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

John M. Griffin† Kevin Mei‡

February 29, 2024

Abstract

Through blockchain addresses used by "pig butchering" victims, we trace crypto flows and uncover methods commonly used by scammers to obfuscate their activities, including multiple transactions, swapping between cryptocurrencies through DeFi smart contracts, and bridging across blockchains. The perpetrators interact freely with major crypto exchanges, sending over 104,000 small potential inducement payments to build trust with victims. Funds exit the crypto network in large quantities, mostly in Tether, through less transparent but large exchanges—Binance, Huobi, and OKX. These criminal enterprises pay approximately 87 basis points in transaction fees and appear to have recently moved at least $75.3 billion into suspicious exchange deposit accounts, including $15.2 billion from exchanges commonly used by U.S. investors. Our findings highlight how the "reputable" crypto industry provides the common gateways and exit points for massive amounts of criminal capital flows. We hope these findings will help shed light on and ultimately stop these heinous crimes.

*This paper is dedicated to all pig butchering victims, those defrauded and those enslaved, and especially the victim who gave us the impetus to write this paper. We are thankful for helpful comments from David Dicks, Gleb Domnenko, Cesare Fracassi, Sophia Hu, Brandon Kirst, Samuel Kruger, Alex Pettyjohn, Alex Priest, Marius Ring, Amin Shams, Michael Sockin, Qinxi Wu, and seminar participants at Baylor University, 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 bulk 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.

†McCombs School of Business, University of Texas at Austin.

‡McCombs School of Business, University of Texas at Austin.

Crypto friendship or romance scams have proliferated. Random social media or text messages attempting to develop an online relationship are now commonplace. In a subset of cases, the friendly relationships slowly morph into full-blown scams known as "pig butchering" or *sha zhu pan*, which, in the extreme, bleed lonely, sick, and distressed victims, often with little exposure to investments and crypto, into the loss of their life savings. Though varied in nature, the origin of these scams is often even darker, as the manpower powering the communications is often enslaved in compounds thought to hold 220,000 victims in Southeast Asia.[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 the network? 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. If illicit financial flows continue to grow and are uninterrupted, then the criminal network will typically expand. With this in mind, the international financial system has developed a framework, including Know Your Customer (KYC) and Anti-Money Laundering (AML) provisions, 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 thus typically needs to be converted from and back to fiat currencies, such as U.S. dollars. 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.

Although cryptocurrencies are designed to be anonymous, the nature in which the transactions clear on the blockchain provides a ledger that tracks the movement of funds. Thus,

[1] Section 1 provides a brief overview of the nature of the schemes and summary evidence compiled from government reports, investigative reporting, and documentaries.

the transactions are quasi-anonymous in that, by applying algorithms and substantial effort, it is often possible to determine where funds enter, move through, are swapped into different cryptocurrencies, and exit the crypto ecosystem.

We utilize data from pig butchering victim reports to determine the cryptocurrency addresses where victims were directed to send their funds by scammers. We start with 3,256 Ethereum addresses, 770 Bitcoin addresses, and 702 Tron addresses. Most addresses are used ten or more times, and 28% of addresses are used more than one hundred times. Of these initial sets, Ethereum addresses receive $5.8 billion in funds, compared to $389 million for Tron and $373 million for Bitcoin. Given that the Ethereum addresses represent approximately 88% of the total funds, we begin by examining Ether (ETH, the native cryptocurrency on Ethereum) and token (commonly known as ERC-20 tokens) transactions on the Ethereum blockchain.

Our primary approach is to track the flows entering and exiting scammer addresses and apply detailed bulk tracing algorithms to follow the paths of ETH and ERC-20 tokens that trade on the Ethereum blockchain. Based on blockchain information 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 that of many other adjacent nodes connected to the scamming network and many other reported victim cases.

We trace victim funds in bulk and follow their paths to centralized exchange deposit addresses from January 2020 to February 2024.[2] Figure 1 plots the resulting network for a three percent sample of nodes from the traced network and highlights many features. First, the figure shows how crypto often originates from large exchanges where investors commonly

[2]The data and analyses in this paper were last updated on February 20, 2024.

have accounts (Coinbase, Crypto.com, and Binance) and flows into the network. Second, funds are often swapped for Tether (known as USDT) through Tokenlon. Third, after circulating through various hops in the network, 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, the scammer network initiated 104,460 deposits to centralized exchanges for amounts below $10,000, most commonly in small amounts clustering 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, 31,980 transactions are sent to Western exchange deposit addresses, including Coinbase (15,249) and Crypto.com (15,433), while the remainder is concentrated in Binance, Huobi, and OKX.[3] We find 83% of potential inducement payments are sent from addresses used in more than ten transactions, suggesting limited monitoring by crypto exchanges.

Since scammers are unlikely to return large sums of stolen funds, we consider deposit addresses that receive more than $100,000 as more likely to be scammer deposit addresses. 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 have loose KYC procedures and are perceived to be outside of U.S. jurisdiction.[4] To more fully understand the scope of the network, we apply "deposit address clustering" (Victor, 2020) by tracking addresses that send funds into these deposit addresses and finding other recipient deposit addresses associated with the same user.[5] To avoid capturing payments made by criminals for things like inducement

[3]Throughout this paper, we include Coinbase, Crypto.com, Kraken, Gemini, and FTX as Western exchanges because these can be accessed by US-based users.

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

[5]This heuristic relies on the facts that an exchange customer may have multiple deposit addresses and

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 $75.3 billion of Ethereum-based inflow through February 2024 to these addresses. Portions of this total could capture funds associated with other related networks that interact with the criminal networks; however, additional robustness analyses indicate that this is likely a conservative lower-bound estimate and the total size may be considerably larger.

After analyzing the network unveiled from tracing scammed funds forward, we also trace backwards from 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 $15.2 billion of funds that originate from five Western exchanges over the last four years, from over 1.25 million 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 path, we observe many distinct features of the network graph 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 may help obfuscate the true source of their funds. We estimate that transaction costs for a network of this scale total to 87 basis points as a portion of outflows to exchange deposit addresses. In contrast, Soudijn and Reuter (2016) find costs of 7-16% to move physical Euro bills from Europe to Columbia and money laundering commission estimates range from 4-12% (US Treasury Department, 2002) and 10-20% (US Treasury Department, 2007). Cryptocurrencies thus appear to be a much more cost-effective channel for moving illicit funds across borders. In total, scammer swap transactions may constitute more than 58% of Tokenlon transactions since 2022. We observe large inflows from potentially Chinese

any funds sent to these may only be accessed through the exchange; therefore, if a given blockchain address transfers tokens to two exchange deposit addresses, then it is likely that the two addresses are controlled by the same user. Deposit addresses are each assigned to a single verified account or user and thus provide an opportunity to examine the broader scope of the flows a user receives.

victims in 2020; however, after the Chinese financial authorities banned cryptocurrency trading in late 2021, there appears to be a dramatic decrease in Chinese victims and a shift to US-based victims. Overall, in the set of addresses touched by the criminals, we find $1.172 trillion dollars of volume, 84% of which is in Tether.

As a placebo test, we compare a trace analysis of pig butchering addresses to phishing scam addresses. Pig butchering networks have larger transactions and receive more funds than phishing scams. Transactions in phishing scams use proportionally more ETH and lead towards Uniswap, Kucoin, and Binance. This also highlights how our methods can be applied to other criminal crypto spaces. We also trace 770 Bitcoin addresses and find that the Bitcoin scam network funnels scammed funds into Tokenlon, Binance, Huobi and OKX. We follow these paths from the Bitcoin to the Ethereum blockchain and find 78% of Bitcoin cross-chain paths intersect with our Ethereum trace paths, further indicating the importance of the Ethereum network in criminal activity. We find the network of scammer nodes is highly connected, likely indicating that there exist widely-used services that funnel funds for extremely large and possibly related criminal networks.

It is our hope that this research, along with those of other researchers and practitioners will expose how crypto finances these dark activities.[6] This project highlights how large-scale tracing of tainted funds can help expose and understand criminal financial activity that can hopefully be used as a roadmap in other criminal contexts.

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

[6] "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 an attorney at Gibson Dunn and has previously served as counsel for 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).

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. Third, the Ethereum network appears to drastically reduce barriers for illicit financial flows of transnational organized crime. Fourth, romance scammers prefer the stablecoin Tether over other cryptocurrencies and the Ethereum network 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 February 16, 2024, despite recent crackdowns.

1 Related Literature and Background on Pig Butchering and Crypto

1.1 Related Literature

Our paper relates to three main literatures. First, there is a growing literature examining dark market activity in the crypto space. Meiklejohn et al. (2013) show how clustering algorithms can be used to identify Bitcoin transactions moving funds through the Silk Road, a darknet marketplace that operated between 2011 and 2013. 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. They estimate that 27 million Bitcoin users conduct $76 billion in annual activity, which by some estimates is $3/4^{\text{th}}$ of the size of the U.S. drug trade. 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.[7] Amiran et al. (2022) studies the role of cryptocurrencies in terrorism financing. The academic literature mainly focuses on dark market activity in Bitcoin. In contrast, we detail the nature of activity on Ethereum, which includes techniques such as swaps between tokens and multiple transactions to seemingly evade detection. Since we only focus on funds in the network for one type of scheme and the funds we track are larger than those tied to the dark markets for Bitcoin in 2020 (Makarov and Schoar, 2021), the amount of criminal activity on Ethereum may be many times larger than previously estimated. We also make a methodological contribution by showing how bulk tracing multiple streams of funds moving through the network, including from Bitcoin to Ethereum, can help provide a more complete map of broader cryptocurrency networks.

Second, there is a growing literature related to other types of nefarious trading activity in crypto, including price manipulation, pump-and-dump schemes, and wash trading.[8] Cong et al. (2023a) examine common crypto scams including those of investment, ICO, rug pulls, phishing, blackmail, and Ponzi schemes. Gandal et al. (2018) show price manipulation of Bitcoin in 2014. Griffin and Shams (2020) show that Bitcoin prices were manipulated upward through the partially unbacked printing of Tether, which helped to fuel Bitcoin and other cryptos in 2017 and 2018. Li et al. (2018) and Hamrick et al. (2021) provide detailed evidence of pump-and-dumps of crypto tokens. Phua et al. (2022) estimate that 38.7% or $12 billion of capital from 5,935 ICOs were likely scams. Pennec et al. (2021) and Cong et al. (2023b) study crypto wash trading. Cong et al. (2023b) shows that wash trading accounts for trillions

[7] Chainalysis (2023) produces an annual summary report that tracks possible amounts of stolen funds, scams, sanctions, dark markets, ransomware, cyber security, fraud shows, child abuse materials, terrorism finance, and malware. They estimate over $20 billion in such total illegal activity in 2022 with $5.9 billion in scams in 2022, most of which they estimate to be investment and giveaway scams, not romance scams. They note that their figures are undercounting and that romance scams appear to be growing. 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. Sokolov (2021) finds that Bitcoin transaction activity and fees increased around times of ransomware activity in 2014-2015.

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

of dollars of fake trading and over 70% of centralized exchange volume, with varying degrees across exchanges.

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 the recognition that "money is the lifeblood of organized crime" led to the adoption of the anti-money laundering (AML) regime in Italy.[9] 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. Organized crime often purchase legitimate enterprises for money laundering (Mirenda et al., 2022) or utilize cash and various shell companies to obfuscate transactions moving into the banking system. Overall, examining criminal fund flows in the traditional banking system or through cash transfers is primarily limited to prosecuted case records, which explains the lack of academic research and reliable estimates of such activity. In a survey of the literature, Levi (2015) states: "we have little information about the mechanisms of financing." This paper seeks to partially fill this void.

1.2 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 in the form of a text, WhatsApp message, or messages on social media platforms to the wrong person.[11] The scammers are looking for a victim who is lonely, going through tough times (such as

[9] Draca and Machin (2015) survey a growing literature on the economic relation between crime and unemployment, earnings, and education, and find that the economic incentives for crime are important. Leukfeldt et al. (2019) examine criminal investigations of organized crime in the Netherlands and find that technological knowledge for cybercrime is often gained through a smaller set of technically skilled enablers in online market places.

[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."

a medical condition or divorce), and has sufficient cash.[12] First, there is a friendship or trust-winning stage, often spanning multiple months, which can also include the illusion of romantic potential.

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 actually 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 funds 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 real, 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

[12] A survey by the Global Anti-Scam Organization of 550 victims showed that victims from all stages in life are susceptible. Victims typically range between 30 to 60 years old, are often well-educated, and include both men and women. https://www.globalantiscam.org/post/statistics-of-crypto-romance-pig-butchering-scam

[13] A survey of 550 victims as of 2022 found that 77% emptied their savings accounts and 33% were driven into debt by scammers. https://www.globalantiscam.org/post/statistics-of-crypto-romance-pig-butchering-scam

sometimes counsel the victim through the financial loss.

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 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. It is reported in Cambodia, one of the compounds housing a large number of enslaved people 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 .[16] 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.[17] Many perpetrators are thought to 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). Variants of scamming operations

[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 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] https://www.nytimes.com/2023/08/28/world/asia/cambodia-cyber-scam.html

[17] 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.

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).

1.3 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 US 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.[18] The exchanges credit user accounts with the new funds, but continue to store the funds in centralized *exchange wallets*. Users can trade cryptocurrencies completely within the ecosystem of their given centralized exchange. This entire process occurs "off-chain", or only within the records of the cryptocurrency exchange.

If a user tries to send cryptocurrencies to another entity that is outside of their exchange, they must provide the receiving address, similar to a traditional bank transfer. The exchange will debit the user's account and complete the transaction using the central exchange wallet. From a centralized exchange, users can also transfer tokens from their account to an externally-owned address they control, or directly from the exchange to another user's account on a different exchange. Externally-owned addresses can transfer crypto to other addresses including smart contracts. For example, one of the most common types of contracts is a *swap*, where one type of ERC-20 token is exchanged for another ERC-20 token, through services like Uniswap. Cong and He (2019), Harvey et al. (2022), and Makarov and Schoar (2022) describe various aspects of smart contracts and the decentralized finance landscape. Transactions between addresses are recorded on the blockchain.

Importantly, if a cryptocurrency user intends to spend their cryptocurrency in the real-

[18] According to victim reports, scammers often help onboard victims to a known cryptocurrency exchange. Victims must authenticate their identifies through anti-money laundering and know-your-customer (AML/KYC) processes of these exchanges, then fund their accounts.

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.[19] Any money sent to that address would then be credited to their Binance account.

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 network relies on three main types of data: data on victim reports of pig butchering, blockchain transaction-level data, and blockchain address identity data. From online message boards, dedicated crypto-scam reporting websites, and first-hand personal accounts, we collect a total of 1,065 addresses. Additionally, the United States Institute of Peace (USIP) shared a large set of additional addresses used in pig butchering scams.[20]

We apply screens through information collected on Etherscan to remove any addresses that are likely unrelated to pig butchering. The resulting dataset includes 4,728 (3,256 on Ethereum, 770 on Bitcoin and 702 on Tron) addresses reported to be associated with pig butchering scammers.[21]

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

[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) for their generous help in sharing data.

[21] In Figure IA.2, we plot the cumulative use of addresses over time across different blockchains and find that Ethereum has consistently been the most common within our sample.

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 also use token price information from CoinMarketCap.com to convert quantities to dollar values, using prices as of the end of the day for currencies like Bitcoin, Ether, and Wrapped Bitcoin. We collect data on cryptocurrency identities for address hashes and token hashes from Etherscan.com, the most popular source of data of this type. We supplement this with checks using Ciphertrace and web searches.

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 addresses, which are the addresses where victims were directed to send their crypto, and then following the paths of tainted funds. We use a variant of the Ether, ERC-20 token, and Bitcoin bulk-tracing tool developed by Integra FEC to simultaneously follow multiple paths.[22] 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. This tool includes proprietary criteria to terminate a trace path if funds reach an address that is unlikely to be 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 exchange wallet; (ii) the path reaches five hops; or, (iii) the path reaches an address that appears to be involved in any other type of non-pig butchering activities.

The first criteria terminates 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.[23]

[22]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.

[23]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).

Tracing can reliably go much further than five hops, but we terminate the trace at five hops because a large proportion funds have already flowed to an exchange within five hops, as we will present later, and we wish to maximize the probability that the deposit addresses we reach are controlled by a scammer.[24]

We trace Bitcoin under a similar framework though tailored for the specifics of its blockchain transaction architecture. Bitcoin transactions follow the common input heuristic such that any two addresses that both send money in a transaction can be confidently called a *cluster* controlled by the same entity, as detailed in papers such as Meiklejohn et al. (2013). Following this methodology, we expand our scope to include addresses within the same cluster as the original reported scammer address. We also trace Bitcoin sent to the Ethereum blockchain using a proprietary cross-blockchain bridge tracing mechanism.

In summary, we focus on Ethereum paths that start from exchange wallets sending funds to scammer addresses and end at user deposit addresses. Our analysis is oriented "from-exchange to-exchange" to focus both on how funds enter and exit the crypto ecosystem and to manage the complexity as paths grow with each hop. Our approach allows us to 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 backwards from potential scammer deposit addresses in Section

[24]Cloud computing costs also grow with each hop. 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.

5, such that summing the total lifetime flow to these deposit addresses indicates the size of the pig butchering network. We further collect all nodes that have appeared in both the trace and back-trace and study features of the network in Section 6.

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 a relationship, the scammer coached him through the investment process, including funding his account at an exchange and transferring approximately $70,000 in Bitcoin, $25,000 in Ether, and $370,000 in USDC to a spoofed exchange. All told, this middle-class victim, a diligent saver, 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 network. 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 funds 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.[25] Scammed funds often cycle through many nodes. Ultimately, most funds enter Binance

[25]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 US Financial Crimes Enforcement Network and thus must freeze funds in response to the US justice system.

as Tether, with large transactions also entering OKX and Huobi. Smaller amounts reach Coinbase and Crypto.com. As we will see later, most of these payments to Coinbase and Crypto.com fit the characteristics of inducement payments.

2.4 Reported scammer addresses

Figure 3 shows the 3,256 Ethereum, 702 Tron and 770 Bitcoin addresses reported by the victims that meet the criteria outlined above. Notably, victims may include multiple addresses within the same report, such as in cases when scammers provide different addresses to victims.[26] The horizontal axis is the number of total transactions by the node, and the vertical axis is the total dollar inflow. Most nodes have an inflow of above $10,000 and below $10 million.

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.[27] Other tokens are occasionally transacted, but our focus is on these cryptocurrencies, unless otherwise noted.[28] 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 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 monitored inflows and outflows. The fact that addresses are used so frequently suggests that the monitoring process is not robust and that scammers are not too concerned about the exchange prohibiting such activity. The combined total amount is

[26] 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.

[27] It could be that victims send funds primarily in USDC, for example, but the address's primary token is Tether because that address has many other Tether transactions.

[28] 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.

$5,835 million in Ethereum, $389 million in Tron and $373 million in Bitcoin. Table I displays summary statistics on Ethereum scammer addresses. These addresses vary in size, with an interquartile range of 21 to 197 transactions and $76K to $1.4M in total inflow. Across all reported Ethereum addresses, the mean inflow is $1.9M. Outflows tightly match inflows, due to the common practice of forwarding funds and periodically switching addresses. The median address is active for 68 days.

3 Tracing the Network

We now present our main analysis: destinations from bulk-tracing reported scammer addresses. Figure 1 presents a sample of Ethereum trace paths that illustrate many of the features we find in the scammer networks.[29] 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 darkest shades representing large transaction amounts and lighter colors representing smaller transactions. The red triangles are reported scammer addresses. All other circular nodes are addresses encountered in the trace with, with pink indicating externally-owned addresses and shades of blue indicating exchange-controlled deposit addresses. Each scammer node is sized proportionally to the amount received and is positioned closest to nodes they transact with the most, such that 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 $10K, light blue is between $10K and less than $100K, blue from $100K to $1 million, and black at $1 million and over. The green counterpart of this color convention applies to the edges starting from exchanges.

[29] To reduce complexity, we show only a three percent sample. The sample was generated by picking a random set of about 200 scammer nodes in the Ethereum blockchain, and then randomly selecting paths connected to and including those nodes which start from and terminate at exchanges. The total sample contains 5,758 nodes and 16,431 edges.

The figure shows how crypto enters the network 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 bulk tracing results of the 3,256 scammer addresses. In Panel A, edge thickness is proportional to transaction amounts and edge colors correspond to cryptocurrency used. $447 million from Crypto.com enters scammer addresses, $418 million from Coinbase, and $248 million from Binance, followed by smaller amounts from other exchanges. These 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 $2.3 billion entering these addresses from all exchanges.[30] Yet, the reported addresses touch over $5 billion in funds. Many of these funds may be other funds moving through the system, as funds are sent to and back to Hop one, two, and three, and Tokenlon. This massive recirculation is one way to obfuscate funds. Tokenlon plays a large role in the network as shown by the crypto swapping in Panel A and totals in Panel B with large flows enter as USDC and Ether, only to return as DAI and Tether. Ultimately, Tether is the most common crypto used when re-entering exchanges.

We trace $4.3 billion to exchanges.[31] Important exit points include $952 million sent to Binance, $438 million to OKX, $155 million to Huobi. Only $67.5 million (or 1.5%) was sent to Coinbase and Crypto.com. Panel B indicates that over $1 billion enters exchanges within three hops. Transactions to OKX appear to move mostly within three hops, while transactions to Binance continue to occur even five or more hops away.[32] For early hops

[30]Plotted in the Internet Appendix in Figure IA.4.
[31]The remainder met the halting criteria before reaching an exchange.
[32]The bulk tracing tool counts hops starting after the first out-bound transaction of any starting addresses.

the funds appear in ETH, USDC, and Wrapped BTC, but in later stages the funds are almost exclusively in Tether with some DAI.[33] Overall, crypto typically moves from Western Crypto.com and Coinbase to Eastern-centered Binance, Huobi, and OKX.

We also examine whether exchange sources have changed over time from January 2021 to February 2024. Most of the funds enter the network 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 network from Western exchanges. The Tokenlon funds entering the network also appear larger in 2021, but one should interpret this as funds from other victims that has already been swapped through Tokenlon. Panel B shows that Tether (USDT) consistently appears to be the dominant crypto entering reported scammer addresses throughout the period. ETH and USDC are popular in late 2021 and 2022. Wrapped Bitcoin appears in 2022 and DAI in 2023.

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 2023 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.[34]

In total, the pattern from exchanges points to a potential shift from Eastern 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 Eastern-centered exchanges prior to 2021.[35] We examine this and other

Therefore, the trace shows a sixth nodes when programed to terminate at five hops.

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

[34]Indeed, 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.

[35]A caveat to our results is that exchanges are only a proxy for victim location. Additionally, because

features in more detail in Section 6.

4 Outflows from the Network

We now focus on outflows from these scammer networks to deposit addresses. We interpret these results with a backdrop that centralized exchanges typically must adopt know-your-customer protocols, implying that each deposit address is linked to a specific identifiable 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 us an avenue to size total transaction costs and proceeds of the scam operation.

4.1 Deposit Addresses

We follow the trace path to 14,350 user deposit addresses. Figure 5 splits deposit addresses into four groups based on amount of funds received in the trace path. There are more than 8,000 deposit addresses that receive less than $10K for a combined $15.1 million. These small payments are consistent with the characteristics of inducement payments, which we discuss in more detail in the next subsection. These small payments could also be interpreted as a situation where smaller amounts of scammer funds interacted with some other entities and their small transactions went back to the exchange. 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, Gate.io, MXC, and Bitkub, which are thought of as more anonymous. We interpret these larger flows as likely scammer-owned deposit addresses.

Panels A and B of Table II decompose deposit addresses into those that have less or more than $100,000 traced from the scam network and to each individual address. Notably, the total inflow and total outflow should match almost exactly because these correspond to user accounts held by exchanges, which flush all funds out of these accounts and into exchange

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.

wallets. We interpret addresses with less than $100,000 as likely victim deposit addresses. They receive inbound transfers from a median of five addresses (i.e., in-degree is five).[36] If these are funds flowing to victims, then it also implies that exchanges may have had multiple chances to curtail interactions between the scammer and the victim but did not.

Figure IA.6 examines the time-series of flows to all deposit addresses that received more than $100,000 from scammers. Huobi seemed to be the dominant exchange in early and mid-2022 but lost volume to Binance after mid-2022. OKX is prevalent in late 2022 and 2023, with smaller exchanges like Bitkub and Gate.io also emerging, indicating the widespread nature of these scamming operations across various exchanges. We pay less attention to the raw amount of funds received as these may be more of a function of the time series of when victim addresses were collected and active. Panel B of Figure IA.6 shows the summary across the entire period in terms of large inflows and shows that Binance ($925 million) is by far the largest exchange, followed by OKX ($391 million), and Huobi ($100 million). This reiterates that the majority of funds are funneled to non-Western exchanges.

Figure IA.7 summarizes our earlier findings by presenting the average transaction sizes exiting and entering exchanges. While funds exiting Coinbase and Crypto.com have a mean transaction size of $12K and $14K respectively, funds entering these exchanges average $2-5K. 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 $9K, $10K and $13K respectively, and yet transactions entering these exchanges dwarf even the funds leaving U.S. exchanges. 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.

[36] Based on the mechanics of deposit addresses, the custodial exchange will be at least one of the inbound relationships with this address.

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 network 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 payments and finds that most are $1,000 or less. We find 98,509 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 number of times an address is re-used over time. 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 114 days and a 75th percentile of 218 days, or 4-8 months, as presented in Table IA.II, which can be interpreted as the duration before scammers switch addresses.

In total, we observe 104,460 potential inducement payments, including 23,627 to Binance, 28,692 to Huobi, 13,892 to OKX, and 31,980 to five Western exchanges, the bulk of which is concentrated in Crypto.com (15,433) and Coinbase (15,249). In many cases, a *clean*, or previously unused, address sent potential inducement payments, such as 409 addresses that sent to Coinbase and 313 addresses to Crypto.com. However, as few as 60 addresses were responsible for over 7,198 transactions to Coinbase and 78 addresses for 9,359 to Crypto.com. The frequent re-use implies that there is relatively little rigorous monitoring from exchanges.

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

We document 56,688 unique exchange deposit addresses that receive transactions of up to $10,000 from potential inducement payment senders, as plotted in Figure IA.8, which we interpret as a lower bound of the number of addresses that receive inducement payments. Most new deposit addresses are concentrated in Binance and Huobi through 2021, while OKX, Coinbase, and Crypto.com appear more commonly in late 2021 through 2023. In summary, we find 12,146 Binance, 12,355 Huobi, 5,676 OKX, 12,792 Coinbase, and 11,381 Crypto.com deposit addresses that may have received inducement payments.

4.3 Transaction Costs

We calculate the aggregate transaction costs incurred within this trace, also known as gas fees, and present summary statistics in Table III. Ether and ERC-20 token transfers are typically agnostic to the amount transferred. Within our sample, we see an average gas fee of $6.07 and a median of $2.70 per transaction. As a percentage of the amount transferred, the median is nine basis points, and the mean is 6.06%.

Swaps were associated with higher gas fees with a median of $20.03 per transaction, or 32 basis points of the final amount. Swaps also have the opportunity of gaining or losing money due to the spread. The median loss was 25 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]

Transaction costs are an incentive for the network to aggregate payments, move larger amounts at once, and minimize costs. For example, transactions below $10,000 have a mean gas fee of 9.89% of the transferred amount and mean swap losses of -0.87%, whereas amounts above one million paid 0.0003% in gas fees and -0.02 % in swap losses.

Altogether, this network includes $5.8 million in ETH and token gas fees, $1.9 million in swap gas fees, and an aggregate loss of $6.4 million in swaps, for a total of $14 million in transaction costs. This represents the total fees used to move hundreds of millions of dollars

[38]The percentages are based on token prices as of midnight on the transaction date.

across multiple hops. If we conservatively consider $13 million as the total transaction cost needed to transfer the $1.6 billion into the largest deposit addresses with more than $100,000 inflow, then transaction costs amount to 0.87% of flows to scammer deposit addresses.[39]

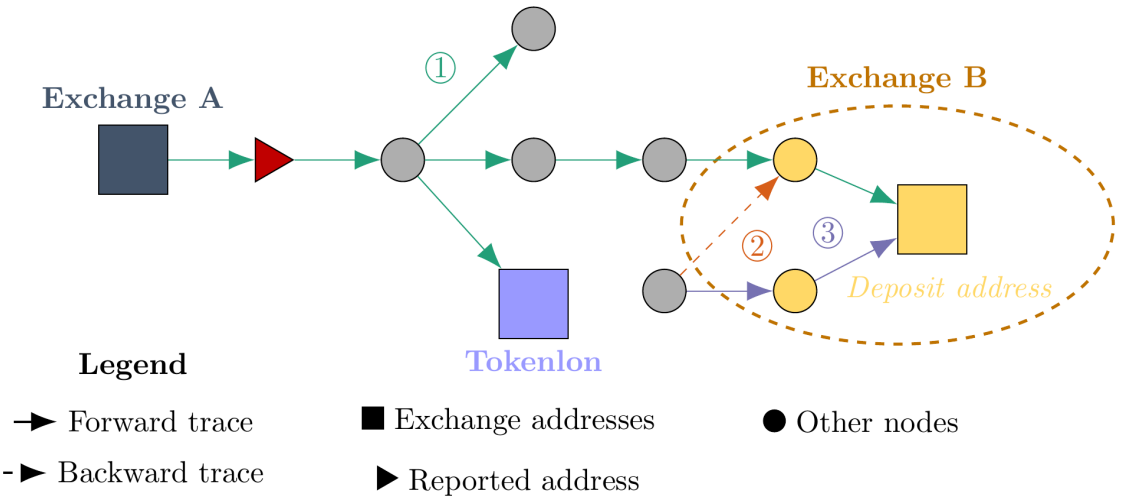
5 Sizing the Scamming Network

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

5.1 Sizing Methodology

We collect all Ethereum deposit addresses that have received more than $100K in total across four tracing steps: (i) initial paths found from reported scammer addresses; (ii) *re-traces* by finding post-swap paths for tokens that interact with Tokenlon; (iii) Bitcoin paths that can be traced across the WBTC bridge; and (iv) a second retrace of (ii) and (iii). We focus on a total of 2,787 potential scammer deposit addresses, as plotted in Figure IA.9. Figure IA.10 plots $25.8 billion flowing into these deposit addresses over time. 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

[39]The denominator in this calculation, $1.6 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 0.87% as a conservative estimate.

"deposit address clustering." 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 owned by that same address.[40] The heuristic associates any given address that deposit 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 network.

5.2 Sizing Results

These identified deposit addresses are potentially scammer deposit addresses on exchanges, where funds exiting the networks can no longer be traced on-chain. Figure 9 plots the results of these findings over time from January 2020 to February 2024 and highlights two results. We sum all inflows to these addresses and find $75.3 billion, most of which is concentrated in exchanges typically considered outside of U.S. jurisdiction. Of these exchanges Binance is the overall largest destination. Huobi was popular in 2020-2021, while OKX is more popular from 2021-2023.

As a robustness analysis, we decompose our steps in Figure IA.11. The original deposit trace is in the darker color, while an incremental amount traced through the deposit clustering heuristic and retracing. The heuristic effectively captures more activity prior to 2021. To further gauge the potential size of related funds, we can further apply the deposit clustering heuristic a second time to the larger set of deposit addresses to see if there are further related deposit addresses. This step increases our estimate from $75.3 billion to $237.6 billion. We expect that this larger number likely contains looser connections. Nevertheless, the calculation indicates that there is a substantial amount of capital closely interacting with these networks.

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

5.3 Backtracing

Note that these estimates include all funds entering into deposit addresses. If a network sent funds from say OKX to Binance, it would lead to the double-counting of funds. Additionally, the funds may be due to other activities of the criminal networks. 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 $40.2 billion of the $75.3 billion can be attributed to exchanges.[41,42]

Identifying flows exiting exchanges provides an avenue to assess the magnitude of pig butchering's financial harm to victims. If we consider all addresses that have been found in both the forward and backward traces, and apply the consistent set of screens as those earlier in the paper, then we can 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 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 $15.2 billion from Western exchanges in transactions of less than $500,000, which we interpret as a lower bound of the total amount defrauded from victims using Western exchanges. This entered the scammer network through a total of 1,257,088

[41] See Figure IA.12. The remainder did not reach a source within five hops, or the path reached an address that triggered the termination criteria from Section 2.

[42] 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 $500K and plot these results in Figure IA.13. 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 overly conservative estimate because the backtrace paths stop at large nodes and thus does not include all paths from exchanges.

transactions, with a mean of over $12k per transaction. The total includes $3.1 billion from Coinbase, $4.5 billion from Crypto.com, and $5.2 billion from Kraken.

The prior analyses primarily depicted flows from exchanges to the network, or from the network to exchanges. In addition, we now the sum of each transaction within the network. All volume within the network totals to $1,172 billion, as plotted in Figure IA.14 split by cryptocurrencies. We find that 84% 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 excessive 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 thus creating more dead-end paths for any potential investigator to follow. These efforts are potentially costly to the criminals: each transaction incurs transaction fees and dusting tokens are essentially lost revenue. Tactics to obfuscate the flow of funds may potentially be signs of nefarious intentions. Three other empirical examples shed light on how these criminal networks operate: first, the shift in sources of inflows after a government crackdown, second, the extensive use of token swaps, and third, the high degree of connectedness of the whole network and its subsets.

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.[43] 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 2019 through 2023, grouped by the active hour of the day, by month. The size of each square is proportional to total volume,

[43]News reports of these decisions are presented in Table IA.I.

and colors are indicative 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-US exchanges. After this announcement, however, activity begins to wane, and by December 2021, we see an increase in activity from US waking hours. This provides corroborating evidence of a shift in the victim base from Eastern victims to Western 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 of 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.[44]

6.2 Use of Tokenlon swaps

The scammer networks use decentralized exchanges such as Uniswap and Tokenlon to swap between different cryptocurrencies. Similar to the excessive mixing of funds, this transaction incurs transaction fees; however, to someone who may be looking for money laundering channels, a decentralized exchange may be cheaper than swapping in a centralized exchange and can make it more challenging for some popular tracing tools to follow a path of funds. While Uniswap is arguably the most popular decentralized exchange, Tokenlon is relatively obscure and may be a distinctive trait of pig butchering scams.[45]

In Figure 12 Panel A, we plot the number of Tokenlon transactions over time as found

[44] As reported in outlets such as the BBC.

[45] Uniswap is a consistently top 3 decentralized exchange with more than 20% market share while Tokenlon is ranked in the 30-50 range with 0.1-0.2% market share according to CoinMarketCap (https://coinmarketcap.com/rankings/exchanges/dex/)

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 58% of all Tokenlon swap transactions per month. This suggests that if a given crypto user chooses to swap with Tokenlon, their trading helps the scammers to obfuscate the flow of funds. Our numbers are also likely undercounted as we are only tracing those parts of the network we can identify. As shown earlier (in Figure IA.5) 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.

6.3 Connectedness

We wish to understand whether scammer networks are interconnected. In Figure IA.16 we plot the number of distinct partitions within the data and the number of addresses we add with each trace. The original 3,256 nodes begin as 3,256 separate partitions of the network. When considering just the in-bound and out-bound relationships of these nodes, and ignoring any connections to exchange addresses, we find that there are approximately 1,504 partitions, a smaller number because many addresses have edges between each other. After considering just one further step along the trace, the number of partitions falls to approximately 180. The total number of partitions after five hops is 118. More importantly, we find that more than 99% of nodes are connected within one large, interconnected network. 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 present in several countries, we believe (b) is the most likely.

7 Additional Analyses

Because of the size and complexity of our identified scammer networks, we undertake additional analyses to evaluate the robustness of our results, including a placebo comparison, evaluating the sensitivity to victim-reported addresses, and additional third-party verification.

7.1 Placebo Comparison

We wish to understand how pig butchering networks differ from other scamming activity on Ethereum. We build a placebo test by tracing a sample of 1,000 addresses reported by victims and potential victims of phishing scams.[46] Phishing scam addresses commonly deal in small amounts, often collecting less than $10,000 (as shown in Figure IA.15). In contrast, pig butchering addresses commonly receive more than $1 million. Phishing scams commonly interact with DeFi exchanges such as Uniswap and move money to Uniswap, Kucoin, Binance and other decentralized exchanges. Pig butchering draws in substantially more directly from exchanges like Crypto.com and Coinbase, while funneling funds into Binance, Huobi, and OKX at much higher rates (Figure IA.17). Lastly, pig butchering scammers are much more likely to use Tether while phishing scammers use proportionally more Ether and other ERC-20 tokens (Figure IA.18).

7.2 Path Sensitivity

Reports of scammer addresses may be imprecise. We minimize these errors by filtering the addresses we trace to exclude potentially problematic addresses or obvious errors, such as by removing large addresses and smart contracts. We do not know the verification process of our data, but one of our sources reports to implement verification for many of the victim

[46] 51 addresses never transacted leaving 949 addresses to examine.

reports. In an earlier version, we also implemented results with this substantially smaller sample of 1,065 addresses and found most findings of a similar nature, though with a total network size of $29 billion.

7.3 Further Analysis on Deposit Addresses

We also conduct extensive checks on our deposit addresses, including checking if any have been identified by third-party sources. For example, if a potential scammer deposit address is identified as belonging to a hedge fund, then it would imply that the *true* flow of funds substantially deviated such that we traced funds that were later transferred to that hedge fund. After checking 630 deposit addresses on Ciphertrace, all 630 results were returned as unknown origin.

We examine if our results are driven by a few errant deposit addresses. In Figure 13, 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 reduces concerns that they are only loosely connected to victims. 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 that the one address that has received over $1 billion, but the vast majority receives substantially less (as shown in Figure IA.19). The top 100 of our 14,350 deposit addresses account for $19.0 billion of our total $75.3 billion in inflow to larger scammer deposit addresses.

We consider addresses from the forward trace and back trace that meet our criteria above, and check their flow to deposit addresses. Within this broadest definition of the networks we study, we perform a robustness check on the amount of likely inflows to criminal deposit addresses. We find a total of $73.6 billion of transactions with more than $100K into deposit addresses, which is similar to the total exits we found before. This robustness analysis suggests that the network is bounded and does not seem to endlessly branch off to other

terminal deposit addresses. Ultimately, when considering that the majority of large deposit addresses are centering on Binance, we interpret this to be consistent with our earlier results and indicating that this is a highly connected set of networks that facilitates the flow from Western exchanges to exchanges with weaker KYC/AML procedures.

7.4 Bitcoin Tracing and Swaps

Figure IA.20 shows the Bitcoin transactions of a single address to illustrate the activity. Transactions on Bitcoin frequently originate from Coinbase or Square Cash App. These transactions are generally forwarded through multiple transactions into the scammer's collection point. The collection network also uses dusting transactions which consists of small Bitcoin transactions meant to confuse standard tracing algorithms by causing unrelated entities to be clustered together.

As discussed in more detail in Section 2, we expand on our list of reported addresses and rely on the common input heuristic to identify the broader clusters associated with each address. We present the destinations in Figure IA.21 and find that these trace paths lead to similar destinations: $65 million to Tokenlon, $47 million to Binance, $32 million to Huobi, and $12 million to OKX. Given that these are two different blockchains, we cannot ascertain whether these Huobi and OKX addresses are related to the deposit addresses found in Ethereum. However, the prominence of Tokenlon remains a distinct finding and offers a chance for tracing these 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 actually transferring into a Tokenlon-affiliated Ethereum ERC-20 token called imBTC, which can then be traded for the third-party Wrapped Bitcoin. Interestingly, of the 1,192 transactions of this type corresponding with 129 unique Ethereum addresses, 101 of these addresses already appeared in our original Ethereum trace, suggesting that our collected Bitcoin addresses are related to our Ethereum addresses.

8 Conclusion and Implications

There are several practical implications of our study. First, large crypto exchanges like Binance, Huobi, OKX act as exit points for $75.3 billion in criminal proceeds. 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 KYC/AML provisions are profiting by facilitating money laundering. Fourth, the consistent patterns and substantial cross-pollination across addresses point to a large coordinated network, or several networks sharing similar services. In contrast to reports, these scams should thus not be treated simply as individual crimes, which is the norm for law enforcement. Fifth, Western 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 are just one transfer away from disappearing. 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 monitor the pig butchering networks and their inducement payments to circumvent ongoing scams.

More generally, our analysis shows that the "legitimate" crypto space commonly serves as the entry and exit point to the illegitimate space and in so is facilitating the cheap and easy flow of funds that is the lifeblood enabling both pig butchering and modern-day slavery. Overall, our findings suggest that criminal networks are moving substantial funds cheaply and without much fear of detection. There is much that can be done to tighten controls on the funds feeding these large criminal networks. Our methods can also be applied to uncover the nature of other criminal networks.

References

Amiran, Dan, Bjørn N. Jørgensen, and Daniel Rabetti, 2022, Coins for bombs: The predictive ability of on-chain transfers for terrorist attacks, *Journal of Accounting Research* 60, 427–466.

Anderson, Keith B., 2021, To whom do victims of mass-market consumer fraud complain?

Barragan, Carlos, 2023, The romance scammer on my sofa, Atavis.

Chainalysis, 2023, The 2023 crypto crime report.

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

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

Cong, Lin William, and Zhiguo He, 2019, Blockchain disruption and smart contracts, *The Review of Financial Studies* 32, 1754–1797.

Conrad, Alfred H., and John R. Meyer, 1958, The economics of slavery in the ante bellum south, *Journal of Political Economy* 66, 95–130.

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

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

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

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

FTC, 2023, Romance scammers' favorite lies exposed, Online Report.

Gandal, Neil, JT Hamrick, Tyler Moore, and Tali Oberman, 2018, Price manipulation in the bitcoin ecosystem, *Journal of Monetary Economics* 95, 86–96.

Griffin, John M., and Samuel Kruger, 2024, What is Forensic Finance?, University of Texas, Working Paper.

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

Hamrick, J.T., Farhang Rouhi, Arghya Mukherjee, Amir Feder, Neil Gandal, Tyler Moore, and Marie Vasek, 2021, An examination of the cryptocurrency pump-and-dump ecosystem, *Information Processing and Management* 58, 102506.

Harvey, Campbell R., Tarek Abou Zeid, Teun Draaisma, Martin Luk, Henry Neville, Andre Rzym, and Otto van Hemert, 2022, An investor's guide to crypto.

Leukfeldt, E. Rutger, Edward R. Kleemans, Edwin W. Kruisbergen, and Robert A. Roks, 2019, Criminal networks in a digitised world: on the nexus of borderless opportunities and local embeddedness, *Trends in Organized Crime* 22, 324–345.

Levi, Michael, 2015, Money for crime and money from crime: Financing crime and laundering crime proceeds, *European Journal on Criminal Policy and Research* 21, 275–297.

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

Makarov, Igor, and Antoinette Schoar, 2021, Blockchain Analysis of the Bitcoin Market, Working Paper.

Makarov, Igor, and Antoinette Schoar, 2022, Cryptocurrencies and Decentralized Finance (DeFi), Working Paper.

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

Mirenda, Litterio, Sauro Mocetti, and Lucia Rizzica, 2022, The economic effects of mafia: Firm level evidence, *American Economic Review* 112, 2748–2773.

Pennec, Guénolé Le, Ingo Fiedler, and Lennart Ante, 2021, Wash trading at cryptocurrency exchanges, *Finance Research Letters* 43, 101982.

Phua, Kenny, Bo Sang, Chishen Wei, and Gloria Yang Yu, 2022, Don't trust, verify: The economics of scams in initial coin offerings.

PWC, 2023, 5th annual global crypto hedge fund report.

Reiter, Jonathan, and Bitrace, 2024, Connecting chinese and american scam victims, Working Paper.

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

Solomon, Feliz, 2023, China unleashes crackdown on 'pig butchering.' (it isn't what you think.), Wall Street Journal.

Soudijn, Melvin, and Peter Reuter, 2016, Cash and carry: the high cost of currency smuggling in the drug trade, *Crime, Law and Social Change* 66, 271–290.

UN, 2023, Online scam operations and trafficking into forced criminality in southeast asia: Recommendations for a human rights response.

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.

US Treasury Department, 2002, 2002 National Money Laundering Strategy.

US Treasury Department, 2007, 2007 National Money Laundering Strategy.

Victor, Friedhelm, 2020, *Address Clustering Heuristics for Ethereum*, 617–633 (Springer International Publishing).

Wang, Fangzhou, and Xiaoli Zhou, 2023, Persuasive Schemes for Financial Exploitation in Online Romance Scam: An Anatomy on *Sha Zhu Pan in* China, *Victims & Offenders* 18, 915–942.