Towards Understanding and Analyzing Instant Cryptocurrency Exchanges

YUFENG HU, Zhejiang University, China
YINGSHI SUN, Zhejiang University, China
LEI WU*, Zhejiang University, China
YAJIN ZHOU, Zhejiang University, China
RUI CHANG, Zhejiang University, China

In this paper, we examine a novel category of services in the blockchain ecosystem termed **Instant Cryptocurrency Exchange (ICE) services**. Originally conceived to facilitate cross-chain asset transfers, ICE services have, unfortunately, been abused for money laundering activities due to two key features: the absence of a strict Know Your Customer (KYC) policy and incomplete on-chain data of user requests. As centralized and non-transparent services, ICE services pose considerable challenges in the tracing of illicit fund flows laundered through them.

Our comprehensive study of ICE services begins with an analysis of their features and workflow. We classify ICE services into two distinct types: *Standalone* and *Delegated*. We then perform a measurement analysis of ICE services, paying particular attention to their usage in illicit activities. Our findings indicate that a total of $12,473,290 illegal funds have been laundered through ICE services, and 432 malicious addresses were initially funded by ICE services. Based on the insights from measurement analysis, we propose a matching algorithm designed to evaluate the effectiveness of ICE services in terms of efficiency and prevention of traceability. Our evaluation reveals that 92% of the user requests analyzed were completed in less than three minutes, underscoring the efficiency of ICE services. In addition, we demonstrate that the algorithm is effective in tracing illicit funds in situations where ICE services are used in malicious activities. To engage the community, the entire dataset used in this study is open-source.

CCS Concepts: • **Security and privacy → Pseudonymity, anonymity and untraceability**.

Additional Key Words and Phrases: Instant Cryptocurrency Exchanges, blockchain, anti-money laundering

ACM Reference Format:
Yufeng Hu, Yingshi Sun, Lei Wu, Yajin Zhou, and Rui Chang. 2024. Towards Understanding and Analyzing Instant Cryptocurrency Exchanges. *Proc. ACM Meas. Anal. Comput. Syst.* 8, 3, Article 48 (December 2024), 24 pages. https://doi.org/10.1145/3700430

1 Introduction

The blockchain ecosystem has experienced rapid evolution in recent years. The invention of Ethereum [48] laid the foundation for smart contracts through Ethereum Virtual Machine (EVM) [19],

*Corresponding Author: Lei Wu (lei_wu@zju.edu.cn).

Authors' Contact Information: Yufeng Hu, yufenghu@zju.edu.cn, Zhejiang University, Hangzhou, China; Yingshi Sun, yufenghu@zju.edu.cn, Zhejiang University, Hangzhou, China; Lei Wu, lei_wu@zju.edu.cn, Zhejiang University, Hangzhou, China; Yajin Zhou, yajin_zhou@zju.edu.cn, Zhejiang University, Hangzhou, China; Rui Chang, crix1021@zju.edu.cn, Zhejiang University, Hangzhou, China.

ACM 2476-1249/2024/12-ART48
https://doi.org/10.1145/3700430

significantly improving the diversity of blockchain applications. Consequently, numerous public blockchains, such as Binance Smart Chain [3], Polygon [42], and Arbitrum [1], have emerged as contenders, offering compatibility with Ethereum smart contracts and contributing to the growing landscape of the blockchain ecosystem.

In an ecosystem with multiple blockchains, the need for asset transfer and exchange across different chains, known as *bridging* [14], becomes evident. Traditionally, there are two commonly used methods for bridging assets across chains. The first method involves centralized exchanges (CEXes), such as Binance [2] and Coinbase [12]. The second method relies on smart contract-based bridges, such as Poly Network [26] and Stargate [17]. However, both methods are impeded by efficiency and privacy issues. Bridging through CEXes can be cumbersome, typically requiring users to deposit assets from source chains into CEXes, initiate trades to target assets, and then withdraw the assets to target chains. Using CEXes for bridging also requires registration and strict verification of user identity information. On the other hand, smart contract-based bridges often take hours or even days [5, 44] to bridge assets from the source chain to the target chain. In addition, due to the decentralized feature of the bridges, the relevant data about user requests must be fully revealed on-chain.

To address these challenges, a novel type of services called **Instant Cryptocurrency Exchange (ICE) services** has emerged. ICE services, which are centralized services, offer the ability to bridge cryptocurrency assets across chains with a short delay and without the need for strict user identity verification. ICE services streamline the asset bridging process to just a few steps and complete asset bridging within a short delay. This makes them a convenient and expedient option for users looking to bridge assets across chains.

Specifically, current ICE services exhibit two distinct features. First, *they lack a strict Know Your Customer (KYC) policy*: unlike CEX-based bridging, they do not require account registration or extensive verification of personal identity. Second, *they lack detailed on-chain request information*: unlike smart contract-based bridges, they do not record all relevant data on the blockchain, thus avoiding public disclosure of information that could track cross-chain activities.

However, these features of ICE services have contributed to their abuse in malicious activities within the blockchain ecosystem. ICE services can serve as initial sources of funds or as a tool to launder illicit funds in malicious activities, particularly after the sanction of Tornado Cash [43] by OFAC [27]. For example, the attacker in the BitKeep incident [37] laundered more than $2 million illicit funds through multiple ICE services, including SimpleSwap, FixedFloat, and SideShift. In addition, there are measurement analysis [20] and investigations [7, 52, 53] reporting cases in which ICE services have been used to launder money in malicious activities. Our analysis (see Section 4.4) shows that ICE services have laundered $12,473,290 illicit funds from exploit and phishing activities in total, and provided initial funds for 432 malicious addresses.

With the increasing usage of ICE services in malicious activities, they have not received enough attention from academia or industry in the blockchain ecosystem. In this research, we take the first step towards understanding and analyzing ICE services. Specifically, our research is driven by the following three research questions.

- **RQ1: What are the features of ICE services and how do they work?** Our initial objective is to comprehend the features of ICE services and determine their workflow. Our research begins with the definition and collection of ICE services. Then, by interacting with the collected services through user requests, we summarize the workflow and categorization for the ICE services.
  In summary, we have collected **nine** ICE services and submitted user requests. Our analysis indicates that the ICE service workflow typically includes accepting funds through *deposit*

addresses, managing funds within *hot wallets* and finally withdrawing those funds to users. Based on the different management strategies, we categorize ICE services into two distinct types: *Standalone* ICE services, which manage their own hot wallets, and *Delegated* ICE services, which transfer funds between hot wallets and external delegated services.

- **RQ2: What is the current state of ICE services usage and its impact?** Our analysis aims to unveil the features of the ICE service ecosystem, including user behavior features and the security impact associated with their usage in malicious activities. To this end, we perform a measurement analysis using the data we have collected.
  Our analysis reveals a concentrated ICE service market, with four services dominating 91% of the volume of user requests. 84% of user requests occur on Bitcoin, Ethereum, and other EVM-compatible blockchains. Users typically engage with ICE services infrequently, mainly in tokens of *Ether*, USDC, and USDT, and typically bridge assets of value less than $500 per request. Furthermore, we have discovered $12,473,290 illicit funds laundered through ICE services, and identified 432 malicious addresses that were initially funded by ICE services and participated in malicious activities.
- **RQ3: What is the effectiveness of ICE services in terms of efficiency and in preventing traceability?** Finally, we evaluate the features of ICE services regarding their efficiency and ability to prevent traceability. Using insights from the measurement, we propose a matching algorithm to correlate user deposits and withdrawals across EVM-compatible chains. Evaluation of ground-truth data from two services reveals that the matching algorithm is able to achieve an accuracy of 80%. It suggests that, although ICE services do not disclose details of user requests, temporal and pricing features can still be used to accurately correlate user deposits and withdrawals for ICE services.
  In terms of practical applications for the matching algorithm, we first examine the performance of ICE services. Our findings reveal that 92% of the matched requests are finalized in three minutes in EVM-compatible chains, highlighting the efficiency of ICE services. Furthermore, we apply the matching algorithm to investigate the money laundering activities of malicious entities through ICE services. This demonstrates the potential of the matching algorithm to trace money flows in the cases where ICE services are involved in the money laundering process.

Contributions. In summary, our main contributions in this research are listed as follows:

- To the best of our knowledge, our study is the *first* comprehensive research effort delving into *ICE services*, detailing their features and the workflow. By investigating **nine** ICE services, we have identified two main categories of ICE services based on fund management methods: *Standalone* and *Delegated*.
- We conducted an extensive measurement study on the ICE service ecosystem using multiple data sources. This study explored multiple features such as low request frequency, small transaction value, and the concentration of certain tokens within ICE services. Furthermore, we investigate the usage of ICE services in malicious activities, identifying $12,473,290 illicit funds laundered through, and 432 malicious addresses initially funded by ICE services.
- We evaluated the effectiveness of ICE services, focusing on their efficiency and their ability to prevent traceability. To achieve this, we proposed a matching algorithm, derived from insights gained during our investigative efforts, aimed at matching deposits with withdrawals made through ICE services. Our analysis shows that 92% of the matched requests were completed in three minutes, highlighting the high efficiency of ICE services. Furthermore, by applying the matching results, we investigated the money laundering practices of malicious entities

utilizing ICE services. Our work demonstrated that the matching algorithm could effectively trace money flows in the cases where ICE services are misused for illicit purposes.

2 Background

2.1 Ethereum and Smart Contracts

The blockchain was invented as a public verifiable, distributed, and append-only ledger for Bitcoin [36]. Ethereum [48] extends the blockchain with the concept of generic state transition and enables the blockchain to run deterministic programs called *smart contracts* on the Ethereum Virtual Machine (EVM). Due to the popularity and high transaction fee of Ethereum, several EVM-compatible blockchains are created, such as Binance Smart Chain (BSC) and Polygon.

Addresses are the basic unit of action in blockchain. There are two types of addresses in Ethereum: EOAs and CAs. Externally Owned Accounts (EOAs) are controlled by external private keys outside of the blockchain, and they are capable of signing transactions to initiate transfers and invoke smart contracts. Contract Accounts (CAs) contain codes deployed by EOAs or other CAs, and can only be controlled by the codes deployed. CAs can have internal states that persist on the blockchain, and can read internal and global blockchain states during smart contract invocations.

Transactions are signed by EOAs to invoke smart contracts or initiate transfers. The smart contract can then initiate arbitrarily calls to other smart contracts capped by the gas limit of the transaction.

Events are emitted to represent notable incidents that occurred during the execution of smart contracts. Events are not part of the blockchain state; they are used instead to notify the relevant parties outside the blockchain. For example, events are used by wallets to record historical token transfers for users.

2.2 Tokens

In the context of blockchain, **tokens** refer to a digital asset that represents a unit of value or a specific right. Tokens can be transferred between addresses to represent the transfer of value. Tokens can also be created (*minted*) or destroyed (*burnt*). The token implemented as a *native* mechanism to pay transaction fees and reward block producers is called the "native token". In Ethereum, the native token is called *Ether*.

The ERC-20 standard. Besides the native token, smart contracts can also be used to implement tokens. To facilitate the usage of tokens in the DeFi ecosystem, the ERC-20 standard [46] is proposed. ERC-20 standard defines the interfaces that must be implemented by all tokens. The standard also requires that any transfer must trigger a corresponding `Transfer` event with transfer details.

Events and Token Decimals. As EVM does not have built-in support for floating point numbers, to accurately represent token values, most tokens utilize integers with decimal places. Most tokens define an attribute called `decimals`, indicating the number of decimal places of the token. The `value` in the ERC-20 transfer events are raw values with `decimals`. For example, consider the USDC token with 6 decimal places. A `Transfer` event with `value` equals to 10^6 represents the transfer of 1 unit of the USDC token. By convention, The native token *Ether* has a decimal of 18.

3 An Overview of ICE Services

To analyze ICE services, we first need to understand their definition, classification, and workflow, as mentioned in the **RQ1** in Section 1. Therefore, in this section, we provide a qualitative overview of ICE services. First, we present the definition of ICE services, comparing ICE services with CEXes and cross-chain bridges, highlighting the unique privacy and efficiency features of ICE services. Second, we introduce the methodology for collecting ICE services from various sources and interacting

with collected services. Finally, by analyzing the user request procedure and related transactions, we perform an analysis of the workflow and classification of ICE services.

3.1 The Definition of ICE Services

In the context of this study, **Instant Cryptocurrency Exchange services** (*ICE services* for short) are defined as *centralized services* that *efficiently* bridge assets across different chains, *without requiring strict user identity verification and publishing bridging details on-chain.*

As introduced in Section 1, there are two other methods to bridge assets across chains: CEXes and cross-chain bridges. Compared to these methods, ICE services are superior in both privacy and efficiency. From the perspective of privacy, ICE services do not impose KYC requirements or publish user request details through on-chain transactions. From the perspective of efficiency, ICE services process user requests more quickly by operating as centralized services and involving fewer steps. The differences between ICE services, CEXes, and cross-chain bridges are summarized in Table 1. In addition, in Section 3.1.1 and Section 3.1.2, we compare in detail the features of ICE services with other methods.

3.1.1 Compared to Centralized Exchanges (CEXes). CEXes can also be used to bridge assets across different blockchains. However, ICE services provide better privacy for users compared to CEXes, which typically require registration and strict user identity information. ICE services do not enforce a KYC policy or even registration for their users, ensuring user privacy.

From the perspective of efficiency, ICE services are also superior. Asset bridging through CEXes involves multiple manual steps, including depositing assets, initiating a trade to the target asset, and withdrawing the asset to the destination chain. Each step may incur additional delays [13]. Furthermore, CEXes record user trades internally, requiring users to explicitly deposit to and withdraw from CEXes for their assets to be used in the blockchain ecosystem. In contrast, ICE services automatically handle user requests through on-chain transactions upon user initiation, thereby enhancing efficiency in asset bridging.

3.1.2 Compared to Cross-chain Bridges. ICE services offer better privacy for users compared to cross-chain bridges, which are decentralized services specializing in bridging assets across chains. Cross-chain bridges send transactions to smart contracts with *detailed* data of bridging requests, which bridges use to fulfill the bridge request. As a result, the destination of a cross-chain request can be effectively identified using on-chain data.

In contrast, ICE services are centralized and allow users to initiate requests and deposit assets directly to service-managed addresses. Although ICE services fulfill user requests with on-chain transactions, these are plain transfers, making it difficult to precisely match deposits and withdrawals. By operating as black boxes, ICE services enhance user privacy.

From the perspective of efficiency, cross-chain bridges typically involve relaying requests across chains and additional consensus mechanisms, which may increase delays [5, 44]. ICE services, being centralized, streamline the process, with delays mainly involving transaction confirmations, thus ensuring greater efficiency in asset bridging.

3.2 The Collection of ICE Services

To conduct further analysis, we collect ICE services from the blockchain ecosystem. Our methodology involves the following steps:

(1) *Collecting candidate services.* We use aggregator websites [40, 41] that list exchange services, including ICE services, to compile a list of potential candidates. These platforms help us identify ICE services while excluding known centralized exchanges.

Table 1. Feature comparison between ICE services and CEXes & cross-chain bridges.

Feature	Strict KYC	Bridging Details On-chain	Efficiency
CEXes	✓	✗	✗
Cross-Chain Bridges	✗	✓	✗
ICE Services	✗	✗	✓

Table 2. ICE services collected in our study with the community influence metrics (based on the number of followers of the official Twitter accounts) and reported usages in malicious activities (Abused).

Type	*Service*	*URL*	*# of Twitter Followers*	*Abused*
Standalone	ChangeNOW	https://changenow.io/	185,513	e.g., [31, 32, 53]
	FixedFloat	https://fixedfloat.com/	47,089	e.g., [7, 52, 53]
	SideShift	https://sideshift.ai/	14,365	[54]
	eXch	https://exch.cx/	9,135	e.g., [33, 34]
	ChangeHero	https://changehero.io/	8,335	[21]
	Alfacash	https://www.alfa.cash/	885	
Delegated	SimpleSwap	https://simpleswap.io/	66,838	e.g., [28, 35]
	StealthEx	https://stealthex.io/	49,359	
	LetsExchange	https://letsexchange.io/	12,597	

(2) *Information gathering for candidate services.* For each candidate service, we collect data on their interaction procedures, user policies, and community influence (through social media metrics like Twitter). We also assess whether the service provides historical data and if it has been involved in any past malicious activities.
(3) *Filtering ICE services.* Using the gathered information, we filter and refine the list of ICE services. First, we exclude services that do not meet the definition of ICE service. Next, we remove services lacking on-chain information (see Section 6.1 for more details). Finally, we select services based on community influence and usage in malicious activities for further analysis.

We have collected **nine** ICE services, as summarized in Table 2. The community influence metric is represented by the column "# of Twitter Followers". ICE services involved in historical malicious activities are labeled in the "Abused" column. For each collected ICE service, we manually submit real user requests and document the entire workflow and all related transactions. This includes recording all addresses involved, such as deposit addresses and hot wallets used by the services.

3.3 The Workflow of ICE Services

By analyzing the data collected in Section 3.2, we have summarized the workflow of ICE services. Generally, ICE services follow a four-step process to complete user requests for asset bridging across chains, as illustrated in Figure 1. Specifically, the workflow of the ICE services can be outlined as follows.

3.3.1 ❶ *User Request.* As centralized services, ICE services receive a request from the user, which includes request information including the source and target currency with their corresponding amounts and destination address. This is the only step in the ICE services that occurs off-chain, and the detailed information of user requests is not disclosed for user privacy.

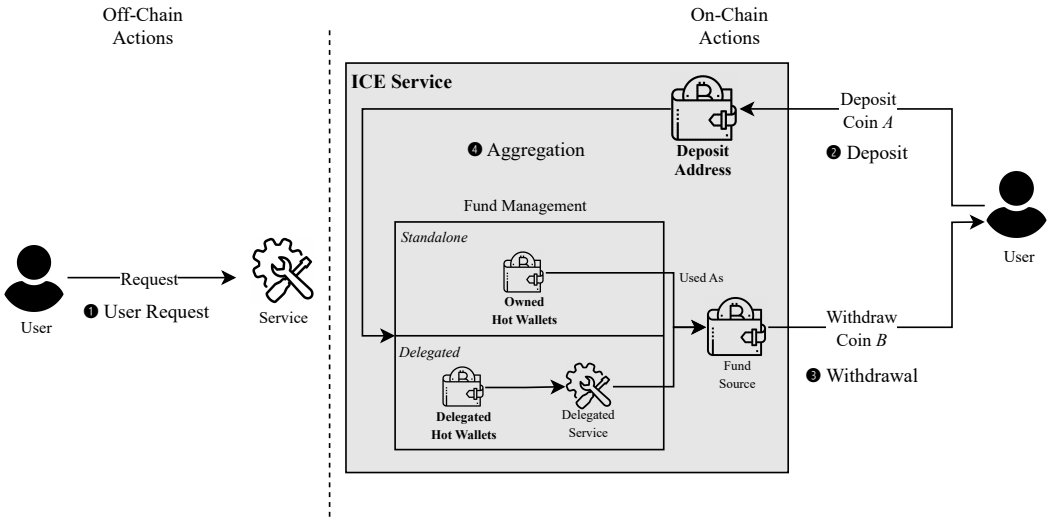


Fig. 1. The workflow of ICE services.

3.3.2 ❷ *Deposit.* To establish a clear correspondence between off-chain user requests and on-chain user deposits, ICE services provide a *deposit address* to the user and request the user to transfer the deposit assets to this address. For ICE services, the deposit addresses are created and managed by the services.

After providing the deposit address, the service awaits the confirmation of the user deposit transaction to the deposit address. The deposit addresses are under the control of the service, enabling the funds to be processed later in the fund management. User transactions transferring input funds to the deposit addresses are referred to as "deposit transactions".

3.3.3 ❸ *Withdrawal.* Once the user deposit transaction is confirmed, ICE services proceed to send the requested currency to the destination address from the fund source of the services. The source of the fund is determined by the fund management of the service, and the classification of the ICE services is based on different methods of fund management. Transactions to transfer funds from hot wallets to users are called "withdrawal transactions".

It should be noted that, from the perspective of user privacy, the funds received by users originate from the fund source with multiple sources, making it challenging to trace the sources of the withdrawn funds.

3.3.4 ❹ *Aggregation.* Finally, ICE services commonly aggregate the funds received in the deposit addresses to the hot wallets. For blockchains with the UTXO model that allow multiple inputs in a transaction (e.g. Bitcoin), this aggregation step is optional. [1] For other account-based blockchains, including EVM-compatible blockchains like Ethereum, the aggregation process is used to pool small user deposits for the convenience of fund management. Transactions initiated by ICE services to aggregate funds in deposit addresses are called "aggregation transactions".

[1]Our analysis shows that some services (e.g., the FixedFloat) also aggregate funds in Bitcoin.

3.4 The Classification for ICE Services

From the workflow introduced in Section 3.3, the only component in which ICE services can differ is the fund management of the services. From the analysis of user requests and fund management for the services listed in Table 2, we have classified ICE services into two categories:

(1) **Standalone.** The fund management of *Standalone* ICE services are standalone, by managing their own hot wallets in different blockchains, not relying on external services. All user deposits of *Standalone* ICE services are transferred to the deposit addresses owned by the service, and then aggregated to the hot wallets in account-based blockchains. All funds withdrawn by users are from the wallets owned by the service, specifically the hot wallets on account-based blockchains.

(2) **Delegated.** As the name suggests, *Delegated* ICE services delegate fund management to other services. Like *Standalone* ICE services, the *Delegated* ICE services receive user deposits in deposit addresses managed by the services, and then aggregate user deposits to hot wallets. However, compared to *Standalone* ICE services, the hot wallets for *Delegated* ICE services are intermediary, and funds collected in hot wallets are deposited to delegated services. Conversely, the withdrawn funds from the *Delegated* ICE services also originate from delegated services.

Different strategies can be chosen to implement ICE services. Compared to the *Standalone* ICE services using owned hot wallets, *Delegated* ICE services have several advantages. In essence, by delegating the fund management to other services, *Delegated* ICE services significantly reduce the complexity of service implementation. From the perspective of users, *Delegated* ICE services serve as a *proxy* to initiate asset bridging requests to the delegated services.

However, delegating fund management also presents practical challenges. First, most CEXes charge fees for deposits and withdrawals, which can result in the increased cost of user requests in *Delegated* ICE services. Second, deposits from ICE services to CEXes can be provisioned due to potentially illegal fund sources, leading to losses of the ICE services.

In contrast, ICE services of *Standalone* type functions more like standalone money pools in black-boxes that serve user requests using their own funds and hot wallets. From the perspective of users, the security and privacy of users of *Standalone* ICE services are entirely up to the services, without any impact from the delegated services like *Delegated* ICE services.

Answer to RQ1: Compared to other methods for asset bridging across blockchains, ICE services provide the features of efficiency and privacy. Typical ICE services begin with an off-chain *user request* followed by three on-chain actions: *deposit*, *withdrawal*, and *aggregation*. The approach to *fund management* between deposit and withdrawal can differ for ICE services. Consequently, ICE services can be divided into two main categories: *Standalone* ICE services that maintain their own hot wallets, and *Delegated* ICE services that move funds from hot wallets to external delegated services.

4 A Measurement On ICE Services

After the qualitative overview in Section 3, we now conduct a measurement of ICE services to obtain a comprehensive understanding of their current status and impact, as outlined in **RQ2** in Section 1. In this section, we first present an introduction to our analysis methodology in Section 4.1 and then proceed with the measurement. The measurement is divided into three parts, each addressing a sub-research question within **RQ2**, as follows:

- **RQ2.1**: What are the features of user behavior for ICE services across chains?
- **RQ2.2**: What are the features of on-chain activity for ICE services?
- **RQ2.3**: How are ICE services involved in malicious activities?

Specifically, we analyze user requests using historical data from two representative ICE services in Section 4.2 to answer **RQ2.1**. Next, we measure the on-chain activities of all ICE services on Ethereum in Section 4.3 to answer **RQ2.2**. Finally, we investigate the usage of ICE services in malicious activities in Section 4.4 to answer **RQ2.3**.

4.1 Methodology

Based on the workflow summarized in Section 3, we analyze the ICE services collected using both off-chain and on-chain data with the methodology described below.

4.1.1 Off-chain Data Analysis. ICE services may choose to display historical statistics or recent user operations on their front-end pages to show their popularity and activity. Some services also offer APIs to access this information. During the information gathering phase (see Section 3.2), we identified two services, FixedFloat [18] and SideShift [39], which actively expose part of their historical requests. Consequently, we deployed crawlers to periodically access the FixedFloat front-end page and use the SideShift APIs to collect historical user requests.

The exposed historical data includes timestamps, source and target cryptocurrencies and blockchains, and precise input amounts. Each historical user request is represented by a tuple:

$$\mathcal{H} = (H_t, H_c^{in}, H_v^{in}, H_c^{out}, H_v^{out})$$

where H_t is the timestamp, H_c^{in} and H_c^{out} are the input token and value, and H_v^{in} and H_v^{out} are the output token and value, respectively. For FixedFloat, output amounts are calculated based on prices from the time of crawling. In contrast, SideShift provides precise output amounts directly through its APIs. *Note that detailed user deposit and withdrawal addresses, as well as transactions, are excluded for privacy considerations.*

Our evaluation of crawled historical requests reveals that more than 75% of on-chain requests are recorded, and all historical requests have corresponding on-chain transactions. This indicates that most of the crawled data is reliable and reflects actual user activity. The collection and analysis of off-chain data is used to address **RQ2.1**. Furthermore, historical user requests serve as ground-truth data used in Section 5.

4.1.2 On-chain Data Analysis. Based on the analysis presented in Section 3, we collect and analyze on-chain data used to address **RQ2.2** and **RQ2.3** for ICE services using the following steps:

(1) *Data Collection.* Hot wallets, as defined in Section 3, are central to ICE services. We collect data on hot wallet activities from external sources. Specifically, we begin by querying all token transfers related to the service's hot wallets from Etherscan [15], filtering out tokens not supported by the service.
(2) *Hot Wallet Analysis.* Based on the hot wallet data collected, we identify aggregation and withdrawal transactions. As detailed in Section 3, *aggregation transactions* are those that send assets from deposit addresses to hot wallets, while *withdrawal transactions* send funds to users. For *Standalone* ICE services, both types of transactions can be identified for their hot wallets. However, in *Delegated* ICE services, funds are withdrawn directly from the delegated services, so withdrawal transactions cannot be identified.
(3) *Deposit Analysis.* To accurately identify deposit operations, potential deposit addresses are first extracted from aggregation transactions, as introduced in Section 3. These addresses are then filtered to ensure that all destinations are the service's hot wallet addresses. Finally, the filtered addresses are confirmed as the deposit addresses involved in deposit operations.

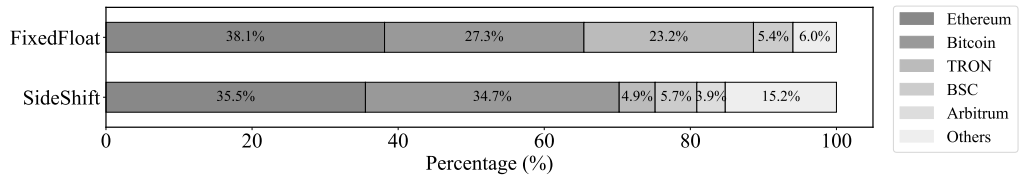
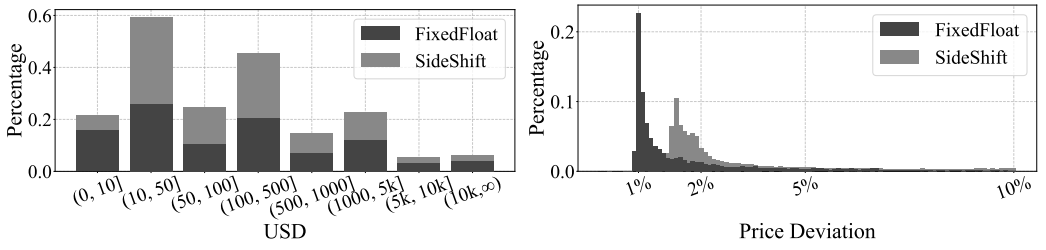


Fig. 2. Chain value distribution of the historical user requests.



(a) Request Value Distribution (b) Price Deviation Distribution

Fig. 3. Feature summarization of historical user requests for FixedFloat and SideShift.

4.2 Answer to RQ2.1: Historical User Request Analysis

As mentioned in Section 4.1, we are able to obtain historical user requests with partial details for all chains supported by FixedFloat and SideShift. The crawled historical requests span from February 2023 to September 2023. Using these historical requests, we are able to analyze user behavior for all the chains supported by these services, to summarize the features, and gain insights for representative ICE services.

4.2.1 Chain Value Distribution. To understand user behavior for ICE services, we first analyze the distribution of the value of historical user requests across different blockchains (*chain value distribution* for short). The chain value distribution is calculated by the total value of user deposits for all supported blockchains. The total value is determined by aggregating user requests using historical prices for different chains.

Figure 2 shows the chain value distribution for FixedFloat and SideShift. It is clear that Ethereum and EVM-compatible blockchains (Binance Smart Chain, TRON and Arbitrum) are among the most popular chains for ICE services usage. The result demonstrates that the growth of the DeFi ecosystem has contributed to the growth of ICE services to meet the demand for cross-chain asset bridging. In addition, Bitcoin is also popular, likely due to its widespread use, high transaction volume, pseudonymity, and difficulty in tracing money flows.

4.2.2 Request Value Distribution. To analyze user behavior when using ICE services, we calculate the historical value of each user request. The value of each user request is calculated using the deposit token and amount, based on historical CEX prices at the time of the user request provided by Binance [2] and Coinbase [12]. We then summarize the frequency and ratio of the historical request value for each service.

The results, shown in Figure 3a, indicate that the average value of historical requests is relatively low. Specifically, only 56% of the historical requests for FixedFloat exceed $100, and the ratio is 45%

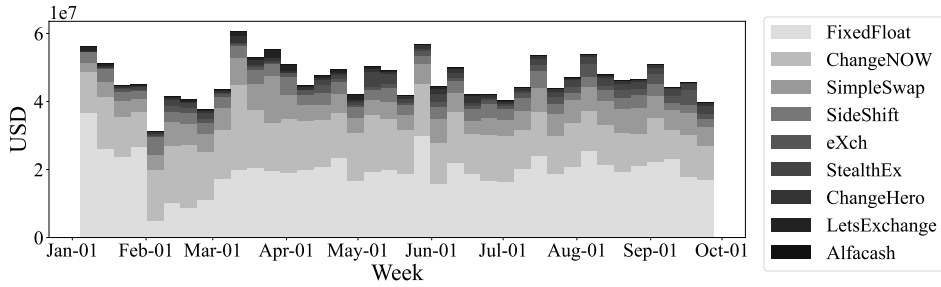


Fig. 4. Weekly user deposits of analysed ICE Services on the Ethereum blockchain.

for SideShift. For both services, the proportion of requests that exceed $10,000 is lower than 5%. This suggests that users are more likely to bridge smaller amounts through ICE services.

4.2.3 Exchange Price Deviation. ICE services determine the exchange price for user requests based on the current market price, typically calculated from the prices of the major CEXes, with additional fee charges. To estimate the average exchange price deviation of ICE services, we compare the total dollar value of the output token and amount with the historical price provided by CEXes.

Figure 3b presents the results, showing the proportion of user requests by their price deviation. As indicated, the average price deviation for both services ranges from 1% to 5%. The result suggests that most requests of ICE services are close to the market price and the fees charged by the ICE services are relatively low. These low fees may contribute to the popularity of ICE services. In addition, different services can adopt various fee strategies, further enhancing their appeal within the ICE service ecosystem.

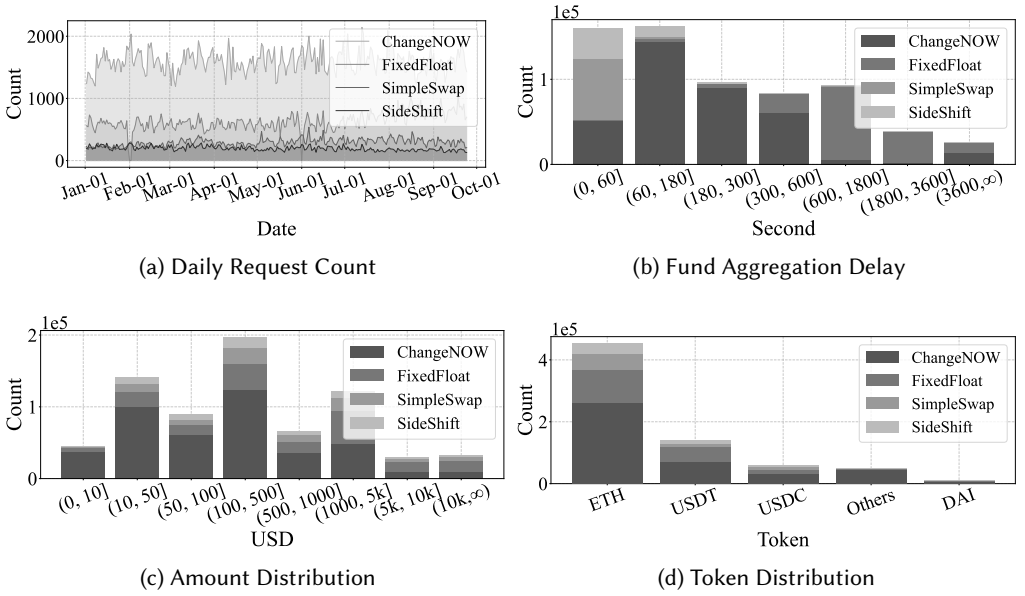
4.3 Answer to RQ2.2: On-chain Activity Analysis

After analyzing selected ICE services based on historical user request data, we observed that ICE services are widely used on EVM-compatible chains, with Ethereum being the most prominent blockchain. Therefore, we further examined the on-chain activity of all ICE services with hot wallets on the Ethereum blockchain. The on-chain data used in the analysis spans from January 2023 to September 2023, focusing on user deposits. For the sake of conciseness, we present the feature analysis for four widely used and dominant ICE services: FixedFloat, ChangeNOW, SimpleSwap and SideShift, following the trading volume analysis.

4.3.1 Trading Volume. First, we summarize the total trading volume of the ICE services shown in Figure 4. In summary, a total dollar value of $1,775,752,143 has been deposited in ICE services since 2023, with a weekly average of $46,730,319. FixedFloat, ChangeNOW, SimpleSwap and SideShift are among the most popular ICE services, occupying over 91% of the total trading volume in the analyzed ICE services.

The statistics indicate that the ecosystem of ICE services is dominated by the top popular services. In addition, the total value processed through ICE services is large, indicating a huge need for assets bridging across blockchains. Figure 4 also suggests that the daily volume of ICE services is relatively stable.

4.3.2 User Request Frequency. The frequency of user requests is defined as the total count of daily requests to the service. Figure 5a summarizes the daily request frequency of each service analyzed. The most widely used service, ChangeNOW, processes an average of 1,594 user requests each day. For the other services, the daily deposit frequency is 631 for FixedFloat, 292 for SimpleSwap, and



(a) Daily Request Count

(b) Fund Aggregation Delay

(c) Amount Distribution

(d) Token Distribution

Fig. 5. Feature summarization of on-chain activities for dominate ICE Services.

194 for SideShift. Furthermore, we found that all the deposit transactions occur in different blocks, indicating a temporal difference between deposit activities.

The frequency analysis of user requests indicates that *most user requests can be distinguished by the time of the deposit transaction on-chain*, which is a key insight for the matching algorithm.

4.3.3 Deposit Address Aggregation Delay. The delay in aggregating the deposit address is defined as the delay in seconds between the users transferring the funds to deposit addresses and the service aggregating funds into hot wallets. As shown in Figure 5b, ICE services generally aggregate funds from deposit addresses with a short delay. In total, the funds of more than 92% of the user deposits are aggregated into hot wallets within 3,600 seconds (1 hour) for the services analyzed. For SideShift and SimpleSwap, 97.9% and 98.1% of the total deposits are aggregated within 300 seconds (5 minutes), respectively. For ChangeNOW and FixedFloat, 96.3% and 92.6% of the deposits are aggregated within 3,600 seconds (1 hour), respectively.

Fund aggregation is a crucial step for ICE services in account-based blockchains. ICE services typically opt for quick aggregation of deposited funds into hot wallets to ensure proper functioning.

4.3.4 Request Value Distribution. Figure 5c represents the distribution of the historical value of user deposits for the services analyzed. The total value of each user request is low on average, which is consistent with the analysis in Section 4.2.2. For FixedFloat and SideShift, 45.3% and 63% of all requests have a value lower than $500, respectively. For ChangeNOW and SimpleSwap, 75.8% and 53% of all requests have a value lower than $500, respectively. Similarly to the findings in Section 4.2.2, the average value of each user request is low, with more than half of user requests having a total value less than $500.

4.3.5 Token Distribution. Finally, Figure 5d presents the token distribution of on-chain activities for each service. Although multiple tokens are supported by ChangeNOW and SimpleSwap, we

Table 3. A summary of initial funding by ICE services to malicious actors.

Service	Funded Addresses	Total Funded (in *Ether*)
FixedFloat	264	287.42
ChangeNOW	113	97.03
SideShift	45	14.11
eXch	12	3.44
Total	434	402.0

can conclude that for all the analyzed services on Ethereum, *Ether*, USDT and USDC are the most common tokens in user requests, while other tokens are rarely used.

Specifically, for ChangeNow, more than 91% of the user deposits are in *Ether*, USDT, and USDC, while other tokens only account for up to 9% of the user deposits. For other services, the ratio is even lower, with only 5% of user deposits in tokens other than the popular ones mentioned above. This indicates that users commonly bridge widely accepted and valuable tokens across blockchains.

4.4 Answer to RQ2.3: Usage Analysis of ICE Services in Malicious Activities

As introduced in Section 1, ICE services have been reported to be used in malicious activities. Using the address labels on Etherscan [15] and MetaDock [6], we measure the usage of ICE services in malicious activities on the Ethereum blockchain. The usage of ICE services in these activities occurs in two main ways: *providing initial funds to malicious actors* and *laundering illicit funds*.

4.4.1 ICE services as initial fund sources. Malicious actors require initial funds, such as gas fees, to send transactions. For example, in address poisoning attacks [20], attackers need gas fees to send transactions that mimic normal user transfers. Malicious actors can create malicious addresses by withdrawing funds from ICE services to obscure the real source of funds.

To analyze the usage of ICE services in providing initial funds, we examine the *initial funding* addresses, which are the senders of the first native tokens (i.e., *Ether*) received by malicious addresses, using the MetaDock API [6]. We identified **434 addresses related to phishing and scam activities that received initial funds from ICE services, with a total amount of 402 *Ether*.** Table 3 summarizes the services providing initial funds to these malicious activities. FixedFloat and ChangeNOW are among the most widely used ICE services, providing initial funds to 264 and 113 addresses, respectively. For instance, the address `Fake_Phishing179443` (`0x4b09...d8c6`) was initially funded by FixedFloat, and the funds were used as gas fees for sending over 5,000 transactions for fake token and address poisoning attacks.

Multiple incidents also report attackers initially funded by ICE services, including FixedFloat and ChangeNOW [8, 29, 30]. To better understand the usage of ICE services in funding exploiters, we collected addresses labeled as exploiters and identified their initial fund sources. In total, we found 8 addresses related to historical exploits initially funded by FixedFloat, including the exploiters of Platypus Finance (`0xeff0...3958`) [22] (with a total loss over $8.5M) and Team Finance (`0x161c...99fd`) [25] (with a total loss over $14.5M). Additionally, we identified 7 exploiter-related addresses initially funded by ChangeNOW, including the exploits of Arcadia Finance (`0x5c75...050d`) [4] (with a total loss of over $455K) and the LeetSwap (`0x705f...85c3`) [10] (with a total loss of over $624K). In particular, some attackers, such as those targeting Team Finance and LeetSwap, bridged illicit profits to Ethereum for money laundering, with their gas fees initially provided by ICE services.

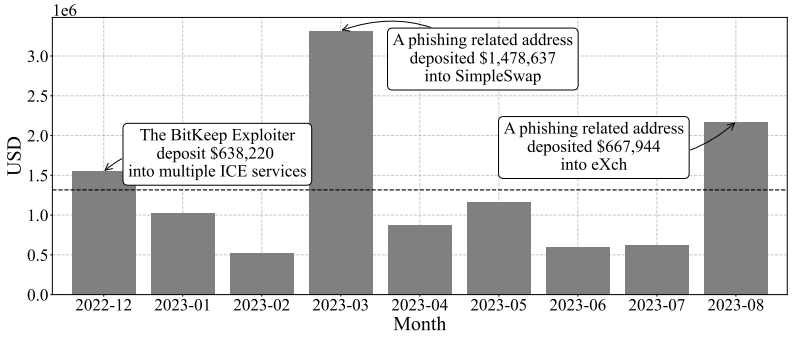


Fig. 6. Monthly malicious funds laundered through ICE services. Months with more malicious funds laundered are marked with corresponding key incidents.

By providing initial funds to addresses involved in phishing, scam and exploit activities, ICE services facilitate the initiation of malicious activities without revealing the real identity of the attackers. Therefore, more regulation on the usage of ICE services in malicious activities is necessary for their maintainers.

4.4.2 ICE services as money laundering tools. In addition to serving as initial funding sources, ICE services are commonly used for money laundering due to their privacy features. Using malicious address labels collected from Etherscan [15] and MetaDock [6], we identify direct deposits of malicious funds into ICE services. Specifically, when a malicious address deposits into ICE services directly, the corresponding time, address, and total value are recorded and analyzed. In total, **we have identified a total of $12,473,290 malicious funds deposited into multiple ICE services.** Most of these illegal funds laundered are illicit profits from phishing and scam activities, with attackers in several exploit incidents also using ICE services.

A summary of monthly money laundering activity directly related to ICE services, along with their corresponding key incidents, is presented in Figure 6. On average, $1,316,464 malicious funds are deposited directly into ICE services each month. One of the largest money laundering activities through ICE services involves the address `Fake_Phishing7064` (`0x8452...6fb8`), which has laundered over $1.4M through multiple ICE services, including SideShift and eXch. This address was used by the notorious Monkey Drainer [51], which has been shut down [11]. Another example is the BitKeep exploiter [37]. In this incident, the exploiter address (`0x9f12...f855`) drained and collected illicit profits from vulnerable wallets, swapped all assets into *Ether*, and deposited them into multiple ICE services for money laundering, including ChangeNOW, SimpleSwap, and SideShift.

Due to the complexity of tracing money flow and the lack of labels for malicious actors, only direct deposits related to ICE services on the Ethereum blockchain are analyzed. Other malicious actors may transfer illicit funds to intermediate addresses before depositing them into ICE services. Furthermore, ICE services usage on other popular EVM-compatible chains (such as Binance Smart Chain and TRON) is not included in our analysis. Therefore, the results calculated above serve only as a lower bound, although we have proven that more than $12,473,290 illicit funds have been laundered through ICE services.

Answer to RQ2: The ICE service ecosystem is highly concentrated, with four dominant services accounting for over 91% of the trade volume. More than 84% of user requests target Bitcoin, Ethereum, or other EVM-compatible blockchains. Users interact with ICE services infrequently, with an average of no more than 1,594 daily requests. User requests primarily involve major tokens like *Ether*, USDC, and USDT. Most requests involve assets of value less than $500. We also analyze the usage of ICE services in malicious activities. In summary, we identified more than $12,473,290 malicious funds laundered through ICE services. In addition, we found 432 malicious addresses that are initially funded by ICE services.

5 Match-Based Advanced Analysis on ICE services

After examining the ecosystem of ICE services, we perform an advanced analysis of their two key features: efficiency and privacy, addressing **RQ3** proposed in Section 1.

In this section, we first summarize the insights from Section 3 and Section 4. Based on these insights, we propose a heuristic-based matching algorithm to correlate user deposits and withdrawals within account-based blockchains [2]. We then construct a ground-truth dataset using the data collected in Section 4.1. The evaluation of the algorithm on this ground-truth dataset shows an overall accuracy rate of more than 80%. This result indicates that, despite ICE services not revealing user request information on-chain, temporal and value features can be used to correlate user deposits and withdrawals, thereby compromising user privacy.

Finally, using the results of the matching algorithm, we evaluate the efficiency of ICE services and find that they are efficient in quickly transferring funds to users after deposit confirmation. The matching results are also used to analyze the money laundering processes associated with malicious activities involving ICE services.

5.1 Insights

In this section, we summarize insights from the workflow outlined in Section 3 and the measurement analysis presented in Section 4.

(1) *Transaction Ordering.* As detailed in Section 3, within a single request, the withdrawal transaction must occur only after the confirmation of the user deposit to the deposit address. ICE services will initiate withdrawal for users only after confirming deposit transactions.
(2) *Low Price Deviation and User Request Frequency.* According to the analysis in Section 4, the price deviation from market prices is relatively small for each user request ((less than 5% for most requests). Additionally, user deposit and withdrawal transactions can be distinguished based on block timestamps due to the infrequent nature of user requests.
(3) *Efficiency of ICE services.* As defined in Section 3, ICE services are designed to provide *instant* asset bridging across chains. To ensure rapid processing, these services must promptly initiate withdrawals for users after confirmation of deposit transactions.

These insights are used separately in different phases of the matching algorithm. Specifically, the assumption of workflow and transaction ordering is used in operation identification in Section 5.2.1. The feature of low price deviation is used to calculate the value of each user request in Section 5.2.2. Finally, the low request frequency and efficiency features are used to efficiently match user withdrawals with deposits in Section 5.2.3.

5.2 The Matching Algorithm

Based on the insights summarized above, we now construct the algorithm to match user deposits and withdrawals for ICE services. The algorithm is divided into three phases: 1) operation identification,

[2]Currently, the algorithm is implemented to support Ethereum, BSC, TRON, Polygon, Arbitrum, Avalanche and Optimism.

which identifies user deposit and withdrawal operations using the methodology proposed in Section 4.1; 2) value calculation, which calculates the dollar value of each identified user operation; 3) matching, which matches user deposits and withdrawals across supported chains by dollar value and time difference. In the following, we elaborate each phase in detail.

5.2.1 Operation Identification. The first step of the matching algorithm is to correctly identify the deposit and withdrawal operations related to the target service. In this phase, all transactions related to hot wallets in multiple chains are collected from Etherscan [15], and are used to identify deposit and withdrawal operations.Each operation contains detailed information on the type of operation, timestamp, user address, and token with the corresponding amount.

5.2.2 Value Calculation. Once the deposit and withdrawal actions of the target service are identified, it is necessary to determine the dollar value of the user operations before they can be matched. The value of each operation is found by multiplying the amount of the token by the historical price of the token at the time of the operation. Historical price data are retrieved using APIs from Binance [2] and Kucoin [23].

5.2.3 Matching. After identifying the operation and calculating the value for each operation, the algorithm iterates over all the deposits and finds potential withdrawals for each deposit. Potential withdrawals are filtered by two metrics: the difference in dollar value V and the difference in time T between withdrawals and the target deposit. Parameters (V, T) can be adaptively selected for different services. In the matching process, we also consider the factor of address reuse in the withdrawal process, because users tend to reuse addresses in different blockchains. The withdrawal with the same address as the deposits has higher priority.

If multiple candidate withdrawals are identified, the withdrawal with minimal V and T is chosen. If no candidate withdrawals are identified, it either means that the matching has failed or the fact that the correlated withdrawal is on an unsupported chain (e.g. Bitcoin).

5.3 Evaluation

To evaluate the matching algorithm, we perform an evaluation using the historical user request data obtained in Section 4.1. In this section, we first describe our methodology for ground-truth construction. Then, we evaluate the result of the algorithm against the ground-truth data and present the effectiveness and the accuracy of our proposed algorithm. Finally, we present an analysis of the failure cases in our matching algorithm.

5.3.1 Ground Truth Construction. As introduced in Section 4.1, we have collected off-chain data of historical user requests for two services: FixedFloat and SideShift. To evaluate the effectiveness of the algorithm, we first construct a ground-truth dataset by correlating on-chain activities and historical user requests,

Specifically, the ground-truth data are constructed in the following steps:

(1) *History.* As introduced in Section 4.1.1, each historical user request is comprised of a tuple: $\mathcal{H} = (H_t, H_c^{in}, H_v^{in}, H_c^{out}, H_v^{out})$, which correspond to timestamp, input token and value, output token and value, respectively.
(2) *On-Chain Operations.* In the operational identification phase (Section 5.2.1), the deposit and withdrawal operations are identified with the following information: the tuple for deposit $\mathcal{D} = (D_t, D_c, D_v)$ and withdrawal $\mathcal{W} = (W_t, W_c, W_v)$.
(3) *Deposit-History Correlation.* The historical user requests are correlated with the on-chain deposit operations by the condition $|H_t - D_t| \leq T_D$ and $|H_v^{in} - D_v| \leq V_D$, which means that the time and amount of the on-chain deposit must be within a threshold compared to the

Table 4. The evaluation result of the matching algorithm on two representative ICE services.

Service	*FixedFloat*	*SideShift*
Ground-Truth	186,282	47,201
False Positive	15,739 (10.4%)	1,267 (2.92%)
Incorrect Delay Threshold	19,291 (12.81%)	1,746 (4.02%)
Matched	150,567	43,382
Accuracy	**80.8%**	**91.9%**

historical user request. In this process, the value threshold V_D for native tokens (e.g., *Ether* in the Ethereum blockchain) is higher than the ERC-20 tokens, because the deposited native tokens are also used as gas fees, while the ERC-20 tokens are transferred losslessly.

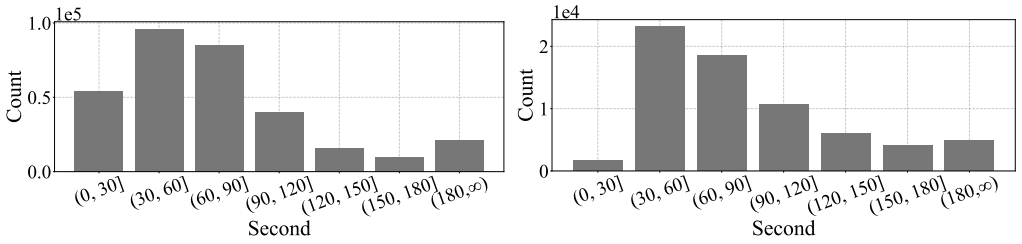
(4) *Full-Record Correlation.* After the previous step, most historical user requests are matched with the corresponding on-chain deposit operations. Using the destination data from the historical user requests, we identify the corresponding withdrawal in the destination chain by the following conditions: $W_t - D_t \leq T_W$ and $|H_v^{out} - W_v| \leq V_W$, which corresponds to the condition that the withdrawal time must be later than the deposit time within a given time window of T_W, and the withdrawal amount is within the threshold of V_W.

In total, among the 201,452 historical user requests for FixedFloat supported by our algorithm, we identified 186,282 correlated on-chain activities. For SideShift, the total historical user requests are 50,259, and 47,201 on-chain activities for ground-truth data are identified. The failure of matching historical user requests with on-chain activities involves two reasons. First, variations in the selection of parameters during the ground-truth construction process can result in the failure to handle edge cases where historical requests are correlated with multiple or no corresponding on-chain operations. Second, although it has been verified that the majority of exposed historical user requests are accurate in relation to on-chain operations, services may occasionally expose incorrect data due to the complexity of user requests (e.g., the cancellation of user requests).

Nevertheless, we have correlated more than 90% of the historical user requests with the corresponding on-chain deposit and withdrawal operations, which shows the reliability of the collected on-chain and off-chain data and the ground truth construction process. Therefore, the constructed ground-truth data can serve as a baseline for the algorithm evaluation.

5.3.2 Matching Result Evaluation. Using ground-truth data, we evaluate the proposed algorithm, and the results are presented in Table 4. The result illustrates that our algorithm achieves an accuracy rate that exceeds 80% to match user deposits and withdrawals. The algorithm effectively pairs deposits and withdrawals on supported blockchains. In particular, the accuracy improves as user activity decreases, evidenced by a jump from 80.8% for FixedFloat with a daily request frequency of 631 to 91.9% for SideShift with 194 requests, as detailed in Section 4.3.

Further analysis of algorithm mismatches revealed two primary causes. The first, *False Positive*, occurs when a non-matching request being more suitable than the correct one based on temporal and value features. The second, *Incorrect Delay Threshold*, involves outlier requests with delays exceeding the algorithm's 5-minute cutoff. The disproportionately high error rate for FixedFloat suggests that the 5-minute threshold, established from real user request evaluations in Section 3 and ground truth data analysis in Section 5.3.1, may not be optimal.



(a) FixedFloat (b) SideShift

Fig. 7. Deposit to withdraw delay for the services in ground-truth dataset.

5.3.3 The Efficiency of ICE Services. As introduced in Section 1, the first property of ICE services is *efficiency*. Using the results of the matching algorithm, we evaluate the efficiency of ICE services. Specifically, by analyzing the delay between the timestamps of the deposit and corresponding withdrawal transactions of the matching results, we are able to estimate the average delay of user requests and the efficiency of ICE services.

We measure the delay from user deposits and withdrawals of the matching results, and the result is summarized in Figure 7.In summary, more than 93% of all user requests for FixedFloat are processed in 180 seconds (3 minutes). For SideShift, more than 92% of user requests are processed in 3 minutes. Through the analysis of the delay of historical user requests, we can conclude that ICE services are efficient in facilitating asset bridging requests with short delay.

5.4 Matching Algorithm in Malicious Activity Analysis

Using our proposed matching algorithm, we can trace malicious funds laundered through ICE services on supported blockchains.

As introduced in Section 4.4.2, we have collected and analyzed malicious addresses which directly deposited into ICE services. Using our proposed algorithm, we can analyze their withdrawals with statistical data and several case studies. In this section, we present a comprehensive study on malicious funds deposited into ICE services from October 2022 to September 2023.

5.4.1 Results. The study is conducted for the two services used in the evaluation of the matching algorithm, namely FixedFloat and SideShift. For each direct deposit of malicious funds into these services, we search for the record in the result of the matching algorithm with the information of the corresponding withdrawal (possibly on Ethereum or other blockchains). If no record was found, it either means that the matching algorithm fails or that the withdrawal is not on a chain supported by the algorithm. As we focus on large-scale money laundering activities through ICE services, deposits from malicious addresses with a total value less than $100 are ignored for the conciseness of the analysis results, as small deposits are more likely for the purpose of initial funding.

In total, 143 malicious addresses have directly deposited in FixedFloat in 395 deposits, with a total value of $1,305,152. For all malicious funds deposited, 185 (46.8%) deposits related to 65 (45.5%) addresses are found in the matching result, with a total value of $529,362 (40.5%). For SideShift, 87 malicious addresses have directly deposited into SideShift in 275 deposits, with a total value of $363,442. For all malicious funds, 108 (39.2%) deposits related to 39 (44.8%) addresses are found in the matching result, with a total value of $93,940 (25.8%).

Table 5. The withdrawal destinations of the deposits from malicious addresses into two ICE services, with corresponding total value and number of addresses.

Chain & Service	*FixedFloat*		*SideShift*	
	Value	Addresses	Value	Addresses
Ethereum	312,812.49	36	47,410.93	33
TRON	129,131.23	77	30,311.45	50
BSC	65,872.47	58	14,612.66	15
Polygon	21,546.37	14	617.90	3
Arbitrum	-	-	635.40	5

As shown in the statistics, our proposed algorithm has a decent coverage on the malicious addresses with deposits into ICE services. Therefore, our proposed algorithm can be efficiently used in the money flow tracing of malicious activities.

5.4.2 The Destinations of the Withdrawals. The withdrawal destinations of the deposits from malicious addresses for the two analyzed services are summarized in Table 5.

As shown in the table, a common destination for withdrawals from malicious addresses in Ethereum is the Ethereum blockchain itself. In this situation, the ICE services are used as an exchange within the same blockchain. However, compared to swapping using decentralized applications like Uniswap [45], exchanging through ICE services does not directly reveal the destinations and therefore prevents money flow analysis. Using ICE services, malicious actors can stealthily exchange illicit profits to other addresses. According to our further analysis, most of the funds withdrawn from ICE services have been deposited into multiple CEXes.

Another common destination for illicit funds is TRON, which has been a popular blockchain for illegal activities according to external reports [24]. In total, 127 malicious addresses have bridged $159,442.68 illicit funds to the TRON blockchain.

5.4.3 Case Studies. In this section, we present several case studies of applying the matching algorithm on the deposits of malicious addresses.

For the first example, the address `Fake_Phishing11675` (`0xd6d3...8523`) was used to aggregate phishing profits from other phishing addresses and cash out. In total, the address deposited illicit funds of a total value of $202,527.9 into FixedFloat in 11 deposits. Using the matching algorithm, we found that the withdrawal has gone to a single Ethereum address `0xe749...c45b`, where a large portion of illicit funds are then transferred and deposited into CEXes including Binance [2] and BtcTurk [16]. A small portion of the illicit funds are deposited into FixedFloat again.

For the second example, the address `Fake_Phishing179956` (`0xf8f8...3283`) was used in a fake MEV bot scam. The illicit profits of a total value of $12,594.7 were separated into 5 deposits into SideShift. Using the matching algorithm, we found that the funds were withdrawn to address `0xbbc5...0d4a` on the Binance Smart Chain. The funds were then deposited into SideShift again, and withdrawn on Ethereum to address `0xbcab...cd31`. Finally, a large portion of the funds are separated into multiple deposits into SideShift and withdrawn to be deposited into Binance.

These case studies reveal the usage of the ICE services as part of or the entire chain of money laundering by malicious activities. By depositing illicit funds into ICE services, the money flow tracing of malicious activities can be broken, due to the mixture of funds inside the hot wallets of ICE services. The case studies also exhibit the usage of the matching algorithm in analyzing the fund flow of malicious activities leveraging ICE services for money laundering.

Answer to RQ3: Although ICE services keep user requests off the blockchain, it is still possible to correlate user deposits and withdrawals accurately by analyzing temporal and transactional value data. The effectiveness of the proposed matching algorithm is evident from our evaluation. For practical applications, it is noteworthy that more than 92% of the matched requests are completed within three minutes, highlighting the efficiency feature of ICE services. Moreover, the investigation into money laundering activities by malicious entities through ICE services highlights the potential of the proposed algorithm for tracing illicit money flows when ICE services are misused.

6 Discussion

6.1 Limitations of the Methodology on Collecting ICE Services

We acknowledge that this study has its limitations in not covering a specific type of service we have termed *Wrapped* ICE services. These services rely *entirely* on CEXes for asset bridging without using aggregated hot wallets, and *all addresses* involved in interactions are provided by CEXes. From the perspective of on-chain transactions, it is impossible to distinguish the activities of *Wrapped* ICE services from those of their dependent CEXes. Consequently, no data can be collected to analyze user behavior and activities. However, such ICE services are not mainstream, and their number is limited. To our knowledge, Changelly [9] is the only widely used service in practice.

In contrast, ICE services covered in this research can be categorized as *Managed*, with their funds and addresses managed either fully (*Standalone*) or partially (*Delegated*) by the services themselves. Specifically, *Standalone* ICE services manage all addresses themselves, while *Delegated* ICE services provide deposit addresses managed by the services, using hot wallets to aggregate user deposits before transferring them to CEXes.

The standard and methodology for collecting ICE services, as detailed in Section 3.2, encompass the majority of known ICE services. The nine *Managed* services examined in this study, particularly the *Standalone* type, are the most representative in terms of community influence (measured by metrics on social networks) and usage in malicious activities.

6.2 Limitations of the Matching Algorithm

Our proposed matching algorithm in Section 5 has the following limitations.

First, this algorithm can only be applied to ICE services of the *Standalone* type. However, as discussed in Section 4, a large portion of activities and most of the abuse in the ecosystem are contributed by the *Standalone* ICE services. We have assessed the effectiveness of the proposed matching algorithm and confirmed its ability to associate transactions with their final destinations in Section 5. We have also introduced real-world cases in which malicious actors conduct multi-hop transfers of illicit funds before depositing them into CEXes and use ICE services to prevent money flow tracing analysis. These examples demonstrate that this research and the proposed matching algorithm are important for understanding the ecosystem and tracing illicit fund flow when ICE services are involved in the money laundering process in malicious activities.

Second, this algorithm cannot be applied to the Bitcoin ecosystem. It requires finding all transactions related to the services to locate user deposit and withdrawal transactions. However, as outlined in Section 3, the UTXO model of Bitcoin means that many ICE services do not consolidate funds into hot wallets on these blockchains, making it difficult to segregate service-related transactions.

Lastly, this algorithm may require further refinement to improve accuracy and reduce false positives, especially regarding the delay threshold.

6.3 The AML Policy of the ICE Services

Compared to mixing services [49], which are dedicated to Bitcoin mixing, ICE services are more general centralized services that support asset bridging across multiple chains. While ICE services do not require registration or identity information (as requested by KYC requirements), most of them claim that they have implemented an AML policy to ban blacklisted addresses, freeze potentially malicious user requests, and maintain detailed records of user requests.

However, we argue that current AML policies enforced by ICE services are ineffective, as demonstrated by the usage analysis of ICE services in malicious activities in Section 4.4. Address blacklists and manual reports, which may take hours (or even days) to process, are not efficient for promptly banning malicious addresses following an incident. Typically, investigators need to submit formal requests to access internal records from these services. In contrast, our proposed algorithm can quickly identify withdrawals by malicious actors using ICE services, enabling immediate action.

7 Related Works

7.1 Research on ICE Services

To the best of our knowledge, we are the first to propose the concept and conduct a comprehensive analysis on ICE services. Several previous studies have analyzed services with similar features. Specifically, Yousaf et al. [50] focused on the analysis of a popular ICE service, ShapeShift, for user behaviors and patterns, using a poorly designed API to retrieve the *full* information about historical requests. However, ShapeShift fixed the API issue and imposed strict registration and KYC policy after reported by The Wall Street Journal [38] to be widely used in money laundering, making it a CEX rather than an ICE service.

Following on the work of Yousaf et al. [50], Zhang et al. [55] provides a preliminary analysis on ShapeShift and other ICE services using heuristic methods. Compared to these research studies, our work defines and systematically analyzes ICE services, including a detailed workflow and classification analysis, comprehensive statistical measurements, and an algorithm to match the inputs and outputs for ICE services.

7.2 Money Laundering Tools in Blockchain

The need for money laundering for malicious activities in the blockchain ecosystem has been widespread. However, analyzing money laundering tools is difficult due to the lack of on-chain analysis tools and ground-truth data. To further enhance user privacy on Bitcoin, mixing services [49] are used to mix the money flow between different users. For Ethereum and EVM-compatible networks, Zero-Knowledge Proof (ZKP) based cryptocurrency mixers [47], the most typical of which is Tornado Cash, are widely used in malicious activities. This study is complementary to empirical studies on real-world methods of money laundering in malicious activities.

8 Conclusion

In this study, we focus on a new type of service called Instant Cryptocurrency Exchange (ICE) services. Compared to CEXes and cross-chain bridges, ICE services provide efficient and privacy-preserving asset bridging to users. Subsequently, ICE services have been abused in malicious activities, while there has been a lack of comprehensive research for them.

In this work, we provide a thorough analysis of ICE services, including their definition, workflow, and classification. Then we conduct a comprehensive measurement on the ecosystem of ICE services, especially focusing on their usage in malicious activities. We have identified $12,473,290 illegal funds laundered through and 432 malicious addresses initially funded by ICE services. Finally, using the insights summarized from the measurement, we proposed a matching algorithm, which is

capable of matching user deposits and withdrawals for ICE services with high accuracy. Using the matching algorithm, we have proven that despite the efficiency of ICE services, they are potentially unable to prevent traceability. Through case studies, we have proven that our proposed algorithm can be useful in tracing illicit funds.

Acknowledgments

We thank all anonymous reviewers for their invaluable comments. This work is partially supported by the National Key R&D Program of China (No. 2022YFE0113200), the National Natural Science Foundation of China (NSFC) under Grant 62172360, U21A20464, and U21A20467. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of funding agencies.

References

[1] Arbitrum. 2024. *Arbitrum - The Future of Ethereum.* Retrieved July 16th, 2024 from https://arbitrum.io/
[2] Binance. 2023. *Binance - Cryptocurrency Exchange for Bitcoin, Ethereum & Altcoins.* Retrieved October 10th, 2023 from https://www.binance.com/
[3] Binance. 2024. *BNB Smart Chain (BSC): Bring Smart Contracts to BNB Chain.* Retrieved July 16th, 2024 from https://www.bnbchain.org/en/bnb-smart-chain/
[4] Tom Blackstone. 2023. *Arcadia Finance hacker used reentrancy exploit, team demands return of funds.* Retrieved December 21st, 2023 from https://cointelegraph.com/news/arcadia-finance-hacker-used-reentrancy-exploit-team-demands-return-of-funds
[5] The Block. 2023. *Multichain pledges to compensate users after 'force majeure' incident.* Retrieved December 21st, 2023 from https://www.theblock.co/post/232120/multichain-pledges-to-compensate-users-after-force-majeure-incident
[6] BlockSec. 2023. *MetaDock Browser Extension | MetaDock.* Retrieved December 21st, 2023 from https://blocksec.com/metadock
[7] BlockSec. 2023. *Twitter.* Retrieved July 29, 2024 from https://x.com/BlockSecTeam/status/1648907160699695109
[8] BlockSec. 2023. *Twitter.* Retrieved December 21st, 2023 from https://twitter.com/BlockSecTeam/status/1612704890903728131
[9] Changelly. 2024. *Cryptocurrency Exchange - Crypto & Altcoin Swap Platform with Lowest Fees.* Retrieved July 16th, 2024 from https://changelly.com/
[10] Jesse Coghlan. 2023. *Base's largest DEX, LeetSwap, halts trading amid exploit concerns.* Retrieved December 21st, 2023 from https://cointelegraph.com/news/leetswap-dex-halts-trading-amid-exploit-fears
[11] Jesse Coghlan. 2023. *Twitter.* Retrieved December 21st, 2023 from https://cointelegraph.com/news/notorious-monkey-drainer-crypto-scammer-says-they-re-shutting-down
[12] Coinbase. 2023. *Coinbase - Buy & Sell Bitcoin, Ethereum, and more with trust.* Retrieved October 10th, 2023 from https://www.coinbase.com/
[13] Coinbase. 2024. *How long does a purchase or deposit take to complete? | Coinbase Help?* Retrieved July 16th, 2024 from https://help.coinbase.com/en/coinbase/trading-and-funding/buying-selling-or-converting-crypto/how-long-does-a-purchase-or-deposit-take-to-complete
[14] Coinbase. 2024. *What is bridging in crypto?* Retrieved July 16th, 2024 from https://www.coinbase.com/learn/wallet/what-is-bridging-in-crypto
[15] Etherscan. 2023. *Ethereum (ETH) Blockchain Explorer.* Retrieved October 10th, 2023 from https://etherscan.io/
[16] Best Exchange. 2024. *BtcTurk - Finansal Hizmetler.* Retrieved July 16th, 2024 from https://www.btcturk.com/
[17] Stargate Finance. 2023. *Stargate.* Retrieved December 21st, 2023 from https://stargate.finance/
[18] FixedFloat. 2024. *FixedFloat | Instant cryptocurrency exchange.* Retrieved July 16th, 2024 from https://ff.io/
[19] The Ethereum Foundation. 2024. *ETHEREUM VIRTUAL MACHINE (EVM).* Retrieved July 16th, 2024 from https://ethereum.org/en/developers/docs/evm/
[20] Bowen He, Yuan Chen, Zhuo Chen, Xiaohui Hu, Yufeng Hu, Lei Wu, Rui Chang, Haoyu Wang, and Yajin Zhou. 2023. TxPhishScope: Towards Detecting and Understanding Transaction-based Phishing on Ethereum. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS 2023, Copenhagen, Denmark, November 26-30, 2023*, Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda (Eds.). ACM, 120–134. https://doi.org/10.1145/3576915.3623210
[21] Y. Hu, Y. Sun, Y. Chen, Z. Chen, B. He, L. Wu, Y. Zhou, and R. Chang. 5555. MFGSCOPE: A Lightweight Framework for Efficient Graph-based Analysis on Blockchain. *IEEE Transactions on Dependable and Secure Computing* (jul 5555), 1–16. https://doi.org/10.1109/TDSC.2024.3431011

[22] ImmuneFi. 2023. *Hack Analysis: Platypus Finance, February 2023.* Retrieved December 21st, 2023 from https://medium.com/immunefi/hack-analysis-platypus-finance-february-2023-d11fce37d861

[23] KuCoin. 2023. *Crypto Exchange | Bitcoin Exchange | Bitcoin Trading | KuCoin.* Retrieved October 10th, 2023 from https://www.kucoin.com/

[24] TRM Labs. 2023. *Illicit Crypto Ecosystem - A Comprehensive Guide to Illicit Finance Risks in Crypto.* Retrieved December 21st, 2023 from https://www.trmlabs.com/report

[25] Parikshit Mishra. 2022. *Crypto Launchpad Team Finance Suffers $14.5M Exploit.* Retrieved December 21st, 2023 from https://www.coindesk.com/business/2022/10/27/crypto-platform-team-finance-suffers-145m-exploit/

[26] Poly Network. 2023. *PolyBridge.* Retrieved December 21st, 2023 from https://bridge.poly.network/

[27] U.S. Department of the Treasury. 2022. *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash.* Retrieved December 21st, 2023 from https://home.treasury.gov/news/press-releases/jy0916

[28] PeckShield. 2022. *Twitter.* Retrieved July 29, 2024 from https://x.com/PeckShieldAlert/status/1579842411907362816

[29] PeckShield. 2022. *Twitter.* Retrieved December 21st, 2023 from https://twitter.com/PeckShieldAlert/status/1587271475475939328

[30] PeckShield. 2022. *Twitter.* Retrieved December 21st, 2023 from https://twitter.com/PeckShieldAlert/status/1662650590546264064

[31] PeckShield. 2024. *Twitter.* Retrieved July 29, 2024 from https://x.com/PeckShieldAlert/status/1813845309342306496

[32] PeckShield. 2024. *Twitter.* Retrieved July 29, 2024 from https://x.com/PeckShieldAlert/status/1770732800615776604

[33] PeckShield. 2024. *Twitter.* Retrieved July 29, 2024 from https://x.com/PeckShieldAlert/status/1789942188454850841

[34] PeckShield. 2024. *Twitter.* Retrieved July 29, 2024 from https://x.com/PeckShieldAlert/status/1759399281201733917

[35] PeckShield. 2024. *Twitter.* Retrieved July 29, 2024 from https://x.com/PeckShieldAlert/status/1767078331693084773

[36] Bitcoin: A peer-to-peer electronic cash system. 2008. *Nakamoto, Satoshi.* Technical Report.

[37] Ezra Reguerra. 2022. *Hackers drain $8M in assets from Bitkeep wallets in latest DeFi exploit.* Retrieved July 29, 2024 from https://cointelegraph.com/news/hackers-drain-8m-in-assets-from-bitkeep-wallets-in-latest-defi-exploit

[38] Justin Scheck and Shane Shifflett. 2018. *How Dirty Money Disappears Into the Black Hole of Cryptocurrency.* Retrieved October 10th, 2023 from https://www.wsj.com/articles/how-dirty-money-disappears-into-the-black-hole-of-cryptocurrency-1538149743

[39] SideShift. 2024. *SideShift.ai - REST API.* Retrieved July 16th, 2024 from https://docs.sideshift.ai/

[40] SwapSpace. 2023. *SwapSpace - More than a crypto exchange.* Retrieved October 10th, 2023 from https://swapspace.co/

[41] SwapZone. 2023. *Instant cryptocurrency exchange aggregator - Swap crypto with the Lowest Fees.* Retrieved October 10th, 2023 from https://swapzone.io/

[42] Polygon Technology. 2024. *Polygon PoS | The most efficient blockchain protocol.* Retrieved July 16th, 2024 from https://polygon.technology/polygon-pos

[43] Tornado.Cash. 2022. *Tornado cash. Non-custodial private transactions on Ethereum.* Retrieved July 16th, 2024 from https://github.com/tornadocash/tornado-core

[44] Tusima. 2023. *Cross-Chain Bridges: An Introduction, Current Status, and Risks.* Retrieved December 21st, 2023 from https://medium.com/@TusimaNetwork/cross-chain-bridges-an-introduction-current-status-and-risks-2f99cd0c28db

[45] Uniswap. 2023. *Home | Uniswap Protocol.* Retrieved December 21st, 2023 from https://uniswap.org/

[46] Fabian Vogelsteller and Vitalik Buterin. 2015. ERC-20: Token Standard. *Ethereum Improvement Proposals* 20 (2015).

[47] 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*, Ying Ding, Jie Tang, Juan F. Sequeda, Lora Aroyo, Carlos Castillo, and Geert-Jan Houben (Eds.). ACM, 2022–2032. https://doi.org/10.1145/3543507.3583217

[48] Gavin Wood et al. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper* (2014), 1–32.

[49] 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 *WWW '21: The Web Conference 2021, Virtual Event / Ljubljana, Slovenia, April 19-23, 2021*, Jure Leskovec, Marko Grobelnik, Marc Najork, Jie Tang, and Leila Zia (Eds.). ACM / IW3C2, 33–44. https://doi.org/10.1145/3442381.3449880

[50] Haaroon 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, 837–850. https://www.usenix.org/conference/usenixsecurity19/presentation/yousaf

[51] ZachXBT. 2022. *Twitter.* Retrieved December 21st, 2023 from https://twitter.com/zachxbt/status/1584955933452484613

[52] ZachXBT. 2023. *Twitter.* Retrieved July 29, 2024 from https://x.com/zachxbt/status/1557108652825247746

[53] ZachXBT. 2023. *Twitter.* Retrieved July 29, 2024 from https://x.com/zachxbt/status/1723757797316133240

[54] ZachXBT. 2024. *Twitter*. Retrieved July 29, 2024 from https://x.com/zachxbt/status/1546162687264100354
[55] Zongyang Zhang, Jiayuan Yin, Bin Hu, Ting Gao, Weihan Li, Qianhong Wu, and Jianwei Liu. 2022. CLTracer: A Cross-Ledger Tracing framework based on address relationships. *Comput. Secur.* 113 (2022), 102558. https://doi.org/10.1016/J.COSE.2021.102558

Received August 2024; revised September 2024; accepted October 2024