	0	138	380	711	2,467
In Degree	3,476	18	23	1	5	10	22	252
Out Degree	3,476	3	3	1	2	3	4	24

Panel B. Small deposit addresses ($<$ \$100K)	count	mean	std	min	25%	50%	75%	max
Transaction Count	82,597	26	82	1	3	5	15	1,959
Total Inflow (\$K)	82,597	353	7,008	0	0	2	21	1,106,257
Total Outflow (\$K)	82,597	354	7,082	0	0	2	21	1,143,940
Average Transaction Size (\$K)	82,597	10	203	0	0	1	3	44,371
Days Active	82,597	272	340	0	6	125	455	2,722
In Degree	82,597	5	11	1	2	2	4	1,089
Out Degree	82,597	2	1	0	2	2	3	49

Table 3. Transaction costs within the trace network

This table presents summary statistics on the cost of transactions that occurred within the trace. Transfer gas fees include all gas fees paid for Ether and ERC-20 gas fees. Transfer fee ratio is the gas fee paid divided by the total amount within the transaction. Swap gas is the gas fee associated with swap transactions and swap fee ratio is the gas fee divided by the total outgoing amount within a swap. Swap profit is the difference between the incoming and outgoing amounts. This difference is signed such that positive amounts represent a gain and negative amounts represent a loss from the swap.

Panel A. All transactions	count	mean	std	25th	50th	75th	Total ($)
Transfer Gas Fees ($)	1,419,317	5.56	9.2	1.18	2.46	6.22	7,887,593
Transfer Fee Ratio (%)		5.93%	60.04%	0.01%	0.1%	1.37%	
Swap Gas Fees ($)	49,793	41.94	57.26	7.59	17.36	53.99	2,088,477
Swap Fee Ratio (%)		2.83%	52.41%	0.05%	0.27%	1.25%	
Swap Profit ($)		-64.48	4019.49	-101.88	-12.07	14.6	-3,210,816
Swap Profit Ratio (%)		-0.52%	3.5%	-1.2%	-0.19%	0.29%	

Subpanels by transaction size:

Panel B: $< \$10K$	count	mean	std	25th	50th	75th	total ($)
Transfer Gas Fees ($)	887,841	4.88	8.49	1.07	2.19	5.16	4,331,476
Transfer Fee Ratio (%)		9.48%	75.69%	0.13%	0.68%	4.00%	
Swap Gas Fees ($)	27,311	37.10	50.41	6.94	15.36	46.93	1,013,166
Swap Fee Ratio (%)		5.04%	70.69%	0.31%	0.99%	2.99%	
Swap Profit ($)		-41.00	2609.97	-35.04	-5.71	3.55	-1,119,745
Swap Profit Ratio (%)		-0.86%	4.04%	-1.59%	-0.40%	0.29%	

Panel C: $\$10K$ to $\$1M$	count	mean	std	25th	50th	75th	total ($)
Transfer Gas Fees ($)	515,805	6.63	10.04	1.37	3.02	8.28	3,421,288
Transfer Fee Ratio (%)		0.02%	0.04%	0.00%	0.01%	0.02%	
Swap Gas Fees ($)	21,942	47.98	63.24	8.57	20.32	64.01	1,052,835
Swap Fee Ratio (%)		0.15%	0.28%	0.01%	0.05%	0.16%	
Swap Profit ($)		-99.10	4539.45	-316.08	-54.32	122.85	-2,174,368
Swap Profit Ratio (%)		-0.12%	2.66%	-0.76%	-0.08%	0.33%	

Panel D: $> \$1M$	count	mean	std	25th	50th	75th	total ($)
Transfer Gas Fees ($)	15,671	8.60	14.14	1.80	4.24	11.10	134,829
Transfer Fee Ratio (%)		0.0005%	0.0009%	0.0001%	0.0002%	0.0006%	
Swap Gas Fees ($)	540	41.62	92.88	8.05	17.79	43.33	22,476
Swap Fee Ratio (%)		0.0020%	0.0061%	0.0003%	0.0007%	0.0017%	
Swap Profit ($)		154.25	17561.01	-2057.97	-244.87	573.81	83,297
Swap Profit Ratio (%)		0.0828%	1.0740%	-0.0489%	-0.0098%	0.0185%	

Internet Appendix
How Do Crypto Flows Finance Slavery?
The Economics of Pig Butchering

A Data Generated from Victim Reports

We gather data on scammer addresses from a geographically diverse set of sources. The first source of addresses is directly from victims. These victims provided 35 unique Ethereum and Bitcoin addresses. The second source includes 38 addresses from journalists covering pig butchering scams. These addresses include both the scammer addresses shared by victims and scammer addresses from investigative reporters covering the scammers in Southeast Asia.

Third, we also use data collected by victim advocacy groups and other researchers. Jan Santiago from PIDCO and Raymond Hantho from Chainbrium shared a set of 12,554 addresses used in pig butchering scams. They gather data from victim groups, other partners, and by extracting data from direct scammer interactions. A portion of these addresses are attributed to sources as shown in Figure IA.1. This was collected for a report for the United States Institute of Peace and we thank USIP, Jan Santiago, and Raymond Hantho. We also have one Ethereum and four Tron addresses from International Justice Mission on locations where families impacted by human trafficking have been asked to pay ransoms.

Lastly, we use data from public forums such as bitcointalk.org, scamwatcher.com, and chainabuse.com. This includes 296,310 scam reports or 120,725 unique addresses and is not exclusively related to pig butchering. 57,756 of these addresses were categorized as "Other" scams; however, upon reading these victim reports, many are clearly related to pig butchering.[55]

We review 400 reports by hand and categorize them by the type of scam. These data are then used to train an OpenAI o3-mini model to classify the remaining victim reports. We use the Chat Completion API and use the feature where the model will rank the log likelihood of the next model token.[56]. Using this feature, we only keep reports if the model returned a ranked probability of $> 99\%$. This yields 8,354 addresses categorized as pig butchering scams. 2,122 of these reports were originally labeled by victims as pig butchering, romance, or fake returns, 4,652 were originally labeled as "Other," and the remainder were other scams.

In total, we begin our analysis with 18,165 addresses across the Ethereum, Bitcoin, and Tron addresses after removing duplicates across the datasets. We removed 445 addresses that have been publicly identified as exchanges, as reported on etherscan.com. Our data also contains addresses without transactions, either because they were extracted from scammer websites but did not successfully attract investments or because victim reports may contain invalid cryptocurrency addresses. In total, we use 10,200 addresses with actual transactions. After using the 2,000 transactions threshold as a cutoff, we are left with 9,902 addresses. We also exclude three outlier addresses with implausibly large outliers: THPvaUhoh2Qn2y9THCZML3H815hhFhn5YC, 0xe49f5543cf74db087399b6cc083c31b50fcada67, and

[55] For example, one report reads: *It started with a Matching that I received on Tinder, then the person sent me a message directly asking me how Im doing, then offered to switch to Whatsapp, thing done we kept in touch, from time to time. others she sends me screenshots of what she does showing me how much she earns per day, I doubted the first day knowing that I dont know the person so I called her in a video call and took a screen thereafter. I started on the platform with a small amount to test its reliability with the support of the scammer, she always explains to me what to do and how I can predict the results, I increased the amount afterward making sure that I can use all the features and everything is working fine I was able to withdraw $ 1000 then the scammer asked me that the curve is good and BTC can hit $ 40K when it was $ 20K, after having invested all my 10K savings and made 13K gain, I wanted to test the withdraw my money function, and I am amazed, I can no longer withdraw and they ask me to pay 40% on my earnings, I have started looking for terms of use that werent available on the site, then I started looking if this site is reliable on search engines until I found out that I was the victim of a scam, I have never been the victim of a scam before, but this time if the platform is so well done that you cannot doubt that it is a SCAM!.*

[56] This feature is described by OpenAI in this link.

0x0ed724bea3d48d2c5c725c8404f33459963a5127. The sample used for tracing has a total of 9,899 observations. This includes 590 addresses that have been included solely as a result of relabeling by the OpenAI model and were not mentioned in other sources.

Importantly, we have continued to gather data from victims, which influences our results. In an earlier draft, our dataset included 3,256 Ethereum addresses with $5,835 million in lifetime inflow and 770 Bitcoin addresses with $373 million. This draft includes 4,512 Ethereum addresses (39% increase) with $8,275 inflow (42% increase) and 4,394 Bitcoin addresses (6.3x increase) with $2,666 million (6.9x increase). As a result, the total flow we trace has increased; however, the lifetime inflow to deposit addresses has not proportionally increased because multiple origin addresses often lead to the same set of deposit addresses, as discussed in Section 7.

B Tracing Methodology

We trace all Ether and tokens that enter scammer addresses and follow the traced paths until any of the following termination criteria are met: (i) the path meets an identified exchange wallet; (ii) the path meets an unidentified but large address that has more than 2,000 transactions; (iii) the path reaches five hops; (iv) the path reaches an address that appears to be involved in any other type of non-pig butchering activities such as yield farming or NFT trading; or, (v) traced amounts diminish to be less than 0.00001 ETH or token quantities, which are known as "dusting" transactions designed to obfuscate tracing.

The first criteria terminate traces to any identified exchange wallet and ensures that we do not follow spurious flows leaving exchanges. This screen is the most commonly triggered criteria and thus we interpret our results as describing how flows enter exchanges. Trace paths reaching Binance, Huobi, OKX, Coinbase, Crypto.com, and Tokenlon account for 80.3% of terminated trace paths.

If a path ends at a centralized exchange wallet, then the penultimate node prior to that hop will be a user's deposit address at that exchange. We capture these addresses and further validate that they are deposit addresses by only storing those that: (i) never receive ERC-20 tokens from the exchange wallet; (ii) the average Ether transaction from the exchange is less than $1,000 (which could be transaction or gas fees); (iii) never send tokens directly to another entity (because these should come from the exchange wallet). To mitigate the influence of large addresses involved in activities other than pig butchering, we also exclude any deposit addresses that have more than 2,000 transactions or transact in more than five different ERC-20 tokens.

Second, we set a 2,000 transaction threshold to account for the possibility a given large address is an unlabeled exchange or over-the-counter organization acting as an exchange. If the threshold were higher, we would likely capture more funds as part of the network but the certainty in the results would decrease. Thus, there may be relevant deposit addresses that we do not capture.[57] This threshold also terminates paths that enter large, unidentified swap contracts. The only exceptions are basic Uniswap swap transactions and Tokenlon contracts, which warrant further investigation given their ubiquity. We restart the trace after Tokenlon swaps to uncover the ultimate deposit addresses.

While funds can be reliably traced beyond five hops, we terminate the trace because a large proportion of funds have already flowed to an exchange within five hops, as presented in Figure IA.5, and we wish to maximize the probability that the deposit addresses we reach are controlled by a scammer.[58] Additionally, calculating trace paths is computationally resource-intensive, and each incremental hop is costly.

We terminate paths that reach addresses involved in various other non-pig butchering activities. We create a list of included functions and a list of excluded functions and drop any address that uses a function

[57] If a deposit address within the full scammer network receives some funds from a large node that we do not trace through, then we may still include that deposit address in our network if it also receives funds from other smaller nodes in our path.

[58] In earlier analysis we performed tracing to ten hops, but observe that most funds reached destinations in the first five hops. This added more deposit addresses and increased the size of the network, but otherwise results were similar.

on the list of excluded functions. We determine these lists in three steps: (i) based on the background knowledge that pig butchering scammers often transfer and swap ERC-20 tokens, we include all functions listed on the Etherscan contracts for Tether, Wrapped ETH, Uniswap V2, Uniswap V3, and Tokenlon;[59] (ii) we review the top 100 functions called by all addresses found within the trace and categorize them into the included functions list if they appear to be related to transferring or swapping tokens; (iii) all other functions, such as those related to yield farming or NFT trading, as well as all functions outside of the top 100 functions, are categorized as excluded functions.

Lastly, we do not follow extremely small transaction sizes. Addresses distribute excessively small amounts of crypto to interfere with the performance of tracing software. We stop following amounts of less than 0.00001 Ether or other ERC-20 token quantities.

The most important potential limitation is the risk of tracing funds to an address that does not belong to a scammer. The criteria above serve as conservative guardrails to mitigate this risk. For example, the most often triggered stopping criteria are reaching large known or unknown addresses. Stopping at exchanges is an important guardrail, which is why we work backward from exchange hot wallets and cluster at deposit addresses. The 2,000 transaction guardrail helps avoid following the "wrong" transaction in the case of co-mingled funds, such as when a scammer sends money to an address that already holds a balance from other potentially illicit activities. Similarly, tracing the flow of funds for a fewer number of hops increases confidence and reduces the complexity of the network, but also leaves parts of scammer networks unexplored. Our research design aims to be conservative in these trade-offs.

C Tracing Bitcoin Addresses

Bitcoin clustering builds on the idea that multiple addresses providing input to the same transaction can be linked and that this procedure can be applied iteratively to form clusters that are highly likely to be under the control of the same user. This procedure is detailed in papers such as Meiklejohn et al. (2013) and applied to following flows of crypto funds in Griffin and Shams (2020). We expand on our list of reported addresses and rely on the common input heuristic to identify the broader clusters associated with each address. Other aspects of tracing are similar to our Ethereum tracing, though tailored to the Bitcoin blockchain. For example, we use a similar procedure to identify cluster of exchange addresses and stop tracing at exchange deposit addresses. If a cluster has more than 300 addresses or collectively more than 2,000 transactions, then we do not trace through that cluster. We ignore transactions below 0.0001 Bitcoin to avoid clustering any dusting transactions.

[59] The functions that appear on the Tether contract essentially also appear on other ERC-20 tokens.

D Internet Appendix Figures

Figure IA.1. Sources of reported addresses from the USIP
This figure plots the sources of the addresses provided to us by the United States Institute of Peace (USIP). The horizontal axis plots the named source and the vertical axis plots the number of addresses. At the top of each bar, we present the count within that group as well as the share as a percent of all addresses. Bars are divided by proportion of addresses associated with Ethereum, Tron, and Bitcoin, as indicated in the legend.

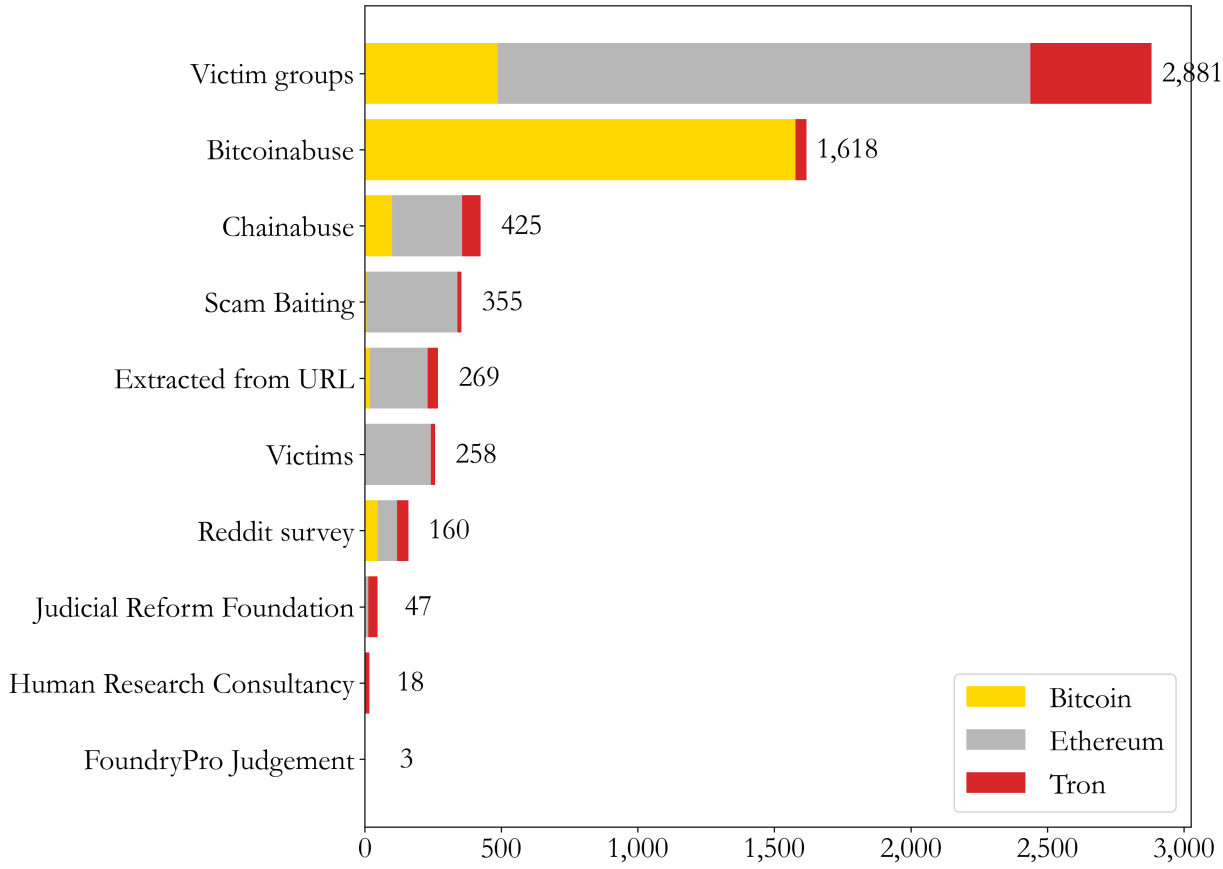


Figure IA.2. Inflow to reported addresses by blockchain
This figure plots the total inflow to reported addresses by month, split by blockchain across Ethereum, Tron and Bitcoin. The horizontal axis plots time and the vertical axis plots the dollar inflow. Ethereum, Bitcoin and Tron are decomposed and plotted by color, as indicated in the legend.

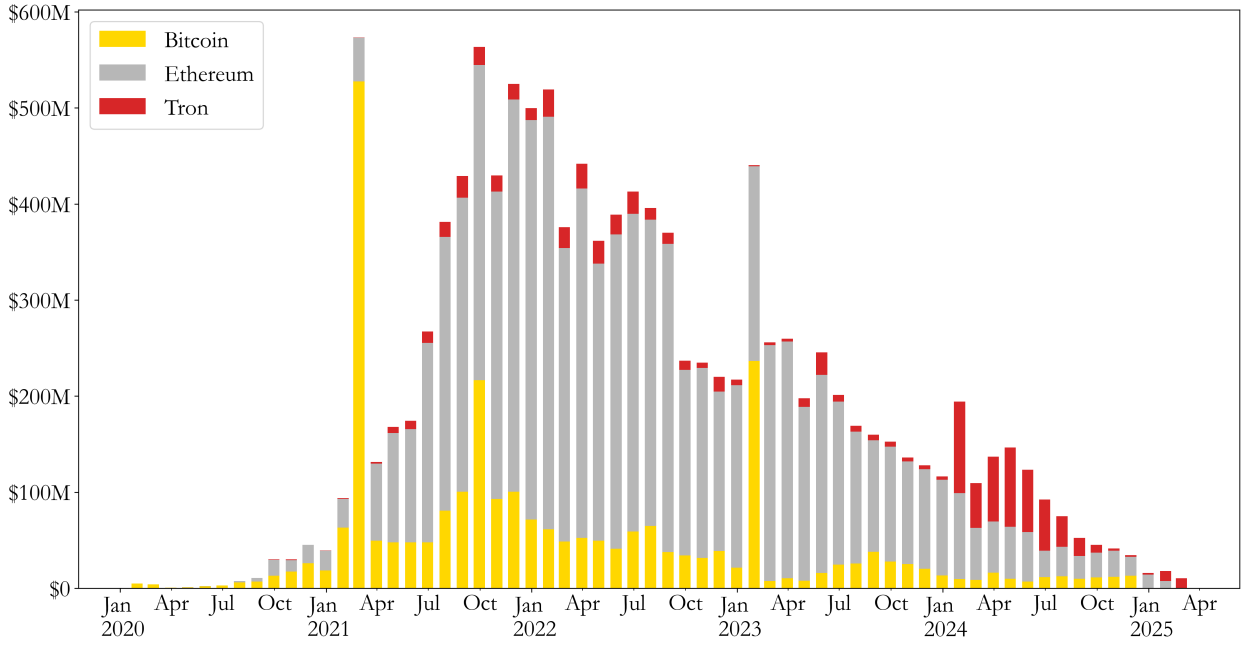


Figure IA.3. Methodology and trace paths

This figure presents a diagram of nodes and edges to depict the trace paths used in this paper. Nodes include three types: (1) triangle is an address that was reported by victims as a destination for pig butchering scam funds; (2) squares are exchange addresses based on information from Etherscan and other online sources; (3) circles represent other nodes found in the trace path. Edges are distinguished as either forward trace paths in solid lines, or backward trace paths in dotted lines. An additional dotted circle delineates addresses that are identified as exchange-controlled deposit addresses.

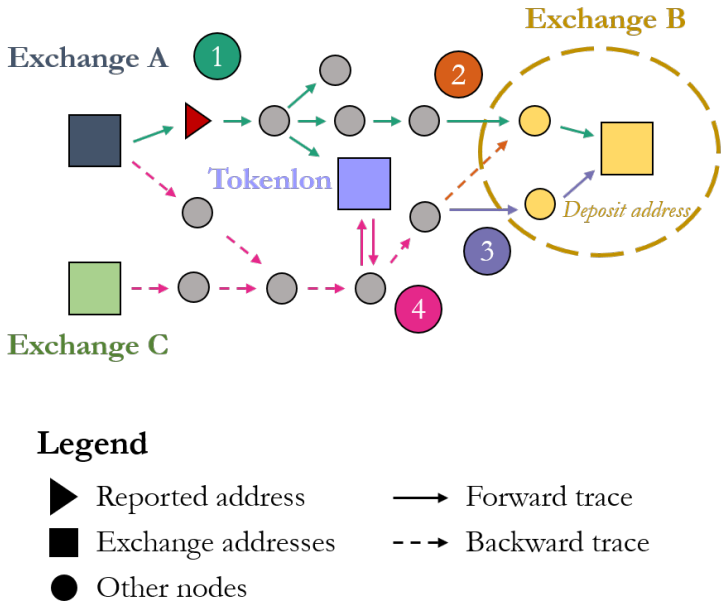
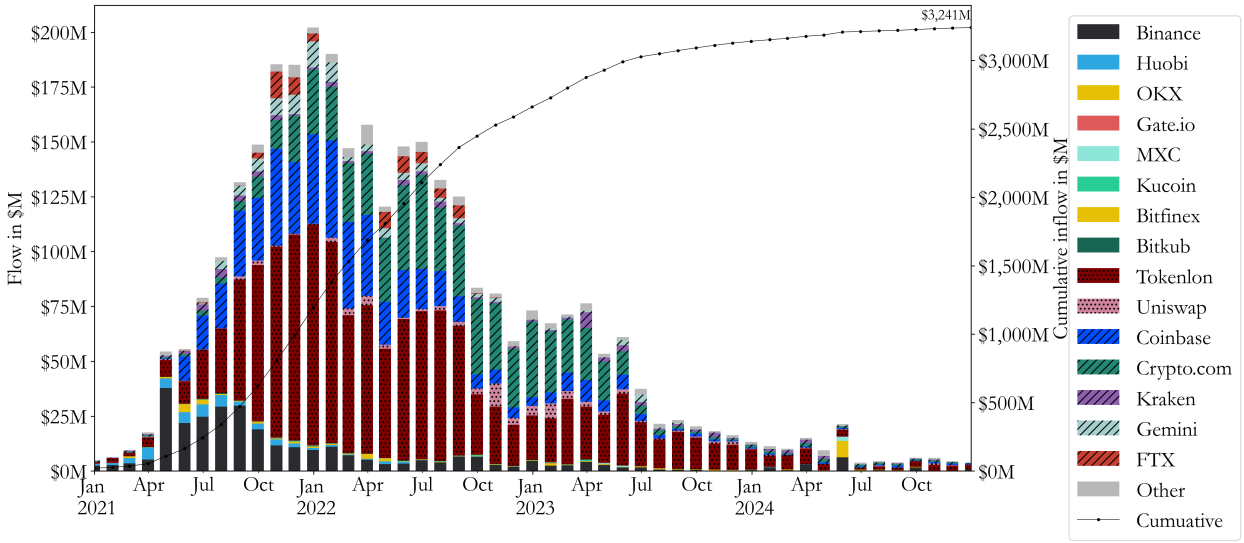


Figure IA.4. Flow of funds from exchanges to scammer addresses
This figure plots flows from exchange addresses to victim-reported scammer addresses over time. It excludes any inflow to reported addresses that originates from non-exchange addresses. Panel A and Panel B decompose this flow by exchange and token, respectively. The bars correspond to the left vertical axis and represent their monthly inflow. The curve stretching across the bins corresponds to the right vertical axis and graphs cumulative inflow.

(a) Flow of funds to exchanges to scammer addresses by exchange



(b) Flow of funds to exchanges to scammer addresses by currency

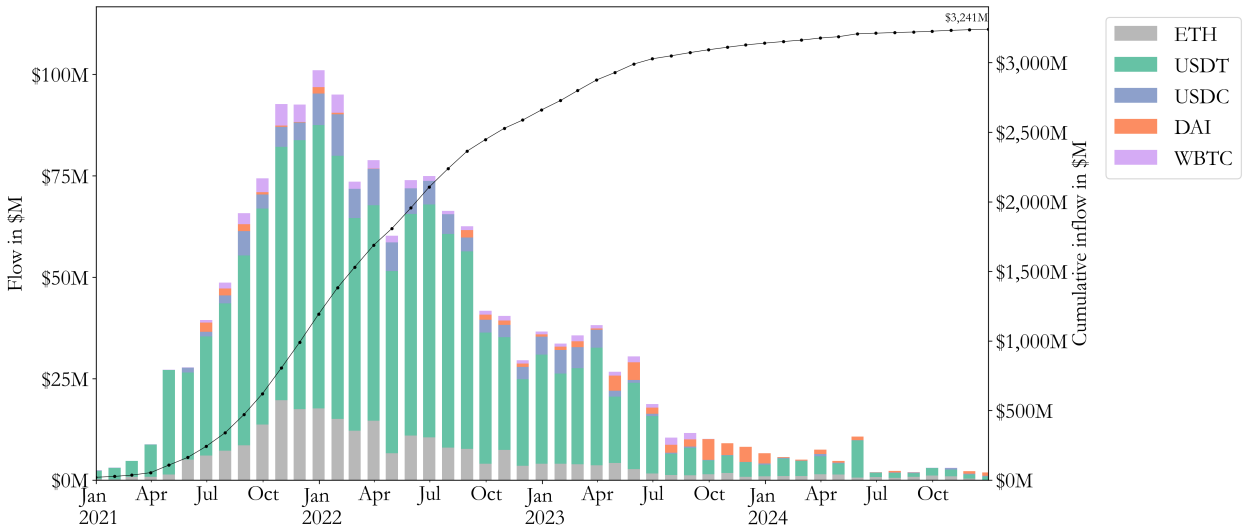


Figure IA.5. Flow of funds to each subsequent hop in the forward trace
This figure plots the amount of funds traced according to the number of hops where the corresponding transactions were found. The height of each bin corresponds to the total inflow into each group, and each bar has been decomposed by currency as displayed in the legend.

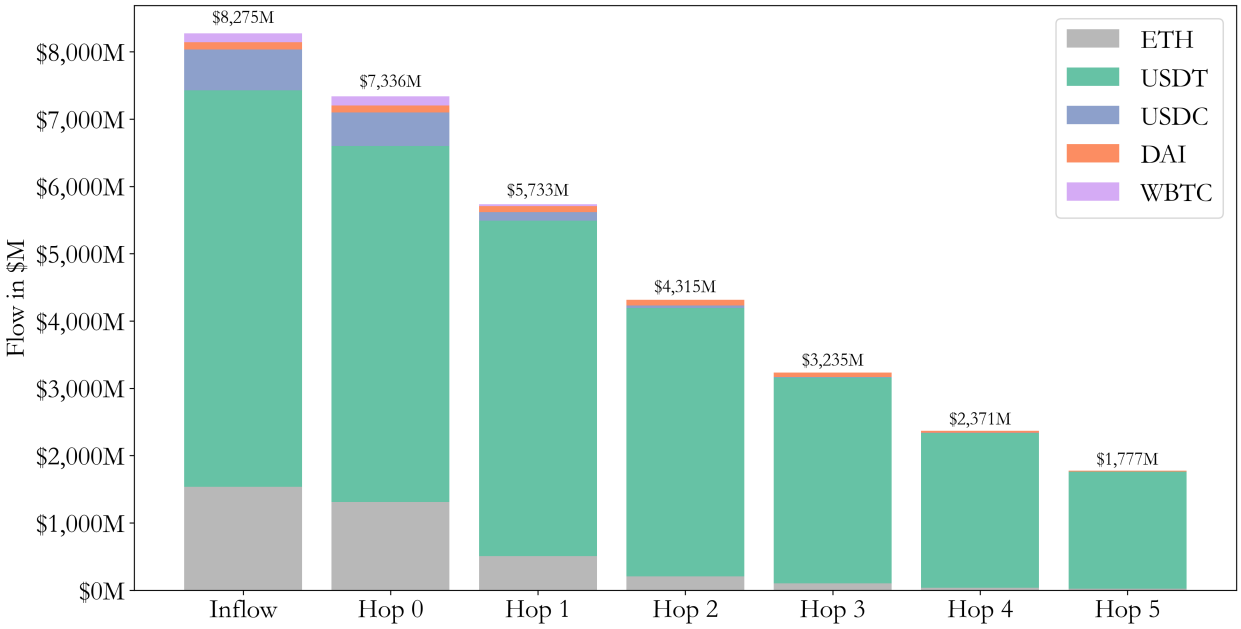
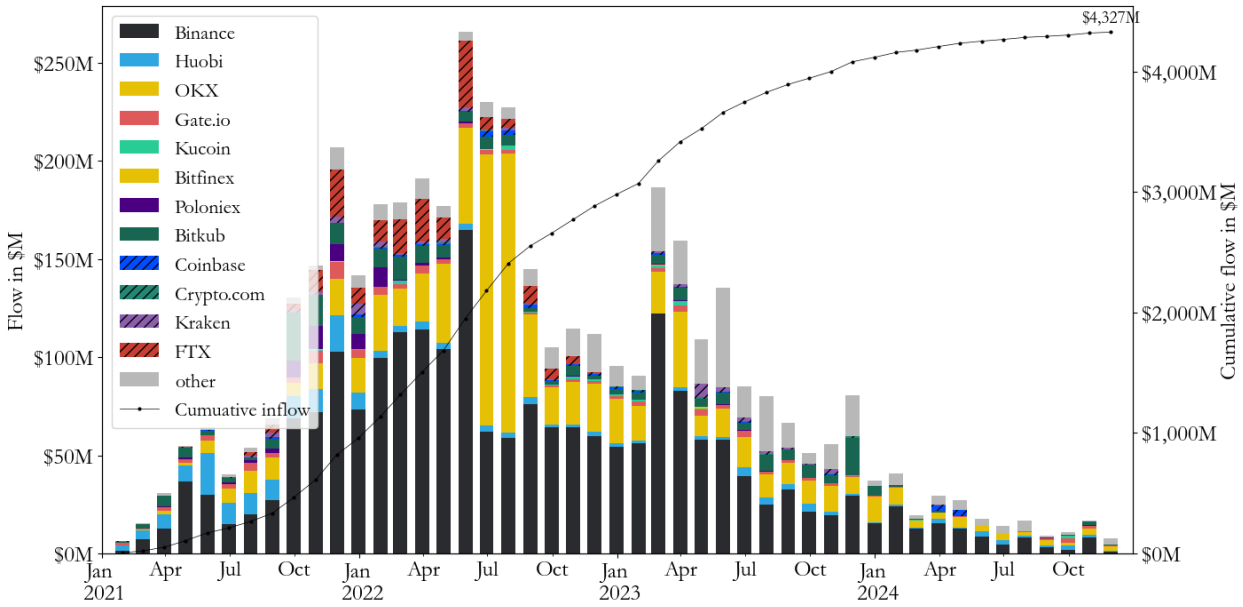


Figure IA.6. Traced flows to large deposit addresses
This figure shows the flow from the trace path into exchange deposit addresses with a traced amount of more than or equal to $100,000 Panel A shows the time series of the flow into exchange deposit addresses alongside the cumulative inflow curve (read in the right vertical axis), and Panel B shows the aggregate inflow into each deposit related exchange across the whole timespan.

(a) Total traced to large addresses, over time



(b) Total traced to large addresses, aggregated by exchange

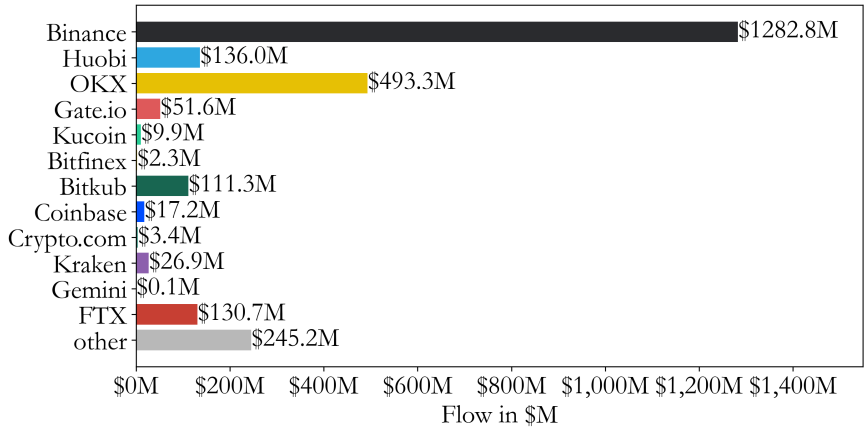


Figure IA.7. Average inflow and outflow from exchanges
This figure plots the comparison between transactions from exchanges into the scammer network and transactions from the scammer network into exchanges for the forward trace. Panel A plots the average transaction size, and Panel B plots the total transaction amount from and to exchanges decomposed by cryptocurrency. Error bars in Panel A indicate 95% confidence intervals for each bin.

(a) Average inflow vs. outflow transactions

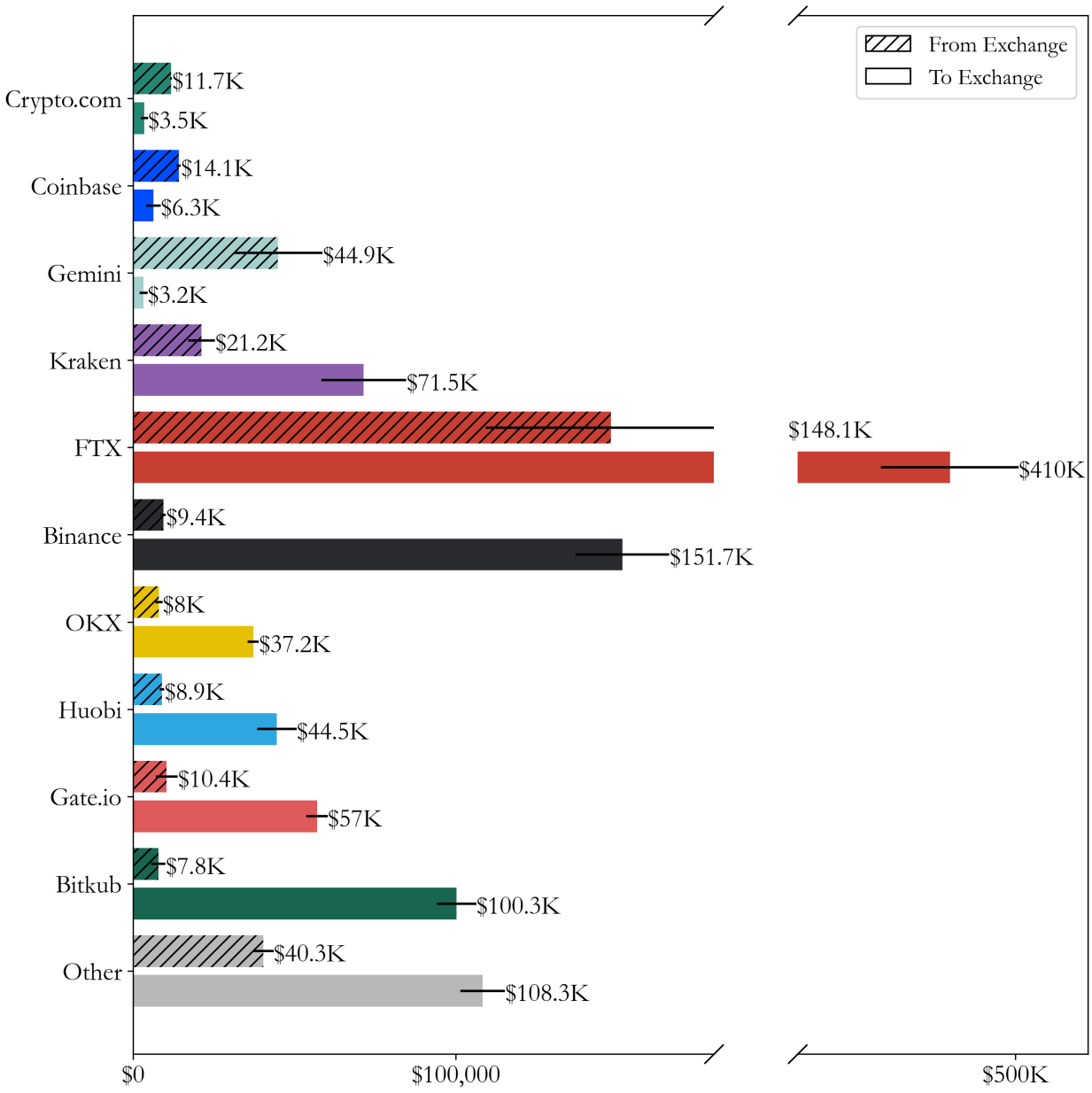


Figure IA.8. Number of unique deposit addresses
This figure plots the number of unique deposit addresses found after expanding on inducement payment senders. The horizontal axis plots date and the vertical axis plots the number of addresses. The total number for each corresponding exchange is given in the legend.

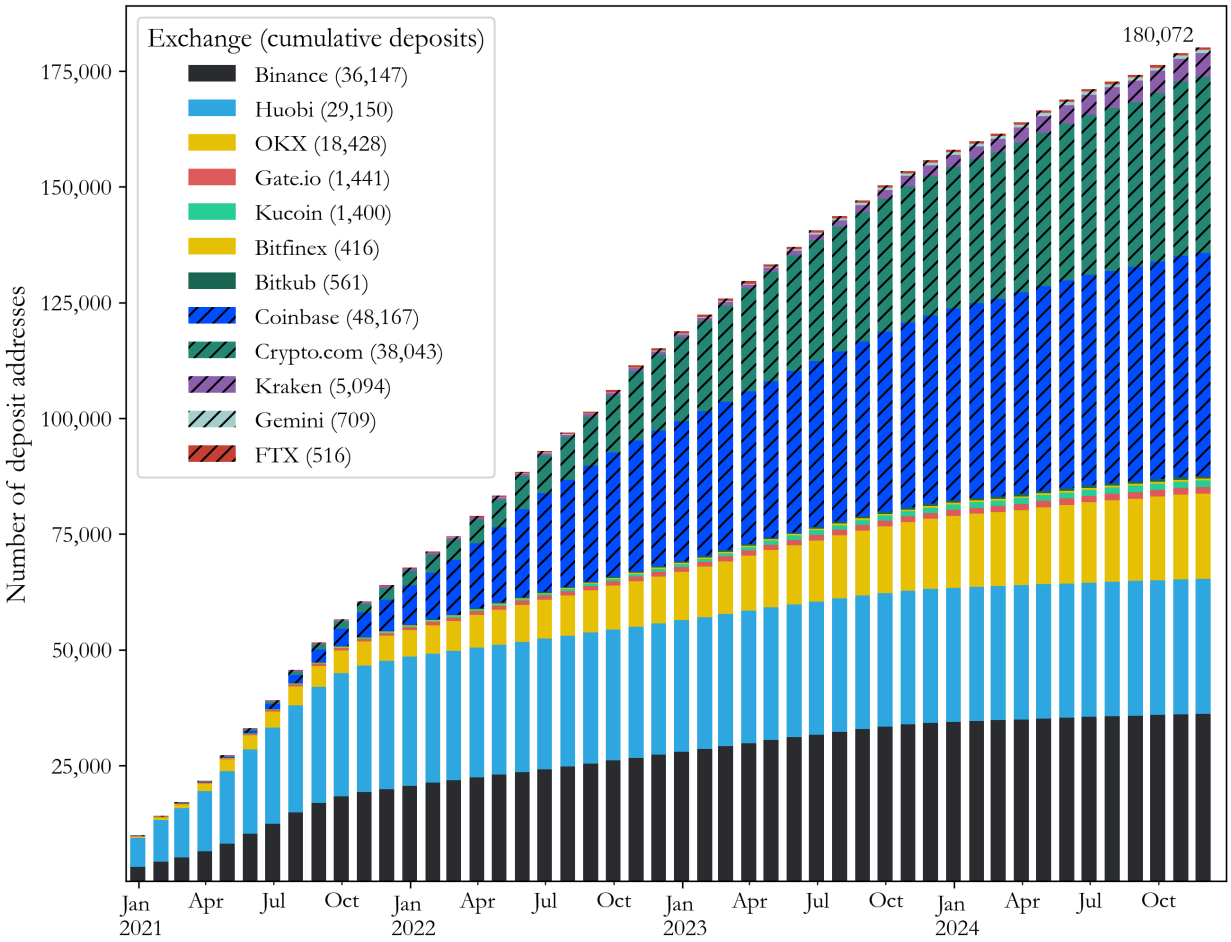


Figure IA.9. Number of large deposit addresses
This figure plots the number of large deposit addresses associated with each exchange. The dark bars represent the number of large, potential scammer deposit addresses found in the initial trace. The light colored bars tabulates the number of addresses that originate from the retraced transactions.

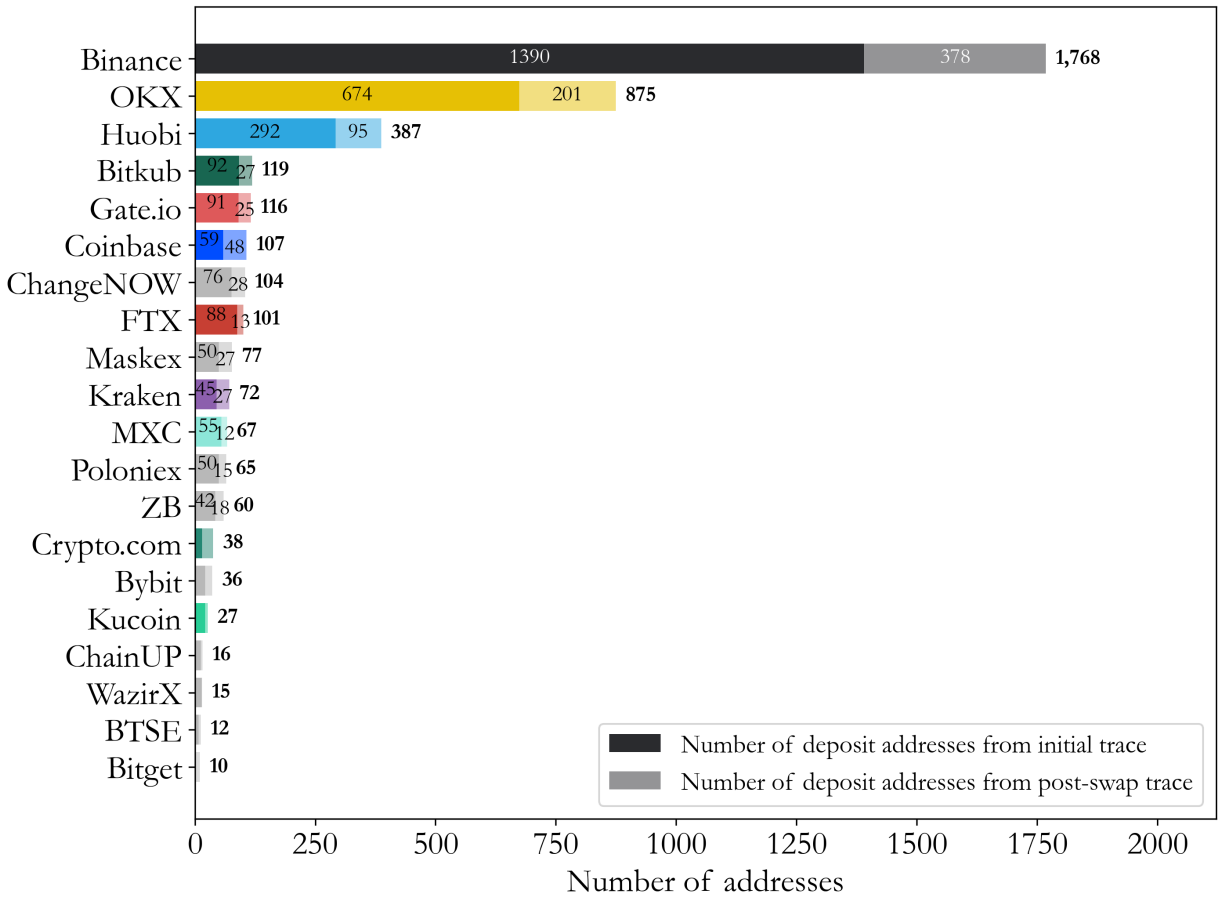
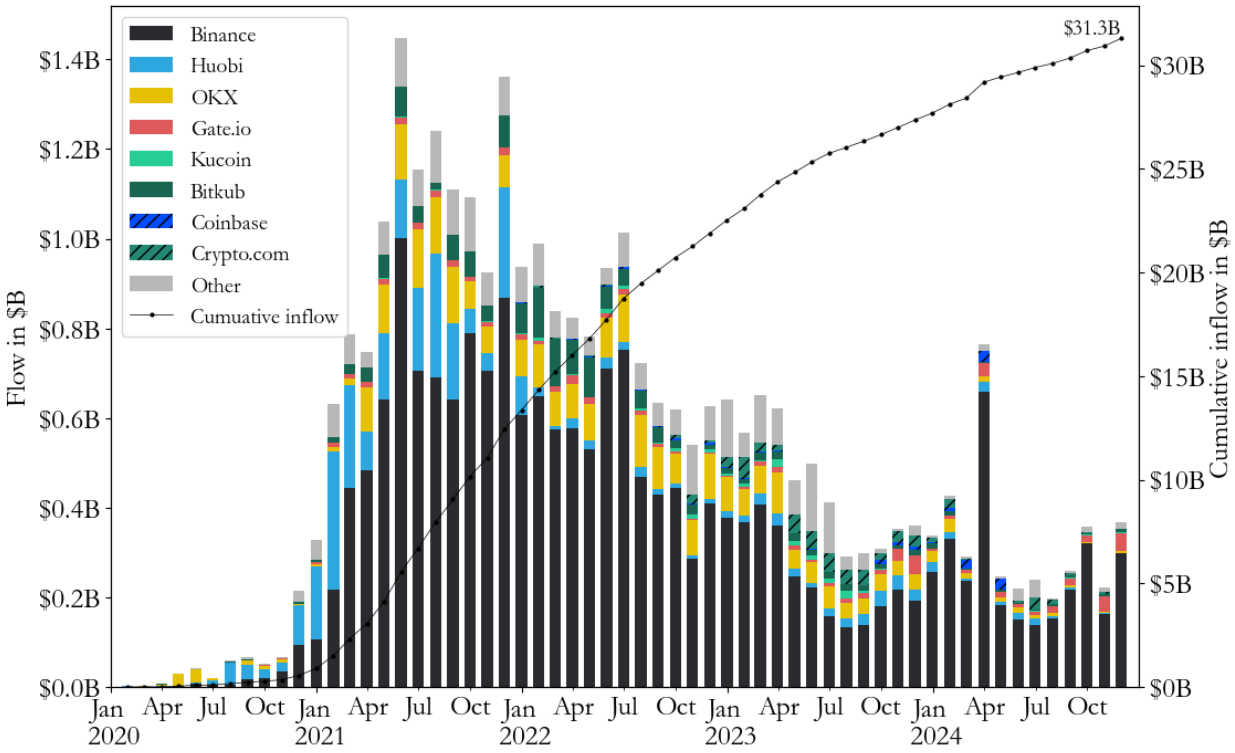


Figure IA.10. Inflow to associated deposit addresses
This figure shows the source of total inflow to deposit addresses, sorted by the controlling exchange. Panel A shows the time series of the flow into exchange deposit addresses alongside the cumulative inflow curve (read in the right vertical axis), and Panel B shows the aggregate inflow into each deposit related exchange across the whole timespan.

(a) Total inflow to scammer deposit addresses over time



(b) Total inflow to scammer deposit addresses by exchange

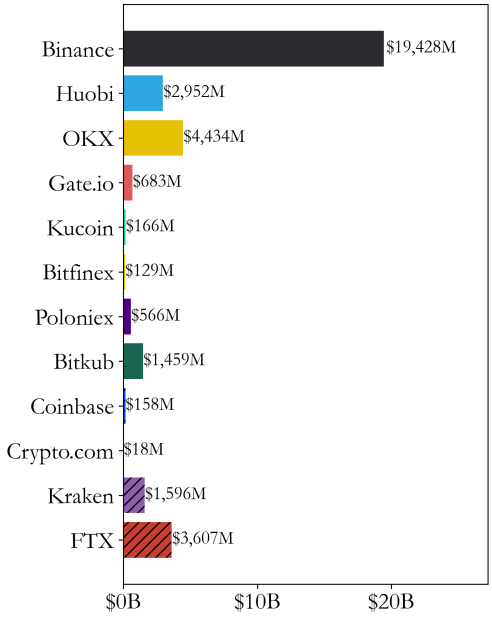


Figure IA.11. Inflow to associated deposit addresses
This figure shows the total inflow to deposit addresses, decomposed by the methodology used to this find each deposit address. The date in the horizontal axis represents the date of the transactions sending to deposit addresses, and the dollar amounts in the vertical axis correspond to the sum of all flows to deposit addresses at each date.

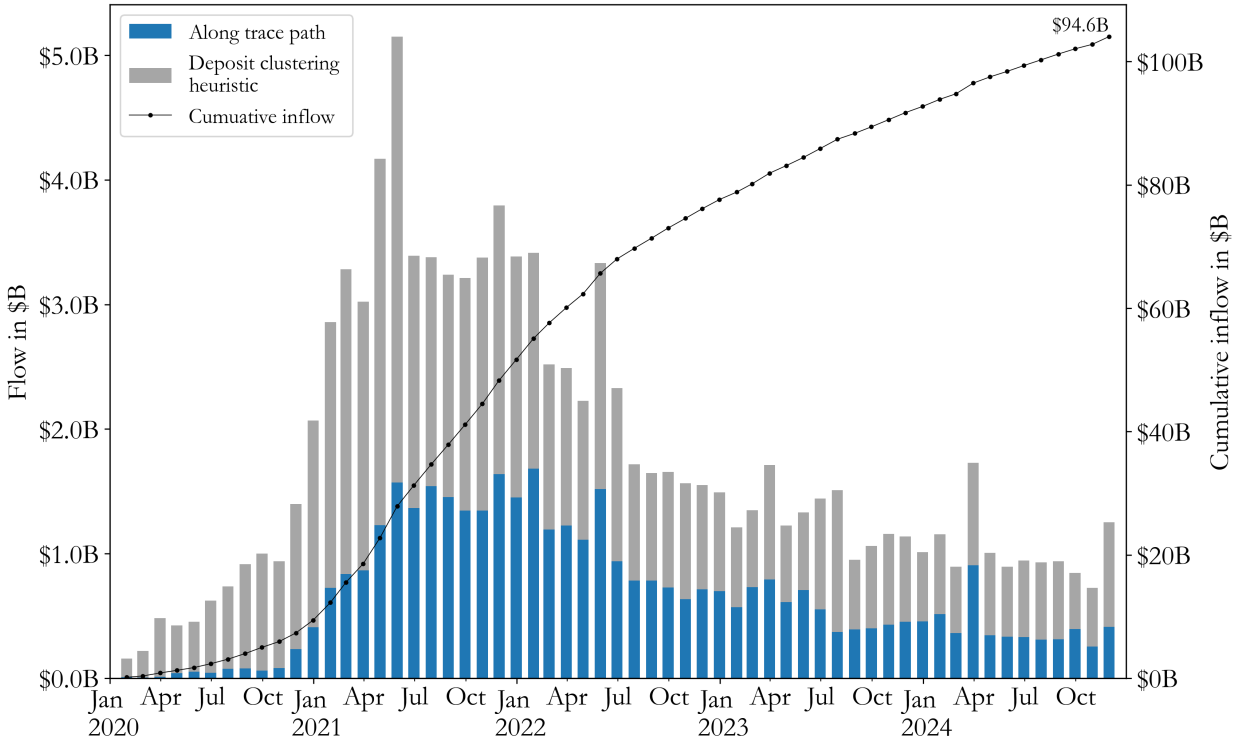


Figure IA.12. Sources to trace path of associated deposit addresses
This figure plots a backtrace that originates from scammer deposit addresses and traces backwards to find the source of funds. This plots monthly flows leaving exchange wallets and the total amount of funds that can be attributed to each exchange. All funds can later be traced to potential scammer deposit addresses.

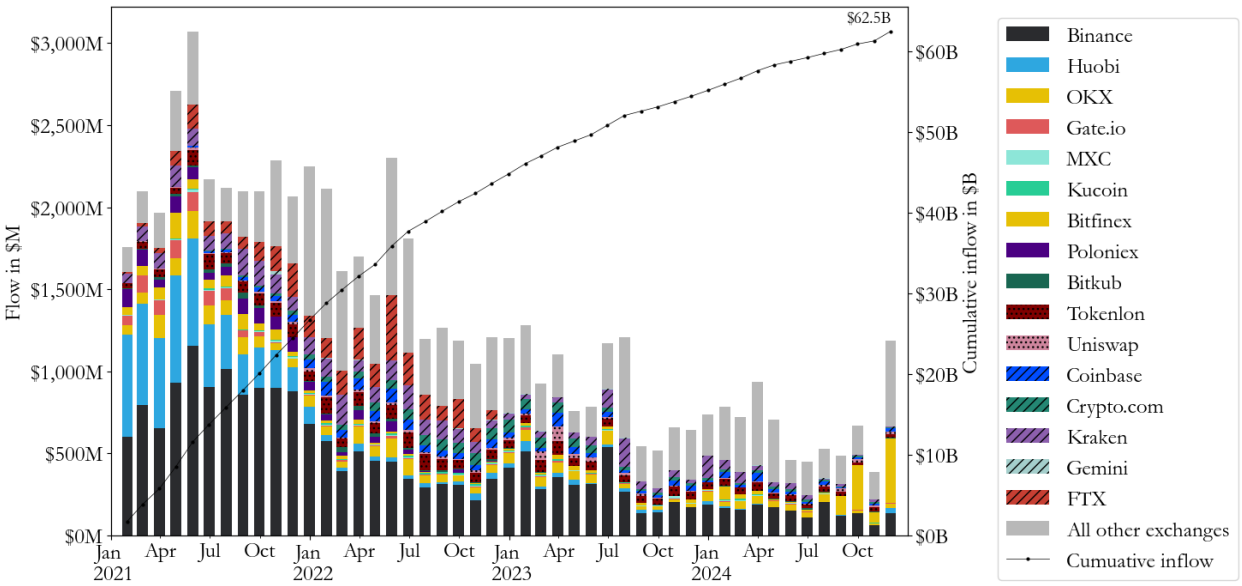


Figure IA.13. Total flows within scammer networks
This figure plots the total flows within the scammer networks, split by the top six cryptocurrencies by value, with colors indicated in the legend at the bottom. Percentages are plotted for Tether (USDT), USDC, and Ether (ETH). The top three bars plot flows from exchanges to the network, the next three bars plot flows to exchanges from the network, and the bottom bar plots total volume throughout the network. Totals within each bar are indicated to the right.

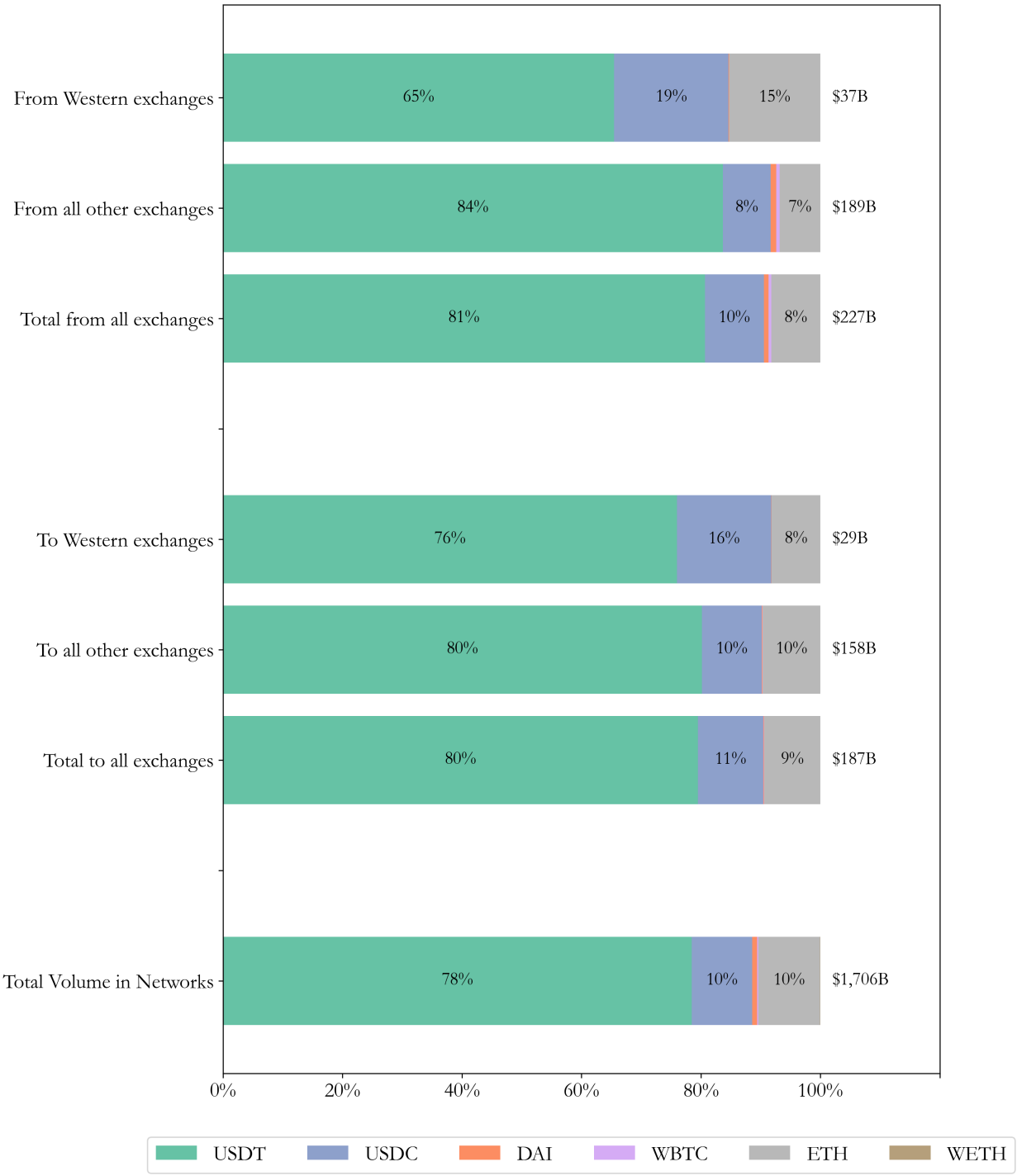


Figure IA.14. Histogram of small transactions in forward trace
This figure plots a histogram of transactions of less than $2,000 found within the forward trace. The horizontal axis plots dollar amounts binned in bins of $5, and the vertical axis plots frequency of transactions.

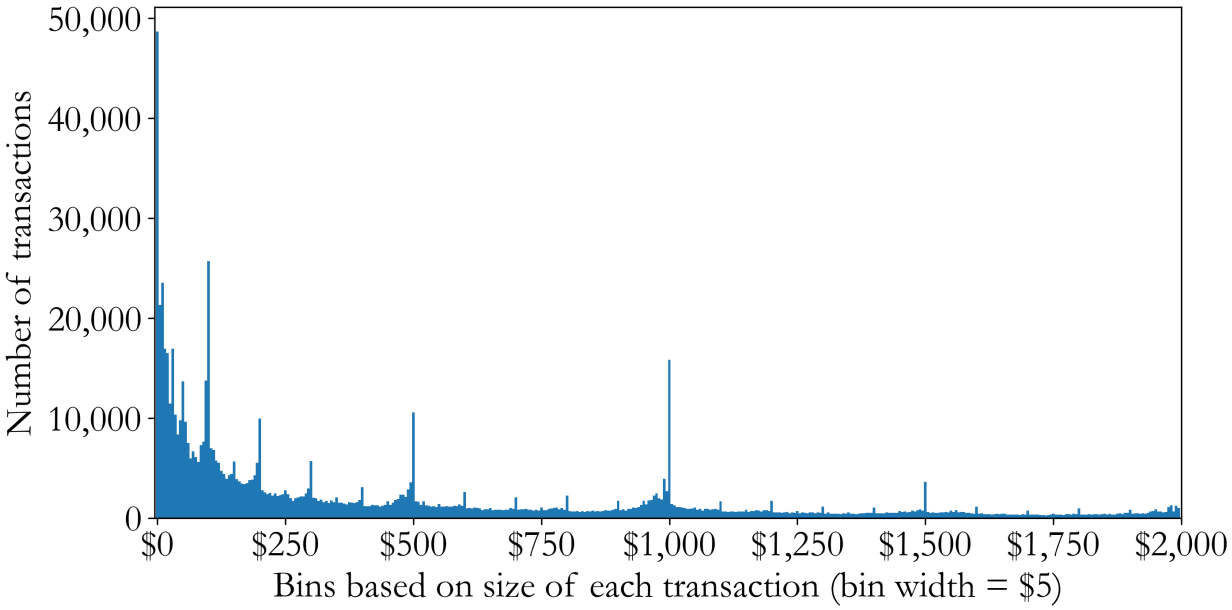
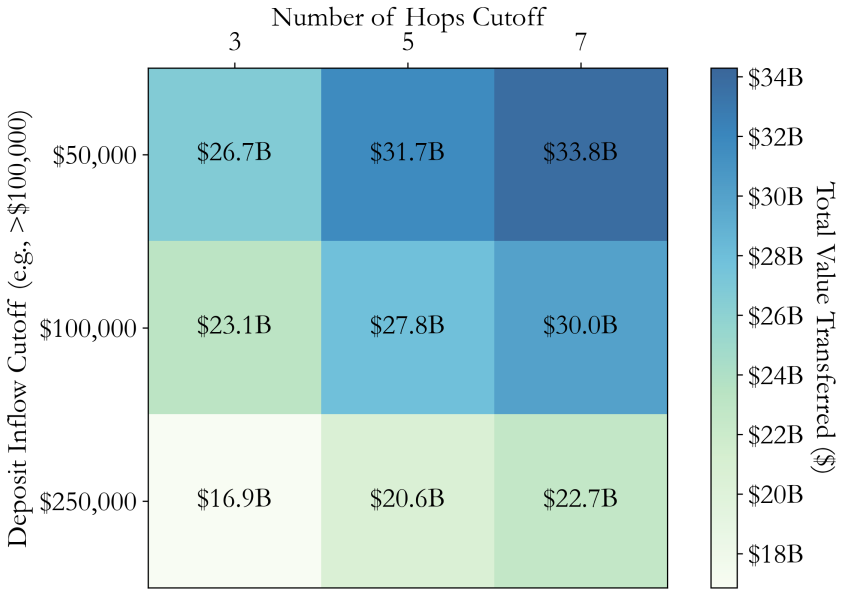


Figure IA.15. Sensitivity analysis
This figure displays sensitivity analysis on three criteria: number of hops, deposit size criteria, and transaction account. The matrix value plots the annual inflow in the three years between 2021-2023. Panel A varies number of hops and deposit size while keeping the transaction count criteria at the base case of 2,000. Panel B varies number of hops and transaction count while keeping the deposit size cutoff at the base case of $100,000.

(a) Sensitivity analysis on number of hops and deposit size criteria



(b) Sensitivity analysis on number of hops and transaction count

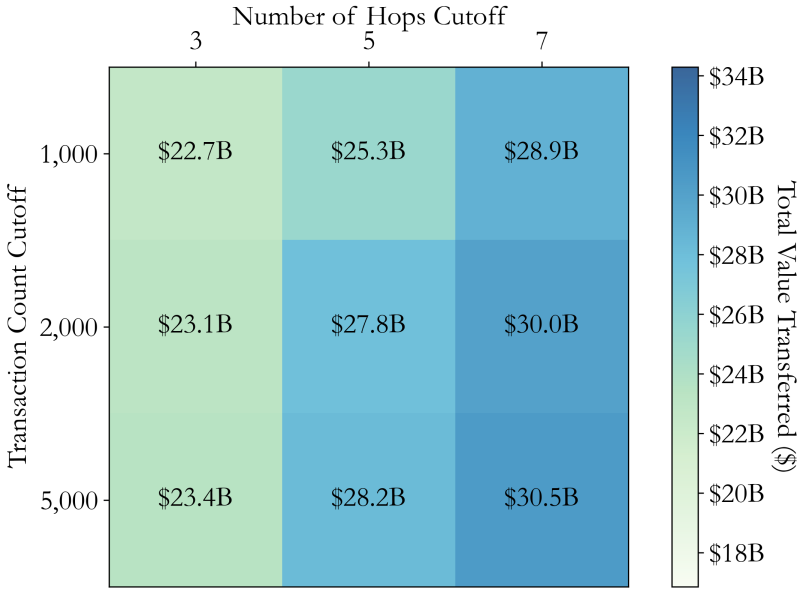
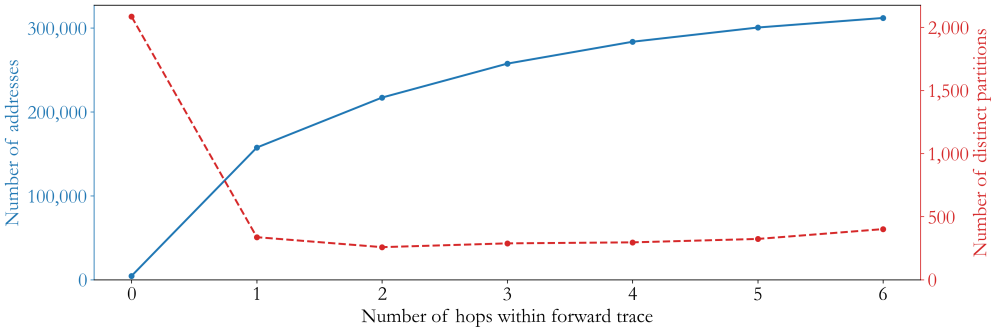


Figure IA.16. Scammer network: size of network and partitions
This figure plots the size of the scammer network. This figure shows the number of distinct, non-connected partitions after each number of hops. Nodes associated with exchanges are excluded. Hop 0 represents the connected graph of originally reported addresses, including any edges linking them to other reported addresses. Each later hop includes the nodes that receive funds within that hop.

(a) Pig butchering networks



(b) Largest connected network, as a share of total traced paths

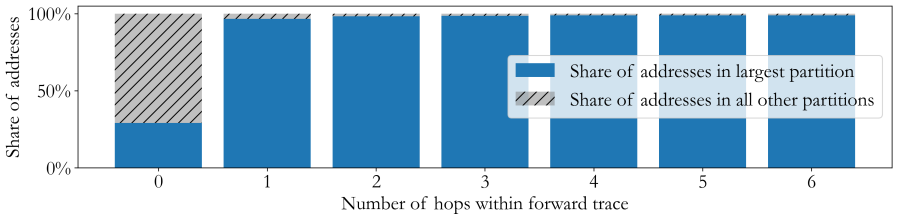


Figure IA.17. Top 100 deposit addresses ranked by total inflow received
This figure ranks the total inflow received by the top 100 deposit addresses. The y-axis plots the total received within each address on the left-hand side, and the running cumulative sum over the top 100 addresses on the y-axis. Bars are colored by exchange, as indicated in the legend.

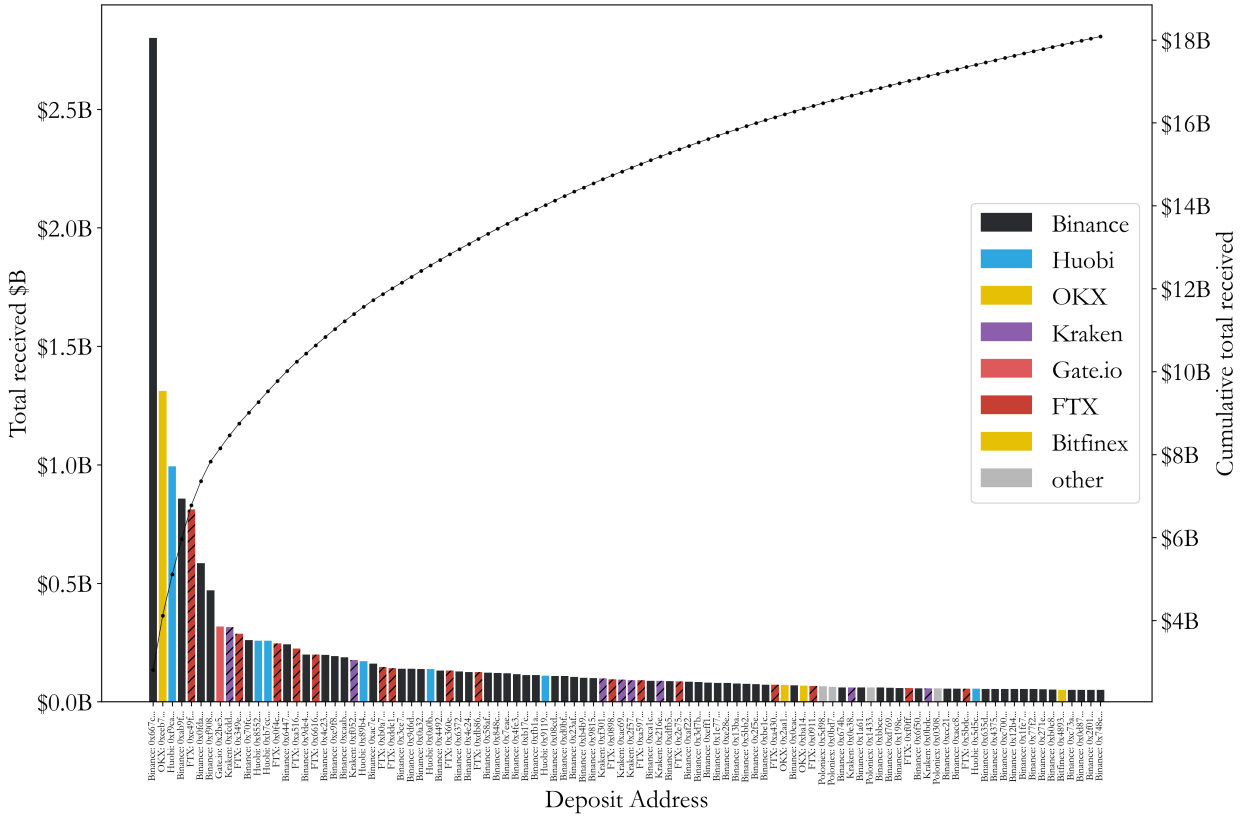


Figure IA.18. Flow of funds from exchanges to scammer addresses
This figure plots flows from exchange addresses to victim-reported scammer addresses over time, excluding the 590 addresses from reports classified by the OpenAI o3-mini. It excludes any inflow to reported addresses that originates from non-exchange addresses. The bars correspond to the left vertical axis and represent their monthly inflow. The curve stretching across the bins corresponds to the right vertical axis and graphs cumulative inflow.

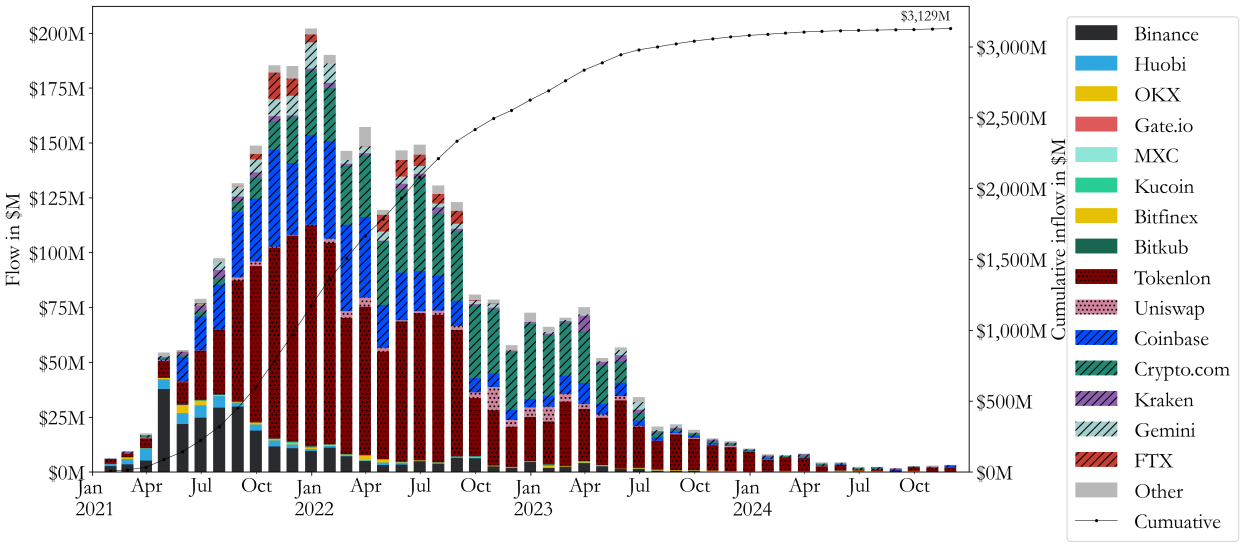


Figure IA.19. Scammer bitcoin network graph
This figure shows a network surrounding one scammer. The thickness of the edges is proportional to the amount transacted between the connected nodes, and the size of the nodes is proportional to the amount each holds, with the notable exception of the "Scammer" and "Tokenlon" nodes which have been enlarged for visibility.

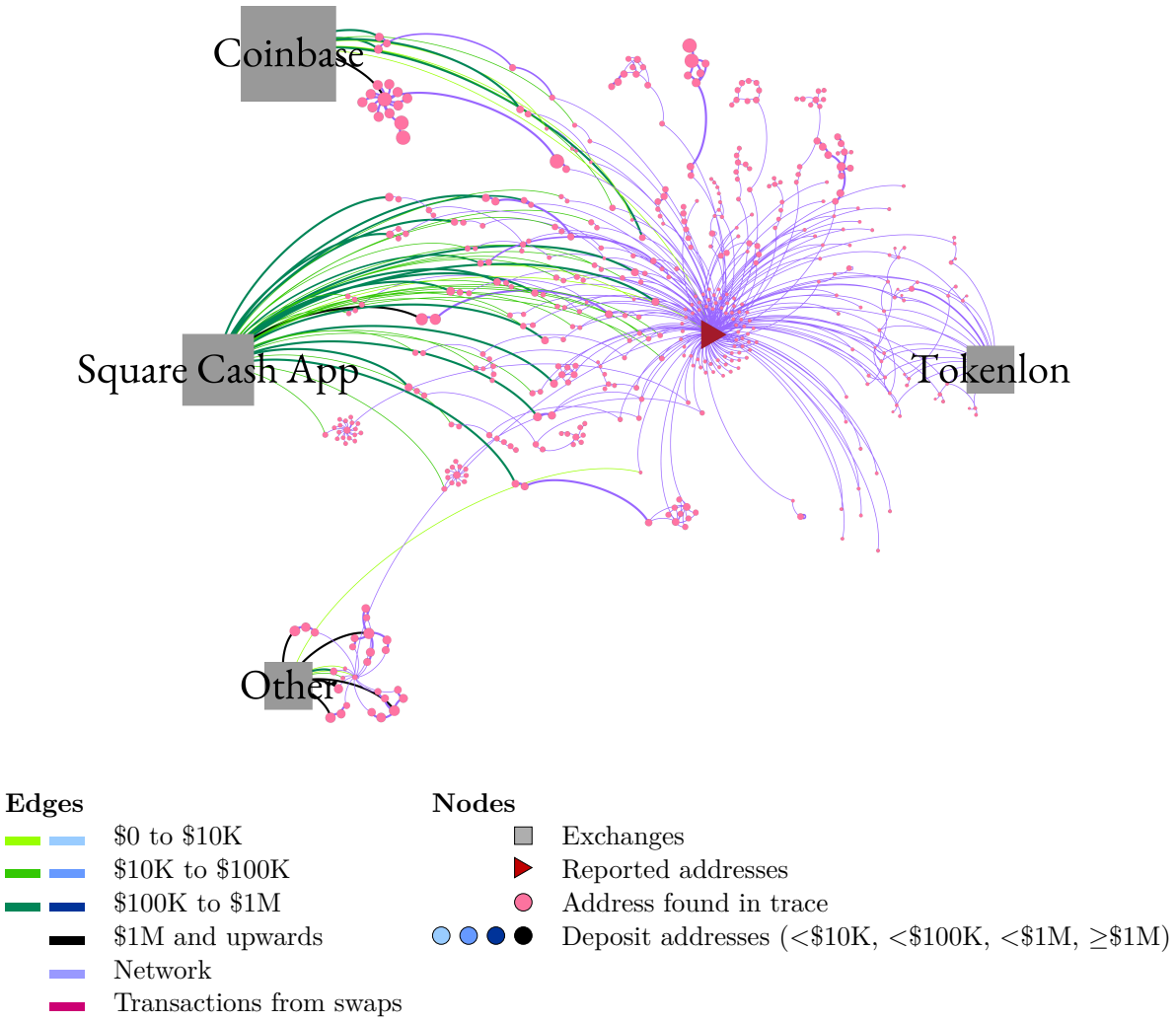
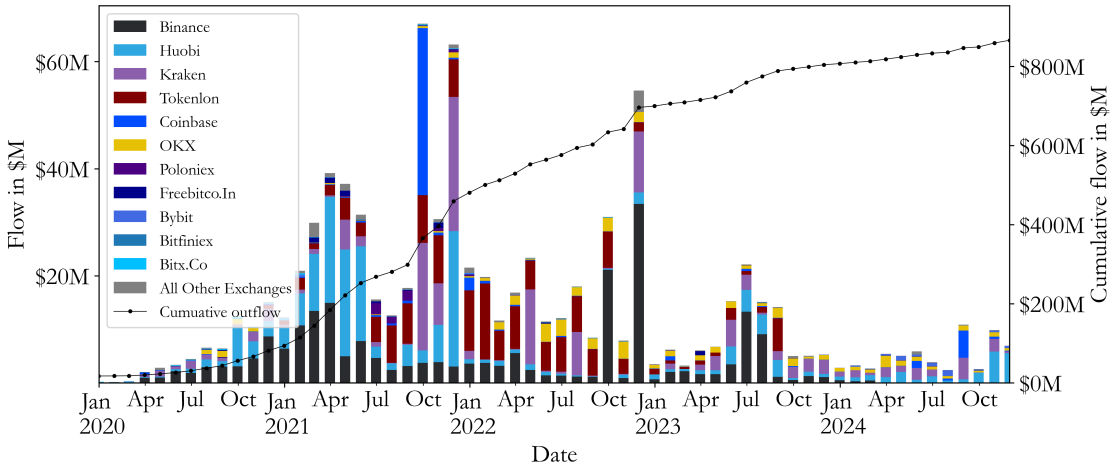
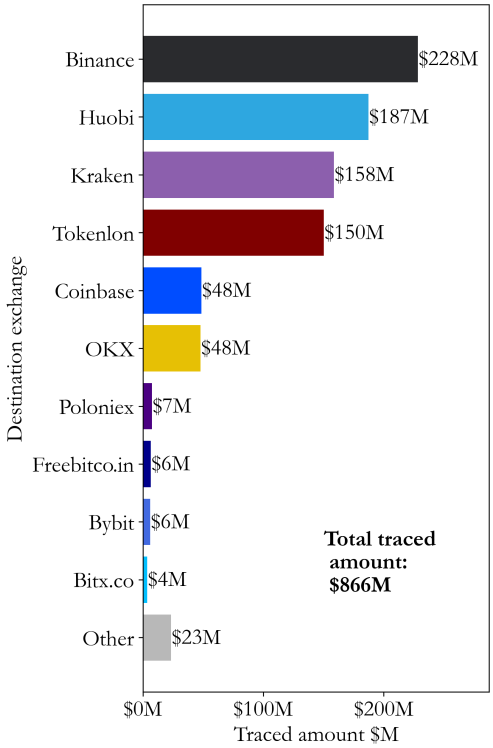


Figure IA.20. Bitcoin trace destinations
This figure plots the results from a trace of Bitcoin addresses. The top panel plots amounts traced to exchanges over time and the bottom panel aggregates to each exchange.





E Internet Appendix Tables

Table IA.1. Number of days active for inducement payment senders
This table presents statistics on number of days active for each inducement payment sender. The first row presents statistics on number of days active for the full sample. The next four rows presents statistics splits by the total number of transactions by each sender to a given destination exchange. The last five rows group by the destination exchange.

	Number of days active							
	count	mean	std	min	25%	50%	75%	max
Full Sample	40,691	57	123	1	1	5	56	2,412
Grouped by number of total transactions:								
1	16,016	1	0	1	1	1	1	1
2-5	15,484	60	115	1	4	19	63	1,758
6-10	3,765	117	148	1	28	67	146	1,522
10+	5,426	173	187	1	49	113	228	2,412
Grouped by destination exchange:								
Binance	10,937	65	143	1	1	4	58	1,758
Coinbase	8,424	48	108	1	1	4	44	1,164
Crypto.com	5,643	53	105	1	1	7	56	1,253
FTX	356	20	61	1	1	1	4	536
Gemini	482	21	55	1	1	1	11	479
Huobi	6,365	66	109	1	1	19	92	1,196
Kraken	1,604	40	109	1	1	1	31	2,412
OKX	6,880	61	136	1	1	1	50	1,550

Table IA.2. Dates of crackdowns related to pig butchering
This table presents dates of law enforcement crackdowns related to pig butchering and news sources.

China urges banks, Alipay to crack down harder on cryptocurrencies (6/21/2021) https://www.reuters.com/technology/chinas-central-bank-urges-financial-institutions-crack-down-cryptocurrencies-2021-06-21

China's top regulators ban crypto trading and mining, sending bitcoin tumbling (9/21/2021) https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/

Cambodian police raid alleged cybercrime trafficking compounds (9/24/2022) https://www.reuters.com/world/asia-pacific/cambodian-police-raid-alleged-cybercrime-trafficking-compounds-2022-09-21/

Bungalows, cars seized in Singapore's billion-dollar swoop on money laundering (8/15/2023) https://www.reuters.com/world/asia-pacific/bungalows-cars-seized-singapores-billion-dollar-swoop-money-laundering-2023-08-17/

Myanmar Rebel Offensive Helps China's Cybercrime Crackdown (10/20/2023) https://www.voanews.com/a/myanmar-rebel-offensive-helps-china-s-cybercrime-crackdown/7362836.html

Binance and CEO Plead Guilty to Federal Charges in $4B Resolution (11/21/2023) https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution

Table IA.3. False positive testing
This table compares data from a data set on reported scams to the addresses within our trace. Column 1 and 2 presents scam categories and the number of addresses reported in each category. Column 3 tabulates the number of reported addresses that also appear within the our trace. Column 4 presents Column 3 as a percent of Column 2.

Category	Number of Addresses	Number of Addresses In Trace	Fraction of Addresses In Trace
Phishing	15,734	287	1.82%
Impersonation	3,374	34	1.01%
Other Hack	2,855	54	1.89%
Fake Project	1,518	55	3.62%
Rug Pull	1,069	7	0.65%
Fake Returns	925	106	11.46%
Contract Exploit	883	4	0.45%
Airdrop	833	9	1.08%
Other Blackmail	489	4	0.82%
Donation Scam	81	0	0.00%
Sim Swap	63	1	1.59%
Ransomware	24	2	8.33%
Sextortion	16	0	0.00%
Other Investment Scam	4	0	0.00%