On How Zero-Knowledge Proof Blockchain Mixers Improve, and Worsen User Privacy

Zhipeng Wang
Imperial College London
United Kingdom
zw720@ic.ac.uk

Stefanos Chaliasos
Imperial College London
United Kingdom
s.chaliasos21@imperial.ac.uk

Kaihua Qin
Imperial College London
United Kingdom
kaihua.qin@imperial.ac.uk

Liyi Zhou
Imperial College London
United Kingdom
liyi.zhou@imperial.ac.uk

Lifeng Gao
Imperial College London
United Kingdom
li.gao16@imperial.ac.uk

Pascal Berrang
University of Birmingham
United Kingdom
p.p.berrang@bham.ac.uk

Benjamin Livshits
Imperial College London
United Kingdom
b.livshits@imperial.ac.uk

Arthur Gervais
UCL & UC Berkeley
United Kingdom & USA
arthur@gervais.cc

ABSTRACT

Zero-knowledge proof (ZKP) *mixers* are one of the most widely-used blockchain privacy solutions, operating on top of smart contract-enabled blockchains. We find that ZKP mixers are tightly intertwined with the growing number of Decentralized Finance (DeFi) attacks and Blockchain Extractable Value (BEV) extractions. Through coin flow tracing, we discover that 205 blockchain attackers and 2,595 BEV extractors leverage mixers as their source of funds, while depositing a total attack revenue of 412.87M USD. Moreover, the US OFAC sanctions against the largest ZKP mixer, Tornado.Cash, have reduced the mixer's daily deposits by more than 80%.

Further, ZKP mixers advertise their level of privacy through a so-called anonymity set size, which similarly to k-anonymity allows a user to hide among a set of k other users. Through empirical measurements, we, however, find that these anonymity set claims are mostly inaccurate. For the most popular mixers on Ethereum (ETH) and Binance Smart Chain (BSC), we show how to reduce the anonymity set size on average by 27.34% and 46.02% respectively. Our empirical evidence is also the first to suggest a differing privacy-predilection of users on ETH and BSC.

State-of-the-art ZKP mixers are moreover interwoven with the DeFi ecosystem by offering *anonymity mining (AM)* incentives, i.e., users receive monetary rewards for mixing coins. However, contrary to the claims of related work, we find that AM does not necessarily improve the quality of a mixer's anonymity set. Our findings indicate that AM attracts privacy-ignorant users, who then do not contribute to improving the privacy of other mixer users.

CCS CONCEPTS

• **Security and privacy → Pseudonymity, anonymity and untraceability**.

KEYWORDS

Privacy; Anonymity; Blockchain; DeFi; Mixer

ACM Reference Format:
Zhipeng Wang, Stefanos Chaliasos, Kaihua Qin, Liyi Zhou, Lifeng Gao, Pascal Berrang, Benjamin Livshits, and Arthur Gervais. 2023. On How Zero-Knowledge Proof Blockchain Mixers Improve, and Worsen User Privacy. In *Proceedings of the ACM Web Conference 2023 (WWW '23), May 1–5, 2023, Austin, TX, USA.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3543507.3583217

WWW '23, May 1–5, 2023, Austin, TX, USA

ACM ISBN 978-1-4503-9416-1/23/04…$15.00
https://doi.org/10.1145/3543507.3583217

1 INTRODUCTION

It is well-known that non-privacy-focused permissionless blockchains, such as Bitcoin and Ethereum, offer pseudonymity rather than anonymity [2, 10, 12]. While privacy-preserving blockchains [14, 21, 30] aim to protect their users' privacy, retrofitting a blockchain with privacy has proven challenging and remains an active research area [7, 13, 19, 20, 28, 29, 31, 32, 37]. The solution space can be broadly divided into *(i)* privacy-by-design blockchains and *(ii)* add-on privacy solutions, which are retrofitted, e.g., as a Decentralized Application (DApp) on top of non-privacy-preserving blockchains.

ZKP mixers, inspired by Zerocash [30], are one of the most widely-used blockchain privacy solutions, where a user deposits a *fixed* denomination of coins into a pool and later withdraws these coins to an address. The goal of ZKP mixers is to break the *linkability* between a deposit and a new withdrawal address. The most active ZKP mixer on ETH, Tornado.Cash (TC), reports an anonymity set size of 51,286 for its largest pool (i.e., 1 ETH pool) on August 8th, 2022. This number is simply derived from the count of equal user deposits and suggests that, given a withdrawal transaction, the corresponding deposit can be hidden among the 51K deposits. Moreover, to attract users, ZKP mixers offer anonymity mining (AM) incentives, where users can receive rewards for mixing coins.

ZKP mixers have also attracted the attention of centralized regulators. On August 8th, 2022, the US Treasury's Office of Foreign Assets Control (OFAC) placed sanctions [36] on TC due to alleged facilitation of money laundering. To our knowledge, this is the first time that centralized regulators sanctioned a decentralized and open-source application.

In this work, *(i)* we investigate to what degree adversarial actors use ZKP mixer, *(ii)* how the OFAC sanctions affect mixer usage, *(iii)* we challenge the mixer's reported anonymity set sizes

through heuristic intersections, and attempt to validate our heuristics through public side-channel data, and *(iv)* we investigate the privacy implications of anonymity mining.

We summarize our contributions as follows:

1. Analyzing Multi-Blockchain ZKP Mixers Usage: We empirically investigate through coin flow tracing the deposit and withdrawal behavior on the two most popular ZKP mixers, TC (on ETH) and Typhoon.Network (TN) (on BSC). For mixer withdrawals, we discover that 141 malicious addresses and 545 BEV extractors withdraw coins from a mixer as the adversarial source of funds. For mixer deposits, we find that 172 malicious addresses and 2,376 BEV extractors deposit a total of 412.87M USD into TC (cf. Section 4).

2. OFAC Sanctions Impact on Mixers: We are the first to analyze how OFAC sanctions affect ZKP mixers. We find that, although 487 user addresses have still deposited 62.59M USD into TC after the sanctions, the total daily TC deposits have decreased by 83%. Additionally, we discover that more than 85% post-sanction TC withdrawn assets are transferred to intermediary addresses before being sent to Centralized Exchanges (CEXs) or DeFi platforms, which indicates that users likely attempt to bypass the platforms' censorship (cf. Section 5).

3. Anonymity Mining's Impact on Privacy: We are the first to study and empirically evaluate the impact of AM in ZKP mixers. Contrary to the claims of related work [18], we find that AM does not always increase mixers' anonymity set size quality, because AM appears to attract privacy-ignorant users with a primary interest in mining rewards. After pruning privacy-ignorant user addresses, we find that the *advantage* (cf. Eq. 1) that an adversary links a withdrawer to the correct depositor rises from 7.00% (before AM launch) to 13.50% (after AM launch) on average (cf. Section 6).

4. Measuring Mixer Anonymity Set Size: We propose five on-chain data heuristics to derive a more accurate mixer anonymity set size, than naively enumerating equal user deposits. Combining heuristics proves powerful, as our evaluation shows that an adversary can reduce the anonymity set size on average by 27.34% and 46.02% of TC (on ETH) and TN (on BSC) respectively. We are hence the first to provide quantitative evidence indicating a user behavior difference w.r.t. privacy on two non-privacy-preserving blockchains. Our results also show that the biggest anonymity set continues to attract privacy-aware users, similar to how liquidity attracts liquidity in financial exchanges (cf. Section 7).

2 BACKGROUND

2.1 Blockchain and Smart Contracts

Permissionless blockchains act as a distributed ledger on top of a peer-to-peer (P2P) network. Smart contracts are quasi Turing-complete programs that typically execute within a virtual machine and allow users to construct various applications. For instance, DeFi is a financial ecosystem that runs autonomously on smart-contracts-enabled blockchains. The total locked value in DeFi has reached over 41B USD at the time of writing. Many DApps are inspired by and mirror traditional centralized finance systems, such as asset exchanges, lending and borrowing platforms, and margin trading systems [11, 24, 26, 39, 45]. A transaction can be used to transfer blockchain tokens or to trigger the execution of smart contract functions. The sender of a transaction pays for the cost of the entire smart contract execution caused by that transaction.

Transactions are propagated over a public P2P or a private relay network, prior to being validated by miners. Miners hence have the unilateral power to determine the transaction order in their mined blocks, creating an information asymmetry that yields a financial gain, i.e., Miner Extractable Value (MEV) [11]. Generalizing MEV, non-mining traders can also manipulate the transaction order and front-run their victims by paying higher transaction fees to extract *blockchain extractable value* (BEV) [25]. Related work [25] indicates that the dominant BEV activities include sandwich attacks [45], liquidations [24], arbitrages [44], and replay attacks [25].

2.2 Mixing Services for DeFi

Mixing services allow users to mix their coins with other users in an effort to break linkability of addresses. The literature features various proposals for mixing service designs, which can be centralized [7, 13, 31, 37] or governed by smart contracts.

As DeFi adoption increases and all transactions, balances, senders, and recipients are public, the demand for privacy in DeFi has led to the launch of ZKP mixers. To date, the largest ZKP mixer on Ethereum is TC [33], which launched in December 2019. TC operates four ETH pools (i.e., 0.1, 1, 10 and 100 ETH pools) which support the deposit and withdrawal of a fixed amount of ETH. When a user deposits a fixed amount of ETH into a TC pool, the user should safely back up a deposit *note*; to withdraw, the user should provide the deposit *note*, which needs to be verified by the TC smart contract. TC also supports the mixing of other tokens (e.g., USDC, USDT, etc), but most users appear to be mixing ETH. The total ETH deposited in TC reached over 3.54M ETH[1] (4.70B USD) at the time of writing.

AMR [18] is a new mixer design similar to TC, but additionally rewards its users for their participation in the system. Such incentivization of paying rewards is similar to the currently popular liquidity mining, also called "DeFi farming", an attempt to attract more users. More users should translate to a larger anonymity set size, as AMR proclaims. Soon after AMR, TC was updated to support anonymity mining [34] to incentivize users to keep their deposited ETH in mixer pools for a longer time period. ZKP mixers can also run on other smart contract-enabled blockchains, e.g., Typhoon.Cash (TP) on ETH, TN and Cyclone on BSC.

2.3 OFAC Sanctions against TC

On August 8th, 2022, the US Treasury's OFAC placed sanctions [35, 36] on TC, due to alleged assistance of money laundering. OFAC added the TC website and related addresses to the "Specially Designated Nationals And Blocked Persons" (SDN) list. According to the sanctions, US citizens are no longer legally allowed to use the TC website or involve any property or interest transactions with the addresses in the SDN list. To our knowledge, this is the first time that centralized regulators sanction decentralized applications. The sanctions caused a series of consequences. For instance, many DeFi platforms (e.g., Uniswap), Front-running as a Service (FaaS) platforms (e.g., Flashbots), and miners (e.g., Ethermine) choose to censor TC-related transactions or addresses interacting with TC [8].

[1]We adopt the coin prices on CoinMarketCap on October 1st, 2022, e.g., 1 ETH = 1,330 USD, 1 BNB = 285 USD.

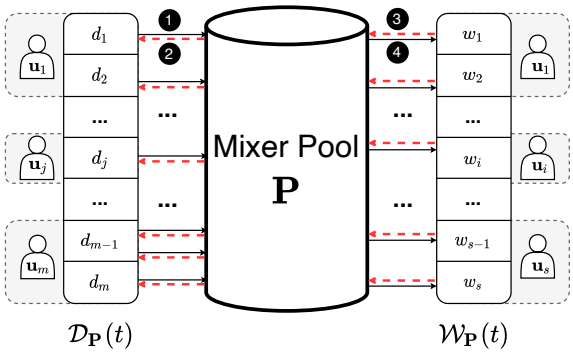


Figure 1: System Model for a mixer pool, where $\mathcal{D}_{\mathbf{P}}(t) = \{d_1, ..., d_m\}$ and $\mathcal{W}_{\mathbf{P}}(t) = \{w_1, ..., w_s\}$. '⟶' represents a transfer of coin, and '⇠' represents a *note* transfer. When a user u deposits coin into pool P (in step 1), u receives a *note* from P (in step 2). To withdraw, u needs to provide *note* to P (in step 3), and will receive coin after P verifies *note* (in step 4). A user can control multiple addresses. An address can be used to deposit or withdraw multiple times.

3 SYSTEM MODEL AND PRIVACY METRICS

In this section, we outline our system and privacy metrics.

3.1 System Model

Address: Users have at least one public/private key-pair (corresponding to their *address*), which controls cryptocurrency assets on a permissionless blockchain. To transfer or trade an asset, a user signs a transaction with its private key. Each transaction corresponds to an event with various publicly readable features, such as the time of day and the transaction fees.

Coin Transfer: A transfer of a coin is a tuple tr = (bn, from, to, amt, coin), where bn is the block number (i.e., timestamp), amt is the amount of coin that is transferred from the address from to to.

Coin Flow: A chain of transfers of coin between addresses.

Link: Two addresses a_1 and a_2 belong to the same user are linked. Denoted as $\textsc{Link}(a_1, a_2) = 1$.

Cluster: A cluster is a set of mutually-linked addresses.

Mixer Pool: A mixer pool, denoted as **P**, is an aggregation of cryptocurrency assets governed by smart contracts (cf. Fig. 1). Users can only deposit and withdraw a specific cryptocurrency coin. To avoid that deposit/withdrawal asset amounts leak privacy, mixer pools typically only accept a fixed currency denomination. The proper use of a mixer pool **P** requires choosing one address to deposit and another ideally unlinkable address to withdraw.

A *depositor* is an address to deposit coin into **P**, and a *withdrawer* is an address to receive coin from **P**. At time t, given a pool **P**, denote its depositor set as $\mathcal{D}_{\mathbf{P}}(t)$ and withdrawer set as $\mathcal{W}_{\mathbf{P}}(t)$.

To track users' coin flows before and after interacting with a mixer pool, we extend the depositor and withdrawer set (cf. Fig. 9).

Depositors Extension: At time t, we let $\mathcal{D}_{\mathbf{P}}(t) = \mathcal{D}_{\mathbf{P}}^{(1)}(t)$, and define the depositors in distance n (where $n > 1$), $\mathcal{D}_{\mathbf{P}}^{(n)}(t)$, as the set of addresses that transfer coin to the addresses in $\mathcal{D}_{\mathbf{P}}^{(n-1)}(t)$.

Withdrawers Extension: At time t, we let $\mathcal{W}_{\mathbf{P}}(t) = \mathcal{W}_{\mathbf{P}}^{(1)}(t)$ and define the withdrawers in distance n (where $n > 1$), $\mathcal{W}_{\mathbf{P}}^{(n)}(t)$, as the set of addresses that receive coin from the addresses in $\mathcal{W}_{\mathbf{P}}^{(n-1)}(t)$.

3.2 Privacy Metrics

Knowing the depositor set $\mathcal{D}_{\mathbf{P}}(t)$ of a pool **P** at time t, we define the *observed* anonymity set and the *true* anonymity set of the pool.

Observed Anonymity Set: Given a mixer pool **P** at time t, the observed anonymity set $\mathbf{OAS}_{\mathbf{P}}(t)$ of a pool **P** is the set of unique deposit addresses, i.e., $\mathcal{D}_{\mathbf{P}}(t)$.

True Anonymity Set: At time t, the true anonymity set $\mathbf{TAS}_{\mathbf{P}}(t)$ of a pool **P** is the set of addresses with a positive deposit balance in the pool, i.e., the set of depositors whose deposited assets have not yet been completely withdrawn from the pool **P**.

Note that the true anonymity set might not be apparent from observing the blockchain data, because it is the mixer's intention to obfuscate the addresses depositing into the mixer pool. However, an adversary can leverage on-chain data to compute a more "realistic" anonymity set, which can be more representative than $\mathbf{OAS}_{\mathbf{P}}(t)$.

Simplified Anonymity Set: Given a mixer pool **P** at time t, the simplified anonymity set $\mathbf{SAS}_{\mathbf{P}}(t)$ is the set of depositors with a positive balance, which is computed by leveraging on-chain data to simplify the pool state. Note that $\mathbf{SAS}_{\mathbf{P}}(t) \subseteq \mathbf{OAS}_{\mathbf{P}}(t)$.

Privacy Metric: The probability that an adversary without prior knowledge links a withdrawer (who withdraws at time t) to the correct depositor is $\mathrm{Adv}^{o}_{\mathcal{A}}(t) = 1/|\mathbf{OAS}_{\mathbf{P}}(t)|$.

If the adversary can link a withdrawer w, to a target set of depositors $\mathbf{SAS}_{\mathbf{P}}(t)$, then the probability that the adversary links w to the correct depositor is $\mathrm{Adv}^{s}_{\mathcal{A}}(t) = 1/|\mathbf{SAS}_{\mathbf{P}}(t)|$.

We further define $\mathrm{R}_{\mathrm{Adv}}$ as the increase of $\mathrm{Adv}^{s}_{\mathcal{A}}(t)$ over $\mathrm{Adv}^{o}_{\mathcal{A}}(t)$, to represent the *advantage* that an adversary links a withdrawer to the correct depositor after simplifying the anonymity set (cf. Eq. 1).

$$\mathrm{R}_{\mathrm{Adv}} = \frac{\mathrm{Adv}^{s}_{\mathcal{A}}(t) - \mathrm{Adv}^{o}_{\mathcal{A}}(t)}{\mathrm{Adv}^{o}_{\mathcal{A}}(t)} \tag{1}$$

4 EMPIRICAL MIXER ACTIVITY

To gather empirical insights into the activities of existing ZKP mixers, we crawl the deposit, withdrawal events and transactions of the 73 pools on four ZKP mixers: TC, TP, TN and Cyclone, from December 16th, 2019 (i.e., the inception time of TC) to October 1st, 2022. We observe that 97.36% of the mixer users deposit assets into TC and TN, and that the number of TP depositors has not changed since February, 2021 (cf. Fig. 2). Therefore, we focus on analyzing the two most active mixers, TC and TN.

We analyze the top four active pools in TC (0.1, 1, 10 and 100 ETH pools) and TN (0.1, 1, 10 and 50 BNB pools). For TC, we crawl the deposit and withdrawal events data from the Ethereum block 9,116,966 (December 16th, 2019) to 15,650,000 (October 1st, 2022). The TC 1 ETH pool is the most active (51,770 deposits and 49,086 withdrawals), while the TC 100 ETH pool has the smallest depositor and withdrawer set (6,433 deposit and 11,069 withdraw addresses). The TC pools accumulate deposits of 3.54M ETH (4.70B USD). Moreover, from TN's inception at BSC block 5,230,899 (February 27th, 2021) until block 21,800,000 (October 1st, 2022), we find that 6,814

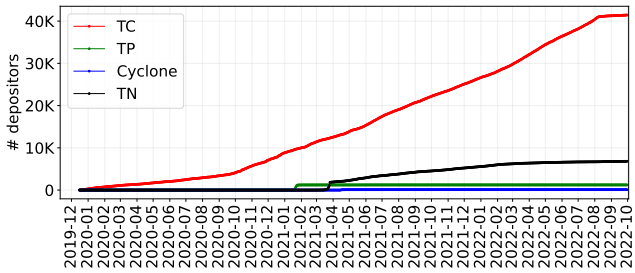


Figure 2: ZKP mixer depositors over time. 41,441 (83.61%) **and** 6,814 (13.75%) **depositors appear in TC and TN, respectively.**

Table 1: Deposits/withdrawals in TC ETH and TN BNB pools.

Pool	# Deposits	# Withdrawals	# Depositors	# Withdrawers
TC 0.1 ETH	26,069	22,281	11,941	13,227
TC 1 ETH	51,770	49,086	17,843	23,592
TC 10 ETH	45,238	44,228	16,227	21,872
TC 100 ETH	30,301	29,553	6,433	11,069
TN 0.1 BNB	10,485	9,877	3,972	4,541
TN 1 BNB	13,151	12,901	3,890	4,362
TN 10 BNB	4,886	4,860	1,675	1,983
TN 50 BNB	607	604	231	288

addresses generate 29,129 deposits in the four BNB pools, accumulating 93,409.5 BNB (26.62M USD).

4.1 Depositors and Withdrawers

The four TC ETH pools contain 39,821 depositors and 61,026 withdrawers, depositing 88.82 ETH (118K USD) and withdrawing 56.52 ETH (75K USD) on average. In each pool, the number of withdrawers is greater than depositors, indicating that a user may adopt multiple addresses to withdraw than to deposit. Moreover, 58,998 (84.95%) withdrawers have zero ETH before receiving ETH from TC.

Cross-pool Mixer Usage. Because a mixer pool only supports a fixed currency denomination, users may utilize multiple pools to mix arbitrary amounts of assets. We find that 327 depositors utilize all four TC pools, and 9,962 (25.02%) deposit in more than one pool. Additionally, 60 users withdraw from all four pools, and 7,479 (12.26%) use more than one pool to withdraw. Likewise, for TN, we observe a slight increase in overlaps on both depositors (33%) and withdrawers (25%) appearing in at least two pools. The overlap of pools may help an adversary to link addresses (cf. Section 7.1).

4.2 ZKP Mixer Coin Flow

In addition to immediate depositors and withdrawers, we are also interested in the coins' wider flow to get their origins and destinations. For example, users move their coins from exchanges or DeFi platforms via intermediary addresses into and outside the mixer.

To track where the deposited ETH in TC are transferred from and where the withdrawn ETH are transferred to, we extend our pool model to cover depositors and withdrawers in distance 2. We crawl the transaction history of user addresses before October 1st, 2022.

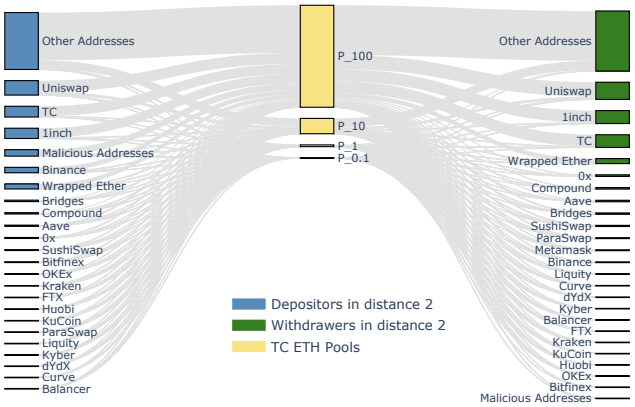


Figure 3: Prior-sanction TC ETH pools coin flow. The shown bandwidth of each flow represents the magnitude of the aggregate ETH transferred from depositors in distance 2 to TC (via depositors in distance 1), or from TC to withdrawers in distance 2 (via withdrawers in distance 1).

For each depositor $d^{(1)}$ in a TC p ETH pool, we extract *the most recent* transfers of p ETH that $d^{(1)}$ receives before depositing into TC, and obtain the depositors in distance 2 that transfer ETH to $d^{(1)}$. Similarly, we obtain the withdrawers in distance 2 by extracting *the most recent* transfers of p ETH that the withdrawers in distance 1 send after withdrawing from TC. Then, we tag the depositors and withdrawers in distance 2 using manually crawled labels from Etherscan. We finally cluster the addresses into different platforms based on their labels.

Fig. 3 visualizes the ETH flow via four TC ETH pools before August 8th, 2022. We observe that the top 10 clusters in distance 2 cover 48.11% of the total deposit volume, and transfers from Decentralized Exchanges (DEXs), e.g., Uniswap, alone amount to 750.2K ETH (21.74% of the total deposit volume). DEXs are also the most popular DeFi platforms to which TC users transfer their withdrawn ETH (27.2% of the total withdrawal volume). This is probably because users are swapping ETH to other tokens on DEXs. We also observe that 10.64% of the total deposit volume is re-deposited into TC.

4.3 Why Do Users Resort to Mixers?

Based on the coin flow, we analyze mixer user behaviors and find the following motivations for adopting mixers.

Money laundering: Because mixers break the linkability between addresses, users can use them to conceal their traces. To do so, users withdraw ETH from a mixer pool to a fresh address, and then transfer their assets (via intermediary addresses) to CEXs, e.g., Binance and Huobi, to receive fiat currencies. We crawl 364 labeled CEX addresses from Etherscan and identify that 63 out of them appear in the TC withdrawer sets in distance 2, which may attempt to leverage intermediary addresses to hide their traces. We find that 4,062 addresses transfer 26.2K ETH (34.85M USD) into CEXs.

Anonymity mining: TC incentivizes users to adopt mixers through AM [34]. Users can earn rewards for depositing and withdrawing funds from a TC ETH pool, and interacting with TC anonymity mining contract (see Section 6 for more details). Our findings show

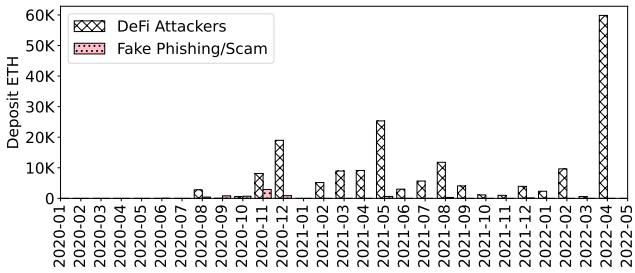


Figure 4: TC deposit amounts of malicious addresses in distance 1 before May, 2022. DeFi Attackers deposit more assets than Fake Phishing/Scam addresses.

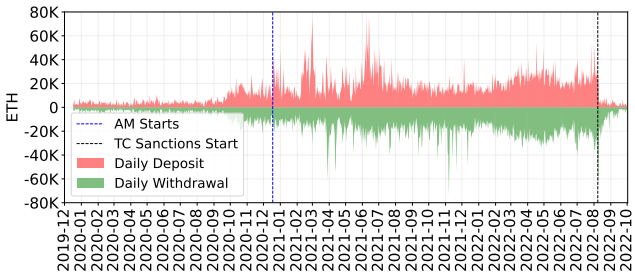


Figure 5: Daily transactions in TC ETH pools. There was a panic exit when the OFAC sanctions were announced.

that 1,141 depositors and 1,290 withdrawers are used to receive AM rewards, while depositing 532.3K ETH (707.98M USD) and withdrawing 512.6K ETH (681.79M USD) respectively. Furthermore, we find that addresses using AM typically deposit and withdraw multiple times. For instance, among the top 100 withdrawers with the highest withdrawal amount, 40 addresses received AM rewards.

Extracting BEV: Mixers also provide opportunities to BEV extractors (a *BEV extractor* is an address which is used to perform a sandwich attack, liquidation, or arbitrage) to enhance their privacy. To understand how many BEV extractors utilize TC, we contacted the authors of [25] to reuse their quantification results on sandwich attacks, liquidations, and arbitrage from block 6,803,256 (December 1st, 2018) to block 12,965,000 (August 5th, 2021). We then analyze whether the 11,289 BEV extractors identified in [25] appear in TC depositor and withdrawer sets. We find that 2,185 addresses are used for sandwich attacks, 128 for arbitrages, and 73 for liquidations (cf. Table 3), while depositing 115,980.5 ETH (154.25M USD) into TC. Furthermore, 545 BEV extractors withdraw 45,536.8 ETH from TC.

Launching attacks: Malicious actors may adopt mixers to hide their identities. To gain initial insights into how malicious users adopt TC, we first crawl 6,611 blockchain phishing- and attack-related addresses from the dataset provided by the DeFi Attack SoK [46]. This dataset contains data from *(i)* Etherscan, *(ii)* Rekt News, *(iii)* Slowmist, *(iv)* Cryptosec, and *(v)* CryptoscamDB. We regard the 6,611 addresses as *malicious addresses* and find that 205 addresses out of them appear in TC depositor and withdrawer sets.

We find that 172 malicious addresses deposit 194,448 ETH (258.62M USD) into TC, while 141 addresses withdraw 3,523.4 ETH from TC (cf. Table 3). We further cluster the 205 malicious addresses into three categories: *(i)* Fake Phishing/Scam (31.22%), which are labeled as "Phish / Hack" on Etherscan or scam addresses on CryptoscamDB; *(ii)* DeFi attackers (68.29%), which attacked a DeFi platform; *(iii)* CEX attackers (0.49%), which steal assets from a CEX.

Fig. 4 shows the malicious addresses directly depositing ETH into TC overtime. Malicious addresses seem to be careful to use mixers: The first time a malicious address deposits ETH into TC is in July, 2020, when the anonymity set size exceeds 1,000 (cf. Fig. 2).

5 OFAC SANCTIONS IMPACT ON ZKP MIXERS

In this section, we investigate how OFAC sanctions affect mixers.

Impact on Mixer Usage. To understand how users interact with ZKP mixers before and after the sanctions, we plot the daily deposited and withdrawn ETH and BNB in TC and TN pools from December 16th, 2019 to October 1st, 2022 in Figures 5 and 10. We observe that the graphs of daily deposits and withdrawals seem to be approximately symmetrical before the TC sanctions were announced (i.e., August 8th, 2022). Interestingly, there was a panic exit on August 8th, 2022: 230 TC withdrawers withdrew their 48,900 ETH due to the sanctions. The TC daily deposits decreased by approximately 83% after August 8th, 2022. Moreover, there were almost zero daily deposits and withdrawals in TN during July 2022, but there was a tiny increase in August after the sanctions (cf. Fig. 10). This is likely because privacy-seeking users leverage TN to replace TC to hide their identities.

Post-Sanction TC Deposits. Although the TC official websites are banned by the US OFAC, users can still interact with TC contracts (e.g., through TC command line interface (CLI)) to deposit and withdraw assets. We notice that the deposits in TC are not zero after the sanctions started: from block 15,304,706 (August 9th, 2022) to 15,650,000 (October 1st, 2022), 487 addresses deposited 47,056.8 ETH (62.59M USD) into TC pools. Only 75 (15.40%) out of the 487 addresses ever deposited TC before the sanctions started.

Post-Sanction TC Coin Flow. Moreover, we find that 671 addresses withdraw 170,826.3 ETH (227.20M USD) from TC ETH pools. To understand the post-sanction TC ETH pools coin flow, we adopt extend the mixer pools to cover the distance 2 depositors and withdrawers. As shown in Fig. 11 in Appendix B, we observe that after August 8th, 2022, more than 85.49% of the withdrawn ETH are transferred to intermediary addresses in distance 2, before interacting with CEXs or DeFi platforms. We speculate this is likely because TC users attempt to bypass the censorship of CEXs or DeFi platforms, which claim to ban addresses receiving assets from TC [8].

Impact on Mining TC Transactions. OFAC sanctions against TC also have an influence on Ethereum miners. As shown in Fig. 12, we plot the distribution of TC transactions mined by various mining pools over time. Ethermine is the largest mining pool that mined the most TC transactions before August 8th, 2022. However, we observe that, after the sanctions started, Ethermine stopped processing any transactions related to deposits and withdrawals in TC (cf. Fig. 12 in Appendix B).

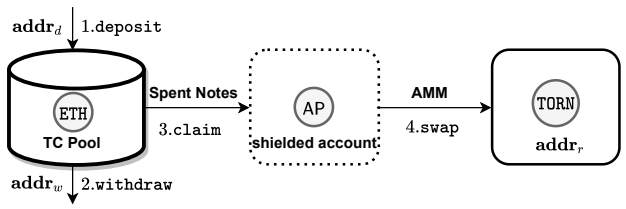


Figure 6: Overview of the TC anonymity mining.

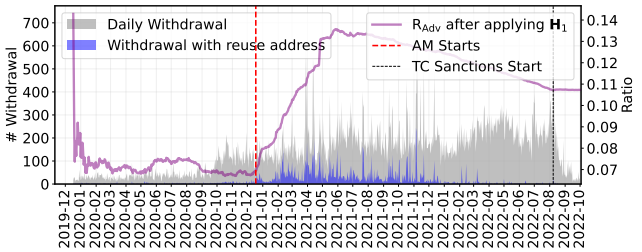


Figure 7: The AM launch does not increase the number of daily withdrawals but attracts privacy-ignorant users. Heuristic 1 performs better after AM started, i.e., the advantage of the probability that an adversary links a withdrawer to the correct depositor (cf. Eq. 1), rises from 7.00% to 13.50%.

6 INCENTIVIZED ZKP MIXER POOLS

Spearheaded by the introduction of AMR [18], we have witnessed a number of real-world mixer pools [34] (cf. Section 2.2) introducing rewarding governance tokens through *anonymity mining* (AM). In this section, we analyze how AM affects user privacy.

6.1 Anonymity Mining in TC Pools

TC incentivizes users to maintain their assets in TC ETH pools through AM [34]. Users receive TORN tokens as rewards through a so-called shielded liquidity mining protocol as follows (cf. Fig. 6).
(1) Deposit: A user deposits ETH into a TC pool using addresses $\mathbf{addr}_d$, and receives a deposit *note*.
(2) Withdraw: When the user withdraws ETH from a TC pool, the deposit note becomes a *spent note*.
(3) Claim: After withdrawing from a pool, the user submits the *spent note* to the pool to claim the Anonymity Points AP. Because AP is determined by the deposit amount and duration (both are private information), AP is stored privately on a shielded account[2].
(4) Swap: A user can convert the shielded AP to public TORN tokens using a dedicated TC (AMM) exchange. The user receives the TORN tokens in an address $\mathbf{addr}_r$ that can be different from the user's deposit or withdrawal address.

$$\mathrm{AP}_{\mathbf{u}}(t) = \sum_{p\in\{0.1,1,10,100\}} \mathrm{Weight}_p \cdot \sum_{i=1}^{v_p} \left(t^w_{p,i} - t^d_{p,i}\right) \qquad (2)$$

Equation 2 from TC outlines the amount of AP a user $\mathbf{u}$ is entitled to at time t, where Weight_p is a predefined parameter to calculate a user's AP in various pools. Weight_p is predefined as 10, 20, 50 and 400 in TC 0.1, 1, 10, and 100 ETH pools, respectively. v_p corresponds to the number of withdrawals in the $\mathbf{P}_p$ pool before time t. $t^d_{p,i}$ and $t^w_{p,i}$ are the block numbers of $\mathbf{u}$'s i-th deposit and withdrawal, $0 \le i \le v_p$. For instance, if a user $\mathbf{u}$ deposits twice 1 ETH into $\mathbf{P}_1$ at block 11,476,000 and 11,476,100, and deposits 10 ETH into the $\mathbf{P}_{10}$ pool at block 11,476,000, and $\mathbf{u}$ withdraws all the deposited funds at block 11,476,200, then $\mathbf{u}$'s AP is $20\times(100+200)+400\times200 = 86{,}000$.

6.2 Linking User Addresses through AM

AM aims to attract users to deposit more coins over a longer timeframe. However, AM also increases the required user interactions with mixers (e.g., claiming to receive rewards), and may thus provoke the leakage of privacy-compromising information. We explore how to link users' withdrawals and deposits by solving Equation 2.

We first identify the addresses that received TORN tokens from TC pools. From block 11,474,710 (December 18th, 2020) to 15,650,000 (October 1st, 2022), we identify 15,659 TC Reward Swap events, and find that 1,844 addresses received TORN. We then extract the converted AP value in swap events.

Receive Rewards with Deposit Address. In the following, we show that re-using a deposit address to receive rewards can deteriorate a user's privacy. We discover that among the 1,844 addresses receiving TORN, 1,141 are depositors. We extract their deposit time, receiving TORN time, and the converted values of AP. Based on the data, we divide the 1,141 depositors into three categories:

- 1 *deposit*/1 *claim*/1 *pool:* Out of the 1,141 depositors, 236 only deposited *once* in *one* TC pool and only received TORN tokens from AP with *one* transaction. In this case, Equation 2 can be simplified as $\mathrm{AP}_{\mathbf{u}}(t) = \mathrm{Weight}_p \cdot (t^w_{p,1} - t^d_{p,1})$. Because $\mathrm{AP}_{\mathbf{u}}(t)$ and $t^d_{p,1}$ are known, we can resolve the value of $t^w_{p,1}$ and search if there is a withdrawal transaction in block $t^w_{p,1}$. In total, we find the withdrawals for 53 depositors. For the remaining depositors, we speculate that they have likely not yet converted all their AP.
- *n deposits*/1 *claim*/1 *pool:* 193 addresses deposited *more than once* in *one* TC pool but only received TORN *once*. Equation 2 can be simplified as $\mathrm{AP}_{\mathbf{u}}(t) = \mathrm{Weight}_p \cdot \sum_{i=1}^{v_p} (t^w_{p,i} - t^d_{p,i})$. In this case, we find the possible withdrawals for 51 depositors.
- *n deposits/n claims/n pools:* For the remaining depositors receiving TORN *more than once* or using *multiple* pools, it is challenging to find their withdrawals, because it is uncertain whether they have claimed all AP and Equation 2 is hard to solve. However, we would suggest users avoid reusing addresses to receive TORN, because one conversion of AP for a depositor shows that this depositor has already (partly or entirely) withdrawn the deposits.

In total, we can find the possible withdrawal transactions for 104 addresses, indicating that re-using a deposit address for receiving AM rewards can deteriorate users' privacy.

[2] According to [34], a shielded account is a secret key newly generated by a user, which is used to encrypt and submit claim and withdrawal data without revealing the user's identity. For recoverability, the user encrypts this secret key using his ETH public key and stores the encrypted result on-chain.

6.3 AM's Impact on Mixer Anonymity Set

To understand how AM affects a mixer pool's anonymity set, we investigate the privacy-ignorant addresses attracted by AM. As shown in Fig. 7, we first plot the number of daily withdrawal transactions in TC ETH pools. We then highlight the withdrawals in which deposit addresses are reused to receive withdrawn assets.

We observe that the daily withdrawals in TC ETH pools are not affected by AM as intended: the number started increasing before AM launch on October 18th, 2020. However, AM does attract more users who reuse the deposit addresses to withdraw. Such "reusing depositors" are likely interested in mining TORN, but privacy-ignorant.

Based on our observations, we introduce the following heuristic, which identifies privacy-ignorant users that reuse addresses. We apply Heuristic 1 to prune privacy-ignorant user addresses and compute a more accurate mixer anonymity set size (see Section 7.1.1 for more details). We observe that Heuristic 1 performs better after AM started. As shown in Fig. 7, the advantage R_{Adv} (cf. Eq. 1) that an adversary links a withdrawer to the correct depositor rises from 7.00% (before AM) to 13.50% (after AM) on average.

Heuristic for Address Reuse (H_1). If an address appears both in the depositor and withdrawer sets, then the deposits and withdrawals of this address are conducted by the same user (cf. Fig. 8(a)).

In conclusion, contrary to the claims of related work [18], we find that AM does not always contribute to the mixers' anonymity set size as expected, because it attracts privacy-ignorant users.

7 MEASURING MIXER ANONYMITY SET SIZE

In the following, we propose heuristics to measure a mixer pool's anonymity set size, which is more representative than the naive $\mathbf{OAS}_\mathbf{P}(t)$. Our heuristics are best-effort methods and subject to known limitations [27, 38]. We thus attempt to construct ground truth from side channels to validate our heuristics (cf. Appendix C).

7.1 Linking Heuristics

We propose the following heuristics (cf. Fig. 8) to leverage on-chain data and insights from our empirical study to link addresses and prune the $\mathbf{OAS}_\mathbf{P}(t)$. Appendix A summarizes the extended system model and definitions which are used in our linking heuristics.

7.1.1 **H_1** - *Address Reuse.* **Observation:** We observe that an address can be reused to both deposit and withdraw, which could be incautious behavior and leak privacy [4, 38].

Heuristic 1: If an address appears both in the depositor and withdrawer sets, we assume that the deposits and withdrawals of this address are conducted by the same user (cf. Fig. 8(a)). We apply Eq. 4 in Table 2 to compute a depositor's balance and extract the depositors with a positive balance to evaluate the anonymity set: $\mathbf{SAS}_\mathbf{P}^{(1)}(t) = \{\mathsf{a} \mid \mathsf{a} \in \mathcal{D}_\mathbf{P}(t) \wedge \mathbf{bal}_\mathsf{a}(t) > 0\}$.

7.1.2 **H_2** - *Improper Withdrawal Sender.* **Observation:** Incautious users may adopt a deposit address a_w to receive the withdrawn funds, while paying the transaction fees using their deposit address a_d. This action infers that a_d and a_w are likely controlled by the same user. This action might happen when users are not familiar with the mixer functionality, which can leak users' privacy.

Heuristic 2: We assume that given a depositor-withdrawer pair $(\mathsf{a}_d, \mathsf{a}_w)$ in a pool, where a_d is not a relayer, if a_d generates a withdrawal and assigns a_w to receive the withdrawn coins, then a_d and a_w belong to the same user (cf. Fig. 8(b)), i.e., $\textsc{Link}(\mathsf{a}_d, \mathsf{a}_w) = 1$.

Let $\mathcal{S}_\mathbf{P}^{\mathsf{nt}}(t)$ be the set of linked address pairs in a pool $\mathbf{P}$. Given $\mathcal{S}_\mathbf{P}^{\mathsf{nt}}(t)$, we merge the balance of the linked addresses to simplify the pool state, and then compute the anonymity set: $\mathbf{SAS}_\mathbf{P}^{(2)}(t) = \{\mathsf{a} \mid \mathbf{bal}_\mathsf{a}(t) > 0 \ \wedge (\mathsf{a}, \mathbf{bal}_\mathsf{a}(t)) \in \textsc{Simp}(\mathbb{S}_\mathbf{P}(t), \mathcal{S}_\mathbf{P}^{\mathsf{nt}}(t))\}$.

7.1.3 **H_3** - *Related Deposit-Withdrawal Address Pair.* **Observation:** To withdraw coins, users are encouraged to choose a new address with no links to the deposit address. However, we observe that, users may adopt different deposit and withdrawal addresses, which are directly linked through a coin transfer.

Heuristic 3: We assume that, given two addresses $\mathsf{a}_d \in \mathcal{D}_\mathbf{P}(t)$ and $\mathsf{a}_w \in \mathcal{W}_\mathbf{P}(t)$, if a_d transferred (received) coins or tokens to (from) a_w before time t, then a_d and a_w are related and under the control of the same user (cf. Fig. 8(c)), i.e., $\textsc{Link}(\mathsf{a}_d, \mathsf{a}_w) = 1$. Let $\mathcal{S}_\mathbf{P}^{\mathsf{tx}}(t)$ be the set of related depositor-withdrawer pairs in a pool $\mathbf{P}$. We simplify the pool state and compute the anonymity set: $\mathbf{SAS}_\mathbf{P}^{(3)}(t) = \{\mathsf{a} \mid \mathbf{bal}_\mathsf{a}(t) > 0 \wedge (\mathsf{a}, \mathbf{bal}_\mathsf{a}(t)) \in \textsc{Simp}(\mathbb{S}_\mathbf{P}(t), \mathcal{S}_\mathbf{P}^{\mathsf{tx}}(t))\}$.

7.1.4 **H_4** - *Intermediary Deposit Address.* **Observation:** We observe that there are multiple depositors in distance 1 whose coins are all transferred from the same depositor in distance 2. Hence, these depositors in distance 1 are likely temporary addresses and are only used to transfer funds into a mixer.

Heuristic 4: We hence assume that given two addresses $d^{(1)} \in \mathcal{D}_\mathbf{P}^{(1)}(t)$ and $d^{(2)} \in \mathcal{D}_\mathbf{P}^{(2)}(t)$, if all $d^{(1)}$'s coins are transferred from $d^{(2)}$ and $d^{(2)}$ is a user account, then $\textsc{Link}(d^{(1)}, d^{(2)}) = 1$.

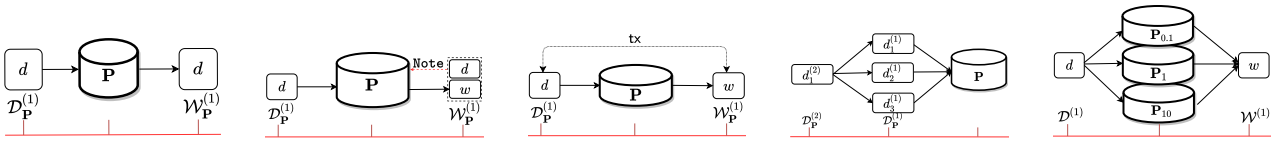
We denote $d^{(1)}$ as an *intermediary deposit address*, $\mathcal{B}_\mathbf{P}^{(1)}(t)$ as the set of intermediary deposit address, and $\mathcal{B}_\mathbf{P}^{(2)}(t)$ as the set of user accounts in distance 2 who transfer coins to an address in $\mathcal{B}_\mathbf{P}^{(1)}(t)$. For each address $d^{(1)}$ in $\mathcal{B}_\mathbf{P}^{(1)}(t)$, we replace it by the address in $\mathcal{B}_\mathbf{P}^{(2)}(t)$ which transfers coins to $d^{(1)}$. We then compute: $\mathbf{SAS}_\mathbf{P}^{(4)}(t) = \{\mathsf{a} \mid \mathbf{bal}_\mathsf{a}(t) > 0 \ \wedge \mathsf{a} \in \mathcal{B}_\mathbf{P}^{(2)}(t) \cup \mathcal{D}_\mathbf{P}^{(1)}(t) \setminus \mathcal{B}_\mathbf{P}^{(1)}(t)\}$.

7.1.5 **H_5** - *Cross-pool Deposit.* **Observation:** Current mixer pools only support the deposit and withdrawal of a *fixed* coin denomination. When a user aims to mix an *arbitrary* amount of coins, the user needs to interact with multiple pools and may not change the respective deposit (or withdrawal) address (cf. Fig. 8(e)).

Heuristic 5: Given a depositor-withdrawer pair $(\mathsf{a}_d, \mathsf{a}_w)$, we assume $\textsc{Link}(\mathsf{a}_d, \mathsf{a}_w) = 1$ if: *(i)* a_d and a_w are both in $m (m > 1)$ pools, *(ii)* in each pool, a_d's total deposit amount equals a_w's withdrawal amount, and *(iii)* for each a_w's withdrawal transaction $\mathtt{tx}^w$, at least one of a_d's deposit transaction $\mathtt{tx}^d$ is generated earlier than $\mathtt{tx}^w$.

Let $\mathcal{S}^{\mathsf{cu}}$ be the set of address pairs $(\mathsf{a}_d, \mathsf{a}_w)$ that satisfy the above conditions. Given $\mathcal{S}^{\mathsf{cu}}$, we simplify the state of a pool $\mathbf{P}$, and then compute the anonymity set $\mathbf{SAS}_\mathbf{P}^{(5)}(t) = \{\mathsf{a} \mid \mathbf{bal}_\mathsf{a}(t) > 0 \ \wedge (\mathsf{a}, \mathbf{bal}_\mathsf{a}(t)) \in \textsc{Simp}(\mathbb{S}_\mathbf{P}(t), \mathcal{S}_\mathbf{P}^{\mathsf{cu}}(t))\}$.

7.1.6 Linking and Measuring Results. Through Heuristics 2–5, we can link 18,705 TC and 9,383 TN address pairs, which form 8,164 and 2,046 clusters, respectively. Moreover, 4,871 (57.14%) TC and



(a) Heuristic 1. (b) Heuristic 2. (c) Heuristic 3. (d) Heuristic 4. (e) Heuristic 5.

Figure 8: Overview of Heuristics 1-5:
***(a)* H_1: A user applies the same address d for deposit and withdrawal.**
***(b)* H_2: A user adopts an address w to receive the withdrawn coin but a deposit address to pay the withdrawal transaction fees.**
***(c)* H_3: A user adopts two distinct addresses d and w to deposit and withdraw in P, while d and w are related in a transaction tx.**
***(d)* H_4: An address $d_1^{(2)}$ in distance 2 controls 3 intermediary addresses $d_j^{(1)}$ $(j = 1, 2, 3)$ in the distance 1, to deposit coin in P.**
***(e)* H_5: A user adopts an address d to deposit into $P_{0.1}$, P_1 and P_{10}, and uses address w to withdraw the same times from the pools.**

1,190 (48.89%) TN clusters only have two addresses. Fig. 13 visualizes the distribution of TC clusters over the number of addresses. Interestingly, we find that the cluster distribution is similar to previous works on Bitcoin address clustering (e.g., Fig. 9(b) in [16]).

Table 4 in Appendix B shows the $\mathbf{SAS_P}(t)$ of mixer pools after applying each heuristic individually. On TC pools, Heuristic 1 reduces the anonymity set by an average of 10.23% from the reported $\mathbf{OAS_P}(t)$. For instance, in the TC 100 ETH pool $\mathbf{P}_{100}$, there are 6,433 unique depositors, but only 5,608 depositors have a positive balance, and therefore contribute to the anonymity set. Consequently, $\mathbf{SAS}_{\mathbf{P}}^{(1)}(t)$ of $\mathbf{P}_{100}$ is 12.82% less than the respective $\mathbf{OAS_P}(t)$. For TN, $\mathbf{SAS}_{\mathbf{P}}^{(1)}(t)$ is reduced by an average of 23.08% from $\mathbf{OAS_P}(t)$.

We can further reduce the $\mathbf{OAS_P}(t)$ by combining two or more heuristics (cf. Table 4). Combining all heuristics yields the largest reduction of $\mathbf{OAS_P}(t)$: after applying Heuristics 1-5 to the TC (TN) pools, an adversary can reduce the reported $\mathbf{OAS_P}(t)$ on average by 27.34% (46.02%). Therefore, the probability that an adversary links a withdrawer (who withdraws at time t) to the correct depositor rises by 37.63% (85.26%) on average (cf. Eq. 3).

$$\mathrm{R_{Adv}} = \frac{1/|\mathbf{SAS_P}(t)| - 1/|\mathbf{OAS_P}(t)|}{1/|\mathbf{OAS_P}(t)|} = 37.63\%\ (85.26\%) \quad (3)$$

7.1.7 User Privacy Behavior. Our heuristics appear to function better on the BSC mixer (TN) than on the ETH mixer (TC). While our study should be repeated once the other mixers grow on both chains (e.g., Cyclone and TP), our empirical evidence is the first to suggest a differing privacy-focus of users on ETH and BSC. One could also argue that privacy-aware users want the best available anonymity set, and will therefore use TC and follow all best practices. As such, a suitable assumption is that anonymity set attracts anonymity set, i.e., the biggest anonymity set will inherently attract more users, and particularly those that worry about privacy (which is analogous to how liquidity attracts liquidity in financial exchanges).

8 RELATED WORK

Mixers on Bitcoin: Mixers were originally applied in anonymous communications [9] and are also applied to enhance Bitcoin users' privacy [23, 40]. Mixcoin [7] and Blindcoin [37] are centralized, trusted mixers that support BTC. CoinJoin [19] allows a user to find other mixing partners to merge multiple transactions, thereby obfuscating the link between senders and recipients. Although the design of CoinJoin [19] is decentralized, its existing implementation, remains centralized but non-custodial. CoinShuffle [28, 29] and Xim [6] achieve better anonymity in a decentralized mixer. Wu *et al.* [40] propose a generic abstraction model for Bitcoin mixers.

Mixers on Smart-contract-enabled Blockchains: ZKP mixers are inspired by Zerocash [30] to obfuscate the link between the users' deposit and withdrawal using zero-knowledge proof. Several ZKP mixers attempt to operate on Ethereum, such as Miximus [3]. AMR [18] proposes how to reward users for participating in a mixer, and shortly after, Blender implements a mixer with a reward scheme. TC follows by adding anonymity mining as a deposit reward scheme for users [34]. Besides ZKP mixers, a notable mixer example that relies on linkable ring signatures and the stealth addresses from Monero [1] is Möbius [20].

Blockchain Privacy Analysis: Many researchers have studied privacy on non-privacy-preserving blockchains (e.g., Bitcoin [2, 12], Ethereum [4, 38]), as well as on privacy-preserving blockchains (e.g., Monero [17, 22, 43], Zerocash [5, 15]). Because ZKP mixers are inspired by Zerocash, our Heuristics 1 and 4 can also be applied to link shielded and deshielded transactions in Zerocash [15]. However, the majority of the transactions (i.e., with 65.6% of the withdrawn value) in [15] involve miners or founders, while this paper investigates generic ZKP mixers, and can be applied to trace malicious addresses. Moreover, recent studies [42] have shown that users' privacy can be leaked when using cross-chain exchanges.

9 CONCLUSION

This paper empirically analyzes the usage of ZKP mixers. We find that 205 malicious addresses and 2,595 BEV extractors leverage mixers as their source of funds, while depositing a total attack revenue of 412.87M USD. We measure that the OFAC sanctions have reduced more than 83% daily deposits in TC. Moreover, our findings show that the advertised anonymity set sizes of popular mixers do not represent the true privacy offered to users. We propose a methodology that can reduce the anonymity set size on average by 27.34% (46.02%) of TC (on ETH) and TN (on BSC) respectively. Worryingly, while previous work suggests that incentivized mixers could improve the offered mixer privacy, we find evidence that speculators are likely to act in a privacy-ignorant manner, deteriorating the overall anonymity set size. We hope that our work engenders further research into user-friendly and privacy-enhancing ZKP mixer solutions.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for providing valuable comments and feedback which helped us to strengthen the paper. We are moreover grateful to Nimiq for partially funding this work. This work was partially supported by the Algorand Centres of Excellence programme managed by Algorand Foundation. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Nimiq and Algorand Foundation.

REFERENCES

[1] Kurt M. Alonso. 2020. Zero to Monero: First Edition. A Technical Guide to A Private Digital Currency; for Beginners, Amateurs, and Experts. https://web.getmonero.org/library/Zero-to-Monero-2-0-0.pdf.

[2] Elli Androulaki, Ghassan O Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. 2013. Evaluating User Privacy in Bitcoin. In *International Conference on Financial Cryptography and Data Security*. Springer, Springer Science & Business Media, Berlin, Heidelberg, 34–51.

[3] barryWhiteHat. 2018. Miximus. Available at: https://github.com/barryWhiteHat/miximus.

[4] Ferenc Béres, István A Seres, András A Benczúr, and Mikerah Quintyne-Collins. 2021. Blockchain is Watching You: Profiling and Deanonymizing Ethereum Users. In *2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*. IEEE Computer Society, Los Alamitos, CA, USA, 69–78.

[5] Alex Biryukov, Daniel Feher, and Giuseppe Vitto. 2019. Privacy Aspects and Subliminal Channels in Zcash. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. ACM, London, UK, 1813–1830.

[6] George Bissias, A Pinar Ozisik, Brian N Levine, and Marc Liberatore. 2014. Sybil-Resistant Mixing for Bitcoin. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*. ACM, Scottsdale, AZ, USA, 149–158.

[7] Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A Kroll, and Edward W Felten. 2014. Mixcoin: Anonymity for Bitcoin with Accountable Mixes. In *International Conference on Financial Cryptography and Data Security*. Springer, Springer, Christ Church, Barbados, 486–504.

[8] Chainalysis. 2022. Understanding Tornado Cash, Its Sanctions Implications, and Key Compliance Questions. Available at: https://blog.chainalysis.com/reports/tornado-cash-sanctions-challenges/.

[9] David L Chaum. 1981. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. *Commun. ACM* 24, 2 (1981), 84–90.

[10] Mauro Conti, E Sandeep Kumar, Chhagan Lal, and Sushmita Ruj. 2018. A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials* 20, 4 (2018), 3416–3452.

[11] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2020. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. In *IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 910–927.

[12] Arthur Gervais, Srdjan Capkun, Ghassan O Karame, and Damian Gruber. 2014. On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients. In *Computer Security Applications Conference*. ACM, New Orleans, LA, USA, 326–335.

[13] Ethan Heilman, Leen Alshenibr, Foteini Baldimtsi, Alessandra Scafuro, and Sharon Goldberg. 2017. Tumblebit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub. In *Network and Distributed System Security Symposium*. The Internet Society, San Diego, California, USA.

[14] Abraham Hinteregger and Bernhard Haslhofer. 2018. An Empirical Analysis of Monero Cross-Chain Traceability. *CoRR* abs/1812.02808 (2018). http://arxiv.org/abs/1812.02808

[15] George Kappos, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn. 2018. An Empirical Analysis of Anonymity in Zcash. In *27th USENIX Security Symposium, USENIX Security*. USENIX Association, Baltimore, MD, USA, 463–477.

[16] Ghassan O Karame, Elli Androulaki, Marc Roeschlin, Arthur Gervais, and Srdjan Čapkun. 2015. Misbehavior in Bitcoin: A Study of Double-Spending and Accountability. *ACM Transactions on Information and System Security (TISSEC)* 18, 1 (2015), 2.

[17] Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena. 2017. A Traceability Analysis of Monero's Blockchain. In *European Symposium on Research in Computer Security (Lecture Notes in Computer Science, Vol. 10493)*. Springer, Oslo, Norway, 153–173.

[18] Duc Viet Le and Arthur Gervais. 2021. AMR: Autonomous Coin Mixer with Privacy Preserving Reward Distribution. In *AFT '21: 3rd ACM Conference on Advances in Financial Technologies*. ACM, Arlington, Virginia, USA, 142–155.

[19] Greg Maxwell. 2013. CoinJoin: Bitcoin Privacy for The Real World. Available at: https://bitcointalk.org/index.php?topic=279249.0.

[20] Sarah Meiklejohn and Rebekah Mercer. 2018. Möbius: Trustless Tumbling for Transaction Privacy. *Proceedings on Privacy Enhancing Technologies* 2018, 2 (2018), 105–121.

[21] Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. 2013. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In *2013 IEEE Symposium on Security and Privacy*. IEEE Computer Society, Berkeley, CA, USA, 397–411.

[22] Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, et al. 2018. An Empirical Analysis of Traceability in the Monero Blockchain. *Proceedings on Privacy Enhancing Technologies* 2018, 3 (2018), 143–163.

[23] Jaswant Pakki, Yan Shoshitaishvili, Ruoyu Wang, Tiffany Bao, and Adam Doupé. 2021. Everything You Ever Wanted to Know About Bitcoin Mixers (But Were Afraid to Ask). In *International Conference on Financial Cryptography and Data Security*. Springer, Virtual Event, 117–146.

[24] Kaihua Qin, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, and Arthur Gervais. 2021. An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities. In *Proceedings of the 21st ACM Internet Measurement Conference*. ACM, Virtual Event, USA, 336–350.

[25] Kaihua Qin, Liyi Zhou, and Arthur Gervais. 2022. Quantifying Blockchain Extractable Value: How dark is the forest?. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 198–214.

[26] Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. 2021. Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit. In *International Conference on Financial Cryptography and Data Security*. Springer, Virtual Event, 3–32.

[27] Matteo Romiti, Friedhelm Victor, Pedro Moreno-Sanchez, Peter Sebastian Nordholt, Bernhard Haslhofer, and Matteo Maffei. 2021. Cross-Layer Deanonymization Methods in the Lightning Protocol. In *International Conference on Financial Cryptography and Data Security*. Springer, Virtual Event, 187–204.

[28] Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. 2014. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. In *European Symposium on Research in Computer Security*. Springer, Wroclaw, Poland, 345–364.

[29] Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. 2017. P2P Mixing and Unlinkable Bitcoin Transactions. In *24th Annual Network and Distributed System Security Symposium, NDSS*. The Internet Society, San Diego, California, USA.

[30] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. 2014. Zerocash: Decentralized anonymous payments from bitcoin. In *Symposium on Security and Privacy*. IEEE, San Francisco, CA, USA, 459–474.

[31] Erkan Tairi, Pedro Moreno-Sanchez, and Matteo Maffei. 2021. A2L: Anonymous Atomic Locks for Scalability in Payment Channel Hubs. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 1834–1851.

[32] Weizhao Tang, Weina Wang, Giulia Fanti, and Sewoong Oh. 2020. Privacy-Utility Tradeoffs in Routing Cryptocurrency over Payment Channel Networks. *Proceedings of the ACM on Measurement and Analysis of Computing Systems* 4, 2 (2020), 1–39.

[33] Tornado.Cash. 2019. Tornado cash. Available at: https://tornado.cash/, before August 8th, 2022.

[34] TornadoCash. 2020. Tornado.Cash Governance Proposal. Available at: https://tornado-cash.medium.com/tornado-cash-governance-proposal-a55c5c7d0703.

[35] U.S. DEPARTMENT OF THE TREASURY. 2022. Cyber-related Sanctions. Available at: https://home.treasury.gov/taxonomy/term/1546.

[36] U.S. DEPARTMENT OF THE TREASURY. 2022. U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash. Available at: https://home.treasury.gov/news/press-releases/jy0916.

[37] Luke Valenta and Brendan Rowan. 2015. Blindcoin: Blinded, Accountable Mixes for Bitcoin. In *Financial Cryptography and Data Security - FC 2015 International Workshops, BITCOIN*. Springer, San Juan, Puerto Rico, 112–126.

[38] Friedhelm Victor. 2020. Address Clustering Heuristics for Ethereum. In *International Conference on Financial Cryptography and Data Security*. Springer, Kota Kinabalu, Malaysia, 617–633.

[39] Zhipeng Wang, Kaihua Qin, Duc Vu Minh, and Arthur Gervais. 2022. Speculative multipliers on defi: Quantifying on-chain leverage risks. In *Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, May 2–6, 2022, Revised Selected Papers*. Springer, Springer, Grenada, 38–56.

[40] Lei Wu, Yufeng Hu, Yajin Zhou, Haoyu Wang, Xiapu Luo, Zhi Wang, Fan Zhang, and Kui Ren. 2021. Towards Understanding and Demystifying Bitcoin Mixing Services. In *Proceedings of the Web Conference 2021*. ACM / IW3C2, Virtual Event / Ljubljana, Slovenia, 33–44.

[41] Pengcheng Xia, Haoyu Wang, Zhou Yu, Xinyu Liu, Xiapu Luo, and Guoai Xu. 2021. Ethereum Name Service: the Good, the Bad, and the Ugly. *arXiv preprint arXiv:2104.05185* (2021).

[42] Haaroon Yousaf, George Kappos, and Sarah Meiklejohn. 2019. Tracing Transactions Across Cryptocurrency Ledgers. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, USA, 837–850.

[43] Zuoxia Yu, Man Ho Au, Jiangshan Yu, Rupeng Yang, Qiuliang Xu, and Wang Fat Lau. 2019. New Empirical Traceability Analysis of CryptoNote-Style Blockchains. In *International Conference on Financial Cryptography and Data Security*. Springer,

Frigate Bay, St. Kitts and Nevis, 133–149.
[44] Liyi Zhou, Kaihua Qin, and Arthur Gervais. 2021. A2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges. *CoRR* abs/2106.07371 (2021). https://arxiv.org/abs/2106.07371
[45] Liyi Zhou, Kaihua Qin, Christof Ferreira Torres, Duc V Le, and Arthur Gervais. 2021. High-Frequency Trading on Decentralized On-Chain Exchanges. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 428–445.
[46] Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. 2022. SoK: Decentralized Finance (DeFi) Attacks. *Cryptology ePrint Archive* (2022), 1773. https://eprint.iacr.org/2022/1773

Table 2: System Model Definitions

Name	Definition	Eq.
Address Balance	$\mathbf{bal}_{\mathsf{a}}(t) = \mathbf{u}_{\mathsf{a}}(t) \times p - \mathbf{v}_{\mathsf{a}}(t) \times p$, where $\mathbf{u}_{\mathsf{a}}(t)$ and $\mathbf{v}_{\mathsf{a}}(t)$ are the numbers of a's deposit and withdrawal, respectively.	(4)
Pool State	$\mathbb{S}_{\mathbf{P}}(t) = \{(\mathsf{a}, \mathbf{bal}_{\mathsf{a}}(t)) \mid \mathsf{a} \in \mathcal{D}_{\mathbf{P}}(t) \cup \mathcal{W}_{\mathbf{P}}(t)\}$	(5)
Merge	$\textsc{Merge}(\mathbb{S}_{\mathbf{P}}(t), (\mathsf{a}_1, \mathsf{a}_2)) = \{(\mathsf{a}, \mathbf{bal}_{\mathsf{a}}(t)) \mid \mathsf{a} \in \mathcal{D}_{\mathbf{P}}(t) \cup \mathcal{W}_{\mathbf{P}}(t) \wedge \mathsf{a} \neq \mathsf{a}_1 \wedge \mathsf{a} \neq \mathsf{a}_2\} \cup \{(\mathsf{a}_1, \mathbf{bal}_{\mathsf{a}_1}(t) + \mathbf{bal}_{\mathsf{a}_2}(t))\}$	(6)
Simplified Pool State	If $\mathcal{S} = \emptyset$, $\textsc{Simp}(\mathbb{S}_{\mathbf{P}}(t), \mathcal{S}) = \mathbb{S}_{\mathbf{P}}(t)$; Else: $\textsc{Simp}(\mathbb{S}_{\mathbf{P}}(t), \mathcal{S}) = \textsc{Simp}\left(\textsc{Merge}(\mathbb{S}_{\mathbf{P}}(t), (\mathsf{a}_i, \mathsf{a}_{i+1})), \mathcal{S}'\right)$ where S is a set of linked addresses and $\mathcal{S}' = \mathcal{S} \setminus \{(\mathsf{a}_i, \mathsf{a}_{i+1})\}$	(7)

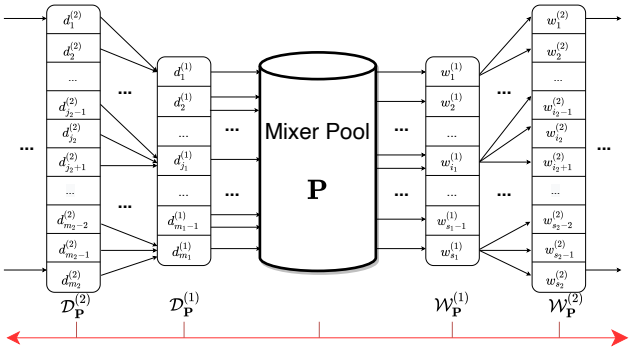


Figure 9: Extended model of a mixer pool. The mixer pool model in Fig. 1 can be extended to a model, which can cover depositors and withdrawers in longer distances.

A EXTENDED SYSTEM MODEL

We propose the following definitions to further describe mixers and summarize the key definitions in Table 2.

Address Balance in A Pool: An address's balance is the amount of coins that an address holds *in a pool* at a time t (cf. Eq. 4).

Pool State: A pool's state is the set of tuples constituted by all depositors, withdrawers, and their balances in $\mathbf{P}$, at time t (cf. Eq. 5).

A pool $\mathbf{P}$'s state is determined by users' balances. For instance, if d_1 deposits once, d_2 deposits twice, and w_1 withdraws once in a 100 coin pool $\mathbf{P}_{100}$ before time t, then $\mathbf{P}_{100}$'s pool state is $\mathbb{S}_{\mathbf{P}_{100}}(t) = \{(d_1, 100), (d_2, 200), (w_1, -100)\}$. If there exists a link between a depositor and a withdrawer in a pool $\mathbf{P}$, we can simplify the pools' state. For instance, if $\textsc{Link}(d_1, w_1) = 1$, then we can simplify the state as $\textsc{Simp}\left(\mathbb{S}_{\mathbf{P}_{100}}(t), (d_1, w_1)\right) = \{(d_2, 200)\}$.

Simplified Pool State: Given a pool's state $\mathbb{S}_{\mathbf{P}}$ and a set $\mathcal{S}$ consisting of linked address pairs, we compute the Simplified Pool State by merging the balances of linked addresses (cf. Eq. 7).

B ADDITIONAL MEASUREMENT RESULTS

Fig. 10 shows the daily transactions in TN BNB pools. Table 3 depicts the malicious addresses and BEV extractors which leverage TC to hide their traces in various distances. Fig. 11 shows the post-sanction TC ETH pools coin flow. Fig. 12 shows the TC transactions mined by various mining pools. Table 4 describes the measurement results when Heuristics 1-5 are applied to TC ETH and TN BNB pools. Fig. 13 shows the distribution of linked TC clusters.

Table 3: 205 malicious addresses and 2,595 BEV extractors leverage TC to hide their traces.

Pattern	Address Type	Total	Distance $n=1$	Distance $n=2$
Mixer $\xrightarrow{n}$ Malicious Addresses	Fake Phishing Scam	19	13	8
	DeFi Attacker	121	81	49
	CEX Attacker	1	0	1
Malicious Addresses $\xrightarrow{n}$ Mixer	Fake Phishing/Scam	58	26	35
	DeFi Attacker	113	88	56
	CEX Attacker	1	0	1
Mixer $\xrightarrow{n}$ BEV Extractors	Sandwich Attacker	431	240	230
	Arbitrageur	72	48	45
	Liquidator	51	27	34
BEV Extractors $\xrightarrow{n}$ Mixer	Sandwich Attacker	2,185	495	2,096
	Arbitrageur	128	33	124
	Liquidator	73	56	60

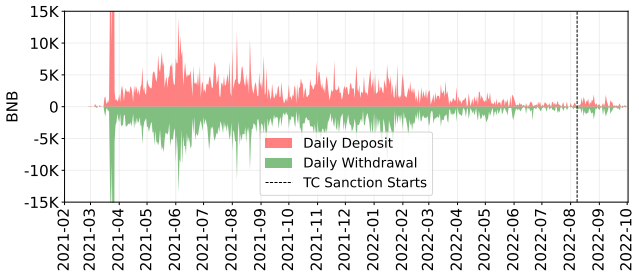


Figure 10: Daily transactions in TN BNB pools. There were almost zero deposits and withdrawals in TN during June and July 2022, but the activities increased after the TC sanctions.

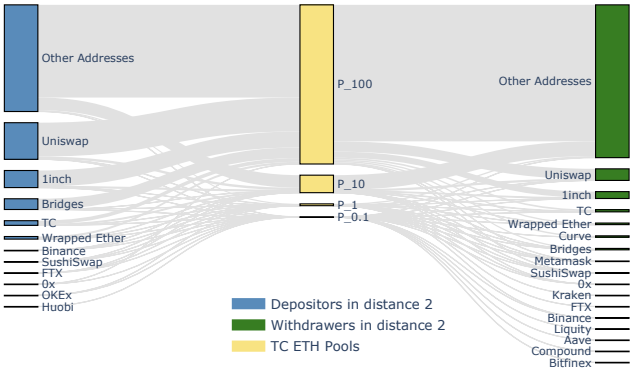


Figure 11: Post-sanction TC ETH pools coin flow. After the sanctions, more than 85% of the TC withdrawn ETH are transferred to intermediary addresses in distance 2, rather than being transferred to DeFi platforms or CEXs.

C HEURISTIC VALIDATION ATTEMPT

Our heuristics in Section 7.1 are best-effort methods and may yield false positives and negatives, a known challenge of related work [2, 27, 38]. For Heuristic 1, it is likely that our assumptions are accurate: When an address a is under the control of a user **u**, a's deposits or withdrawals in a mixer pool should be generated by

Table 4: Heuristics 1-5 applied to TC ETH and TN BNB pools before October 1st, 2022. $|\mathrm{SAS}_{\mathrm{P}}^{(n)}(t)|$ represents the Anonymity Set Size after applying Heuristic n. The percentages show the difference between the simplified anonymity set and $\mathrm{OAS}_{\mathrm{P}}(t)$.

Pool	$\lvert\mathrm{OAS}_{\mathrm{P}}(t)\rvert$	$\lvert\mathrm{SAS}_{\mathrm{P}}^{(1)}(t)\rvert$	$\lvert\mathrm{SAS}_{\mathrm{P}}^{(2)}(t)\rvert$	$\lvert\mathrm{SAS}_{\mathrm{P}}^{(3)}(t)\rvert$	$\lvert\mathrm{SAS}_{\mathrm{P}}^{(4)}(t)\rvert$	$\lvert\mathrm{SAS}_{\mathrm{P}}^{(5)}(t)\rvert$	Heuristic Combinations			
							$H_1 + H_2$	$H_1 + H_2 + H_3$	$H_1 + H_2 + H_3 + H_4$	$H_1 + H_2 + H_3 + H_4 + H_5$
TC 0.1 ETH	11,941	10,745 (−10.02%)	11,894 (−0.39%)	9,890 (−17.18%)	11,439 (−4.20%)	11,857 (−0.70%)	−10.38%	−26.76%	−30.07%	−30.68%
TC 1 ETH	17,843	16,422 (−7.96%)	17,791 (−0.29%)	15,445 (−13.44%)	17,077 (−4.29%)	17,733 (−0.62%)	−8.28%	−20.83%	−24.44%	−24.98%
TC 10 ETH	16,227	14,587 (−10.11%)	16,187 (−0.25%)	14,348 (−11.58%)	15,460 (−4.73%)	16,111 (−0.71%)	−10.38%	−20.34%	−24.51%	−25.14%
TC 100 ETH	6,433	5,608 (−12.82%)	6,407 (−0.40%)	5,754 (−10.55%)	5,975 (−7.12%)	6,347 (−1.34%)	−13.23%	−21.14%	−27.47%	−28.57%
TN 0.1 BNB	3,972	2,820 (−29.00%)	3,702 (−6.80%)	2,501 (−37.03%)	3,946 (−0.65%)	3,934 (−0.96%)	−33.91%	−54.00%	−54.76%	−55.39%
TN 1 BNB	3,890	2,868 (−26.27%)	3,626 (−6.79%)	2,531 (−34.94%)	3,852 (−0.98%)	3,845 (−1.16%)	−29.23%	−48.15%	−49.56%	−50.41%
TN 10 BNB	1,675	1,156 (−30.99%)	1,605 (−4.18%)	1,068 (−36.24%)	1,666 (−0.54%)	1,635 (−2.39%)	−33.07%	−47.58%	−48.48%	−50.15%
TN 50 BNB	231	217 (−6.06%)	217 (−6.06%)	204 (−11.69%)	231 (0.00%)	213 (−7.79%)	−12.12%	−21.65%	−21.65%	−28.14%

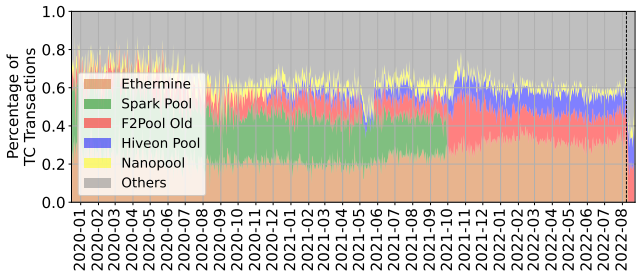


Figure 12: TC transactions mined by various mining pools before August 23rd, 2022. Ethermine mined the most TC transactions before August 8th, 2022, but stopped processing TC transactions after the sanctions are announced.

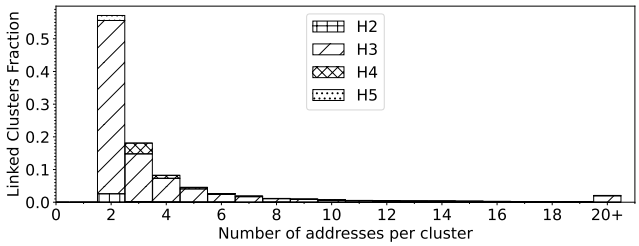


Figure 13: Number of addresses per TC cluster. 4,871 (57.14%) **TC clusters only have two addresses.**

u. Unfortunately, for Heuristics 2–5, we have no ground truth to verify that two different addresses belong to the same user. Therefore, to validate our Heuristics 2–5, we leverage three orthogonal privacy-exposing side-channels that help to validate our heuristics based on data from, *(i)* airdrops [38], *(ii)* the Ethereum Name Service (ENS) [41] and *(iii)* the DeFi explorer Debank. Given our reproducible dataset, we find that our heuristics yield an average F1 score of 0.55. For more detailed validation results, we refer the reader to the preprint of this work: https://arxiv.org/pdf/2201.09035.pdf.

D APPLICATION: TRACING MALICIOUS ADDRESSES

We provide the example of Upbit Hackers to show how to apply our linking results in TC to trace malicious addresses. On November

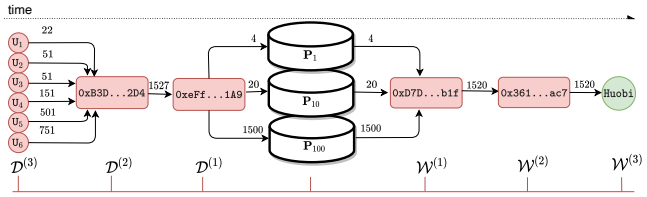


Figure 14: Applying linking heuristics to trace Upbit Hackers.

27th, 2019, hackers stole 342K ETH from Upbit, a South-Korean centralized cryptocurrency exchange. As shown in Fig. 14, *(1)* A depositor `0xeFf` receives 1,526.95 ETH from address `0x5a8`, which obtains the same amount of ETH from four labeled Upbit Hackers. *(2)* `0xeFf` then deposits 1,524 ETH into TC 1, 10, and 100 ETH pools before block 11,972,040. *(3)* From our linking results, we find that `0xD7D` withdraws the same amount from TC during block 11,971,270 and 11,972,098, and then transfers 1,520 ETH to address `0x361`, which finally exchanges all ETH to fiat currency (e.g., USD) on a CEX, Houbi. Given the address's registration information on Huobi, it would be able to pinpoint the hacker's off-chain identity.

E DISCUSSION AND IMPLICATIONS

Our analyses show that although users may reveal their transaction history because they are not familiar with the workflow of mixers (cf. Section 7), or they only use mixers for rewards rather than privacy (cf. Section 6), most of the users can still stay anonymous. Our approach can be generalized to analyze any other ZKP mixers which adopt the same design as TC, e.g., Cyclone and TP.

To improve the existing ZKP mixer design, a helpful functionality could be to warn users proactively about potential risks. For example, TC could exploit our methodology and results to provide a service that would compute the probability that a provided address for a withdrawal could be linked with a depositor. In this way, users would know the risk of linking their addresses before withdrawing funds from the mixer. Moreover, besides the anonymity set size and the OFAC sanctions, there might be other potential factors (e.g., AM profits and ETH or BNB prices) which could also affect the usage of ZKP mixers. We leave the detailed analysis for future work.