

Evasion Under Blockchain Sanctions

Endong Liu
University of Birmingham
Birmingham, United
Kingdom
exl309@student.bham.ac.uk

Mark Ryan
University of Birmingham
Birmingham, United
Kingdom
m.d.ryan@bham.ac.uk

Liyi Zhou*
The University of Sydney
Sydney, Australia
liyi.zhou@sydney.edu.au

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

Abstract

Sanctioning blockchain addresses has become a common regulatory response to malicious activities. However, enforcement on permissionless blockchains remains challenging due to complex transaction flows and sophisticated fund-obfuscation techniques.

Using cryptocurrency mixing tool Tornado Cash as a case study, we quantitatively assess the effectiveness of U.S. Office of Foreign Assets Control (OFAC) sanctions over a 957-day period, covering 6.79 million Ethereum blocks and 1.07 billion transactions. Our analysis reveals that while OFAC sanctions reduced overall Tornado Cash deposit volume by 71.03% to approximately 2 billion USD, attackers still relied on Tornado Cash in 78.33% of Ethereum-related security incidents, underscoring persistent evasion strategies.

In this paper, we identify three significant, structural limitations in current sanction enforcement practices: (i) fragmented censorship in blockchain consensus and application layer; (ii) the complexity of obfuscation virtual asset services exploited by users; and (iii) the susceptibility of naïve binary sanction classifications to dusting attacks. Our analysis and findings contribute to ongoing discussions around regulatory effectiveness in Decentralized Finance by providing empirical evidence, clarifying enforcement challenges, and informing future compliance strategies in response to sanctions and blockchain-based security risks.

CCS Concepts

• Security and privacy;

Keywords

Blockchain; Sanction; Compliance; Ethereum; Tornado Cash; Transaction Tracking; Fund Obfuscation; Decentralized Finance; DeFi

ACM Reference Format:

Endong Liu, Mark Ryan, Liyi Zhou, and Pascal Berrang. 2026. Evasion Under Blockchain Sanctions. In *Proceedings of the ACM Web Conference 2026 (WWW '26)*, April 13–17, 2026, Dubai, United Arab Emirates. ACM, New York, NY, USA, 12 pages. <https://doi.org/10.1145/3774904.3792715>

1 Introduction

Sanctioning or blacklisting blockchain addresses is a strategy used by regulators to counter activities such as money laundering and terrorist financing. Despite ongoing efforts, enforcing sanctions

on permissionless blockchains remains challenging, due to the complexity of transaction flows and the ease with which assets can be moved across addresses and protocols. For example, the U.S. Office of Foreign Assets Control (OFAC) sanctioned 170 addresses on Ethereum [8] that collectively held an initial balance of 499,769.74 ETH (983 million USD) at the time of designation. Following these sanctions, adversaries transferred funds to newly created addresses and employed a range of obfuscation techniques to evade detection. By the end of the observation period (March 21, 2025), only 145,579.38 ETH (286 million USD) remained.

Among these OFAC-sanctioned addresses, Tornado Cash (TC) represents the most significant case, constituting 44.17% of the initial and 99.12% of the remaining balance. As a privacy-focused cryptocurrency mixing pool, TC can break the on-chain linkability between deposit and withdrawal transactions. From our empirical analysis, TC processed over 2 billion USD during the sanctioned period from August 8, 2022 [35] to March 21, 2025 [36] (957 days). Remarkably, in 78.33% of 60 Ethereum-related security incidents during this period, attackers continued to leverage TC, illustrating persistent circumvention of sanctions by sophisticated actors.

While prior research has predominantly focused on tracing security incidents [15, 21, 38, 43, 46] or reconstructing the linkability of anonymous transactions [11, 18, 39, 40], our study broadly assesses regulatory effectiveness by systematically evaluating the impact of sanctions. We identify three structural limitations in the current sanction enforcement framework as our main contributions:

- **Fragile Sanction Enforcement:** We empirically evaluate the effectiveness of OFAC sanctions on Ethereum (§4) across a comprehensive dataset spanning 957 days of the entire sanction period, encompassing 6.79 million blocks and 1.07 billion transactions. We demystify the censorship gaps in consensus layer (§4.1) and application layer (§4.2), and provide temporal analysis on user reactions (§4.3). Our findings indicate that, although the overall TC deposit volume decreased by 71.03% during the sanction period compared to a similar pre-sanction timeframe, TC remains the primary tool for laundering malicious proceeds in Ethereum-related security incidents.
- **Comprehensive Obfuscation Patterns and Ecosystem:** We detect notable user strategies (§5.1), such as short dormant time (used to reduce the risk of assets being frozen), split-and-merge patterns (associated with money laundering), and test-depositing transactions (used to probe sanction enforcement policies). We further find that users can leverage the entire Ethereum service landscape to obscure fund origins (§5.2), including cross-chain bridges, Decentralized Exchanges (DEXs), Centralized Exchanges (CEXs), alternative privacy-enhancing tools, and other Decentralized Finance (DeFi) platforms.

*Co-supervised this research project.



This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

WWW '26, Dubai, United Arab Emirates

© 2026 Copyright held by the owner/author(s).

ACM ISBN 979-8-4007-2307-0/2026/04

<https://doi.org/10.1145/3774904.3792715>

- **Naïve Binary Classification Vulnerability:** We provide an argument to demonstrate that binary classification systems (sanctioned / non-sanctioned) used in the OFAC list exhibit inherent vulnerabilities to *dusting attacks* in Appendix B, where small amounts of sanctioned funds are strategically distributed to arbitrary addresses, finally resulting denial of service. Our analysis also reveals that 12.00 ETH from sanctioned services were used to dust addresses controlling at least 9 million ETH (over 750,000×) within 48 hours after sanctions took effect (§4.3.3).

2 Background

This section outlines the necessary background for the paper.

2.1 Ethereum and Its Service Ecosystem

Ethereum is a permissionless blockchain system that supports smart contracts, which are programs that can be deployed and executed by anyone on the network. Unlike Bitcoin’s Unspent Transaction Output (UTXO) model [24], Ethereum employs an account-based model where each address maintains a state including its balance and other attributes [42]. The native cryptocurrency, Ether (1 ETH = 10^{18} Wei), serves both as a medium of exchange and as “gas” to pay for all on-chain computational operations. Transactions are processed by miners (Proof-of-Work) or validators (Proof-of-Stake after the “Merge” in September 2022), who receive rewards for including transactions. Its ecosystem encompasses various services:

Privacy-Enhancing Tools: Mixing services like TC aim to break the on-chain linkability between deposit and withdrawal transactions. It operates via fixed-denomination mixing pools (e.g., 0.1 ETH, 1 ETH, 10 ETH, and 100 ETH), utilizing Zero-Knowledge Proofs (ZKPs) to provide a cryptographic proof of commitment ownership without revealing specific commitments. Other tools like Umbra [33] and Railgun [30] leverage stealth addresses to prevent observers from connecting multiple payments to the same entity. While these tools serve legitimate privacy needs, they fundamentally challenge traditional regulatory approaches.

Exchanges: There are two primary types of cryptocurrency exchanges. DEXs like Uniswap [34] and 1inch [1] operate entirely on-chain through smart contracts, enabling peer-to-peer trading without custodial intermediaries. Most operate through an Automated Market Maker (AMM), which use mathematical formulas to price assets based on the ratio of tokens in liquidity pools. CEXs such as Binance [6] and Coinbase [10] function as traditional financial intermediaries, maintaining order books, and custodial user funds. CEXs act as gateways between fiat and crypto, typically enforcing different levels of compliance requirements.

Cross-Chain Bridges: Services that facilitate asset transfers between different blockchain networks to expand interoperability. Unlike token standards (e.g., ERC-20 [13]) which provide consistent interfaces, cross-chain bridges lack standardization in their implementation, message formats, and identifier systems. The differences in their architectures [2] create significant technical challenges for cross-chain transaction monitoring and fund tracing.

Other DeFi Services: Applications in DeFi providing lending, Non-Fungible Token (NFT) trading, and other financial services through smart contracts without traditional intermediaries [41].

2.2 Regulatory and Enforcement

The pseudonymous and decentralized nature of blockchains challenges traditional censorship frameworks.

Regulatory Evolution: Traditional Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) frameworks require Know-Your-Customer (KYC) for customer identification and Know-Your-Transaction (KYT) for transaction monitoring. The Financial Action Task Force (FATF) has extended these requirements to virtual asset service providers through recommendations like the “Travel Rule” [14], which conflicts with blockchain’s pseudonymous design.

Blockchain Sanctions: The U.S. OFAC has expanded their sanctions regimes to include specific blockchain addresses and services. Sanctions on TC in August 2022 targeted an autonomous smart contract system that is abused to launder over 7 billion USD worth of cryptocurrency, including over 455 million USD stolen by the North Korean state-sponsored Lazarus Group [35]. This action classifies privacy technology itself as a compliance risk, marking a significant escalation in regulatory response to blockchain privacy tools. As a result, recent works [4, 20, 45] and protocols [30, 47] consider compliance requirements in their designs and implementations.

Enforcement Through Multiple Vectors: The decentralized nature of blockchain systems has necessitated multi-layered censorship approaches that operate at different levels of the technology stack: (i) block producers can refuse to include transactions involving sanctioned addresses [37], (ii) user interfaces and front-ends of DeFi applications can block addresses that interact with sanctioned services, and (iii) stablecoin providers and centralized services can freeze assets or close accounts based on their blacklist mechanisms.

3 Models and Metrics

This section formalizes our system model, threat model, and quantitative measures we use throughout the evaluation.

3.1 System Model

This paper follows the system model in the previous works [37, 46]: **Consensus Layer.** A leader is selected to append a block to ledger, who can capture inclusion and sequencing choices that earn rewards and can enact or avoid censorship. **Application Layer.** Smart contracts maintain state and execute bounded logic; when blacklist or oracle checks are embedded, enforcement becomes binding and auditable on-chain. **Auxiliary Services.** (as Off-Chain Application Layer) Front-ends and oracles mediate access and data off-chain, adding friction that is bypassable by direct protocol interaction.

To ease the understanding of the following paragraphs, we proceed by introducing the following notations and definitions:

Block B_i where i corresponds to a block identifier.

Blockchain $\mathcal{L} = \{B_0, \dots, B_i, \dots\}$ also called *Distributed Ledger*.

Address $addr \in ADDR$, where $ADDR$ is the set of valid Ethereum addresses. We use the terms “address” and “account” interchangeably as each account is identified by a unique address, referring to externally owned accounts and smart contract accounts.

Sanctioned Address Set $ADDR_{Sanction} \subset ADDR$.

Blockchain State $s \in \mathcal{S}$ includes (i) the state of all accounts (e.g., balance and transaction nonce), (ii) the state of all smart contracts,

and (iii) blockchain metadata (e.g., block numbers, timestamps, miner addresses, gas used, gas price, etc.) at a given point in time.

Operation $op \in OP$, where OP is the set of operations that modify the state s (e.g., asset transfers and contract invocations).

Balance Function $\mathcal{B}(s, addr) \rightarrow \mathbb{N}_0$ returns the non-negative integer balance (in Wei) for a given address $addr$ in state s .

State Transition $\mathcal{T}(s, op) \rightarrow s'$ returns the new state s' after the current state s applies operation op . Specifically, given a balance operation $op_{\mathcal{B}}$ that affects addresses $\{addr_{from}, addr_{to}\} \subset ADDR$ and amounts $\{a_{sent}, a_{received}\} \subset \mathbb{N}_0$, such that

$$op_{\mathcal{B}} \rightarrow \{ \langle addr_{from}, a_{sent} \rangle, \langle addr_{to}, a_{received} \rangle \}$$

the balance state transition $\mathcal{T}_{\mathcal{B}}$ is

$$\begin{aligned} \mathcal{B}(s', addr_{from}) &= \mathcal{B}(s, addr_{from}) - a_{sent} \\ \mathcal{B}(s', addr_{to}) &= \mathcal{B}(s, addr_{to}) + a_{received} \end{aligned}$$

3.2 Threat Model

We consider adversaries who aim to conceal fund flows originating from sanctioned sources. These adversaries may range from individual actors to state-backed organizations (e.g., Lazarus Group). We assume they have full visibility of the blockchain’s public data and can undertake the following on-chain actions:

- **Dusting:** Adversaries can send arbitrary amounts to random addresses (including innocent accounts) to create ambiguous connections and inflate the scale of transaction tracing graphs, making it more difficult to pinpoint the true flow of funds.
- **Layering:** Adversaries can generate an unrestricted number of addresses and transactions to split (from one source to multiple destinations) or merge (from multiple sources to one destination) their assets. Furthermore, these addresses can be used only once to undermine straightforward clustering heuristics.
- **Interacting:** Adversaries can create their own smart contracts and can interact with any deployed on-chain service, including swapping tokens on DEXs, cashing out via CEXs, bridging to other blockchains, using privacy-enhancing tools, or engaging with DeFi lending and NFT trading platforms.

We assume that adversaries cannot compromise the blockchain’s cryptographic foundations, exploit previously unknown smart contract vulnerabilities, or conspire with a majority of block producers or service providers. Our primary goal and focus is to expose the behavioral patterns of adversaries and the ultimate destinations of assets once they leave malicious or sanctioned accounts.

3.3 Metrics

In this paper, a more practical tracking algorithm that uses a quantitative impurity metric is applied to precisely measure the propagation and concentration of sanctioned funds throughout the Ethereum ecosystem. We provide the algorithm for updating the corresponding metrics of each affected address as sanctioned assets propagate in Appendix A.

Impurity Function $I(s, addr) \rightarrow \mathbb{N}_0$ returns the non-negative integer amount originated from $ADDR_{Sanction}$ in balance (in Wei) for a given address $addr$ in state s , such that

$$0 \leq I(s, addr) \leq \mathcal{B}(s, addr)$$

Impurity Score $\varphi(s, addr)$ is defined as

$$\varphi(s, addr) = \begin{cases} \frac{I(s, addr)}{\mathcal{B}(s, addr)}, & \text{if } \mathcal{B}(s, addr) > 0 \\ 0, & \text{if } \mathcal{B}(s, addr) = 0 \end{cases}$$

By definition, $\varphi(s, addr) = 0$ indicates there is no traceable connection between $addr$ and $ADDR_{Sanction}$ or no balance under $addr$ at the state s , and $\varphi(s, addr) = 1$ shows that all balances under $addr$ are traceable to sanctioned addresses at the state s . This score provides a relative measure of an address’s historical association with sanctioned outflows. It is important to note that this approach aligns with Ethereum’s account model, where the impurity of funds can be treated as an extra state or property of an Ethereum address.

4 Sanction Effectiveness

To examine the sanction effectiveness, we conduct a comprehensive evaluation using historical Ethereum blockchain data. Our analysis covers the entire TC sanction period from Block 15302392 (B_{OFAC} , August 8, 2022) to Block 22097863 (B_{END} , March 21, 2025).

4.1 Gaps in Consensus Layer Censorship

Previous research [37] showed that block producers can and do filter out transactions associated with OFAC-sanctioned entities to avoid including them in their blocks. These censorship behaviors can be driven by external pressures (e.g., regulations) or internal motivations (e.g., ethical or economic considerations). We followed the definition of *Consensus Layer Censorship* in [37] and further divided it into two different situations as the following definitions:

Definition 4.1 (Base Consensus Layer Censorship). A blockchain protocol participant intentionally obstructs the inclusion of a transaction where at least one involved address is sanctioned, such that $tx \notin B_i \mid B_i \in \mathcal{L}$ and $addr(tx) \cap ADDR_{Sanction} \neq \emptyset$.

However, only a part of blockchain protocol participants actively enforce this basic but strict censorship. Due to the censorship-resistant nature of Ethereum, transactions that move assets from a sanctioned address to other addresses still have a possibility to be included in the distributed ledger. Therefore, we adapt the definition to capture the wider censorship.

Definition 4.2 (Derived Consensus Layer Censorship). A blockchain protocol participant intentionally obstructs the inclusion of a transaction where all involved addresses are not sanctioned but at least one holds assets that originate from sanctioned addresses at or above a pre-defined threshold, such that $tx \notin B_i \mid B_i \in \mathcal{L}$ and $addr(tx) \cap ADDR_{Sanction} = \emptyset$ but $\max_{a \in addr(tx)} \varphi(a) \geq \theta$.

Our re-evaluation of block producer behaviors using the proposed impurity score φ revealed a significant discrepancy between the base censorship and derived handling of downstream assets withdrawn from four TC ETH pools. As illustrated in Figure 1, we visualized top block producers on Ethereum, which covers 80.06% of a 6.79 million block sample between B_{OFAC} and B_{END} .

Three block producers, “rsync-builder”, “Flashbots: Builder” and “bloXroute: Regulated Builder”, actively follow OFAC sanctions. The “rsync-builder” demonstrated the most rigorous censorship. It produced 734,343 blocks (10.81% of sampled blocks) without including any direct interactions with four TC ETH pools. However, our

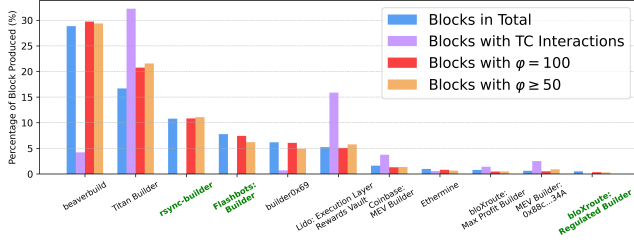


Figure 1: Top block producers on Ethereum between B_{OFAC} and B_{END} . Blocks with TC interactions (purple) represent blocks that contain direct deposits and withdrawals with four TC ETH pools. Blocks with score conditions (red and yellow) indicate blocks that include transactions issued by accounts that meet the condition. Note that “rsync-builder”, “Flashbots: Builder”, and “bloXroute: Regulated Builder” (in green) follow OFAC sanctions to reject direct TC interactions.

analysis of blocks containing senders with high impurity scores ($\varphi = 100\%$ and $\varphi \geq 50\%$) revealed that “rsync-builder” produced these blocks at rates (10.83% and 11.10%, respectively) that closely match its overall block production rate (10.81%). We observed similar patterns with “Flashbots: Builder” and “bloXroute: Regulated Builder”. This consistency demonstrated a critical finding: these block producers appear to follow rigorously base censorship but fail to scrutinize transactions involving addresses that previously received sanctioned funds (derived censorship). This highlights a significant gap in their current enforcement mechanisms.

The remaining 8 block producers only partially complied or did not enforce OFAC sanctions at all, such as “Titan Builder” which contributed the largest proportion (32.24%) of blocks in which exist transactions that directly interacted with TC. Meanwhile, “beaverbuild” led in the number of blocks meeting certain impurity conditions, aligning proportionally with its overall block production.

Furthermore, block producers derive significant revenue beyond transaction fees and block rewards from Maximal Extractable Value (MEV). In this process, MEV bots pay block producers for favorable transaction placement, enabling profitable strategies such as arbitrage [29]. Our investigation revealed that some of these MEV operations were funded by TC, as evidenced by bots like $0x06e8\dots c9fc$ and $0x0000\dots 266c$. This further raises critical compliance concerns, as block producers may unintentionally facilitate the movement of sanctioned assets, exposing themselves to regulatory risks.

Finally, gaps in consensus layer censorship lead the result that the assets derived from sanctioned addresses had been integrated into the entire Ethereum ecosystem. We conducted a comprehensive analysis on approximately 67.94 million addresses holding funds that could have originated from TC at B_{END} . Table 1 summarizes the distribution of addresses and impurity amounts according to the impurity scores. For our initial analysis, we set the impurity threshold $\Phi = 5\%$. However, it is important to note that this threshold is not a definitive recommendation but serves primarily as an experimental baseline for Section 5, as evaluating its efficacy requires ground

Table 1: Distribution of Addresses with their Impurity Amounts and Total Balance Amount by Impurity Scores φ

Score φ	# Address	Impurity Amount I	Total Balance Amount \mathcal{B}
[0%, 5%)	67,321,336 (99.08%)	877,243.20 ETH (76.05%)	127,696,284.34 ETH (99.62%)
[5%, 50%)	560,858 (0.83%)	19,363.70 ETH (01.68%)	224,987.50 ETH (00.18%)
[50%, 95%)	16,665 (00.02%)	4,155.41 ETH (00.36%)	5,832.83 ETH (00.00%)
[95%, 100%]	45,258 (00.07%)	252,763.76 ETH (21.91%)	252,812.50 ETH (00.20%)
Total	67,944,117 (100%)	1,153,526.07 ETH (100%)	128,179,917.19 ETH (100%)

truth data which is not universally available. The selection of an appropriate threshold involves inherent trade-offs that merit careful consideration. In practice, regulators and compliance teams should calibrate this parameter according to their operational constraints, risk tolerance, and available resources (potentially in conjunction with complementary metrics to enhance accuracy).

4.2 Gaps in Application Layer Censorship

While the consensus layer determines whether a transaction is included in the blockchain, most sanction controls sit at the application layer and many of them are bypassable.

4.2.1 Off-Chain and On-Chain Censorship. We separate application layer censorship into off-chain and on-chain forms because the enforcement points and failure modes differ in practice.

Off-chain censorship includes front-ends that hide functions or decline to provide services [16, 17], Remote Procedure Call (RPC) gateways that reject raw transaction submissions [3], and custodial venues that decline deposits or withdrawals under internal compliance rules. However, these decisions do not alter protocol semantics and are therefore non-binding with the blockchain state. A blocked user can switch to another front-end, send the transaction through a permissive RPC endpoint, or interact with the contract directly using a Command Line Tool (CLT).

On-chain censorship refers to logic that is written into smart contracts and evaluated at call time. We use the same definition in Wahrstätter et al.’s work [37] as follows:

Definition 4.3 (On-Chain Application Layer Censorship). A transaction tx is censored by a smart contract, if $tx \in B_i$, where $B_i \in \mathcal{L}$ is blocked by the state s_i , s.t. further state transitions $\mathcal{T}(s_i) \rightarrow s_{i+1}$ are blocked by the respective contract.

The contract itself decides to refuse the state transition when a policy predicate is met, for example, the address is included in its denylist. It provides a clear causal link between the rule and the observed execution outcome such that users cannot bypass it using similar methods against off-chain censorship. However, because of the blockchain transparency, alongside with longer censorship paths (e.g., multisig confirmations and additional on-chain transaction proposal), an informed counterparty can move sanctioned assets before a blacklist update takes effect.

In the remainder of this subsection, our analysis concentrates on on-chain censorship implemented by the blacklist mechanism (i) Chainalysis Sanctions Oracle and (ii) major stablecoin contracts (notably USDT and USDC). The evaluation of off-chain censorship effectiveness can be indirectly derived from downstream service utilization in Section 5.2.

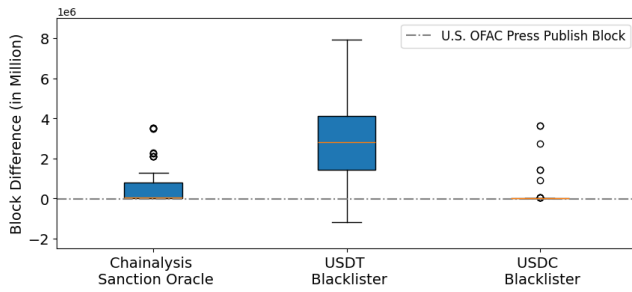


Figure 2: The distribution of block height differences in millions between the first on-chain enforcement transaction and the reference block aligned to the OFAC press-release block number (dashed zero line). Among three enforcement entities, USDC blacklist exhibits the shortest and least variable policy-to-enforcement delay.

4.2.2 Delays in Performing On-Chain Censorship. We tracked two quantities to measure delays. First, the policy-to-enforcement interval: the elapsed window between the official OFAC publication time of a designation and the first on-chain transaction that adds the affected address to a blacklist. Second, the intra-block ordering position of that enforcement transaction: its index within the containing block, normalized by block length, which indicates how much ordering slack existed for adversaries to move first.

For the policy-to-enforcement delay, we selected the block number closest to midnight of the OFAC publication date in Eastern Time Zone as B_{OFAC} and the block number of the first transaction that updates the blacklist as $B_{enforce}$. We report $\Delta_{policy} = B_{enforce} - B_{OFAC}$ in block numbers in Figure 2, which represents the operator’s response time plus any procedural latency. The result shows that USDC blacklist updates land essentially at the OFAC publication time, with the Chainalysis Sanctions Oracle showing small, positive lags. By contrast, USDT blacklist exhibits much larger and more dispersed delays (but sometimes even appearing before), indicating slower and less consistent on-chain censorship.

For the intra-block position, let the enforcement transaction appear at index i (zero-based) in a block with N transactions. We computed a normalized rank $r = \frac{i}{N} \in [0, 1]$, where an r near 1 means the update landed late in the block; users with higher-priority fees could have been executed earlier in the same block. From our analysis, USDC blacklist transactions tend to be mined early in the block (avg. index **29.83%**), reducing intra-block exposure. USDT transactions are appended mid-block (**47.01%**), and Chainalysis oracle additions occur much later (**63.62%**), leaving more room for same-block preemption by outgoing transfers that pay higher fees.

4.3 Differences in User-Level Reaction

Sanctions not only have impacts on enforcement, they also change how users route and time their transactions. Therefore, we further examine the on-chain behavioral adjustments.

4.3.1 Reduction in During-Sanction Activity. We extended the previous study of Wang et al. [40] by examining a comprehensive dataset spanning 966 days before and 957 days after the OFAC sanctions on

Table 2: Impact of the Sanction on TC: while withdrawal volume also declined significantly (-66.80%), they remained slightly higher than deposit volumes (-71.03%), suggesting users prioritized exiting over continued use.

Metric	Action	Pre- B_{OFAC}	Post- B_{OFAC}	Change
# Transaction	Deposit	150,403	42,753	-71.57%
	Withdraw	139,404	44,283	-68.23%
# Address	Deposit	39,397	9,175	-76.71%
	Withdraw	58,567	20,734	-64.60%
Volume (in ETH)	Deposit	3.49M	1.01M	-71.03%
	Withdraw	3.27M	1.08M	-66.80%

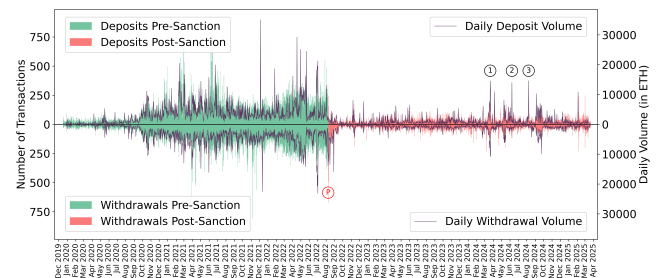


Figure 3: Daily transactions and volumes into the TC ETH pools from December 16, 2019 to March 21, 2025. The x-axis denotes the timeline, while the y-axis captures transaction count and volume of deposits (up) and withdrawals (down). The three circled values mark the top-3 during-sanction daily deposit volumes, each linked to a known security incident. Moreover, a significant spike in withdrawals is observed on the sanction date, marked by the circled letter “P”.

TC. Table 2 shows a substantial reduction in the number of transactions, unique addresses, and total volumes for both TC deposits and withdrawals. Specifically, post-sanction deposit volume fell to only **28.97%** of pre-sanction levels when comparing near equivalently long time periods. Figures 3 displays the daily statistics for deposits and withdrawals. Following the announcement of the sanctions, we observed a significant increase in withdrawal transactions (labeled as Peak **P**). This peak represents the highest daily withdrawal transaction count after OFAC sanctions and also indicates a mass exodus from TC, suggesting that users were prompted to withdraw their assets due to heightened uncertainty.

4.3.2 Limited Effect on Ethereum Attackers. We took a snapshot of the BlockSec database ¹ as of March 21, 2025. This dataset catalogs significant DeFi exploits with losses exceeding 100,000 USD and provides one of the most comprehensive public records of major attacks. Of the **80** total incidents on Ethereum in the dataset, funds were returned to victims in only 9 cases. Among the remaining **71** malicious attacks, attackers in 11 cases retained stolen assets by converting them to non-freezable assets (e.g., ETH or DAI). Notably, among the **60** incidents with active money laundering activity, attackers used TC as their primary laundering method in **47 cases**

¹<https://docs.blocksec.com/phalcon/security-incident-list>

(78.33%). Moreover, we observed that in 35 (49.30%) out of these 71 malicious incidents, attackers sourced their funding from TC to facilitate the exploit transactions. Importantly, 29 (82.86%) of these 35 cases subsequently returned stolen assets back into TC, further obfuscating their on-chain footprints.

Moreover, we identified three significant deposit peaks after the sanction date, as illustrated in Figure 3. The first peak, denoted as Peak ①, occurred on March 21, 2024, predominantly driven by the Heco Bridge Exploiter [26], who contributed 11,200.00 ETH, representing 77.11% of the total deposits (14,522.00 ETH) on that day. The second peak, Peak ②, took place on June 8, 2024, with deposits primarily originating from the Orbit Bridge Exploiter [27]. This attacker deposited 12,930.00 ETH, accounting for 92.18% of the day’s total deposit volume (14,027.00 ETH). The third and most pronounced peak, Peak ③, was recorded on August 8, 2024, with the Nomad Bridge Exploiter [25] depositing 14,509.30 ETH, constituting nearly the entirety (99.50%) of the day’s total 14,581.70 ETH.

4.3.3 Dusting Attacks. Following the announcement of OFAC sanctions on TC, a significant dusting attack emerged: small amounts of ETH were deliberately withdrawn from TC to a wide range of addresses. Our analysis focused on transactions from the smallest TC 0.1 ETH mixing pool within 14,400 blocks (approximately 48 hours) after B_{OFAC} . The dusting targets included prominent entities like Ethereum Foundation, CEXs (e.g., Kraken, Binance, Bitfinex, Gemini, OKX, etc.), and users interacting with DeFi platforms. These dusting attacks effectively flagged numerous unsuspecting recipients as potentially sanctioned or involved in malicious activities.

A direct consequence of these dusting behaviors was the Denial-of-Service attack on services (e.g., Aave Front-End [16]) that are relying on binary classification mechanisms. We observed that dusters used merely 12.00 ETH to taint at least 9 million ETH (over 750,000×) belonging to the affected recipients. This significantly increased the risk of asset freezing and service denial by compliant platforms. The dusting phenomenon underscores the need for continuous and quantitative risk metrics, such as our proposed impurity scores ϕ , that can capture varying levels of exposure to sanctioned funds. Such metrics enable regulators and service providers to implement proportional compliance responses based on precise risk assessments, rather than naïve binary classifications. We also provide detailed arguments in Appendix B.

5 Downstream Fund Flow Analysis

In this section, we present detailed insights into how funds flow after withdrawals from sanctioned addresses. Specifically, we focus on two aspects: first, behavioral patterns prior to depositing into virtual asset services; and second, their subsequent interactions with these service providers. Through this analysis, we aim to enhance the understanding of user strategies and support efforts in tracing sanction-related activities across blockchain ecosystems.

5.1 Behavioral Patterns

Between initial withdrawals and subsequent deposits into Ethereum services, we identify and analyze three primary behavioral patterns.

5.1.1 Time of Initial Asset Transfers. Regarding the time of asset transfers, our observations in Figure 4 show significant variations

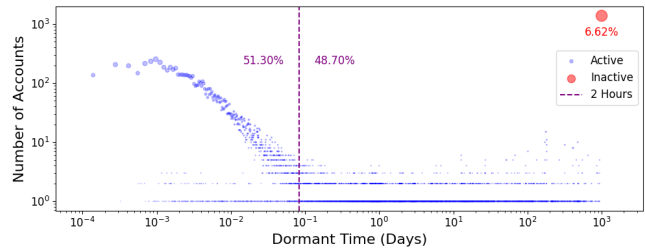


Figure 4: Dormant Time Distribution of TC Withdrawers. 51.30% of withdrawers transfer assets within 2 hours after their first TC withdrawal, while 48.70% express a long-tail distribution pattern that ranges from several hours to hundreds of days. The red circle (6.62% of accounts) represents accounts that remain completely inactive.

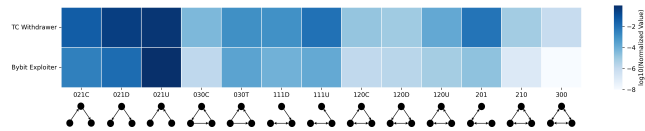


Figure 5: Heatmap comparing transaction patterns between TC withdrawers and the Bybit exploiter based on connected three-node motifs. Dark blue cells of both distributions in 012C, 021D, and 021U show high-intensity activities of asset transferring, splitting, and merging, respectively.

in the duration between the first withdrawal of funds from TC and subsequent movements of assets.

The majority of withdrawers (51.30%) transfer their assets within a 2-hour window following the initial withdrawal, demonstrating a preference for immediate asset relocation. The remaining 48.70% of withdrawers present extended dormant periods ranging from several hours to hundreds of days. This extended dormancy creates a long-tail distribution pattern visible in the scattered data points across the right side of the vertical threshold. The distribution of these delayed transfers appears non-uniform, with varying concentrations at different time intervals. The substantial cluster of inactive ones (6.62% of all TC withdrawers) withdraw assets from TC and engage in no further transaction activity.

5.1.2 Split-and-Merge Pattern. We applied our methods to both TC withdrawers and the Bybit exploiter (the largest known security incident [12] in history until March 2025). Our comparative analysis, as shown in Figure 5, reveals the behavioral similarities between these actors based on the frequency of connected three-node motifs [5]. The *split-and-merge* pattern emerges as a distinctive signature, characterized by entities initially splitting funds across multiple addresses (Motif 021D), transferring them through intermediate addresses (Motif 021C), and finally merging assets (Motif 021U). This technique is specially designed to circumvent transaction monitoring systems and has been documented in both traditional and crypto-specific money laundering studies. This behavioral similarity, combined with widespread usage of TC following security incidents (cf. Section 4.3.2), further raises concerns.

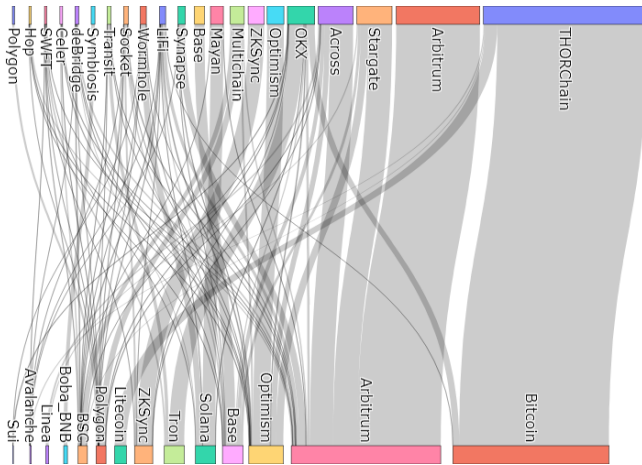


Figure 6: Flow of Funds via Cross-Chain Bridges. We implement custom parsers for 20 bridges and 2 proxy aggregators to get the corresponding target chain from the transaction metadata. Among over 15 destinations, Bitcoin (33.31%) and EVM-compatible blockchains (53.02%) are primary options.

5.1.3 Test-Depositing Sequences. Another behavior involves conducting small exploratory deposits before committing to substantial transfers. Table 3 in Appendix D illustrates this behavior: a user first deposited around 0.1 ETH to KuCoin, then consistently transferred larger amounts (10–12 ETH) in all subsequent transactions.

This sequential approach serves the risk-mitigation purpose, where users perform an end-to-end operational check to ensure their funds can move without being blocked by any undisclosed sanctions control like the off-chain application layer censorship. Our analysis of five services implementing regulatory requirements reveals a precise proportion: 38.55% of Binance, 75.31% of Railgun, 49.02% of OKX, 47.73% of Gate.io, and 46.59% of KuCoin users, who execute multiple deposits, demonstrate this test-then-deposit sequence. In contrast, platforms without sanctions enforcement exhibit different patterns. Users interacting with these services typically skip the testing phase, preferring to transfer substantial amounts in single transactions through primarily one-time intermediate addresses. This behavioral difference creates a detectable marker that compliance systems can leverage.

5.2 Service Utilization

Following our examination of behavioral patterns, we investigated the diverse service providers that TC withdrawers commonly use.

5.2.1 Cross-Chain Bridges. Cross-chain bridges have emerged as pivotal components within the cryptocurrency ecosystem, enabling users to seamlessly transfer assets and messages across disparate blockchain networks. Although these mechanisms facilitate interoperability and expand use cases, they also pose significant challenges to on-chain forensics and censorship efforts, as shown in Figure 6.

Plaintext Metadata. Most cross-chain protocols disclose core transaction parameters in plaintext, including the destination chain identifier and the recipient address on the destination chain. In principle, these metadata enable analyzers to link an outgoing

transaction on one chain to its corresponding incoming transaction on another. However, a lack of standardization across bridging protocols, especially when destination chains are non-Ethereum Virtual Machine (EVM)-compatible, hampers this process. Even identifiers for the same blockchain can vary between services built on top of both EVM-compatible underlying infrastructures. For instance, “Stargate: Pool Native” uses 0x75e8 (30184) to represent the Base blockchain, while “Across Protocol: Ethereum Spoke Pool V2” uses 0x2105 (8453). The former adopts the Endpoint ID defined by LayerZero² and the latter uses the common Chain ID³. Such inconsistencies necessitate the development of custom parsers for each bridge implementation, significantly increasing the effort required to integrate, interpret, and verify metadata across platforms.

To address this challenge, we developed custom parsers for 20 widely used cross-chain bridges and 2 proxy aggregators (OKX: Web3 Proxy and LIFI: LiFi Diamond) frequently involved in TC withdrawals. Our analysis revealed that $I_v = 350,918.15$ ETH ($\varphi \approx 97.37\%$) were bridged out of Ethereum via these platforms, contributing to 32.41% of total impurity volume. EVM-compatible chains accounted for more than half (53.02%) of the bridged impurity volume, including eight Layer-2 rollups and two alternative Layer-1 chains. Among heterogeneous targets, Bitcoin emerged as the dominant destination, capturing 33.31% of bridged volume where 95.95% of them were routed through THORChain. Solana and Litecoin accounted for an additional 4.30% and 2.51%, respectively. However, some bridges such as Chainflip ($I_v = 4,601.81$ ETH, $\varphi = 97.80\%$) and Orbiter ($I_v = 1952.27$ ETH, $\varphi = 93.23\%$) do not provide sufficient on-chain information, preventing identification of destination chains or recipient addresses via transaction analysis.

Cross-Chain Motivations. (i) *Hard Fork Tolerance:* The DAO hard fork [22] in 2016 highlighted Ethereum’s capacity to reverse transactions through community-driven rollbacks. Because this outcome undermined finality for malicious actors, they would bridge funds to different chains, aiming to reduce the likelihood of reversal. (ii) *Heightened Obfuscation:* Each newly designed blockchain or newly developed cross-chain bridge introduces additional complexity into the transaction tracing. This challenge is amplified when intermediary chains provide limited transparency or lack robust blockchain analytics tooling. Moreover, certain blockchains support built-in or composable privacy-enhancing mechanisms (e.g., confidential transactions on Monero, CoinJoin on Bitcoin and TC on Ethereum). Users can strategically route funds through chains with advanced anonymity features to further obscure the provenance of assets. When privacy tools are chained together, e.g., bridging from Ethereum to Bitcoin for CoinJoin, then returning to Ethereum for TC, the difficulty of end-to-end tracing increases exponentially. The limited regulatory or compliance enforcement on newly developed chains (e.g., Boba and Sui) also incentivizes cross-chain transfers for evading detection. (iii) *Lower Fees and Faster Confirmations:* Layer-2 rollups and some Layer-1 blockchains offer significantly reduced transaction costs and faster block finality compared to Ethereum. While these properties benefit users seeking performance and affordability, they are equally attractive to malicious actors seeking to move funds cheaply and efficiently.

²<https://docs.layerzero.network/v2/deployments/deployed-contracts>

³<https://chainlist.org/>

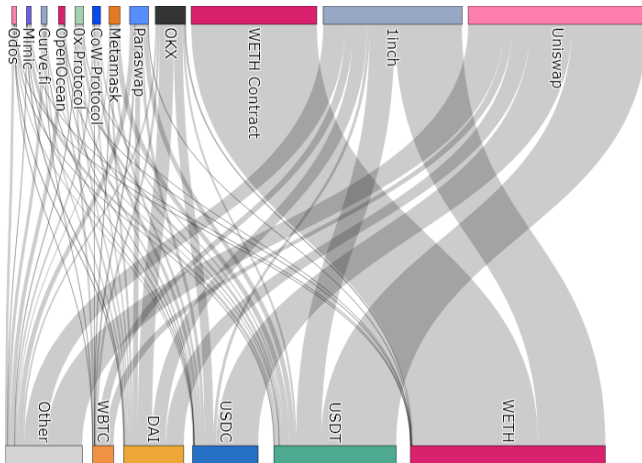


Figure 7: Flow of Funds via Decentralized Exchanges. Over 86.27% of impurity volume are swapped into stablecoins and wrapped tokens. Notably, USDT and USDC have blacklist mechanisms to freeze assets held by sanctioned entities.

5.2.2 Decentralized Exchanges. DEXs are significant choices utilized by sanctioned addresses, accounting for 26.78% of all impurity volume I_v in our database. This preference stems from their permissionless architecture and censorship-resistant design.

Dominant Service Providers. We identified transactions flowing into more than 12 DEX platforms as shown in the upper side of Figure 7. Among these platforms, Uniswap [34] (33.04%) and 1inch [1] (25.64%) dominated downstream DEX activities. Although their official websites profess compliance with sanctions and implement front-end filters [17], these measures can be circumvented through direct on-chain contract invocations via CLT, and finally make off-chain application layer censorship ineffective. Consequently, large volumes of TC-derived funds ($I_v = 289,901.92$ ETH) still flowed into platforms. Specifically, we observed that 102,928.18 ETH (impurity score $\varphi \approx 93.04\%$) channeled through Uniswap and 77,481.93 ETH ($\varphi \approx 95.95\%$) processed via 1inch.

Freezable vs. Non-Freezable Tokens. After analyzing the transaction logs and account state differences, we found that TC withdrawers frequently convert their assets into stablecoins (USDT-22.61%, USDC-12.12%, and DAI-11.12%) or wrapped tokens (WETH-36.03% and WBTC-3.85%) for greater fungibility and cross-chain interoperability. These conversions from highly tainted ETH inputs result in comparably high impurity scores across all tokens. It is worth noting that USDT (Tether [32]) and USDC (Circle [9]) are centrally issued by U.S.-based companies. Their token contracts have explicit blacklist mechanisms, `addBlackList` (`0x0ecb93c0`) and `blackList` (`0xf9f92be4`), theoretically allowing privileged addresses to freeze assets held by sanctioned entities. However, our data showed no statistically significant difference in token selection patterns between potentially freezable tokens (USDT, USDC) and non-freezable alternatives (WETH, WBTC, DAI). This suggests that the theoretical risk of asset freezing does not substantially influence withdrawers' token selection strategies, highlighting a significant gap between technical capability and operational enforcement.

5.2.3 Additional Analysis of Service Usages. Due to the space constraint, detailed analyses of (i) centralized exchanges and (ii) privacy-enhancing tools are moved to Appendix C.

6 Discussion

Sanction enforcement on blockchains is inherently a *Cat-and-Mouse* game. As regulators develop detection and enforcement mechanisms, adversaries continuously adapt with sophisticated evasion strategies. For ethical considerations, no personally off-chain identifiable information is used and no actionable specific for circumvention is revealed. We carefully calibrated our disclosures which indicate that the current censorship framework has structural limitations. Here we also provide practical recommendations for compliance teams and regulated blockchain ecosystem developers: (i) cut policy-to-enforcement latency using fast off-chain enforcement first while updating a permanent on-chain state, (ii) provide a safe and user-initiated “burn” mechanism, so users accidentally exposed to tainted assets can destroy them, and (iii) standardize cross-chain bridge protocols so hops are auditable end-to-end.

7 Related Work

Our work builds upon previous research on blockchain transaction analysis and privacy mechanisms. Prior works by Wu et al. [43] and Gomez et al. [15] established graph-based approaches for tracking malicious funds from security incidents, while Lin et al. [21] proposed density-based detection of money laundering patterns on Ethereum. Anonymity analyses in [7, 11, 18, 39, 40] evaluated the capability of privacy-enhancing protocols using heuristic-based or machine-learning-based approaches. Yousef et al. [44] first identified the complexity of cross-chain tracing between blockchains that have anonymous mechanism, while our research implements custom parsers for major bridge protocols.

Zola et al. [48] first showed the ineffectiveness of sanctions on Bitcoin, but limited their analysis at 2-step transaction graphs. Möser et al. [23] also proposed a risk scoring mechanism on Bitcoin. However, the account model of Ethereum and the capability of smart contracts bring more mechanisms for both censorship and obfuscation. Wahrstätter et al. [37] documented censorship at the block production level, but lacked downstream money flow analysis. Our work provides the first comprehensive empirical analysis of sanction effectiveness on Ethereum, introducing a quantitative framework that evaluates both direct compliance and subsequent circumvention patterns with high precision.

8 Conclusion

This paper presents the first quantitative evaluation of blockchain sanctions effectiveness. We use TC as a case study, analyzing 957 days of Ethereum data. Our findings reveal that while general TC deposit volume decreased by 71.03% during sanctions, malicious actors continued exploiting TC in 78.33% of security incidents. This continued exploitation is facilitated by inconsistent consensus layer enforcement and sophisticated evasion techniques, including specific behavior patterns and strategic service selection. These insights provide concrete recommendations for regulatory authorities and compliance teams, helping them balance privacy concerns with financial oversight requirements using quantitative risk frameworks.

References

- [1] 1inch Network. 2025. Official Website. <https://1inch.com/> Accessed: 2025-10-06.
- [2] André Augusto, Rafael Belchior, Miguel Correia, André Vasconcelos, Luyao Zhang, and Thomas Hardjono. 2024. SoK: Security and Privacy of Blockchain Interoperability. In *IEEE Symposium on Security and Privacy, SP 2024, San Francisco, CA, USA, May 19-23, 2024*. IEEE, San Francisco, CA, USA, 3840–3865. doi:10.1109/SP54263.2024.00255
- [3] Osato Avan-Nomayo. 2022. Infura and Alchemy are now blocking access to Tornado Cash. <https://www.theblock.co/post/162402/infura-and-alchemy-blocking-access-to-tornado-cash> Accessed: 2025-10-06.
- [4] Christian Badertscher, Mahdi Sedaghat, and Hendrik Waldner. 2024. Unlinkable Policy-Compliant Signatures for Compliant and Decentralized Anonymous Payments. *Proc. Priv. Enhancing Technol.* 2024, 4 (2024), 226–267. doi:10.56553/POPETS-2024-0115
- [5] Austin R. Benson, David F. Gleich, and Jure Leskovec. 2016. Higher-order organization of complex networks. *Science* 353, 6295 (2016), 163–166. arXiv:<https://www.science.org/doi/pdf/10.1126/science.aad9029> doi:10.1126/science.aad9029
- [6] Binance. 2025. Official Website. <https://www.binance.com/> Accessed: 2025-10-06.
- [7] Anders Brownworth, Jon Durfee, Michael Junho Lee, and Antoine Martin. 2024. *Regulating Decentralized Systems: Evidence from Sanctions on Tornado Cash*. Staff Reports 1112. Federal Reserve Bank of New York. doi:10.59576/sr.1112
- [8] Chainalysis. 2025. Free Cryptocurrency Sanctions Screening Tools. <https://www.chainalysis.com/free-cryptocurrency-sanctions-screening-tools/> Accessed: 2025-10-06.
- [9] Circle. 2025. Official Website. <https://www.circle.com/> Accessed: 2025-10-06.
- [10] Coinbase. 2025. Official Website. <https://www.coinbase.com/> Accessed: 2025-10-06.
- [11] Hanbiao Du, Zheng Che, Meng Shen, Liehuang Zhu, and Jiankun Hu. 2024. Breaking the Anonymity of Ethereum Mixing Services Using Graph Feature Learning. *IEEE Trans. Inf. Forensics Secur.* 19 (2024), 616–631. doi:10.1109/TIFS.2023.3326984
- [12] Elliptic. 2025. The largest theft in history - following the money trail from the Bybit Hack. <https://www.elliptic.co/blog/bybit-hack-largest-in-history> Accessed: 2025-10-06.
- [13] Ethereum Foundation. 2025. ERC-20 Token Standard. <https://ethereum.org/en/developers/docs/standards/tokens/erc-20/> Accessed: 2025-10-06.
- [14] Financial Action Task Force. 2023. Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html> Accessed: 2025-10-06.
- [15] Gibran Gómez, Pedro Moreno-Sanchez, and Juan Caballero. 2022. Watch Your Back: Identifying Cybercrime Financial Relationships in Bitcoin through Back-and-Forth Exploration. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*, Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi (Eds.). ACM, Los Angeles, CA, USA, 1291–1305. doi:10.1145/3548606.3560587
- [16] Yogita Khatri. 2022. Aave says on-chain wallet address censorship will require DAO consensus. <https://www.theblock.co/post/163586/aave-says-on-chain-wallet-address-censorship-will-require-dao-consensus> Accessed: 2025-10-06.
- [17] Yogita Khatri. 2022. Uniswap Labs now blocks certain crypto wallets from its app's frontend. <https://www.theblock.co/post/143036/uniswap-labs-now-blocks-crypto-wallets-frontend> Accessed: 2025-10-06.
- [18] Alex Márk Kovács and István András Seres. 2024. Anonymity Analysis of the Umbra Stealth Address Scheme on Ethereum. In *Companion Proceedings of the ACM on Web Conference 2024, WWW 2024, Singapore, Singapore, May 13-17, 2024*, Tat-Seng Chua, Chong-Wah Ngo, Roy Ka-Wei Lee, Ravi Kumar, and Hady W. Lauw (Eds.). ACM, Singapore, Singapore, 1768–1775. doi:10.1145/3589335.3651963
- [19] Aztec Labs. 2023. Sunsetting Aztec Connect. <https://medium.com/aztec-protocol/sunsetting-aztec-connect-a786edce5cae> Accessed: 2025-10-06.
- [20] Ya-Nan Li, Tian Qiu, and Qiang Tang. 2024. Pisces: Private and Compliant Cryptocurrency Exchange. In *31st Annual Network and Distributed System Security Symposium, NDSS 2024, San Diego, California, USA, February 26 - March 1, 2024*, The Internet Society, San Diego, California, USA, 1–20. <https://www.ndss-symposium.org/ndss-paper/pisces-private-and-compliant-cryptocurrency-exchange/>
- [21] Dan Lin, Jiajing Wu, Yunmei Yu, Qishuang Fu, Zibin Zheng, and Changlin Yang. 2024. DenseFlow: Spotting Cryptocurrency Money Laundering in Ethereum Transaction Graphs. In *Proceedings of the ACM on Web Conference 2024, WWW 2024, Singapore, May 13-17, 2024*, Tat-Seng Chua, Chong-Wah Ngo, Ravi Kumar, Hady W. Lauw, and Roy Ka-Wei Lee (Eds.). ACM, Singapore, Singapore, 4429–4438. doi:10.1145/3589334.3645692
- [22] Muhammad Izhar Mehar, Charles Louis Shier, Alana Giambattista, Elgar Gong, Gabrielle Fletcher, Ryan Sanayhie, Henry M. Kim, and Marek Laskowski. 2019. Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack. *J. Cases Inf. Technol.* 21, 1 (2019), 19–32. doi:10.4018/JCIT.2019010102
- [23] Malte Möser, Rainer Böhme, and Dominic Breuker. 2014. Towards Risk Scoring of Bitcoin Transactions. In *Financial Cryptography and Data Security - FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, March 7, 2014, Revised Selected Papers (Lecture Notes in Computer Science, Vol. 8438)*. Springer, Christ Church, Barbados, 16–32. doi:10.1007/978-3-662-44774-1_2
- [24] Satoshi Nakamoto. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. White Paper. Self-published. 1–9 pages. <https://bitcoin.org/bitcoin.pdf>
- [25] Rekt News. 2022. Nomad Bridge - Rekt. <https://rekt.news/nomad-rekt/> Accessed: 2025-10-06.
- [26] Rekt News. 2023. HECO Bridge - Rekt. <https://rekt.news/heco-hx-rekt/> Accessed: 2025-10-06.
- [27] Rekt News. 2024. Orbit Bridge - Rekt. <https://rekt.news/orbit-bridge-rekt/> Accessed: 2025-10-06.
- [28] Vladimir Popov, Mikhail Krupin, Andrew Gross, and Georgi Koreli. 2024. Blockchain Privacy and Self-regulatory Compliance: Methods and Applications. <https://ssrn.com/abstract=4787693> SSRN preprint 4787693.
- [29] Kaihua Qin, Liyi Zhou, and Arthur Gervais. 2022. Quantifying Blockchain Extractable Value: How dark is the forest?. In *43rd IEEE Symposium on Security and Privacy, SP 2022, San Francisco, CA, USA, May 22-26, 2022*. IEEE, San Francisco, CA, USA, 198–214. doi:10.1109/SP46214.2022.9833734
- [30] RAILGUN. 2025. Wiki. <https://docs.railgun.org/wiki> Accessed: 2025-10-06.
- [31] Secret. 2025. Secret Tunnel. <https://tunnel.scrtnetwork/> Accessed: 2025-10-06.
- [32] Tether. 2025. Official Website. <https://tether.to/> Accessed: 2025-10-06.
- [33] Umbra. 2025. Official Website. <https://app.umbra.cash/> Accessed: 2025-10-06.
- [34] Uniswap. 2025. Official Website. <https://app.uniswap.org/> Accessed: 2025-10-06.
- [35] U.S. Department of the Treasury. 2022. U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash. <https://home.treasury.gov/news/press-releases/jy0916> Accessed: 2025-10-06.
- [36] U.S. Department of the Treasury. 2025. Tornado Cash Delisting. <https://home.treasury.gov/news/press-releases/sb0057> Accessed: 2025-10-06.
- [37] Anton Wahrstätter, Jens Ernstberger, Aviv Yaish, Liyi Zhou, Kaihua Qin, Taro Tsuchiya, Sebastian Steinhorst, Davor Svetinovic, Nicolas Christin, Mikolaj Barczentewicz, and Arthur Gervais. 2024. Blockchain Censorship. In *Proceedings of the ACM on Web Conference 2024, WWW 2024, Singapore, May 13-17, 2024*. ACM, Singapore, Singapore, 1632–1643. doi:10.1145/3589334.3645431
- [38] Anton Wahrstätter, João Gomes Jr., Sajjad Khan, and Davor Svetinovic. 2023. Improving Cryptocurrency Crime Detection: CoinJoin Community Detection Approach. *IEEE Trans. Dependable Secur. Comput.* 20, 6 (2023), 4946–4956. doi:10.1109/TDSC.2023.3238412
- [39] Anton Wahrstätter, Alfred Taudes, and Davor Svetinovic. 2024. Reducing Privacy of CoinJoin Transactions: Quantitative Bitcoin Network Analysis. *IEEE Trans. Dependable Secur. Comput.* 21, 5 (2024), 4543–4558. doi:10.1109/TDSC.2024.3353803
- [40] 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 2023, Austin, TX, USA, 30 April 2023 - 4 May 2023*. ACM, Austin, TX, USA, 2022–2032. doi:10.1145/3543507.3583217
- [41] Sam Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J. Knottenbelt. 2022. SoK: Decentralized Finance (DeFi). In *Proceedings of the 4th ACM Conference on Advances in Financial Technologies, AFT 2022, Cambridge, MA, USA, September 19-21, 2022*, Maurice Herlihy and Neha Narula (Eds.). ACM, Cambridge, MA, USA, 30–46. doi:10.1145/3558535.3559780
- [42] Gavin Wood. 2025. *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. Yellow Paper. Ethereum Project. 1–42 pages. <https://ethereum.github.io/yellowpaper/paper.pdf> Shanghai Version efc5f9a (2025-02-04).
- [43] Jiajing Wu, Dan Lin, Qishuang Fu, Shuo Yang, Ting Chen, Zibin Zheng, and Bowen Song. 2024. Toward Understanding Asset Flows in Crypto Money Laundering Through the Lenses of Ethereum Heists. *IEEE Trans. Inf. Forensics Secur.* 19 (2024), 1994–2009. doi:10.1109/TIFS.2023.3346276
- [44] Haaron Yousaf, George Kappos, and Sarah Meiklejohn. 2019. Tracing Transactions Across Cryptocurrency Ledgers. In *28th USENIX Security Symposium, USENIX Security 2019, Santa Clara, CA, USA, August 14-16, 2019*, Nadia Heninger and Patrick Traynor (Eds.). USENIX Association, Santa Clara, CA, USA, 837–850. <https://www.usenix.org/conference/usenixsecurity19/presentation/yousaf>
- [45] Zhao Zhang, Chunxiang Xu, and Yunxia Han. 2024. Privacy-Preserving Cryptocurrency With Threshold Authentication and Regulation. *IEEE Trans. Inf. Forensics Secur.* 19 (2024), 6620–6635. doi:10.1109/TIFS.2024.3419694
- [46] Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. 2023. SoK: Decentralized Finance (DeFi) Attacks. In *44th IEEE Symposium on Security and Privacy, SP 2023, San Francisco, CA, USA, May 21-25, 2023*. IEEE, San Francisco, CA, USA, 2444–2461. doi:10.1109/SP46215.2023.10179435
- [47] zkBob. 2025. Official Website. <https://www.zkbob.com/> Accessed: 2025-10-06.
- [48] Francesco Zola, Jon Ander Medina, and Raul Orduna. 2024. Assessing the Impact of Sanctions in the Crypto Ecosystem: Effective Measures or Ineffective Determinants?. In *Computer Security, ESORICS 2024 International Workshops - DPM, CBT, and CyberICPS, Bydgoszcz, Poland, September 16-20, 2024, Revised Selected Papers, Part I (Lecture Notes in Computer Science, Vol. 15263)*. Springer, Bydgoszcz, Poland, 292–308. doi:10.1007/978-3-031-82349-7_20

A Algorithm

In this section, we provide the algorithm for updating the impurity score of each affected address as sanctioned assets propagate.

Algorithm 1: Impurity Updating Algorithm

Data: Blockchain states $\{(s_0, s_1, \dots, s_{n-1}) \mid s \in \mathcal{S}\}$, Valid Ethereum address set $ADDR$, Sanctioned address set $ADDR_{sanction} \subset ADDR$, First state after sanctions s_{OFAC}

Result: Historical records of for $\langle \mathcal{I}, \mathcal{B}, \varphi \rangle$ all involved addresses at each state s where \mathcal{I} is the impurity amount, \mathcal{B} is the balance amount, and φ is the impurity score (cf. Section 3.3)

- 1 **Initialization:**
- 2 $s_0 = s_{OFAC}$;
- 3 **for each address** $addr \in ADDR_{sanction}$ **do**
- 4 Set $\mathcal{I}(s_{OFAC}, addr) = \mathcal{B}(s_{OFAC}, addr)$;
- 5 **end**
- 6 **for each address** $addr \notin ADDR_{sanction}$ **do**
- 7 Set $\mathcal{I}(s_{OFAC}, addr) = 0$;
- 8 **end**
- 9 **State Transition and Attribute Update:**
- 10 **for** $i \in [0, n-1]$ **do**
- 11 Let balance state transition $\mathcal{T}_{\mathcal{B}}(s_i, op_{\mathcal{B}}) \rightarrow s_{i+1}$ where affected addresses and amounts are extracted from the operation $op_{\mathcal{B}}$:
- 12 $op_{\mathcal{B}} \rightarrow \{\langle addr_{from}, a_{sent} \rangle, \langle addr_{to}, a_{received} \rangle\}$;
- 13 **Update:**
- 14 $\mathcal{I}(s_{i+1}, addr_{from}) = \mathcal{I}(s_i, addr_{from}) - \left\lceil \frac{a_{sent} \cdot \mathcal{I}(s_i, addr_{from})}{\mathcal{B}(s_i, addr_{from})} \right\rceil$;
- 15 **if** address $addr_{to} \in ADDR_{sanction}$ **then**
- 16 $\mathcal{I}(s_{i+1}, addr_{to}) = \mathcal{B}(s_{i+1}, addr_{to})$;
- 17 **else**
- 18 $\mathcal{I}(s_{i+1}, addr_{to}) = \mathcal{I}(s_i, addr_{to}) + \left\lceil \frac{a_{received} \cdot \mathcal{I}(s_i, addr_{from})}{\mathcal{B}(s_i, addr_{from})} \right\rceil$;
- 19 **end**
- 20 **for each address** $addr \in \{addr_{from}, addr_{to}\}$ **do**
- 21 **if** $\mathcal{B}(s_{i+1}, addr) \neq 0$ **then**
- 22 $\varphi(s_{i+1}, addr) = \frac{\mathcal{I}(s_{i+1}, addr)}{\mathcal{B}(s_{i+1}, addr)}$;
- 23 **else**
- 24 $\varphi(s_{i+1}, addr) = 0$;
- 25 **end**
- 26 **Store** $\langle \mathcal{I}(s_{i+1}, addr), \mathcal{B}(s_{i+1}, addr), \varphi(s_{i+1}, addr) \rangle$
- 27 **end**
- 28 **end**

B Impossibility of Binary Classification Mechanism

We provide an informal argument demonstrating why naïve binary classification system inevitably fails when faced with dusting attacks, thereby necessitating the continuous, quantitative impurity metrics described in Section 3.3. We also discuss the effectiveness of other classification mechanisms in this section.

Let $ADDR$ be the set of all valid addresses on the blockchain, and define a general binary classification function:

$$C : ADDR \rightarrow \{0, 1\} \quad (1)$$

where $C(addr) = 0$ means address $addr$ is “clean” and $C(addr) = 1$ means $addr$ is “tainted.” Initially, sanctioned addresses are tainted: $C(addr) = 1$ if $addr \in ADDR_{sanction}$, otherwise $C(addr) = 0$.

For a binary classification system to be useful in blockchain analysis, it must satisfy two key properties:

- (1) **Propagation Property:** There must exist some mechanism by which taint propagates from sanctioned addresses to their transaction partners. Without this property, the classification would fail to identify entities interacting with sanctioned addresses.
- (2) **Decidability Property:** The classification must be computationally decidable in reasonable time, meaning there exists an efficient algorithm to determine whether an address is tainted.

Any binary classification system satisfying these minimal properties must implement some form of propagation rule. While the specific rule may vary, it must establish conditions under which an address receiving funds from a tainted address also becomes tainted. We denote this general propagation condition:

$$\mathcal{P}(s, addr_{from}, addr_{to}, v) \quad (2)$$

which evaluates to true when a transaction from $addr_{from}$ to $addr_{to}$ with a value v at the blockchain state s causes taint to propagate.

A dusting attack occurs when an attacker controlling a tainted address $addr_s$ (where $C(addr_s) = 1$) creates transactions

$$tx_i : addr_s \rightarrow addr_i \implies \mathcal{P}(s, addr_s, addr_i, v_i) = True \quad (3)$$

with values v_i deliberately chosen to ensure taint is propagated for many strategically selected target addresses $addr_i$. Let $G(s) \subseteq ADDR$ be the set of all tainted addresses at blockchain state s , with $G(s_{OFAC}) = ADDR_{sanctioned}$ initially. After each dusting attack, $G(s')$ expands to include the targeted addresses.

The fundamental limitation of naïve binary classification system is that it cannot distinguish between significant and trivial taint exposure: an address is either tainted or not. This creates a vulnerability that can be exploited through strategic dusting: a small-value dusting transaction can instantly taint high-value addresses, creating an amplification effect. From our empirical data in Section 4.3.3, just 12.00 ETH in dusting transactions tainted over 9,034,251.58 ETH, an amplification factor exceeding 750,000×

We denote the total value (balance amount) held by tainted addresses flagged by naïve binary classification mechanism as

$$V_{\text{tainted}}(s) = \sum_{addr \in G(s)} \mathcal{B}(s, addr) \quad (4)$$

and denote the total value held by entire addresses as

$$V_{\text{entire}}(s) = \sum_{addr \in ADDR} \mathcal{B}(s, addr) \quad (5)$$

Under propagation rules satisfying the minimal properties, strategic dusting attacks to naïve binary classification system can drive

$$\lim_{s \rightarrow \infty} \frac{|G(s)|}{|ADDR|} \rightarrow 1 \quad (6)$$

$$\lim_{s \rightarrow \infty} V_{\text{tainted}}(s) \rightarrow V_{\text{entire}}(s)$$

When most addresses become tainted, the system cannot distinguish genuine risk from dust-induced taint, rendering the classification meaningless. Services implementing naïve binary classification face an inevitable denial-of-service vulnerability: either block all tainted addresses (causing service failure as $|G(s)|$ grows) or ignore the classification (rendering it useless). This fundamental limitation was observed with services like Aave Front-End [16].

The failure of naïve binary classification system directly necessitates a continuous metric such as our impurity score $\varphi(s, addr) \in [0, 1]$. Under dusting attacks, naïve binary classification marks all recipients as completely tainted, while with our continuous metric, $\varphi(s, addr_i) = \frac{I(s, addr_i)}{B(s, addr_i)} \approx 0$ for addresses with large balances receiving small dust amounts. This allows the system to distinguish between seriously tainted addresses and those with negligible exposure, preserving the utility of the classification system against dusting attacks. Our impurity updating algorithm in Appendix A implements precisely this approach.

In the following of this section, we will discuss the effectiveness of other classification rules from aspect of attackers and evaders:

- (1) **For Time-Based Rules** (e.g., taint expires after time t): (i) Attackers can refresh the dusting attack periodically; (ii) Evaders can bypass the detection via a waiting time longer than t .
- (2) **For Hop-Based Rules** (e.g., taint if receiving from any address that is within h hops of tainted addresses): (i) Attackers can directly issue transactions from tainted addresses to target addresses in 1 hop; (ii) Evaders cannot bypass unless they can move assets through addresses or services that reset or do not share the hop count, and eventually exceed the hop limit h .
- (3) **For Value-Threshold Rules** (e.g., taint if receiving more than θ value from sanctioned addresses):
 - *If the detection only check the value in target addresses:* (i) Attackers can simply send $v > \theta$ in one transaction or analyze on-chain data to send more precision value; (ii) Evaders cannot bypass unless they send the amount exceeding θ to a designated burnt address or divide their balance through services do not apply this detection mechanism.
 - *If the detection also check the value in transactions:* (i) Attackers can divide $v > \theta$ into several transactions and send them sequentially; (ii) Evaders' operations do not change.
 - *If the detection even check the value in source addresses:* (i) Attackers can prepare several addresses totally holding $v > \theta$; (ii) Evaders' operations do not change.
- (4) **For Percentage-Threshold Rules** (e.g., taint if receiving more than $\theta\%$ of balance from sanctioned addresses):
 - *If the detection only check the percentage in target addresses:* (i) Attackers can simply send $v > \theta\% \times B(s, addr_i)$ in one transaction or analyze on-chain data to send more precision value; (ii) Evaders can supply their account with enough "clean" amount to decrease the percentage $\varphi < \theta\%$. This can be done by direct transfer or using balance manipulation (e.g., addresses can drain and restore their balance using services do not apply this detection mechanism, for example, flash loans via DEX and coin mixing via privacy tools).
 - *If the detection also check the percentage in transactions:* (i) Attackers can prepare one or more accounts where each account is under the threshold $\varphi < \theta\%$ and collectively send $v > \theta\% \times B(s, addr_i)$; (ii) Evaders' operations do not change.
 - *If the detection even check the percentage in source addresses:* Both attackers' and evaders operations do not change.

To conclude, naïve binary rules are fundamentally untenable under dusting attacks. We advocate continuous metrics with calibrated thresholds and contextual checks (value, time, hops) to enable enforcement that remains robust to dust and evasion tactics.

C More Analyses of Service Usage

C.1 Centralized Exchanges

CEXs serve as significant on- and off-ramps which bridge the gap between digital and fiat currencies. Their ability to convert large sums of crypto into fiat and vice versa makes them pivotal in off-chain AML and CTF processes. Despite the potential exposure to increased surveillance risks, CEXs remain a frequent choice (10.37%) among TC withdrawers.

KYC vs. Non-KYC Compliance. A CEX that follows KYC compliance typically mandates identity verification procedures, such as submitting government-issued identification, to fulfill regulatory requirements. Users are generally required to pass these checks to deposit or withdraw fiat currencies, and often when transacting significant volumes of assets. However, in practice, many exchanges, which are nominally KYC-compliant, only require partial identity verification, usually triggered when users interact with fiat gateways. In these cases, users who fail to provide the necessary documentation may face service restrictions or be forced into refund mechanisms, particularly when their behavior raises compliance risks (e.g., as observed on platforms like ChangeNOW⁴ and SimpleSwap⁵). To better reflect real-world behavior, we extend the definition of non-KYC-compliant CEXs to include those platforms that do not require personal information for account registration and for crypto-to-crypto transactions. In such settings, linkabilities (i) between deposit and withdrawal interactions with CEX is broken when analyzing on-chain information, and (ii) between CEX's internal accounts and off-chain user identifiers is also broken. As a result, once funds move through these non-KYC-compliant CEXs, tracing them becomes highly improbable unless these exchanges record the transaction history and are willing to share them.

Impurity Volume, Impurity Score and Active Spans. We analyzed 16 CEXs in total, 8 KYC-compliant and 8 non-KYC-compliant, focusing on three key metrics: impurity volume I_v , impurity score φ , and active spans (the number of days on which deposits with $\varphi > \Phi$ are detected). Figure 8 and Table 4 summarize our findings. Several non-KYC-complaint CEXs (e.g., ChangeNOW, FixedFloat, and eXch, highlighted in Table 4) exhibit either a larger number of active days or a higher impurity volume compared to top-tier KYC-compliant CEXs (e.g., Coinbase and KuCoin). We also observed higher impurity scores for deposits into non-KYC-compliant CEXs relative to their KYC-compliant counterparts. The lack of stringent identity checks reduces the risk of immediate account suspension or asset freezing, making these Non-KYC platforms more attractive.

Notably, U.S.-based platforms (i.e., Coinbase and Kraken) demonstrate relatively low impurity amounts and scores. This pattern is likely attributable to strict regulatory under the OFAC sanctions targeting TC, which encourages stricter transaction screening and discourages high-risk deposits. Conversely, due to the complexity of cross-jurisdictional enforcement, some KYC-complaint CEX based outside the U.S. (e.g., OKX and Bybit) may not follow the specific OFAC sanctions. Therefore, their impurity scores resembled those of non-KYC-compliant platforms, even though their official websites claim compliance with AML and CTF policies.

⁴<https://changenow.io/en/terms-of-use/changenow-terms>

⁵<https://simpleswap.io/terms-of-service>

C.2 Privacy-Enhancing Tools

Multiple privacy tools have emerged within the blockchain ecosystem, each employing distinct techniques to break the linkability between transactions. An advanced strategy observed in privacy-focused activities involves the sequential use of multiple privacy protocols, either at different stages of the transaction lifecycle or across different blockchains.

Reuse of Tornado Cash. TC itself also serves as a destination for assets previously withdrawn from its own pools. Our analysis identifies two prevalent patterns of reuse: (i) *Self-Loop*, where users withdraw funds from TC and redeposit nearly identical amounts back into TC, sometimes routing these assets through one or more intermediate addresses; and (ii) *Mix-up*, where withdrawn assets from TC are combined with external funds, thereby reducing the overall impurity score. In total, we detect 54,249.31 ETH involved in such reuse cycles, resulting in an impurity score $\varphi \approx 65.45\%$. Importantly, rapid increases in deposit volume that coincide with a sudden decrease in impurity scores may correlate with security incidents. Specifically, attackers initially seed an address with minor deposits from TC and later use the same channel to launder significant amounts of stolen crypto assets back into TC. This pattern aligns closely with 29 cases documented in Section 4.3.2.

Private Proofs of Innocence in Railgun. Railgun [30] is an Ethereum-based privacy solution that features a mechanism known as *Private Proofs of Innocence*. Deposits into newly created Railgun shielding tokens must wait for one hour to successfully pass an innocence proof before performing any interaction beyond an immediate refund to the originating address. If this proof fails, the funds are automatically returned to their source.

We observe the evolving adoption of this mechanism since its activation in November 2023 [28]. Interestingly, the first detected TC-related refund occurred much later, in June 2024, involving account $0x80Df\dots B1b0$ at Block 20178593. Prior to this event, we identify transfers totaling 15,780.31 ETH, with impurity score $\varphi \approx 99.35\%$, directly from TC into Railgun that did not trigger innocence-proof mechanisms. This finding indicates that Railgun initially allows direct inflows from TC without imposing additional restrictions. Following this specific incident, the Railgun protocol begins to reject funds derived from TC. Nonetheless, there are over 2,320.55 ETH deposited into Railgun after the first refund, but among them only around 506.75 ETH (21.84%) are refunded. This indicates that this mechanism is not effective and users can still successfully circumvent this restriction.

Other Privacy-Preserving Tools. Umbra [18] leverages stealth addresses to conceal recipient identities. Our analysis identifies 6,286.13 ETH transferred from TC into Umbra, carrying a notable impurity score $\varphi \approx 93.07\%$, underscoring its steady adoption. In contrast, Aztec Connect, previously a prominent Ethereum-based privacy solution with inflows of 2,244.93 ETH at impurity score $\varphi \approx 95.71\%$, ceased operations on March 31, 2023 [19], consequently diminishing its latest relevance. Similarly, another deprecated tool is the Secret Network: Bridge, which received 681.16 ETH with impurity score $\varphi \approx 98.71\%$. Its successor, Secret Tunnel powered by Axelar [31], continues providing privacy within Secret Network, keeping on-chain transactions and balances fully confidential.

D Supplementary Experiment Results

Table 3: A Typical Test-Depositing Sequence from Transaction History of Address $0x0E0E\dots 3143$, who contentiously deposited into services with censorship mechanisms (i.e., KuCoin, a KYC-compliant centralized exchange).

Date Time (UTC)	From	Dir	To	Amount (ETH)	Txn Fee (ETH)
2023-01-13 03:06:47	$0x0E0E\dots 3143$	OUT	KuCoin	11.99969862	0.00033165
2023-01-13 02:28:59	$0x4BaC\dots 671F$	IN	$0x0E0E\dots 3143$	12.00000000	0.00072839
2023-01-10 12:06:35	$0x0E0E\dots 3143$	OUT	KuCoin	11.99959166	0.00040296
2023-01-10 11:21:35	$0xC728\dots D5A1$	IN	$0x0E0E\dots 3143$	12.00000000	0.00031041
2023-01-09 10:07:11	$0x0E0E\dots 3143$	OUT	KuCoin	10.59799828	0.00034590
2023-01-09 10:01:11	$0x2c03\dots c42D$	IN	$0x0E0E\dots 3143$	10.59838156	0.00031670
2023-01-08 12:06:35	$0x0E0E\dots 3143$	OUT	KuCoin	11.99973839	0.00030656
2023-01-08 09:49:11	$0x2c03\dots c42D$	IN	$0x0E0E\dots 3143$	12.00000000	0.00037588
2023-01-01 14:06:35	$0x0E0E\dots 3143$	OUT	KuCoin	0.09968959	0.00026543
2023-01-01 13:19:11	$0x2C48\dots 088B$	IN	$0x0E0E\dots 3143$	0.10000000	0.00031183

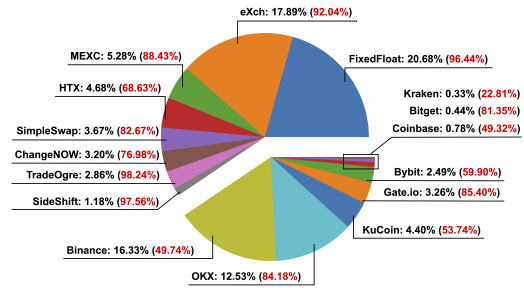


Figure 8: The distribution of tainted funds deposited into selected CEXs, categorized by 8 Non-KYC platforms (up) and 8 KYC-compliant ones (down). The black percentages are proportions of impurity volumes into these platforms, while the red percentages reflect the corresponding impurity scores.

Table 4: Active Span and Impurity Volume of CEX

CEX	Active Span (Days)	Impurity Volume I_v
Binance	822 (85.89%)	20,097.20 ETH (16.33%)
ChangeNOW	802 (83.80%)	3,942.41 ETH (03.20%)
FixedFloat	702 (73.35%)	25,450.88 ETH (20.68%)
eXch	609 (63.64%)	22,018.98 ETH (17.89%)
Coingecko	584 (61.02%)	960.88 ETH (00.78%)
KuCoin	581 (60.71%)	5,422.31 ETH (04.40%)
MEXC	557 (58.20%)	6,504.51 ETH (05.28%)
OKX	500 (52.25%)	15,420.37 ETH (12.53%)
Bybit	430 (44.93%)	3,064.73 ETH (02.49%)
SideShift	286 (29.89%)	1,452.07 ETH (01.18%)
HTX	254 (26.54%)	5,760.38 ETH (04.68%)
Kraken	214 (22.36%)	408.93 ETH (00.33%)
Gate.io	203 (21.21%)	4,007.67 ETH (03.26%)
Bitget	115 (12.02%)	546.41 ETH (00.44%)
SimpleSwap	114 (11.91%)	4,516.20 ETH (03.67%)
TradeOgre	110 (11.49%)	3,525.23 ETH (02.86%)
Total	957 (100%)	123,099.20 ETH (100%)