SoK: A Survey of Mixing Techniques and Mixers for Cryptocurrencies

Juraj Mariani[1,*,†], Ivan Homoliak[1,2,*,†]

[1]*Brno University of Technology (BUT University), Božetěchova 1/2, Brno, 612 00, Czechia*

[2]*Slovak Technical University (Faculty of Informatics and Information Technologies), Ilkovičova 2, Bratislava, 842 16, Slovakia*

Abstract

Blockchain technologies have overturned the digital finance industry by introducing a decentralized pseudonymous means of monetary transfer. The pseudonymous nature introduced privacy concerns, enabling various deanonymization techniques, which in turn spurred development of stronger anonymity-preserving measures. The purpose of this paper is to create a comprehensive survey of mixing techniques and implementations within the vast ecosystem surrounding anonymization tools and mechanisms available in blockchain cryptocurrencies. First, we begin by reviewing classifications used in the field. Then, we survey various obfuscation techniques, helping to delve into actual implementations and combinations of these techniques. Next, we identify the positive and negative attributes of the approaches and implementations included. Moreover, we examine the implications of anonymization tools for user privacy, including their effectiveness in preserving anonymity and susceptibility to attacks and vulnerabilities. Finally, we discuss the challenges and innovations for extending mixing services into the realm of smart contracts or cross-chain space.

Keywords

Survey, mixers, blockchain, privacy-preserving cryptocurrencies, Tornado Cash, CoinJoin, CoinShufle, Zcash

1. Introduction

Blockchain technologies and cryptocurrencies have been on the rising edge since the inception of Bitcoin in 2008 [1]. The decentralized peer-to-peer network effectively removes a centralized intermediary acting as a third party that is present in conventional banking. The elimination reduces costs and increases transaction efficiency. Additionally, by utilizing cryptographic techniques, blockchains ensure secure and transparent record-keeping across the network. An important thing to note is that, contrary to popular belief, blockchain transactions are not anonymous but rather pseudonymous due to the utilization of blockchain addresses that can be clustered. On top of clustering, blockchain addresses can be even linked to IP addresses (e.g., with the utilization of network-level information), providing a binding between physical world identifiers and pseudonymous identifiers. This has led to various methods that focused on increasing anonymity, such as mixing services. Mixing services achieve disconnection between senders and receivers by obscuring the path their transactions take. There are two approaches to mixing: centralized and decentralized, both with their respective pros and cons. Whereas decentralized methods use peer-to-peer networks and security protocols to provide trustless and censorship-resistant mixing, centralized solutions usually need a trusted external middleman to facilitate the mixing process. The argument between centralized and decentralized approaches to mixing continues to be strong, with each demonstrating certain compromises regarding security, convenience, and privacy. This is due to the ever-growing desire for privacy, anonymity, and inability to be tracked in the finance sector.

Therefore, we provide this compilation, summarizing existing mixing approaches and shedding light on their core, underlying principles. In addition, we analyze selected exemplary implementations to

---

understand their practical applications and limitations. In contrast to related work, our focus is directed towards identifying implementational differences that impact security and anonymity.

1.1. Existing surveys

Although there are many surveys looking into different mixing services [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13], they use similar classification criteria, ranging from surface-level observations to inner mechanisms and functionalities that facilitate the process of mixing.

Classification criteria. The most common criterion for classifying mixing services is the presence of a centralized control element, which divides them into centralized and decentralized. Wu et al. [2] assume mixing within the same chain or across various chains, distinguishing cross-chain and single-chain mixing services. We also identify privacy-preserving cryptocurrencies as a type of mixing service. Although not a mixing service in a typical sense, these cryptocurrencies try to maintain privacy and anonymity by hiding transaction details (incl. sender, receiver, and the amount sent) and executing smart contracts in a secure, verifiable, and privacy-preserving manner. Similarly, we consider the capabilities of centralized exchanges (CEXes) as a means to execute mixing either within a CEX or between two CEXes. Mixing services can also be classified according to the inner processes to obfuscate the flow of crypto-tokens, e.g., by swapping, shuffling, zero-knowledge proofs, etc.

1.2. Methodology of paper selection

The selection methodology of papers in our survey consisted of a multistage iterative process of studying and extracting relevant information from articles aimed at blockchain from renowned and distinguished platforms, such as IEEEXplore, SpringerLink, ResearchGate, Scopus, and more. Moreover, we included mixing approaches surveyed in existing surveys, such as *Pakki et al.* [6], *Arbabi et al.* [4], *Wu et al.* [2], and *Xu et al.* [5].

1.3. Contributions

Contributions of this paper are as follows:

- We study and compare various mixing services (see Sec. 4) based on predetermined classification criteria,
- We focus on 19 notable approaches to mixing (3 centralized, 9 decentralized, 1 cross-chain service, and 6 cryptocurrencies) and provide a short description of their mechanisms as well as a review of their properties, considering security/anonymity, possible limitations, and use cases.
- We provide an overview of practical mixing solutions, focusing primarily on mechanisms used within these mixing solutions and protocols as well as how those different approaches enhance/hinder privacy and anonymity.

2. Background

Mixing, as proposed by *David L. Chaum* [14], is a structure severing the connection between the recipient and sender. Chaum envisioned a system in which a mail communication between two correspondents *Alice* and *Bob* is firstly forwarded to a structure that transforms the message in a way that the content of the message does not change, but the message from *Alice* to *Mixer* cannot be linked with the message sent from *Mixer* to *Bob*. In this way, to some extent, modern cryptocurrency mixing services work.

Within this work, we define and understand *mixing service* to be *an entity or an approach, which in some way, obfuscates or severs entirely the connection between the sender and the receiver.*

Using this logic, we understand even centralized cross-chain exchanges or privacy-based cryptocurrencies as de facto mixing services. Note that in the case of centralized cross-chain exchanges, the effect of mixing might happen inadvertently as the result of aggregation to save costs.

Anonymity set. Modern mixers, however, rely strongly on the amount of transactions present in the mixing pool – commonly referred to as an *anonymity set*, to ensure anonymity. It is imperative for a mixing service to have an anonymity set of sufficient size for the effectiveness of flow obfuscation scales with it.

Taint analysis [15, 16] is a method of tracking "dirty" coins – taint (coins previously used in illegal activities) and addresses containing them. This technique has undoubtedly brought many criminals to justice, but it has also sparked warranted concerns regarding the anonymity of all transactions.

2.1. Categorizations

2.1.1. Centralization

All existing surveys categorize mixing schemes into either two or three main groups. Determined by the form of a control structure, there are:

- centralized mixing services,
- decentralized mixing services
- centralized cross-chain approaches,
- (decentralized) privacy-preserving cryptocurrencies.

2.1.2. Inner Processes

An important grouping feature in mixers is the principle of obfuscation. The ecosystem of existing techniques is vast; therefore, we focused on the approaches and methods used by the services described in the included papers and practical services (see Sec. 4). The considered obfuscation techniques involve:

- swapping (e.g., [17, 18]),
- shuffling (e.g., [19, 20]),
- aggregation (e.g., [9, 10, 21]),
- peeling chains (e.g., [9, 10]),
- randomized fees (e.g., [10, 22, 23, 24, 25, 21, 26, 27]),
- randomized delays (e.g., [10, 22, 17, 19, 20, 23, 24, 25, 18, 26, 27]),
- address freshness (e.g., [22, 17, 19, 20, 23, 21, 26]),
- off-chain transactions (e.g., [9, 10, 23]),
- zero-knowledge proofs (e.g., [24, 25, 27]),
- other techniques, such as cross-chain transactions (e.g., [28, 29, 30, 31]), ring signatures (e.g., [26, 23]), TEEs (e.g., [22, 32, 33, 34, 35]), etc.

For a detailed description of these techniques, see Sec. 3

2.1.3. Proposals vs. Implementations

Finally, we can divide approaches by their academic nature vs. the real-world implementation: This results into the following categories:

1. peer-reviewed publications from academia without any implementation or with a proof-of-concept implementation;
2. peer-reviewed publications from academia with full implementation;
3. fully operational implementation, potentially with a white-paper.

3. Categories and Mixing Primitives

In this section, we define and enumerate categories of academic mixing scheme proposals based on the aforementioned grouping factors and illustrate their characteristic features (for details of proposals see Sec. 4).

3.1. Categorization based on (de-)centralization

Centralized mixing service is an unintuitive approach to fund transfer obfuscation in an otherwise decentralized network. The advantage of having a centralized mixing body is reduced network communication overhead and, therefore, increased efficiency and coordination [4, 3]. They provide an easily expandable and straightforward interface at the cost of a centralized nature. A centralized institution is in its entirety trust-based, meaning that users rely on the reputation and goodwill of service providers not to be rid of their capital [3]. Another thing to mention is the opaqueness of a centralized mixer, where such a service may keep track of user information. That is highly undesirable due to the risk of mixers being associated with and facilitating illegal money laundering [7], which can result in legal obligations to provide data to authorities or seizures of said information (as was the case for Bitcoin Fog [36] or Helix [37]).

Decentralized mixers meet the vision of a decentralized service – a key concept for blockchains. A direct consequence can be reduced operation speed and difficulties with scalability. Although not suffering from a centralized trust-based architecture prone to scamming, decentralized mixing services can also suffer from certain attacks. An example of such an attack is a DoS-type attack in which an attacker enters the mixing pool along with other users. The attacker then refuses to sign the transaction, resulting in the inability to execute mixing (famous examples are CoinJoin-based systems [17]). Another possible attack (Sybil attack [38]) can happen when the adversary controls a majority or a large number of transactions in the mixing pool. This allows them to better track and deanonymize other users, rendering the mixing process ineffective.

Centralized cross-chain exchanges *Wu et al.* identified another supplementary class of mixing – cross-chain services [2, 39]. These services further impede taint analysis by transferring funds between cryptocurrencies. They require extensive synchronization and robustness in order to facilitate safe and lossless exchange. The comprehensive list of requirements outlined by *Han et al.* [40] requires database-like and blockchain-like security and resilience qualities. As they are primarily used to transfer currencies across different networks, they do not directly provide mixing in the traditional sense. However, they might execute actions akin to a mixing service – by aggregating transactions and then redistributing them in another currency to the recipient. The path and flow of coins are often obscured by the hidden mechanics of private exchange servers and could offer some degree of obfuscation.

Privacy-preserving cryptocurrencies Additionally, we also identify privacy-preserving cryptocurrencies (e.g., Monero or Oasis). While not mixing services in a traditional sense, we categorize such cryptocurrencies into the mixing space. They often work on the principle of cryptographically hiding the sender, recipient, and the amount sent by a transaction, typically by ring signatures, ZKPs, or encryption, reversible only within a TEE. A mixing-like effect is achieved, as we cannot directly uncover the secret values; we can only prove a transaction and all the values within it are valid.

Although no direct connection might be found, (machine learning) algorithms may, with a certain level of accuracy, be able to find a connection between accounts and deanonymize. Attacks, such as temporal analysis, can leak the hidden link under the right conditions (early withdrawal and use of mixed coins).

3.2. Categorization of primitives used in mixing

Mixing can be based on various mechanism and their combinations. We briefly describe these mechanisms in the following.

Swapping utilizes a simple concept of not transferring funds directly but creating an artificial and (depending on the implementation and desired anonymity) vast, oriented graph structure of transactions.

Funds can be passed between the addresses of other participants and the addresses of the mixing service to interfere with the taint analysis [2].

Shuffling is a mixing technique devised by *Ruffling et al.* and utilized by CoinShuffle [19]. Shuffling functions by grouping a sufficient number of users to form an anonymity set. Within this set, users are ordered into a sequence to begin the shuffling process. The process starts with the first user in sequence, and throughout the process, all transactions are forwarded to the last user. Every user in a sequence produces a transaction and signs it with their secret key. Then, they use public keys of the users one after another to encrypt the transaction(s). Users in the sequence receive all transactions created by users before them and decrypt them using their secret key. The final user verifies the entire chain of transactions created within the sequence and broadcasts them to the environment.

Aggregation or **clustering**, as the name suggests, consolidates all user transactions into a single address [41]. By doing so, the available information to outside observers regarding the source is reduced. In contrast to joint transactions (utilized by CoinJoin, for instance), where transactions from different users are combined in a single point, aggregation focuses on merging multiple transactions from a single user, thereby minimizing the visibility of individual transaction inputs and enhancing privacy and anonymity.

Peeling chains are described by *Balthasar* [11] as sequences of transactions (in the most simplified and academic case as transactions with one input and two outputs) in which a mixing service accumulates funds from users in the anonymity set and redistributes them based on users' needs to output addresses. The redistribution itself involves creating a transaction where a limited amount of funds is transferred to a destination address(es), and the rest of the sum is delivered to another address belonging to the mixing service, creating a tree-like structure.

Randomized fees make the use of mixing processes significantly more challenging to detect by simulating interactions between ordinary users. The approach appeared in MixCoin [12] as a mixer anti-detection measure because a compromised mixing service means a weakened anonymity provided by mixing. Therefore, randomized fees exist not to disconnect the receiver and sender from one another but as a means to retain integrity and hinder detection.

Randomized delay is another process of detection avoidance deployed by mixing services. The mechanism introduces distortions in the timing of processing and production of transactions, thereby decreasing the likelihood of discovery. These delays introduce uncertainty into the transaction process, disrupting the ability to infer patterns or correlations based solely on transaction timing [8]. As opposed to randomized delays, some mixing services provide fixed delays, which can be seen as an advantage to speed-up mixing but on the other hand might cause easier deanonymization.

Unused address generation has been identified as crucial in assisting anonymity on blockchains [42]. It is among the best practices to use a different address in every transaction in the mixing process. It is imperative for the (centralized) mixing body to utilize new addresses in order not to be detected simply by analyzing input and output addresses of past transactions on the ledger, and, by doing that, deanonymize and expose their customers.

Off-chain solutions offer additional user privacy while being lightweight and scalable. Off-chain solutions are a valuable foundation for quick mixing services, mainly in Bitcoin-like systems with lengthy block creation intervals [43]. Users in the anonymity set together create a lightweight transaction with the mixing service, and upon the exchange of capital, only one transaction is broadcast, and more privacy might be maintained than regular transactions.

Zero knowledge proofs are protocols in which prover and verifier try to establish an objective truth. The prover attempts to prove to the verifier the debated term is true, which in the context of blockchains is proof of capital ownership, without disclosing details about themselves [44]. ZKPs can be used in mixing services to provide proof of ownership without disclosing sensitive information.

Other primitives like cross-chain transactions physically sever the connection between recipients by altering the transaction path from within the blockchain network to inter-blockchain [45]. In addition to mixing and privacy usage, these transactions implement interoperability between different chains. *Ou et al.* recognizes this virtue, provides an overview of existing cross-chain services, and outlines necessary principles such systems must possess [46].

4. Review of approaches

Here, we review mixing schemes, which encompass both theoretical proposals and real-world implementations. We examine these designs for their conceptual innovations and the privacy guarantees they strive to provide, while also highlighting any limitations that arise from specific design choices.

4.1. Centralized approaches to mixing

In order to assess and compare the anonymization and security measures provided by various mixing strategies, we must first focus on a list of selected representatives. Centralized mixing platforms such as Helix, Bitcoin Fog, BitLaunder, or Obscuro employ distinct methodologies to anonymize transactions and enhance privacy for users. Each platform offers unique features, protocols, and levels of anonymity, catering to different user preferences and requirements. By exploring the available and popular mixer choices, we can analyze, evaluate, and compare the mechanisms, strengths, and limitations to other mixing services.

Helix. There have been numerous analyses conducted on the operation, security, and privacy extending measures employed by Helix. At the peak of its popularity, Helix has supposedly enabled money laundering of great proportions [13]. This spark of activity has been highly incentivized following the 2017 cease of function and the seizure of Helix and its owner by the government of the United States of America [37]. Based on the approaches outlined above, we can characterize Helix as a service using several privacy measures. Based on the analyses of *Balthasar* [11] and *Möser* [8], it is clear that Helix utilized a form of centralized swapping. To ensure additional privacy, Helix utilized a strategy of multiple hops to swap the coins numerous times, and thus make taint analysis difficult. It also uses innovative approach of clean coins, whereby giving users freshly minted and untainted coins it makes transfers even less traceable. However, it uses approaches commonly associated with reduced privacy, mainly fixed fees and a peeling chain to distribute to multiple users in a single transaction. *Balthasar* identifies this functionality as anonymity-compromising.

Bitcoin Fog. Bitcoin Fog is a Tor-exclusive mixing service belonging to the overall most popular services on the market. Bitcoin Fog utilizes joint transactions to concentrate funds from the entire mixing pool in a handful of its addresses. From there it then sequentially redistributes capital to the end user. Fog's mixing addresses contain large sums of capital and are iteratively split to smaller chunks and to users. Along with random delay mechanisms, it routes funds through randomized transactions to hinder detection. *Möser*'s experiments [8] support these claims by stating that there is no apparent link to an outside observer, particularly due to the delays and randomness. However, an informed adversary with additional context can potentially find evidence of connected transactions and deanonymize users. Furthermore, *Xu et al.* [5] used machine learning algorithms to analyze the topology of services, including Bitcoin Fog and found a surprising lack of features, both topological and contextual, revealing the nature of transactions.

Mixing

Centralized Cross-chain Exchanges
- Aggregation
- Random Delay
- Off-Chain

Privacy-preserving Cryptocurrencies
- ZKPs
- Ring Signatures
- TEEs

Mixing Services

Centralized
- Peeling Chain
- Aggreggation
- Cross-Chain Transactions
- Random Delay
- Random Fee
- Off-Chain

Decentralized
- Random Address
- TEEs
- Swapping
- Shuffling
- Aggregation
- Off-Chain
- ZKPs
- Ring Signatures
- Random Delay
- Random Fee

Figure 1: Categorization of mixing mechanisms.

Obscuro. Although being a centralized service, Obscuro [22] operates distinctly similar to decentralized mixing services. The motivation behind Obscuro is the use of Trusted Execution Environments (TEEs), notably Intel SGX technology [47]. The use of TEEs likely provides additional security and integrity guarantees for Obscuro's mixing operations. TEEs are hardware-based security features that provide a secure and isolated execution environment for sensitive code and data, enhancing the confidentiality and integrity of operations performed within them.

While Obscuro's centralized mixer architecture may have simplified its operations and potentially improved security, it also introduced unwanted vulnerabilities to the system. *Young et al.* [48] describe the presence of specific log files capable of deanonymization if revealed, making the process practically obsolete.

4.2. Decentralized approaches to mixing

In contrast to centralized mixing platforms, decentralized mixers offer alternative approaches to anonymizing transactions and enhancing privacy for cryptocurrency users. It is worth noting that each decentralized mixer uses unique cryptographic protocols, trustless mechanisms, and privacy-enhancing techniques to achieve its objectives. Decentralized solutions are among the options available to users who prioritize privacy and security while minimizing reliance on centralized intermediaries. This text explores the diverse landscape of decentralized mixers, delving into the intricacies of their methodologies and assessing both their strengths and weaknesses.

CoinJoin. CoinJoin is a technique used in Bitcoin transactions to enhance privacy and confidentiality. In 2013, Bitcoin developer Gregory Maxwell created CoinJoin [17], a method that enables multiple users to merge their transactions into a single transaction without the need to expand or modify the existing Bitcoin protocols. This process helps to obscure the connection between input and output addresses. The essence of CoinJoin lies in users of the mixing pool establishing a meeting point (a server) that serves as a collector and creator of the joint collective transaction. The anonymity stems from the indirect interactions between users within the pool. Only the rendezvous server knows their addresses.

We can see that CoinJoin, while providing some degree of anonymity, is fragile. Though there have been continuous efforts to fortify the scheme through various means such as the implementation of CoinJoin variants such as CoinShuffle [19] and CoinParty [20], as well as the integration of additional privacy-enhancing technologies like zero-knowledge proofs and ring signatures or arbitrary values [49]

with differing levels of success and popularity.

CoinShuffle. CoinShuffle [19] is an extension of CoinJoin, i.e., a decentralized mixing protocol designed to enhance privacy and anonymity in cryptocurrency transactions. It utilizes a combination of approaches and widely used cryptographic primitives to achieve these goals. It is a fully decentralized protocol without the need for a rendezvous server, as was the case for CoinJoin, and it employs trustless mixing transactions among participants [2]. It uses the shuffling method described in Sec. 2.1 between mixing peers to make linkages between users anonymous. Like CoinJoin and CoinParty, CoinShuffle provides mixing services free of any service fees due to the lack of centralized authority. Its decentralized nature not only enhances privacy but also mitigates the risk of censorship and single points of failure inherent in centralized mixing services. While single points of failure are not a problem, DoS and Sybil-type attacks are prevalent [17, 38].

CoinParty. CoinParty [20] is a decentralized mixing protocol designed to replace CoinJoin and CoinShuffle mixing protocols by enhancing privacy and transaction anonymity. It introduces threshold cryptography, allowing multiple parties to jointly create and co-sign mixing transactions without revealing too much information. This approach increases overall fault tolerance by distributing trust among multiple participants and preventing any single entity from compromising the mixing process. It forces participants to commit to their inputs and outputs before the mixing process begins, preventing any party from altering their transactions. Using a set of mixing peers and a shuffling process similar to CoinShuffle peers, it establishes a disconnected fund path.

Möbius. Möbius is, unlike all the aforementioned approaches, a mixing service in the form of a smart contract accessible for the Ethereum cryptocurrency. A distinction of Möbius is the utilization of ring signatures, whereby one achieves privacy by hiding behind a group. *Chaum* [14] and later *Shamir* with *Rivest* [50] described a system of group anonymity with preserved proof of ownership. Therefore, funds can be obtained from a Möbius smart contract without revealing the identity of the sender [23].

AMR. AMR is another option for Ethereum anonymity. The service leverages zk-SNARK zero-knowledge proofs [44, 51] with a privacy-driven reward scheme without the employment of third parties. It supports an extensive anonymity set to enhance privacy. Through these approaches, the service guarantees disconnection between depositing and withdrawing transactions [24]. AMR's promises of anonymity and privacy guarantees greatly hinge on the anonymity set available to the smart contract. The size of the set is greatly influenced by the advertised interest reward, which incentivizes users to participate in mixing.

Tornado Cash. Tornado Cash is an Ethereum zero-knowledge privacy tool – a smart contract that accepts transactions with a static number of funds given in advance so that the capital can be later withdrawn with no reference to the original transaction. Users can deposit N-ETH, also known as a coin, into the smart contract along with a hashed secret value. The hash is stored within the contract and can later be used with the help of zero-knowledge proof that the withdrawing subject knows the secret used to create said hash [25]. To further enhance privacy, Tornado Cash supports the use of relayers – entities capable of withdrawing funds from the contract for a user. This is useful for a fresh address that would be unable to pay the gas fee for the transfer. The relayer receives the information necessary for the withdrawal and takes a fee to facilitate the process, as well as the gas fee.

This mixing process has been a popular method of fund flow obfuscation. There have been analyses regarding the privacy provided by Tornado Cash, with results by *Teng et al.* [52] hinting that the most significant hurdle users face is time. A clear connection can be seen between the input and output addresses, which deposit and withdraw identical amounts in a short period of time. The longer the funds stay in the mixing contract, the less likely it is to connect the address endpoints, making the mixing more effective.

Wasabi Wallet. Wasabi Wallet[1] along with Samourai Wallet[2], JoinMarket[3] and others are wallet software with built-in capabilities of mixing transactions, therefore an argument could be made to classify them as mixers. The above-specified Bitcoin wallets utilize variations of the CoinJoin protocol, mainly Chaumian CoinJoin. Transactions are directly executed on the blockchain without needing a trusted third-party server, removing the possibility of attacks against said third party. Wasabi Wallet also supports access through the Tor network, increasing anonymity even more [17, 18].

Zerocoin. Zerocoin's cryptographic structure connects with Bitcoin without altering the security structure and makes use of conventional cryptographic primitives. It may be used to anonymize bitcoins, which can subsequently be spent in "real" transactions with a reduced possibility of detection. This may be accomplished by including Zerocoins in Bitcoin transactions and declaring that they are only valid if signed by a subset of the Zerocoin processing nodes. Zerocoin-aware nodes can interpret the comments and charge transaction fees for validation based on the proofs encoded in the comments, ensuring an incentive for more nodes to offer these services. This technique alters the Zerocoin validation procedure while preserving the anonymity attribute. However, the system may serve as a possible source of information for attackers by disclosing the amount of coins created and spent to all system users. These data may be used to guess the anonymity set for a certain transaction [21].

MixEth. MixEth is a decentralized mixing service designed specifically for Ethereum, operating as a smart contract to provide trustless and efficient coin mixing [27]. Proposed by *Seres et al.*, MixEth leverages zero-knowledge proofs (ZKPs), specifically zk-SNARKs, to ensure that deposits and withdrawals are unlinkable while maintaining transparency and auditability. Users deposit a fixed denomination of Ether into the MixEth smart contract, which stores a hashed commitment. To withdraw, users provide a zk-SNARK proof demonstrating knowledge of the secret associated with a valid deposit without revealing which deposit it corresponds to. This ensures that no link can be established between the input and output addresses.

MixEth's trustless nature stems from its reliance on Ethereum's smart contract infrastructure, eliminating the need for a centralized intermediary. *Seres et al.* emphasize its efficiency, noting that MixEth minimizes gas costs through optimized zk-SNARK circuits, making it practical for Ethereum's high-fee environment. However, MixEth's anonymity is contingent on the size of the anonymity set, which depends on the number of active users depositing into the contract. A small anonymity set can weaken privacy, as an adversary could correlate deposits and withdrawals. Additionally, MixEth is vulnerable to denial-of-service attacks where malicious users flood the contract with deposits to inflate gas costs or disrupt mixing.

4.3. Centralized cross-chain approaches to mixing

Centralized exchanges allow various cryptocurrencies to be traded in a centralized database within the address space of exchanges, thus no transaction is made on public blockchains. However, if users send crypto-currencies to the address space of other exchanges, on-chain transactions need to be executed – the deanonymization can be made with the internal information about the address ownerships of the users at those exchanges. Nevertheless, such transactions might virtually aggregate multiple cross-exchange transfers and thus anonymize senders and/or recipients. Moreover, random delays can be introduced into this process.

Centralized exchanges. Major centralized cryptocurrency exchanges like Binance [28], Coinbase [29], Kraken [30], and OKX [31] can facilitate cross-chain mixing through their centralized trading infrastructure. This model leverages aggregation, where user deposits are pooled into exchange-controlled wallets, obscuring individual transaction origins. Cross-chain trades, such as converting

---

[1]https://wasabiwallet.io/
[2]https://samouraiwallet.com/
[3]https://en.bitcoin.it/wiki/JoinMarket

Bitcoin to Ethereum, might sever transaction paths across blockchains, while randomized delays for blockchain confirmations and unused address generation for withdrawals may further enhance privacy. An advantage is an already large user base that forms a substantial anonymity set, diluting transaction traceability.

Security relies on robust exchange infrastructure, but anonymity is limited by centralized record-keeping, making user data vulnerable to regulatory requests. Taint analysis can exploit transaction patterns if volumes are low or fees are fixed. This model suits traders seeking blockchain interoperability, though dedicated mixers like Tornado Cash often offer far stronger privacy. Centralized exchanges, implemented as parts of trading operations, often lack formal academic analysis but are evident in industry practices [39, 7].

4.4. Privacy-preserving cryptocurrencies

Monero. Monero [26] is a privacy-focused cryptocurrency that inherently incorporates mixing-like functionality into its core protocol, distinguishing it from services like CoinJoin that operate as add-ons to existing blockchains. Monero achieves transaction anonymity through the use of ring signatures, stealth addresses, and Ring Confidential Transactions (RingCT). Ring signatures, as described by *Noether* [53], obscure the sender by mixing their transaction with others in a ring, making it computationally infeasible to determine the true signer. Stealth addresses ensure that the recipient's address is unique for each transaction, preventing address reuse and enhancing unlinkability. RingCT, introduced to hide transaction amounts, further strengthens privacy by encrypting the amount while allowing verification of transaction validity without revealing sensitive data.

Monero's design eliminates the need for an external mixing service, as every transaction is obfuscated by default. According to *Möser et al.* [54], Monero's ring signatures provide a robust anonymity set, but their effectiveness depends on the ring size and the diversity of inputs chosen. Larger ring sizes increase anonymity but raise computational overhead. Despite its strengths, Monero is not immune to attacks. *Möser et al.* highlight that temporal analysis and heuristic clustering can partially deanonymize transactions, especially if users fail to follow best practices like avoiding same-address reuse or if the network has low transaction volume, reducing the anonymity set. Additionally, Monero's privacy features come at the cost of increased blockchain size and slower verification times compared to Bitcoin-based mixers.

Zcash. Zcash is a privacy-preserving cryptocurrency, originating from Zerocoin, that uses zk-SNARKs to enable *shielded transactions*, which obscure sender, recipient, and amount [55]. Zcash relies on cryptographic zero-knowledge proofs, allowing users to opt for shielded (private) or transparent transactions. Shielded transactions use a shielded pool, where zk-SNARKs ensure privacy without revealing transaction details [56]. Zcash's privacy is optional, reducing its anonymity set compared to other privacy-preserving cryptocurrencies with mandatory privacy (e.g., Monero), as many users opt for transparent transactions for compatibility [26]. Vulnerabilities include potential trusted setup compromises and deanonymization through usage patterns [57].

Oasis & Secret. Oasis and Secret are layer-1 blockchains prioritizing privacy through confidential smart contracts executed within TEEs, such as Intel SGX [47]. They process encrypted transaction data (sender, recipient, amount) and metadata in secure enclaves, ensuring confidentiality during execution. Oasis employs *ParaTimes*, customizable computation layers for private transactions, while Secret uses *secret contracts* with cryptographic techniques like secret sharing to maintain privacy during validation [32, 33, 58]. Both obscure transaction details, with anonymity sets determined by user interactions within their respective smart contract frameworks. Their TEE-based approach should provide strong security but can be vulnerable to hardware exploits, such as side-channel attacks, which could expose transaction logs [59].

Although broadly similar in the utilization of TEEs, the currencies differ in execution and implementation of these processes. While Oasis relies heavily on the TEE for security guarantees, Secret enhances

Table 1

Comparison of selected mixing services [4].

Name	Decentralized	Mechanisms									Peer-rev.	Impl. avail.	Account model	Other
		Swap.	Shuffl.	Agg.	Peeling chain	Random fees	Random delay	Fresh addr.	Off-chain	ZKPs				
Helix [9]	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✗	✓	UTXO	–
Bitcoin Fog [10]	✗	✗	✗	✓	✓	✓	✓	✗	✓	✗	✗	✓	UTXO	–
Obscuro [22]	✗	a.	a.	a.	a.	✓	✓	✓	✓	✗	✓	✗	UTXO	TEE
CoinJoin [17]	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	UTXO	–
CoinShuffle [19]	✓	✗	✓	✗	✗	✗	✗	✓	✓	✗	✓	✓	UTXO	–
CoinParty [20]	✓	✗	✓	✗	✗	✗	✗	✓	✓	✗	✓	✓	UTXO	–
Möbius [23]	✓	✗	✗	✗	✗	✓	✓°	✗	✓	✗	✓	✗	Acc.	Ring Sig.
AMR [24]	✓	✗	✗	✗	✗	✓	✓°	✗	✗	✓	✓	✗	UTXO	–
Tornado Cash [25]	✓	✗	✗	✗	✗	✓	✓°	✗	✓	✓	✗	✓	Acc.	–
Wasabi Wallet [18]	✓*	✓	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	UTXO	–
Zerocoin [21]	✓	✗	✗	✓	✗	✓	✗	✓	✗	✓	✓	✓	UTXO	–
MixEth [27]	✓	✗	✗	✗	✗	✓	✓°	✗	✓	✓	✓	✗	Acc.	–
CEX [28, 29, 30, 31]	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✗	✓	–	Cross-Chain
Monero [26]	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✓	✓	UTXO	Ring. Sig.
Zcash [55]	✓	✗	✗	✓	✗	✓	✗	✓	✗	✓	✓	✓	UTXO	–
Oasis [32]	✓	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	Acc.	TEE
Secret [33]	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	Acc.	TEE
Integritee [34]	✓	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✓	Acc.	TEE
Phala [35]	✓	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	Acc.	TEE

* = Wasabi Wallet is a centralized hot wallet provider using a decentralized mixing protocol, a. = applicable, meaning the mechanism is applicable, although not specifically mentioned in the paper. ° = Ethereum mixers' delays can be influenced by user retrieval from the address of the mixer, thus adding user delay.

its TEE-based privacy with secret sharing and encrypted state management. Secret sharing allows validators to verify the correctness of computations without accessing sensitive data, distributing trust across the network [58], meaning the contract states remain confidential even when stored or accessed later. Additionally, as Oasis employs *ParaTimes* layers (compared to Secret's unified anonymity set), the anonymity set is divided into layers, meaning the set is distributed across the system, which could increase the risk of detection.

Integritee & Phala. Integritee and Phala, operating as Polkadot parachains, focus on privacy-preserving computations using TEEs for enterprise (Integritee) and cloud-based applications (Phala) [34, 35]. They execute transactions and smart contracts off-chain in secure enclaves, encrypting data before processing and recording only execution proofs on-chain.

Integritee uses *off-chain workers* for interoperable private computations, while Phala's *pRuntime* supports confidential smart contracts with zero-knowledge proofs for verification [60, 61]. Privacy is, additionally, enhanced by fresh addresses and randomized delays. Like Oasis and Secret, they face TEE vulnerabilities, and small anonymity sets may enable correlation attacks [59].

5. Comparison and Security Analysis of Approaches

The following section offers a comparative security analysis of the various deployed mixing solutions outlined in Sec. 4. By examining their features, mechanisms, performance, and anonymity, this comparison aims to highlight the strengths and weaknesses of the mentioned solution.

5.1. Centralized vs. decentralized

The first comparison metric is the presence or lack thereof of a body governing the obfuscation process. A thing to note is that this work, though including three centralized mixing services, is focused mainly on the decentralized subset (we are counting the cryptocurrencies as decentralized as well). This introduces a skewed ratio of services described within this work that may not correspond to the real world. Although there is a sizable community of researchers in academia providing secure and private

decentralized mixing solutions, a number face implementation difficulties [2]. Some might be too severe, rendering the implementation impossible in the present setting.

Popularity. Within this text, we described 19 mixing "services" - three centralized, nine decentralized, one cross-chain model encompassing all centralized exchanges, and six privacy-preserving cryptocurrencies. Based on the information collected, the centralized counterpart of mixing services (we are considering only actual mixing services here) was much more popular in the crypto space despite the age of decentralized mixing protocols. On the other hand, privacy-preserving cryptocurrencies (decentralized by nature) dominate the space reserved by our definition of mixing (found in Sec. 2). The shift from perhaps weak mechanisms used by the pioneering mixers (e.g., swapping, shuffling or aggregation) toward privacy-preserving cryptographic and hardware constructs (i.e., ZKPs and TEEs) is a step in the right direction, as is the case with Tornado Cash. Despite being forbidden to use, its cryptography was not broken.

Illegal activity. The trend of using centralized mixing services is visible and inferable from the number of reports and assessments on the money laundering industry (using cryptocurrencies) [7, 8]. Although centralized platforms are significantly simpler to maintain and update, they are susceptible to legal seizures and cease-and-desist orders.

Mixing, and centralized mixers in particular, have a tendency to attract illegal activity by promising anonymity and untraceability. With the demonstration of taint analysis, people, including honest civilians seeking better privacy, began to utilize mixing services to escape deanonymization. Centralized mixers have been popular and accessible through the Tor network, providing shelter for those who avoid easy detection. The increase in popularity and traffic alerted authorities (due to illegal activity), and due to most mixers being centralized, they were quickly shut down, and their owners jailed [36, 37].

Decentralized or cross-chain services may not suffer from this effect due to the lack of a centralized authority (in the case of decentralized mixers) or by not being directly responsible for mixing (cross-chain exchanges). Despite this, as could have been seen with Tornado Cash [62], even developers of decentralized mixers may not be safe from repercussions due to misuse of their implementations.

Succeptibility to attacks. Another thing to mention is susceptibility to attacks. Centralized services and exchanges, while often more convenient and user-friendly, pose a threat to users – trust. Users have to trust the centralized entity to use their finances according to predefined specifics. A real and possible scenario is one in which these entities embezzle money from their users and the authors and administrators disappear, leaving users with no way of retrieving it.

Whereas centralized services also provide opportunities for regular attacks conducted toward a server, decentralized services (although actively addressing some issues – centralization and trust, in particular) often offer far simpler attack possibilities without requiring specific skills, as is the case with centralized [17] [38].

In a **Sybil attack**, an attacker creates multiple fake identities (nodes, accounts, or participants) to gain disproportionate control over a network or service. For mixing services, this allows the attacker to dominate the mixing pool, correlate inputs and outputs, thus deanonymize users. Centralized mixers (e.g., Helix, Bitcoin Fog) are particularly vulnerable if they lack participant verification, while decentralized services like Wasabi Wallet (using CoinJoin) can be targeted by attackers flooding the coordination process with malicious peers. As a lot of services rely on a large anonymity set, the problem of Sybil accounts is a serious issue, combated by an extensive pool of users taking part in a transaction.

A **TEE compromise** occurs when vulnerabilities in the hardware, firmware, or software (e.g., side-channel attacks [63], speculative execution flaws like Spectre) allow an attacker to access or manipulate sensitive data, such as mixing keys or transaction details. Services relying on TEEs for privacy are vulnerable if the TEE is breached, undermining their security guarantees. Additionally, memory corruption attacks [64] can enable attackers to exploit SGX vulnerabilities, gaining unauthorized access

to protected memory regions. Rollback attacks [65], which repeatedly reset enclave states, further threaten TEE integrity by allowing manipulation of transaction histories. Moreover, microarchitectural flaws [66] in chip design can introduce exploitable weaknesses, compromising the confidentiality and integrity of TEE-based services.

In a **DoS attack** via transaction denial, a malicious participant in a mixing protocol (e.g., CoinJoin or CoinShuffle) intentionally stalls or aborts the process by refusing to sign a transaction or providing invalid inputs. These attacks exploit the need for synchronous coordination among participants, making decentralized UTXO-based mixers particularly susceptible.

Timing analysis involves analyzing the timing or patterns of transactions to deanonymize users. In Monero, which uses ring signatures to obscure transaction sources, an attacker can exploit temporal correlations (e.g., transaction frequency, block times) to infer which input is the real one in a ring. Timing analysis is a technique for deanonymization, as the time between deposit and withdrawal often makes the strongest connection between nodes. This statistical attack reduces privacy, especially if the attacker controls nodes or observes network traffic.

5.2. Underlying mechanisms

In the modern era of advanced means to conduct taint analysis, there is a need for a resilient and secure mechanism to mix transactions and provide anonymity. Here, we connect existing services with primitives and processes described in Sec. 2.1 and present information regarding the security and anonymity provided.

Centralized mixers. The analyses and tracking of transactions performed by *Balthasar* [11] and *Möser* [8] clearly show the inner structure and key processes involved in famous mixing services such as Helix or Bitcoin Fog. The way they function is that users taking part in mixing send their funds to a dedicated server of the service. The servers (part of the mixing environment) aggregate funds from users and join transactions from different users. The amassed funds are later forwarded (perhaps after a random delay) to central servers. These servers then distribute capital to the respective output addresses using a peeling-chain approach. Both *Balthasar* and *Möser* clearly state that through taint analysis of the input and output addresses, it can be seen that the peeling chain works in clusters and the output addresses are relatively close together, sometimes even in the same peel. This can weaken the process if the attacker has additional information (e.g., Bitcoin amounts).

Xu [5], however, compares Bitcoin Fog with other services (Binance, BitcoinWallet, and CoinPayments) and finds that, although far from ideal, Bitcoin Fog is (out of the mixers specified) the best alternative privacy-wise due to having a diverse peeling tree with little discernible patterns for an uninformed observer.

Obscuro takes a different approach, akin to decentralized systems. It uses shuffling or other decentralized mixing schemes, with order determined by a secure permutation created within trusted environments. The anonymity provided by shuffling is described below and is a constant. Therefore, security is highly dependent on the security of TEE [67, 68, 63, 64, 65, 66, 69] and the process used. Therefore, Obscuro can only be as secure as the underlying mechanism (DoS or Sybil attack-wise) and the trusted hardware. This introduces a new potential for an elaborate attack should the implementation of Obscuro lean on the TEE. Availability of TEEs is also an important consideration, as adoption could be slower due to higher cost. In a centralized service, though, the question of cost does not play a role as significant as in a decentralized service.

Decentralized Bitcoin mixers. A well-defined portion of decentralized mixers of Bitcoin uses either swapping (CoinJoin derivatives) or shuffling (CoinShuffle derivatives) in some form for mixing. Although significant measures are being taken to make decentralized mixers more resilient to simple DoS attacks, the inherent principle is flawed and in favor of centralization.

Anti-detection measures also include randomized delays and fees. An advantage of decentralized mixers is the lack of a mixing fee, which is prevalent in centralized mixing. Centralized services

or decentralized Ethereum smart contract-based solutions use the mixing fee to their advantage by introducing an element of randomness (randomized fees). This helps them to further avoid detection. Another advantage and disadvantage of decentralization is resistance to seizure (unlike centralized, e.g., Helix and more). On the other hand, this means that anonymity depends on the anonymity set and, therefore, on the popularity of the decentralized protocol. The examples provided (Wasabi Wallet and others) can offer decent anonymity if there is a significant enough user base, as the processes require an anonymity set of a specific size. However, as with standalone mixing services, there are still possibilities for an attack. This was allegedly the case for Wasabi Wallet, which violated multiple tactics during the mixing process (lack of randomness in Wasabi's CoinJoin or a weak peeling chain) [70].

Decentralized mixing protocols require off-chain synchronization messages, introducing network overhead along with a possible detection on L2 – L4 network layers.

Decentralized Ethereum mixers.   In Ethereum, a smart contract can facilitate the whole mixing process for the users enlisted in it. Ethereum mixing adopts a hybrid functionality of both types of mixers, where the contract acts as a central authority while not being operated by a governing body or centralized intermediary, providing a transparent and trustless environment for participants. The decentralized nature ensures that the mixing process remains transparent and resistant to censorship, aligning with the notion of decentralization inherent to blockchain technology. A prevalent theme is a shift from the typical mechanisms found in Bitcoin (e.g., swapping, shuffling, etc.) towards randomness (in delay, fees, and addresses) and towards, perhaps, stronger cryptographic constructs. All of the Ethereum mixers we analyzed employed some form of reduced knowledge – either ring signatures (e.g., Möbius) or zero-knowledge proofs (e.g., MixEth and Tornado Cash).

User-added delay.   Research shows [71] that although still possible to track, mechanisms employing zero-knowledge proofs offer strong privacy. A decisive factor, however, remains – the longer the capital stays in the smart contract, the less likely it is to infer a relationship between the sender and the receiver. The same holds true for Bitcoin's UTXO model. User-added delay, although impractical for a conventional user, might help disconnect the connection, perhaps as efficiently as other mechanisms employed by the mixer.

Cross-chain exchanges.   As for crypto exchanges, they do not require a specialized obfuscation process, for the mere act of conversion between currencies might serve as a powerful enough anonymization mechanism. This does not mean these transactions are not traceable; it can only significantly impede the process in the right circumstances. Detection software can identify an address belonging to the exchange, but an exchange service (popular and used) likely has a sizable number of such transactions. A tracking metric may be a conversion calculation. That can work if there is a lack of transactions with similar values, enabling conversion guessing. A possible solution may be the introduction of random delays, though this has an unwanted side effect in a volatile crypto-market with ever-changing coin values.

Privacy-preserving cryptocurrencies.   Privacy-preserving cryptocurrencies, like the ones described in this work, are designed to provide strong anonymity by embedding privacy mechanisms directly into their protocols, eliminating the need for external mixing services. Zcash uses zk-SNARKs to enable shielded transactions, concealing sender, receiver, and amount, though users must opt into these private transactions. Monero employs ring signatures, stealth addresses, and confidential transactions to obscure transaction details by default. Oasis, Secret, Integritee, and Phala leverage confidential smart contracts and TEEs to ensure data privacy during computation, with Integritee and Phala specifically relying on TEEs for secure execution. These mechanisms should make tracing transactions more challenging than in transparent blockchains like Bitcoin, as they break direct links between addresses and transaction data. However, transactions are not entirely untraceable; sophisticated analysis can exploit weaknesses. For instance, detection software may use timing analysis to correlate Monero transactions or identify

patterns in Zcash's optional shielded pool usage. In TEE-based systems (Integritee, Phala), compromised hardware [63, 64, 65, 66, 69] could leak sensitive data, while smart contract vulnerabilities in Oasis and Secret may expose transaction metadata, leading to possible deanonymization. Tracking metrics, such as statistical analysis of ring sizes in Monero or shielded pool activity in Zcash, can narrow down potential transaction sources if the anonymity set is small or usage patterns are inconsistent.

Detection of mixing. The environment is also evolving in terms of detection. There is a renewed interest in detecting mixing services, e.g., chainalysis[4], aimed at bringing mixing transactions to light due to their association with illicit activity. Advances in AI and machine learning have sparked a new wave of research utilizing machine learning to detect illegal activities and mixing [5, 72].

6. Conclusion

This survey provides a comprehensive review of mixing proposals and existing implementations. We began by summarizing a set of review criteria for mixing services, focusing on control structures, obfuscation primitives, and robustness. Subsequently, we systematically analyzed the proposed systems and explored exemplary attack vectors. Furthermore, we provided a detailed comparison of the services and highlighted the threats and limitations inherent to their architectures.

Our review reveals that the mixing ecosystem is diverse and filled with innovative approaches. However, few of the existing solutions have successfully achieved a completely undetectable transfer of capital. This challenge remains highly debated and is further compounded by increasing regulatory scrutiny and governmental backlash.

Addressing these limitations will require new paradigms that balance user privacy, system efficiency, and regulatory compliance. Future work should explore advanced cryptographic techniques, such as multiparty computation and zero-knowledge proofs, alongside decentralized governance models. These efforts are essential to ensure that privacy-preserving financial systems can evolve in a way that is both sustainable and secure in the face of adversarial conditions and regulatory constraints.

References

[1] S. Nakamoto, et al., Bitcoin, A peer-to-peer electronic cash system 21260 (2008).

[2] L. Wu, Y. Hu, Y. Zhou, H. Wang, X. Luo, Z. Wang, F. Zhang, K. Ren, Towards understanding and demystifying bitcoin mixing services, in: Proceedings of the Web Conference 2021, WWW '21, Association for Computing Machinery, New York, NY, USA, 2021, p. 33–44. URL: https://doi.org/10.1145/3442381.3449880. doi:10.1145/3442381.3449880.

[3] F. Miedema, K. Lubbertsen, V. Schrama, R. van Wegberg, Mixed signals: Analyzing Ground-Truth data on the users and economics of a bitcoin mixing service, in: 32nd USENIX Security Symposium (USENIX Security 23), USENIX Association, Anaheim, CA, 2023, pp. 751–768. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/miedema.

[4] A. Arbabi, A. Shojaeinasab, B. Bahrak, H. Najjaran, Mixing solutions in bitcoin and ethereum ecosystems: A review and tutorial, arXiv preprint arXiv:2310.04899 (2023).

[5] C. Xu, R. Xiong, X. Shen, L. Zhu, X. Zhang, How to find a bitcoin mixer: A dual ensemble model for bitcoin mixing service detection, IEEE Internet of Things Journal 10 (2023) 17220–17230. doi:10.1109/JIOT.2023.3275158.

[6] J. Pakki, Y. Shoshitaishvili, R. Wang, T. Bao, A. Doupé, Everything you ever wanted to know about bitcoin mixers (but were afraid to ask), in: Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part I 25, Springer, 2021, pp. 117–146.

---

[4]https://www.chainalysis.com/

[7] R. Van Wegberg, J.-J. Oerlemans, O. van Deventer, Bitcoin money laundering: mixed results? an explorative study on money laundering of cybercrime proceeds using bitcoin, Journal of Financial Crime 25 (2018) 419–435.

[8] M. Möser, R. Böhme, D. Breuker, An inquiry into money laundering tools in the bitcoin ecosystem, in: 2013 APWG eCrime Researchers Summit, 2013, pp. 1–14. doi:10.1109/eCRS.2013.6805780.

[9] Y. Hong, H. Kwon, J. Lee, J. Hur, A practical de-mixing algorithm for bitcoin mixing services, in: Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, BCC '18, Association for Computing Machinery, New York, NY, USA, 2018, p. 15–20. URL: https://doi.org/10.1145/3205230.3205234. doi:10.1145/3205230.3205234.

[10] P. Tippe, C. Deckers, Unmixing the mix: Patterns and challenges in bitcoin mixer investigations, Forensic Science International: Digital Investigation 52 (2025) 301876. URL: https://www.sciencedirect.com/science/article/pii/S2666281725000150. doi:https://doi.org/10.1016/j.fsidi.2025.301876, dFRWS EU 2025 - Selected Papers from the 12th Annual Digital Forensics Research Conference Europe.

[11] T. de Balthasar, J. Hernandez-Castro, An analysis of bitcoin laundry services, in: H. Lipmaa, A. Mitrokotsa, R. Matulevičius (Eds.), Secure IT Systems, Springer International Publishing, Cham, 2017, pp. 297–312.

[12] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, E. W. Felten, et al., Anonymity for bitcoin with accountable mixes, Preprint (2014).

[13] Y. Fanusie, T. Robinson, Bitcoin laundering: an analysis of illicit flows into digital currency services, Center on Sanctions and Illicit Finance memorandum, January (2018).

[14] D. L. Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, Communications of the ACM 24 (1981) 84–90.

[15] E. J. Schwartz, T. Avgerinos, D. Brumley, All you ever wanted to know about dynamic taint analysis and forward symbolic execution (but might have been afraid to ask), in: 2010 IEEE Symposium on Security and Privacy, 2010, pp. 317–331. doi:10.1109/SP.2010.26.

[16] M. Möser, R. Böhme, D. Breuker, 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 18, Springer, 2014, pp. 16–32.

[17] Coinjoin, 2015. URL: https://en.bitcoin.it/wiki/CoinJoin.

[18] Wasabi wallet, 2019. URL: https://en.bitcoin.it/wiki/Wasabi_Wallet.

[19] T. Ruffing, P. Moreno-Sanchez, A. Kate, Coinshuffle: Practical decentralized coin mixing for bitcoin, in: Computer Security-ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II 19, Springer, 2014, pp. 345–364.

[20] J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, K. Wehrle, Coinparty: Secure multi-party mixing of bitcoins, in: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, CODASPY '15, Association for Computing Machinery, New York, NY, USA, 2015, p. 75–86. URL: https://doi.org/10.1145/2699026.2699100. doi:10.1145/2699026.2699100.

[21] I. Miers, C. Garman, M. Green, A. D. Rubin, Zerocoin: Anonymous distributed e-cash from bitcoin, in: 2013 IEEE Symposium on Security and Privacy, 2013, pp. 397–411. doi:10.1109/SP.2013.34.

[22] M. Tran, L. Luu, M. S. Kang, I. Bentov, P. Saxena, Obscuro: A bitcoin mixer using trusted execution environments, in: Proceedings of the 34th Annual Computer Security Applications Conference, ACSAC '18, Association for Computing Machinery, New York, NY, USA, 2018, p. 692–701. URL: https://doi.org/10.1145/3274694.3274750. doi:10.1145/3274694.3274750.

[23] S. Meiklejohn, R. Mercer, Möbius: Trustless tumbling for transaction privacy (2018).

[24] D. V. Le, A. Gervais, Amr: autonomous coin mixer with privacy preserving reward distribution, in: Proceedings of the 3rd ACM Conference on Advances in Financial Technologies, AFT '21, Association for Computing Machinery, New York, NY, USA, 2021, p. 142–155. URL: https://doi.org/10.1145/3479722.3480800. doi:10.1145/3479722.3480800.

[25] A. Pertsev, R. Semenov, R. Storm, Tornado cash privacy solution version 1.4, Tornado cash privacy solution version 1 (2019) 6.

[26] Monero Project, Monero: Private, secure, untraceable, https://www.getmonero.org/, 2025. Accessed: 2025-04-20.

[27] I. A. Seres, D. A. Nagy, C. Buckland, P. Burcsi, MixEth: efficient, trustless coin mixing service for ethereum, Cryptology ePrint Archive, Paper 2019/341, 2019. URL: https://eprint.iacr.org/2019/341.

[28] Binance, Binance, https://www.binance.com/en, 2025. Accessed: 2025-04-20.

[29] Coinbase Ireland Ltd., Coinbase, https://www.coinbase.com/, 2025. Accessed: 2025-04-20.

[30] Payward Inc., Kraken, https://www.kraken.com/, 2025. Accessed: 2025-04-20.

[31] OKX, Okx, https://www.okx.com/, 2025. Accessed: 2025-04-20.

[32] Oasis Network, Oasis network: A privacy-enabled blockchain platform, Oasis Protocol Foundation Whitepaper, 2020. URL: https://oasisprotocol.org/whitepaper.

[33] Secret Network, Secret network: Decentralized confidential computing, Secret Network Whitepaper, 2021. URL: https://scrt.network/about/whitepaper.

[34] Integritee, Integritee: Scalable privacy for polkadot, Integritee Whitepaper, 2021. URL: https://integritee.network/whitepaper.

[35] Phala Network, Phala network: Confidential smart contracts for web3, Phala Network Whitepaper, 2020. URL: https://phala.network/whitepaper.

[36] U. D. o. J. Office of Public Affairs, Individual arrested and charged with operating notorious darknet cryptocurrency "mixer", 2021. URL: https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer.

[37] U. D. o. J. Office of Public Affairs, Ohio resident pleads guilty to operating darknet-based bitcoin 'mixer' that laundered over $300 million, 2021. URL: https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million.

[38] J. R. Douceur, The sybil attack, in: International workshop on peer-to-peer systems, Springer, 2002, pp. 251–260.

[39] H. Yousaf, G. Kappos, S. Meiklejohn, Tracing transactions across cryptocurrency ledgers, in: 28th USENIX Security Symposium (USENIX Security 19), USENIX Association, Santa Clara, CA, 2019, pp. 837–850. URL: https://www.usenix.org/conference/usenixsecurity19/presentation/yousaf.

[40] P. Han, Z. Yan, W. Ding, S. Fei, Z. Wan, A survey on cross-chain technologies, Distrib. Ledger Technol. 2 (2023). URL: https://doi.org/10.1145/3573896. doi:10.1145/3573896.

[41] T.-H. Chang, D. Svetinovic, Improving bitcoin ownership identification using transaction patterns analysis, IEEE Transactions on Systems, Man, and Cybernetics: Systems 50 (2020) 9–20. doi:10.1109/TSMC.2018.2867497.

[42] F. Reid, M. Harrigan, An Analysis of Anonymity in the Bitcoin System, Springer New York, New York, NY, 2013, pp. 197–223. URL: https://doi.org/10.1007/978-1-4614-4139-7_10. doi:10.1007/978-1-4614-4139-7_10.

[43] J. Poon, T. Dryja, The bitcoin lightning network: Scalable off-chain instant payments (2016).

[44] L. Fortnow, The knowledge complexity of interactive proof systems, The Journal of Symbolic Logic 56 (1991) 1092–1094. URL: http://www.jstor.org/stable/2275080.

[45] P. Robinson, Survey of crosschain communications protocols, Computer Networks 200 (2021) 108488. URL: https://www.sciencedirect.com/science/article/pii/S1389128621004321. doi:https://doi.org/10.1016/j.comnet.2021.108488.

[46] W. Ou, S. Huang, J. Zheng, Q. Zhang, G. Zeng, W. Han, An overview on cross-chain: Mechanism, platforms, challenges and advances, Computer Networks 218 (2022) 109378. URL: https://www.sciencedirect.com/science/article/pii/S1389128622004121. doi:https://doi.org/10.1016/j.comnet.2022.109378.

[47] V. Costan, S. Devadas, Intel sgx explained, Cryptology ePrint Archive, Paper 2016/086, 2016. URL: https://eprint.iacr.org/2016/086, https://eprint.iacr.org/2016/086.

[48] E. H. Young, C. Chrysoulas, N. Pitropakis, P. Papadopoulos, W. J. Buchanan, Evaluating tooling and methodology when analysing bitcoin mixing services after forensic seizure, in: 2021 International Conference on Data Analytics for Business and Industry (ICDABI), 2021, pp. 650–654. doi:10.1109/ICDABI53623.2021.9655843.

[49] F. K. Maurer, T. Neudecker, M. Florian, Anonymous coinjoin transactions with arbitrary values, in:

2017 IEEE Trustcom/BigDataSE/ICESS, 2017, pp. 522–529. doi:10.1109/Trustcom/BigDataSE/ICESS.2017.280.

[50] R. L. Rivest, A. Shamir, Y. Tauman, How to Leak a Secret: Theory and Applications of Ring Signatures, Springer Berlin Heidelberg, Berlin, Heidelberg, 2006, pp. 164–186. URL: https://doi.org/10.1007/11685654_7. doi:10.1007/11685654_7.

[51] N. Bitansky, R. Canetti, A. Chiesa, E. Tromer, From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again, in: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, ITCS '12, Association for Computing Machinery, New York, NY, USA, 2012, p. 326–349. URL: https://doi.org/10.1145/2090236.2090263. doi:10.1145/2090236.2090263.

[52] Y. Tang, C. Xu, C. Zhang, Y. Wu, L. Zhu, Analysis of address linkability in tornado cash on ethereum, in: W. Lu, Y. Zhang, W. Wen, H. Yan, C. Li (Eds.), Cyber Security, Springer Nature Singapore, Singapore, 2022, pp. 39–50.

[53] S. Noether, Ring signature confidential transactions for monero, Cryptology ePrint Archive, Paper 2015/1098, 2015. URL: https://eprint.iacr.org/2015/1098.

[54] M. Möser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, N. Christin, An empirical analysis of traceability in the monero blockchain, 2018. URL: https://arxiv.org/abs/1704.04299. arXiv:1704.04299.

[55] D. Hopwood, S. Bowe, T. Hornby, N. Wilcox, Zcash Protocol Specification, Technical Report, Zcash Technical Report, 2016. https://z.cash/protocol.

[56] G. Kappos, H. Yousaf, M. Maller, S. Meiklejohn, An empirical analysis of anonymity in zcash, in: Proceedings of the 27th USENIX Security Symposium, 2018, pp. 463–479.

[57] A. Biryukov, D. Feher, Deanonymization techniques for zcash and other cryptocurrencies, Cryptology ePrint Archive, Paper 2019/811, 2019. https://eprint.iacr.org/2019/811.

[58] G. Enigmatic, Encrypted state management in secret contracts, Secret Network Technical Report, 2022. URL: https://scrt.network/technical-reports.

[59] H. H. Young, C. M. Shields, P. R. Thompson, Security analysis of trusted execution environments, IEEE Security & Privacy 18 (2020) 45–53.

[60] D. Kohlbrenner, R. K. Balakrishnan, Interoperable privacy-preserving sidechains, Polkadot Ecosystem Research 2 (2022) 12–20.

[61] W. Zhang, L. Chen, Zero-knowledge proofs in confidential computing, Journal of Cryptographic Engineering 12 (2023) 321–335.

[62] United States Department of Justice, Tornado cash founders charged with money laundering and sanctions violations, https://www.justice.gov/usao-sdny/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations, 2023. Southern District of New York, accessed April 22, 2025.

[63] F. Brasser, S. Capkun, A. Dmitrienko, T. Frassetto, K. Kostiainen, U. Müller, A.-R. Sadeghi, Dr. sgx: hardening sgx enclaves against cache attacks with data location randomization, arXiv preprint arXiv:1709.09917 (2017).

[64] A. Biondo, M. Conti, L. Davi, T. Frassetto, A.-R. Sadeghi, The guard's dilemma: Efficient code-reuse attacks against intel {SGX}, in: 27th {USENIX} Security Symposium ({USENIX} Security 18), 2018, pp. 1213–1227.

[65] S. Matetic, M. Ahmed, K. Kostiainen, A. Dhar, D. Sommer, A. Gervais, A. Juels, S. Capkun, {ROTE}: Rollback protection for trusted execution, in: 26th USENIX Security Symposium (USENIX Security 17), 2017, pp. 1289–1306.

[66] P. Borrello, A. Kogler, M. Schwarzl, M. Lipp, D. Gruss, M. Schwarz, ÆPIC Leak: Architecturally leaking uninitialized data from the microarchitecture, in: 31st USENIX Security Symposium (USENIX Security 22), 2022.

[67] J. Götzfried, M. Eckert, S. Schinzel, T. Müller, Cache attacks on intel sgx, in: Proceedings of the 10th European Workshop on Systems Security, EuroSec'17, Association for Computing Machinery, New York, NY, USA, 2017. URL: https://doi.org/10.1145/3065913.3065915. doi:10.1145/3065913.3065915.

[68] M. Li, Y. Zhang, H. Wang, K. Li, Y. Cheng, Tlb poisoning attacks on amd secure encrypted virtualization, in: Proceedings of the 37th Annual Computer Security Applications Conference, ACSAC '21, Association for Computing Machinery, New York, NY, USA, 2021, p. 609–619. URL: https://doi.org/10.1145/3485832.3485876. doi:10.1145/3485832.3485876.

[69] T. Cloosters, M. Rodler, L. Davi, Teerex: Discovery and exploitation of memory corruption vulnerabilities in {SGX} enclaves, in: 29th {USENIX} Security Symposium ({USENIX} Security 20), 2020, pp. 841–858.

[70] J. Redman, De-mixing wasabi coinjoin transactions: A deep dive into chainalysis' deanonymizing claims, https://news.bitcoin.com/de-mixing-wasabi-coinjoin-transactions-a-deep-dive-into-chainalysis-deanonymizing-claims/, 2024. Accessed: 2024-12-22.

[71] K. K. Garimella, D. Conway, Zero-knowledge proofs and privacy: A technical look at privacy, 2024. URL: https://www.researchgate.net/publication/380929571_Zero-Knowledge_Proofs_and_Privacy_A_Technical_Look_at_Privacy, accessed: 2025-04-22.

[72] E. S, S. S. S, Identifying illicit transactions in bitcoin tumbler services using supervised machine learning algorithms, in: 2023 12th International Conference on Advanced Computing (ICoAC), 2023, pp. 1–8. doi:10.1109/ICoAC59537.2023.10249782.