IET Blockchain

The Institution of Engineering and Technology

REVIEW OPEN ACCESS

Mixing Services in Bitcoin and Ethereum Ecosystems: A Review

Alireza Arbabi[1] | Ardeshir Shojaeinasab[2] | Homayoun Najjaran[2]

[1]Department of Computer Science, University of Waterloo, Waterloo, Canada | [2]Department of Electrical and Computer Engineering, University of Victoria, Victoria, Canada

Correspondence: Homayoun Najjaran (najjaran@uvic.ca)

Received: 21 March 2025 | **Revised:** 30 April 2025 | **Accepted:** 4 August 2025

Funding: We would like to acknowledge the funding support of **Mastercard Co**. and Mathematics of Information Technology and Complex Systems (MITACS) under IT34028 Mitacs Accelerate.

ABSTRACT

This manuscript presents an exhaustive review of blockchain-based mixing services, aiming to fill the existing gap between academic innovations and real-world implementations. Starting with an identification of the core functionalities and techniques employed by mixing services, the paper delves into detailed explanations of these operational mechanisms. It further outlines an evaluation framework tailored for a rigorous assessment, highlighting the key vulnerabilities and strengths of various solutions. In addition, the study identifies potential attack vectors that compromise these services. The paper explores the dual nature of mixing services: while they contribute to the preservation of privacy—a cornerstone of blockchain technologies—they can also facilitate illicit activities. By addressing key research questions, this study not only offers a comprehensive overview of the current state of mixing services but also sets the stage for future academic discourse in this evolving field.

1 | Introduction

The advent of blockchain technology has had a significant impact on the financial landscape by introducing cryptocurrencies as a new, decentralized form of digital assets [1]. While these digital currencies promise a level of privacy and security, the fundamental structure of blockchain technology—based on transparent and immutable ledgers– - presents challenges to individual privacy [2, 3]. Given the publicly accessible full transaction record, monitoring the movement of funds between cryptocurrency addresses through network modelling, network profiling, and network-based detection is possible [4]. Consequently, if a user receives funds from an identified suspicious address, both the user's address and funds will be flagged as questionable, leading to a reduction in the user's privacy and anonymity.

The effort of balancing transactional transparency with privacy has led to the development of cryptocurrency mixing services, designed to obscure the source and destination of transactions. These mixing services occupy a controversial status. On one hand, they serve as vital tools for privacy preservation and equity. On the other hand, they hold the potential for misuse in money laundering, sanction evasion, ransomware money transfer, and other illicit activities. For instance, studies have demonstrated that SilkRoad extensively utilized crypto mixers to obfuscate its users' funds [5], and various ransomware like Wannacry employed mixing solutions to conceal the flow of their funds [6]. Additionally, the Lazarus Group has leveraged mixing services to obscure over $991 million of stolen funds on behalf of North Korea [7, 8].

Considering this landscape, this review paper provides a comprehensive study of blockchain-based mixing services, targeting academic solutions as well as real-world practitioners. Given the growing influence of mixing services and the profound ethical and technical dilemmas they present, there is an urgent need

TABLE 1 | The proposed two-level keyword assembly structure.

Inclusion	Keywords	Searching field
Context	"Bitcoin" or "Ethereum" or "Cryptocurrency" or "Blockchain"	Title & Keywords & Abstract
Subject	"Mixing" or "Tumbler" or "Payment Channel Hub" or "Money Laundry" or "AML" or "Privacy Preservation" or "Obfuscation" or "Deanonymization"	Title & Keywords & Abstract

for a comprehensive examination that goes beyond disciplinary boundaries. This review aims to fill this gap by not only examining existing models and solutions but also by proposing a unified framework for their evaluation. This synthesis is essential to accelerate research efforts, guide policy-making, and assist in the development of more robust and secure mixing services. To achieve these objectives, we specify and aim to answer the following critical research questions:

- What are the most critical mixing techniques in cryptocurrencies?
- What are the main mixing services provided in academia, and how do they work?
- What are the available real-world solutions, and how do they operate?
- How closely do real-world and academic mixing solutions align?
- Can we propose a framework for evaluating mixing services, and how should these be evaluated?
- To what extent do mixing services render transactions fully anonymous, and how secure are they?
- How regulatory compliance can affect the usage of mixing services, and how it can prevent illicit activities like money laundering, without degrading users privacy?
- What open challenges exist in this field that demand scholarly attention?

Our investigations involve a survey of academic frameworks alongside an analysis of existing market solutions by forensics of current attacks performed on each service to convey some information from the dark side of target mixing services. The literature searching policy of this paper is structured based on preferred reporting items for systematic review and meta-analysis (PRISMA), proposed by Moher et al. [9]. To be specific, A query, a two-level keyword assembly to gather information related to mixing services literature, is defined to address these research questions. Table 1 depicts the related identified keywords. In terms of the research context, a paper can be considered related if it includes at least one of "Bitcoin", "Ethereum", "Cryptocurrency" or "Blockchain" words, either in its title, keywords or its abstract. On the other hand, in terms of the model, only papers that include "Mixing," "Tumbler," "Payment Channel Hub," "Money Laundry," "AML," "Privacy Preservation," "Obfuscation," and "Deanonymization" in their titles, keywords or abstracts are collected. These keywords define the scope and the focus of the paper. As a result, we collected fourteen different academic mixing frameworks, and eight papers discussing the performed attacks on more than twenty real-world mixing services. All gathered academic and real-world solutions will be discussed comprehensively through the following sections.

This paper proposes a first-of-its-kind set of evaluation criteria for mixing services and provides a detailed analysis on what are the weaknesses and strengths of different mixing solutions and the potential for improvement case by case. We also provides an exploration of potential vulnerabilities and outlines a roadmap for future research and development in the field. Ultimately, the research aims to contribute both to the academic discourse and to real-world implementations by identifying ongoing challenges such as fund traceability in a full path from sender to the receivers and the unknown territory of cross-chain mixing.

2 | Background

The introduction of mixers marked a significant transformation in cryptocurrencies, directly addressing the challenges of trust, security, privacy, and efficiency. Essential to the operation and growing acceptance of these blockchain-based mixers are the foundational technologies and principles. We will provide a brief overview of some of these key concepts below before going over how the mixers operate in detail:

2.1 | Blockchain

Introduced in 2008 by the pseudonymous Satoshi Nakamoto for the cryptocurrency Bitcoin, a blockchain is a decentralized and distributed digital ledger technology used to record transactions across multiple computers in a way that ensures the data can only be modified once it's been recorded. Once a block of data has been added to the blockchain, it becomes virtually immutable, protected from alteration without altering all subsequent blocks and the consensus of the network. This characteristic ensures data integrity and transparency. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger. This decentralized nature of the system ensures that no single entity has control over the entire blockchain, and all transactions are publicly recorded, ensuring transparency and trustworthiness [10].

2.2 | Transactions

At the heart of Bitcoin or any other cryptocurrency functioning is its transaction-based public ledger. Transactions here are a play of unspent transaction outputs (UTXOs), which are used wholly in transactions. Given the improbability of a UTXO matching an exact spending amount, most Bitcoin transactions

result in two outputs. One is received by the intended recipient, while the change is sent back to the sender at a new address. Additionally, transaction metadata encompasses public keys, UTXOs, transaction size, and its unique hash. With inputs signed using the sender's private key, validity is readily verifiable via the sender's public key [1].

2.3 | Consensus Mechanisms

One of the revolutionary aspects of blockchain technology is the elimination of central authority, ensuring transactions' validation through consensus mechanisms. These algorithms ensure all nodes in the network agree upon the truth. Bitcoin, for example, utilizes the proof-of-work (PoW) mechanism, where participants (miners) solve cryptographic puzzles to validate transactions and add new blocks. However, concerns regarding energy consumption and scalability have led to the exploration of alternative consensus mechanisms. Proof-of-stake (PoS) is one such alternative where validators are chosen to create new blocks based on the number of coins they hold and are willing to "stake" as collateral. Each consensus mechanism has its trade-offs in terms of security, decentralization, and efficiency [1, 11].

2.4 | Cryptographic Hash Functions

A cornerstone of blockchain technology, cryptographic hash functions, ensure data integrity and security. These functions take an input and produce a fixed-size string of bytes, typically a digest that is unique to each unique input. The SHA-256, predominantly used in Bitcoin, is one such algorithm. These functions are crucial for generating public and private keys, forming blocks, and maintaining data consistency and integrity across the decentralized network [12].

2.5 | Privacy in Cryptocurrencies

While cryptocurrencies offer a robust mechanism for transaction security, privacy remains a nuanced challenge. Traditional banking systems provide privacy by restricting access to transactional information. Cryptocurrencies, on the other hand, announce all transactions publicly. However, privacy is attempted by keeping public keys anonymous, akin to stock exchanges. A key challenge arises when key owners are revealed, potentially unveiling other linked transactions [1]. Furthermore, users' identities can be deanonymized by associating pseudonyms with IP addresses or by abusing Bitcoin's anti-DoS measures [13].

2.6 | Smart Contracts

Beyond traditional transactions, the blockchain ecosystem has given rise to smart contracts. These are digital protocols designed to autonomously execute tasks when predefined conditions are met. Such contracts eliminate third-party interventions and can engender automatic payments, quality controls, and establish trust amongst stakeholders [14]. Not limited to Bitcoin, these contracts have been enhanced on other platforms due to the introduction of features like turing-completeness and blockchain-awareness [15].

2.7 | Decentralized Finance (DeFi)

DeFi represents a conglomerate of decentralized applications aiming to recreate or enhance traditional financial systems (like lending, borrowing, and derivatives) without intermediaries using blockchain technology. Predominantly built upon Ethereum, these platforms leverage smart contracts to ensure transparency, openness, and global accessibility. As DeFi platforms grow, they offer the potential for a more inclusive financial system and present challenges and complexities related to security and regulatory oversight [16].

2.8 | Layer-2 Solutions

As blockchain networks like Bitcoin and Ethereum became more popular, they faced scalability issues, with transaction speeds being a primary concern. Layer-2 solutions are protocols built on top of a primary blockchain (Layer-1) to increase the transaction throughput. One notable example is Bitcoin's Lightning Network, which facilitates off-chain transactions by opening bilateral channels between parties, thus providing faster and cheaper transactions. Similarly, Ethereum is exploring various Layer-2 solutions, like rollups, to alleviate its scalability constraints [17].

2.9 | Zero Knowledge Proof (ZKP)

An intriguing cryptographic tool, ZKP allows for claim verification by an individual without revealing any supportive information. This concept, which emerged in the 1980s, was pioneered by Goldwasser, Micali, and Rackoff from MIT [18].

In summation, the landscape of cryptocurrencies is underpinned by a melange of technical innovations and cryptographic techniques, which collectively aim to create a secure, transparent, and efficient digital monetary ecosystem.

3 | Cryptocurrency Mixers

In order to analyse how mixing services provide anonymity for their users, we will first explain the definition of mixing. Then, we will take a detailed look at the various obfuscation methods and techniques used by academic and real-world services. Additionally, we will evaluate these methods based on their assessed functionalities.

3.1 | Mixing Definition

The mixing process in cryptocurrencies, often referred to as coin mixing or coin tumbling, is a technique employed to enhance the privacy and anonymity of transactions within blockchain networks. It involves the pooling of multiple cryptocurrency transactions from various sources and then redistributing them in a manner that obscures their origin and destination. The

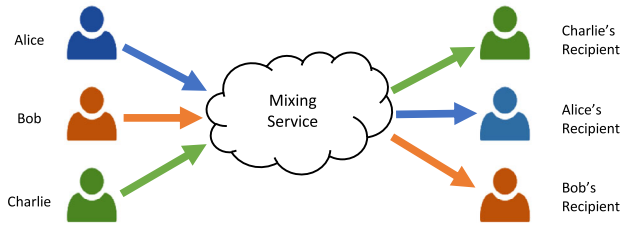

FIGURE 1 | High-level schema of the mixing process. Participants send their funds into the mixing service, and then the service mixes funds and sends them to the specified recipients such that the linking between the corresponding input and outputs is obfuscated.

process typically operates through specialized mixing services or protocols that amalgamate the funds, making it challenging to trace specific coins back to their original owners [19]. By breaking the transactional linkage between addresses and transactions, coin mixing provides a degree of confidentiality, ensuring that the flow of funds remains private and reduces the ability to associate specific transactions with identifiable individuals or entities. This process plays a crucial role in preserving the privacy and anonymity of cryptocurrencies in an increasingly surveilled financial landscape [20]. A high-level schema of the mixing process is depicted in Figure 1.

Before discussing the mixing solutions, it's important to introduce two key terms that will be used later: anonymity set and Taint analysis. anonymity set refers to the number of participants involved in the mixing process, and Taint refers to the amount of cryptocurrency in an account that came from another account. Taint rates between different addresses can be extracted by tracing back from an address to the origins of its received funds. Taint analysis involves traversing the transaction graph to identify possible connections and relations among different graph vertices (cryptocurrency addresses). This type of analysis helps to deanonymize the activities and connections behind the blockchain.

3.2 | Obfuscating Techniques

The objective of this subsection is to present a comprehensive overview of obfuscating techniques utilized by mixing services for both turing-complete and non-turing-complete cryptocurrencies. Subsequently, we will examine how frequently each method is used in both academic solutions and real-world services.

3.2.1 | Swapping

Swapping stands as a prominently employed methodology for obscuring the association between the senders and recipients in a cryptocurrency network [21]. The fundamental concept revolves around interchanging the inputs and outputs among diverse participants to keep their relationships secret, as depicted in Figure 2. By swapping different coins among participants, an intricate meshwork of transactions is created, making it tough to track where the original money came from. The general schema of mixing process is depicted at Figure 1.

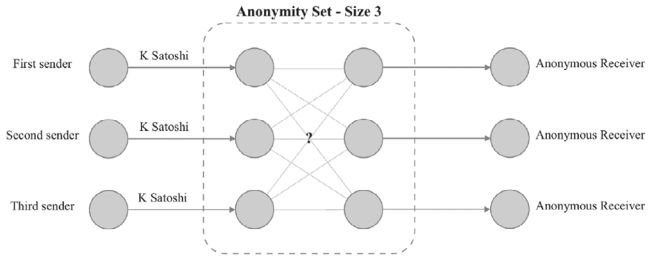

FIGURE 2 | Overview of swapping process [26].

FIGURE 3 | Sample of an aggregating address [26].

3.2.2 | Aggregating Funds

Chang and colleagues discovered specific repetitive transaction patterns in the Bitcoin network, including what they referred to as "sweeper transactions" [22]. These transactions, depicted in Figure 3, involve a large number of input addresses and one or two output addresses referred to as "Aggregation Addresses." In essence, this method consolidates funds from various addresses into one or two aggregation addresses, resulting in a substantial balance in the newly formed address. By centralizing all funds into a single input and sending them to the recipient from there, the aggregation address functions as a tool to obscure transactions, which breaks the traceable links between senders and recipients by creating a many-to-one, then one-to-many association.

3.2.3 | Peeling Chain

A peeling chain is a set of transactions generated by mixing services that form a chain to distribute outputs. The unique property of the peeling chain is that transactions in the chain are similar to normal user transactions with one input and two outputs [23].

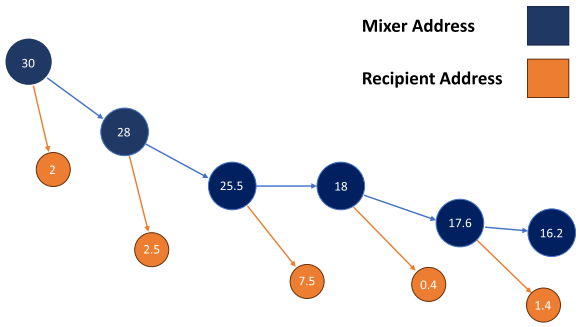

FIGURE 4 | Overview of peeling chain schema.

Therefore, utilizing peeling chains makes mixing transactions more indistinguishable from a normal user. The schematic of peeling chains is depicted in Figure 4. A recent research by Gong et al. discussed the technical dissection of Bitcoin transactions to flag those affiliated with mixing services with a focus on peeling chains as one of the major repetitive patterns in mixing services, a granular analysis is focused on several transaction parameters. The transaction version field designates protocol features, while the lock time parameter signals the earliest possible block height or time a transaction may be added to the blockchain. A critical element, the sequence number within each input yet a lower value implicates the transaction in the replace-by-fee policy or ties its finalization to lock time. Parsing these values for uniformity across a dataset can unearth patterns indicative of automated mixer activities [24].

3.2.4 | Fund Splitting

Fund splitting refers to a process in which users' input coins are divided into smaller denominations and sent through various complex paths, involving multiple participants. Randomization and adding delays in the fund distribution process further complicate the transaction history, making it challenging to link the source and destination of coins.

3.2.5 | Chain Hopping

Chain hopping is a relatively new and promising technology applied by cryptocurrency mixers to boost privacy and anonymity. The idea behind chain hopping is to add an extra layer of security to the mixing process by utilizing multiple blockchain networks and switching between them. This approach makes it challenging to trace funds, even if the original cryptocurrency source is known.

3.2.6 | Randomized Fee

In the majority of mixing services, particularly those that are centralized, users are required to pay fees for utilizing the mixing service. Employing a constant fee structure could lead to a detectable usage pattern, potentially compromising the mixing process graph. To counteract this concern, Bonneau et al. [25] propose the adoption of randomized fees. Implementing a stochastic fee characterized by a continuous range spanning from 0 to a predetermined mixing fee value could eliminate any discernible pattern associated with mixing fees within the mixing transaction graph.

3.2.7 | Randomized Delays

One of the mixing detection patterns, especially in multi-round and multi-output mixing is looking for time-based patterns in committed transactions to the blockchain. If a mixer consistently uses a fixed time delay in all mixing transactions, mixing patterns can be inferred from this property. To tackle this problem, mixers can put random delays for broadcasting transactions. This way, any predictable timing patterns are avoided, making mixing detection more difficult.

3.2.8 | Third-Party Blinding

In centralized mixing setups, a central entity undertakes the mixing process on behalf of participants, affording it comprehensive insight into the connections between senders and recipients. This arrangement raises concerns about potential information leakage, as users must rely on a third party's honest execution of mixing without disclosing those details. To address this challenge, certain prior studies [27, 28] have proposed mixing techniques that aim to shield the mixer entity from knowledge about the involved users. In simpler terms, these mechanisms are structured such that the mixer lacks awareness of the associations between specific inputs and corresponding outputs.

Blindcoin [27] attained this objective through the utilization of the blind signature scheme outlined by Chaum [27], effectively concealing linkage details from the mixer. Heilman et al. [28] introduced a novel approach where both senders and recipients interact with the mixer using cryptographic RSA-based puzzles, ensuring that the mixer entity remains oblivious to the linking information. The high-level schema of TumbleBit is depicted in Figure 6. Further elaboration on these methods is provided in Section 3.2.

3.2.9 | Off-Chain Transactions

Some mixing services employ off-chain transactions to diminish the duration and expenses of the mixing process while enhancing privacy. Due to the inherent untraceability of many off-chain transactions, external observers cannot discern mixing patterns as some transactions are hidden from them. Most off-chain transactions are made through services called payment channel networks (PCNs), like the Lightning [29] and Raiden [30] networks in Bitcoin and Ethereum blockchains, respectively. In the literature, the payment channel networks which supports both performing off-chain transactions and also mixing them are called payment channel hubs (PCHs). In these services, an untrusted tumbler (also called hub) is used and each user need to setup one payment channel with the tumbler, and the tumbler then facilitate the payment from senders to recipients, while obfuscating the linkage between them by utilizing methods like swapping, ZKPs etc. which is discussed in detail in Section 4.

3.2.10 | Fungibility of Inputs

Fungibility, within the context of mixing, signifies the requirement that all inputs involved in the mixing process possess equal values. This criterion obfuscates the linkage between senders and receivers in transactions, making the tracing of transactions challenging due to the uniformity of transaction values.

3.2.11 | Disconnected Fund Flow

The term "being disconnected" denotes severing the complete link between a sender and receiver, preventing any verifiable connection through the transaction graph of the mixer using the maximum-flow algorithm (taint analysis). This can be achieved through swapping methods or by directly delivering cleaned funds to the recipient from an independent address that holds adequate funds. One of the main advantages of maintaining a disconnected mixing graph is the increasing difficulty for a third party to detect mixing transactions since linking the disconnected transactions to each other is a hard task for any entities outside of the mixing process [26].

3.2.12 | Address Freshness

The freshness of addresses means that every time mixing happens, both the mix's escrow addresses and recipients' output addresses should be fresh addresses created specifically for that mixing process. This is required to prevent connecting the current mixing to other addresses that are not related. Moreover, those mixing services which gives mixing guarantees to the participated users should use fresh and unique addresses in order to create reliable mixing guarantees [25]. Therefore, both parties should pick addresses with no other possible source of incomes. This helps maintaining the privacy and isolation of the mixing process. It's important to note that this feature is specifically relevant to address-based cryptocurrencies, such as Bitcoin, and isn't applicable within account-based blockchain networks like Ethereum, since the interactions with mixers are based on the mixers' contracts.

3.2.13 | Trusted-Execution-Environment

A trusted execution environment (TEE) is a secure and separate space within a computer's main working area, which keeps sensitive information and tasks safe from potential threats that could affect the regular parts of the computer. TEEs make sure that only trusted programs can access in the protected space, making it a shielded area for sensitive activities [31]. A TEE could host the mixing process, ensuring that the transaction mixing occurs in a protected and isolated environment with remote attestation (i.e. a third party can verify the correctness of the mixer's operations, like Intel SGX [32, 33] and ARM TrustZone [34]). In this setup, the TEE securely manages the mixing process, safeguards private keys, and shields transaction details. It also establishes secure communication with the mixer's server, enhancing protection against potential threats. By employing a TEE, users benefit from safer and more private cryptocurrency transactions within the mixer.

3.2.14 | Zero-Knowledge Proofs

Zero-knowledge mixers enable a crucial element of trustless mixing by allowing participants to prove the validity of their transactions without revealing sensitive information, such as the sender, recipient, or transaction amount. Through ZKPs, users can mathematically confirm that they possess the necessary information to spend their funds, ensuring the integrity of the mixing process while maintaining confidentiality. This approach adds an extra layer of confidentiality and security to the mixing process.

3.2.15 | Other Techniques

Researchers have designed various academic mixing methods primarily leveraging cryptography, distinct from the mentioned functionalities. These methods mostly involve using cryptographic techniques like RSA-based puzzles (in TumbleBit [28] and BSC [35] papers), ring signatures (in Möbius [36] paper, notably in Monero cryptocurrency [37]), fair-exchange protocol [38], and several other techniques. These methods will be discussed comprehensively in the forthcoming sections. Khalilov et al. proposed a literature on mixing functionalities based on cryptographic concepts [39].

The functionalities described are widely used in cryptocurrency mixing services to achieve anonymity and privacy for users, making it challenging for an attacker with full access to transaction ledgers, such as the Bitcoin and Ethereum blockchains, to trace transactions from their source to their destination. It's important to note that the effectiveness and feasibility of these functionalities depend on the target network's capacity to support them. For instance, the Bitcoin scripting language is not Turing-complete and can only perform limited actions, making it difficult to deploy methods like ZKP-based mixing on the Bitcoin network. Conversely, Ethereum and many other cryptocurrencies which support smart contracts using Turing-complete languages like Solidity support developing complex programs on a smart contract, including advanced ZKP-based mixers etc. Additionally, to have a powerful mixing service, a sufficient number of these functionalities should be combined in parallel or sequentially, making the entire mixing process more obscured and robust against mixing attacks, which is explained in detail in Section 5. For example, a mixer can employ swapping, aggregating, and peeling chain methods sequentially, while leveraging randomized fee and delay among these functionalities to improve the anonymity of the mixing process.

One critical challenge in establishing a trusted mixing service is ensuring atomicity. Mixers are not always honest and might attempt to steal money from users. Therefore, atomicity in this context means that when a user wants to make a payment to its destination, either the payment is successful or the money is returned to the sender's address, preventing the mixing service from stealing the user's funds. This concern is particularly relevant for centralized mixing services. To mitigate this

problem, several methods have been introduced, including third-party blinding, zero-knowledge proofs (ZKP), and cryptographic puzzles. These techniques help ensure that transactions are either completed correctly or reverted without loss to the user, thereby enhancing trust in the mixing service and the obfuscating procedure [40].

Despite the described mixing functionalities which should be employed by a mixing service, internet anonymity plays a pivotal role in enhancing the effectiveness of cryptocurrency mixing services. By ensuring that users access mixing services through anonymous networks like Tor, the network connection between the user and the service is obscured, adding an additional layer of privacy. This anonymity is crucial, as it prevents third parties from tracing the user's IP address and other identifying information back to the original source of the transactions. For instance, the BitcoinFog service is exclusively accessibility via Tor, ensuring that users' connections are shielded from surveillance and tracking which significantly boost the overall security and privacy of the mixing process. Consequently, combining internet anonymity techniques with advanced mixing functionalities creates a robust environment where users can confidently engage in transactions without fear of exposure or tracking, thereby maintaining the confidentiality and integrity of users financial activities through mixing services.

4 | All the Proposed Mixing Frameworks

Following a comprehensive investigation of the concealment techniques used by many mixing services to ensure funds remain untraceable, this section delves into an examination of the prominent mixing frameworks proposed in the literature. Additionally, we evaluate the practical mixing services that are popular among cryptocurrency users. For our analysis of the mixing frameworks, our focus remains strictly on the foundational papers associated with each, and the discussions in the BitcoinTalk community. On the other hand, when it comes to the widely used practical services, we assess various documented attacks on these platforms and consider the results and analysis found in previous studies.

4.1 | Academic Proposed Mixing Approaches

In addressing the anonymity concerns within cryptocurrencies, various mixing frameworks have been proposed in academic literature. These efforts, whether decentralized or centralized, have prioritized users anonymity and privacy rather than maximizing profits for the mixer entities. In this section, we delve into the architecture of 8 decentralized and 5 centralized noteworthy mixing frameworks.

4.1.1 | Decentralized Mixing Frameworks

The core philosophy behind the creation of Bitcoin and other cryptocurrencies was to remove the need for relying on third parties for financial transactions. Consequently, the cryptocurrency community generally seeks to steer away from centralized services, including mixing services. This has led researchers to suggest decentralized mixing frameworks, aligning with the

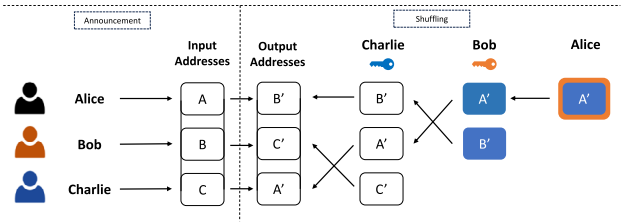

FIGURE 5 | Overview of CoinShuffle's mixing process [42].

fundamental aims of cryptocurrencies, to enhance users' privacy and uphold the primary purpose behind their creation. However, decentralized frameworks generally suffer from a slow mixing process, the need for honest participants majority, and limited scalability.

CoinJoin: CoinJoin is a privacy-enhancing technique that allows multiple users to combine their transactions into a single joint transaction [41]. This process makes it challenging for outside observers to link the original input and output addresses, thus increasing the privacy of participants. CoinJoin is not a complete mixing protocol because it neither describes how participants should be selected, nor how the swapping transaction is actually formed.

CoinShuffle: CoinShuffle was introduced as an enhancement to CoinJoin, presenting it as a fully decentralized system [42]. The protocol initiates with the participation of n users in the mixing procedure. Subsequent to this initiation, each participant generates a new Bitcoin address, intended to serve as their output address in the mixing transaction.

The ensuing step involves the participants shuffling the newly formed output addresses. This shuffling is performed in a manner analogous to a decryption mix network, ensuring that the identities of the address creators remain undisclosed. This procedure unfolds over n distinct shuffling rounds.

In the initial round, a participant, referred to as Alice, signs her transaction using her private key. She then encrypts this transaction employing the public keys of the remaining $n-1$ participants. The resultant encrypted transaction is then relayed to the subsequent participant, Bob. Upon receipt, Bob decrypts the transaction from Alice using his public key. Simultaneously, he signs his personal transaction with his private key, and encrypts it with the public keys of the remaining $n-2$ participants. Both transactions (the decrypted one from Alice and his own) are then passed to the third participant.

This sequence progresses iteratively, culminating when the final participant receives $n-1$ encrypted transactions. This last participant decrypts all received transactions using her private key, appends her own transaction to this collection, and then broadcasts the consolidated list. The schema of this protocol is depicted in Figure 5.

The protocol's success hinges on mutual verification. If participants recognize their respective transactions within the final aggregated list, they will endorse the transaction with their signature. If not, they abstain. However, the main drawback of

both CoinJoin and CoinShuffle frameworks is that, since their protocol puts all inputs and outputs in a single transaction, the anonymity set size is limited to the transaction size. Moreover, they suffer from the bootstraping problem, like how to find a set of users who want to mix their funds using the same protocol, while remaining anonymous over the internet [43]. Also, the absence of mixing fees makes both Sybil and Dos attacks easy for an attacker (All possible attacks and the resilience of each framework to them are discussed in Sections 5 and 6).

Xim: Bissias et al. put forth Xim as a decentralized P2P mixer that employs a swapping mechanism [44]. Participants aiming to mix their funds are paired at random and swap their transaction outputs with each other. To mitigate Sybil and DoS attacks, Xim integrates mixing fees. Participation in a mixing action necessitates expenditure from both parties, rendering such attacks prohibitively costly for potential attackers.

CoinParty: CoinParty was conceptualized by Ziegeldorf and his colleagues as a mixing strategy that functions through the collaboration of multiple third-party mixing peers [45]. Initially, with n participating users, n unique escrow addresses are collaboratively formulated by the mixing peers for users' funds collection. Afterwards, This is followed by the shuffling stage, which is orchestrated similarly to CoinShuffle. Subsequently, the mixing peers sign the shuffled transactions to finalize the mixing process. The jointly generated escrow addresses are the same as the Bitcoin ordinary transactions, resulting in increasing the mixing anonymity. Nonetheless, the absence of mixing fees in this approach diminishes the incentive for mixing peers to work honestly, making the method vulnerable to potential Join-and-Abort attacks.

SecureCoin: Ibrahim introduced SecureCoin as a mixing technique that incorporates the joint-secret-sharing protocol [46] to decrease transaction size while preventing sabotage from mixing peers [47]. In this design, all senders collaboratively establish a unified escrow address for fund aggregation. Subsequently, output addresses are rearranged in a manner similar to the CoinShuffle protocol. Finally, the senders collectively provide their signatures for the ultimate transaction, enabling the transfer of funds from the aggregation address to the designated outputs.

Möbius: Möbius is an Ethereum-based mixing approach within the framework of smart contracts [36]. This method relies on the Ring-Signature [48] scheme and stealth addresses to obfuscate the senders and recipients associations like the strategy observed in Monero [37]. A ring signature is a type of cryptographic digital signature that enables a user to sign a message on behalf of a group (or "ring") without disclosing which individual member's private key was used to create the signature. In terms of mixing, a recipient can withdraw her money from a group of transactions without revealing the corresponding sender of the withdrawn money.

Within the context of Möbius, the process unfolds as follows: senders furnish both their funds and stealth keys to a designated smart contract that orchestrates the mixing of the provided inputs. Subsequently, each recipient can create a ring signature to withdraw their funds from the contract and transfer them to an ephemeral address, culminating in the completion of the mixing procedure. Notably, the deterministic nature of the Ethereum virtual machine (EVM) ensures that the mixing works in a tamper-resistant manner as the entire process occurs on the blockchain, precluding the involvement of any central authority capable of disrupting the integrity of the mixing mechanism.

AMR: AMR is a mixer based on zk-SNARKs, aimed at disrupting the traceability connection between coins deposited and withdrawn by a user within a blockchain governed by smart contracts [49]. The AMR configuration involves participants depositing a predetermined quantity of coins into a smart contract. Subsequently, this contract establishes a Merkle tree structure over the deposits, generating a commitment that represents the deposited transactions. When a recipient wishes to retrieve their funds from the contract, they are required to validate their familiarity with the committed values associated with specific pre-existing deposit commitments that contribute to the computation of the Merkle tree root. This validation is achieved through the employment of zk-SNARK proofs. Additionally, AMR leverages lending platforms (Like Aave [50] and Compound [51]) to provide users with the opportunity to receive interest on their deposited assets. This particular strategy serves as an added motivation for users to retain their funds within the ecosystem.

MixEth: Seres et al. introduced MixEth as a decentralized coin mixing solution for turing-complete blockchains [52]. The core concept of MixEth revolves around the integration of Neff's verifiable shuffles [53] within the framework of coin mixing. In the MixEth protocol, participants within the mixer engage in a multi-round shuffling process of their public keys. In each round of shuffling, a shuffler permutes all public keys using Neff's method, then commits them to the mixer along with a zero-knowledge proof to prove that the permutation was performed correctly. Afterwards, as soon as recipients are confident in the adequacy of the shuffling iterations, they gain the capability to retrieve their assets from the mixing service.

Zether: Zether [54] represents an innovative payment solution tailored for enhancing privacy and confidentiality within account-based blockchain systems, like the Ethereum ecosystem. In zether, users who wishes to obfuscate their coins should establish a new Zether address and deposit their funds into the Zether smart contract (ZSC). Subsequently, Zether generates an equivalent amount of Zether tokens (ZTH) mirroring the deposited funds. With this accomplished, users gain the ability to send their ZTH tokens with a high degree of anonymity through the Zether smart contract.

To achieve privacy, the transferring tokens are obfuscated by encrypting the amount being sent, and the sender's identity is concealed by selecting a group of other Zether accounts by the sender to form an anonymity set and being covered among them (similar to ring signatures [48] in Monero [37]). This set effectively conceals the sender's account among its peers, making it exceedingly challenging for any observer to discern the origin of the transaction. Zether uses a new type of zero-knowledge proofs called Σ-bullets for anonymously transferring funds through its transactions. Due to the space limitations, we refer the readers to the detailed description provided in [54].

4.1.2 | Centralized Mixing Frameworks

While decentralization stands as a core objective within the cryptocurrency community, its practical realization is not always optimally efficient. When it comes to mixing, centralized services shows more scalability, speed, and user-friendliness, compared to decentralized ones. Therefore, several researchers have introduced centralized frameworks aimed at enhancing user privacy and anonymity within the services, and mitigate the risk of fund thefts by malicious mixer entities.

MixCoin: Bonneau et al. presented MixCoin as the first academic centralized mixer [25]. Within this framework, a central mixer undertakes the mixing tasks for all participants. When a user deposit their coins into a designated escrow address, the mixer issues a digitally signed message as a guarantee. Should the mixer act maliciously or misappropriate user funds, this guarantee can be publicly disclosed. By leveraging the mixer's public key, the veracity of this guarantee can be ascertained. Consequently, the reputation of a mixer is derived from its track record of honest mixing and user satisfaction. Furthermore, To obfuscate discernible patterns associated with mixing fees, MixCoin adopts a randomized fee strategy. This tactic is especially potent during sequential mixing—when a user sequentially engages multiple mixers. Integrating randomized mixing fees with varied inter-mixing intervals heightens the level of anonymity.

BlindCoin: Building upon MixCoin's foundation, Valenta et al. put forth BlindCoin, which leverages chaumian blind signatures [27] and a public ledger to curtail a centralized mixer's insight into the linkage between senders and recipients [55]. This design substantially reduces the susceptibility to permutation leaks. However, it's pivotal to acknowledge that, akin to MixCoin, BlindCoin doesn't offer safeguards against potential fraudulent activities or coin stealing by the mixers.

TumbleBit: TumbleBit was proposed as a centralized mixing approach aimed at preventing connections between senders and receivers [28]. In this method, the sender (Alice) and the receiver (Bob) engage with a central entity called a tumbler τ. First, Alice and Bob establish payment channels with τ. Then, Alice creates a 2-of-2 escrow transaction denoted as $T_{\text{escr}}(A, \tau)$, allowing α bitcoins to be accessed through a joint signature from both Alice and τ. Similarly, the tumbler forms another shared transaction denoted as $T_{\text{escr}}(\tau, B)$, and these transactions should be committed to the blockchain. Afterwards, Alice and Bob interact with the tumbler off-chain, employing RSA-based puzzles. These interactions facilitate Bob for receiving a signature from τ for his transaction $T_{\text{escr}}(\tau, B)$, and help τ receiving Alice's signature of her transaction $T_{escr}(A, \tau)$. Finally, τ make a transaction from $T_{\text{escr}}(A, \tau)$ to his fresh generated address, and Bob makes another transaction from $T_{\text{escr}}(\tau, B)$ to his own fresh generated address, and the mixing process finished. Additionally, TumbleBit employs a chaumian blind signature [55] scheme to safeguard the tumbler from learning about participant associations, as it shown in Figure 6.

A^{2}L$^{+/\text{UC}}$. Inspired by TumbleBit [28], the A2L+/UC protocol [40, 43] is introduced as a Payment Channel Hub-based protocol that operates on top of off-chain transactions. It is similar to Payment Channel Networks, but with the distinction that both

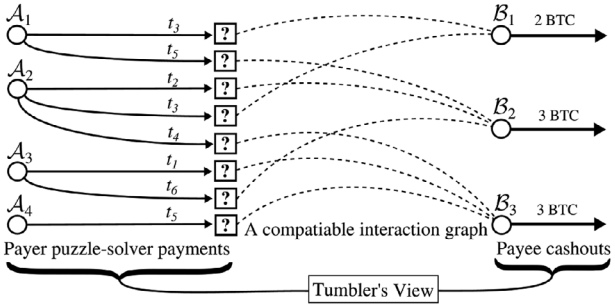

FIGURE 6 | Overview of TumbleBit's mixing graph [28]. Tumbler's view on mixing associations is blinded.

senders and receivers need to establish one off-chain channels with a tumbler to send their transactions. A2L$^+$ uses cryptographic puzzles powered by digital signatures, such as Schnorr or ECSDA [56], to obscure the associations between senders and receivers from the tumbler. In the mixing process, a sender commits a puzzle to the tumbler, and the recipient must solve the corresponding puzzle with the sender's assistance to withdraw the funds from the tumbler. The authors demonstrate that A2L$^+$ is more efficient and faster compared to the original TumbleBit protocols, and they also introduced A2L$^{\text{UC}}$ as a less efficient but Universally Composable service [57], in which we refer readers to the original paper for more technical and cryptographic details. Albeit A^{2}L$^{+/\text{UC}}$ protocol works in a secure and efficient manner, if the tumbler's inputs are not fungible, attackers can link senders to their corresponding recipients based on the amount of transferred funds to and from the tumbler due to the transaction transparency of the corresponding blockchain ledger. In addition to A^{2}L$^{+/\text{UC}}$, several other methods have been introduced for use in both UTXO-based [58] and account-based [59, 60] blockchains. These methods aim to improve the functionality of cryptographic protocols used in TumbleBit and A^{2}L$^{+/\text{UC}}$ while maintaining their overall high-level schema and functionality.

BSC: Heilman and colleagues introduced blindly signed contracts (BSC) as a mixing approach that capitalizes on blind signatures principles akin to those in TumbleBit. This method is designed to establish unlinkability in both on-chain and off-chain contexts. In the on-chain process, the confirmation of all mixing transactions on the blockchain results in a comparatively slow mixing speed. On the other hand, the off-chain strategy leverages micro-payment channel networks [29, 61] to keep some mixing transactions off the primary blockchain. This is advantageous as off-chain transactions exhibit enhanced speed, scalability, and the potential for reduced fees compared to the conventional on-chain transactions.

Obscuro: Obscuro is a mixing protocol that capitalizes on the capabilities of a trusted execution environment (TEE), elaborated upon in Section 3.1. This paradigm allows participants to verify the isolated functionalities through remote attestation, assuring them of a robust mixing set size [62]. The protocol's efficacy was evaluated within the Bitcoin Testnet by its authors, and its adaptability was demonstrated through a smart contract implementation on the Ethereum network [63].

Table 2 outlines the functionalities utilized by academic mixers to obfuscate transactions and facilitate the mixing process. Notably,

TABLE 2 | Functionalities employed by all mixing solutions proposed in academia.

	Swapping	Aggregating	Peeling chain	Splitting	Chain hopping	Random fee	Random delay	Third-party blinding	Off-chain	Input fungibility	Disconnected fund flow	Address freshness	TEE	ZKP	Others
CoinJoin	✓	✗	✗	✗	✗	No fee	a.[a]	n.a.	✗	a.	✗	a.	✗	✗	✗
CoinShuffle	✓	✗	✗	✗	✗	No fee	a.	n.a.	✗	a.	✗	✓	✗	✗	✗
Xim	✓	✗	✗	✗	✗	✗	a.	n.a.	✗	a.	✓	a.	✗	✗	✗
CoinParty	✓	✗	✗	✗	✗	No fee	a.	n.a.	✗	a.	✗	a.	✗	✗	✗
SecureCoin	✓	✓	✗	✗	✗	a.	a.	n.a.	✗	a.	✗	a.	✗	✗	✗
Möbius	✗	✗	✗	✗	✗	n.a.	a.[b]	n.a.	✓	a.	✗	n.a.	✗	✗	✓
AMR	✗	✗	✗	✗	✗	n.a.	a.[b]	n.a.	✗	a.	✗	n.a.	✗	✓	✗
MixEth	✓	✗	✗	✗	✗	n.a.	a.[b]	n.a.	✓	a.	✗	n.a.	✗	✓	✗
Zether	✗	✗	✗	✗	✗	n.a.	a.[b]	n.a.	✗	a.	✗	n.a.	✗	✓	✗
Mixcoin	a.	a.	a.	a.	✗	✓	a.	✗	✗	a.	a.	✓	✗	✗	✗
BlindCoin	a.	a.	a.	a.	✗	✓	a.	✓	✗	a.	a.	✓	✗	✗	✗
TumbleBit	✗	✗	✗	✗	✗	a.	a.	✓	✓	a.	✓	a.	✗	✗	✓
$A^2L^{+/UC}$	✗	✗	✗	✗	✗	a.	a.	✓	✓	a.	✓	a.	✗	✗	✓
BSC	✗	✗	✗	✗	✗	a.	a.	✓	✓	a.	✓	a.	✗	✗	✓
Obscuro	a.	a.	a.	a.	✗	a.	a.	✗	✗	a.	a.	a.	✓	✗	✗

[a]In the following cells of all tables, “a.” stands for “applicable” and “n.a.” stands for “not applicable,” and “-” means that there is not adequate information to determine the corresponding value.

[b]Since withdrawing money from Ethereum-based mixing services can be done whenever users choose to (due to the account-based nature of the Ethereum network), users can add random delays by their own.

several academic solutions incorporates swapping methods by permuting the associations of inputs and outputs, in contrast with aggregating and peeling chain, which weren't signified in academic approaches. On the other hand, certain methodologies such as Möbius, TumbleBit, and BSC utilize cryptographic puzzles such as ring signatures and RSA-based puzzles. Additionally, Obscuro showcased an innovative application of a trusted execution environment, establishing itself as a pioneering approach within this domain. AMR and MixEth also leveraged ZKPs in smart-contract-based cryptocurrencies. It's important to note that the majority of additional obfuscation techniques, such as randomizing fees/delays and employing fresh addresses, can be implemented within these mixing frameworks, even though they were not explicitly mentioned in the papers. Notably, academic frameworks have not extensively addressed cross-chain mixing, despite its significance in the evolving world of decentralized finance.

4.2 | Real-World Mixing Approaches

In this section, we will conduct a comprehensive examination of eighteen commonly employed mixing services accessible within the market. While certain services discussed below may have become outdated by the time of this paper's publication, they merit analysis due to the significant volume of mixing-related data associated with them.

Regarding centralization and decentralization in practical services, a significant portion of them lean towards centralization, especially within the Bitcoin ecosystem. However, this term is completely different in the realm of smart-contract-based cryptocurrencies like Ethereum, Owing to their capacity to execute turing-complete algorithms. To maintain focus on the core subject of this section, discussions related to this aspect have been moved to Section 4.3. Within this section, the first sixteen services are centralized, and the last two services (JoinMarket and Tornado Cash) are decentralized. Given that other decentralized services either lack the necessary robustness or lack adequate reputations, we only discuss those two remarkable services. To the date of this publication, we have not found any reputable service that has more powerful functionalities compared to the mentioned services.

4.2.1 | BitcoinFog

Bitcoin Fog stands as one of the earliest centralized bitcoin mixing services, which was exclusively accessible through the Tor network. This service permits the creation of a maximum of five addresses for depositing bitcoins and takes a (random) fee between 1–3% of the transaction value. The withdrawal process allows for dispersing bitcoins to a maximum of twenty addresses, spanning a timeframe of 6 to 96 h. In a study conducted by Moser [64], an evaluation of this mixer was undertaken by initiating transactions through it and subsequently analysing the resulting transaction graph created by the mixing service.

The graph generated from this evaluation is visualized in Figure 7. Bitcoin Fog aggregates incoming transactions into distinct aggregation addresses referred to as "communities." Notably, some of these communities contain as much as 50,000 BTC. Following this aggregation, output transactions are derived from these communities and directed toward their designated recipients. Noteworthy is BitcoinFog's utilization of randomized fees and varying mixing delays, strategically implemented to hinder external attempts at detecting the mixing graph by analysing fee structures and transaction timing patterns.

It's important to note that BitcoinFog does not mandate participants to send a predetermined sum of money to the mixing service. Consequently, if a user transfers funds that significantly deviate from the average of incoming funds to the mixer, there is a heightened likelihood of detection due to the small anonymity set provided.

Notably, the operator of this service was arrested in 2021 for allegedly running this service, which was considered the longest-running bitcoin money laundering service on the darknet [65].

4.2.2 | BitLaundry

BitLaundry represents an uncomplicated mixing service that differs from Bitcoin Fog in its operational methodology. Unlike Bitcoin Fog, BitLaundry doesn't facilitate the deposition of bitcoins into a virtual wallet. Instead, the service necessitates the specification of destination addresses, the count of outgoing transactions, and a designated time span. This prompts the generation of a one-time-use address, to which a minimum threshold of coins must be sent by the user. The fee structure of BitLaundry's mixing service is split into two parts. The first part constitutes 2.49% of the total amount, while the second part involves a charge of a static amount for each outgoing transaction.

Based on Moser's evaluation in 2013 [64], it was observed that BitLaundry employed fund aggregation as a technique to obscure associations. However, Moser's analysis indicated that due to the limited number of participants within the mixing service, certain inputs were directly linked to corresponding outputs. Consequently, the mixing process exhibited a reduced level of anonymity.

4.2.3 | Blockchain.com

Blockchain.com, a renowned cryptocurrency-focused website and platform, predominantly offers an array of services pertaining to digital currencies, with a primary emphasis on Bitcoin. Notably, within the Blockchain.com wallet's historical features, there existed a service known as "Send Shared." This service operates by facilitating Bitcoin exchanges among various users through a shared wallet structure. During its operation in 2013, it levied a modest mixing fee of 0.5%. At that time, it stood out as an economical option in the landscape of cryptocurrency services.

Moser's examination [64] revealed that this service employed an aggregation technique to obscure the mixing process. Notably, some of the aggregating addresses contained substantial sums, approximately 2000 BTC each. In their examination, they made eleven transactions to this service and detected eight individual

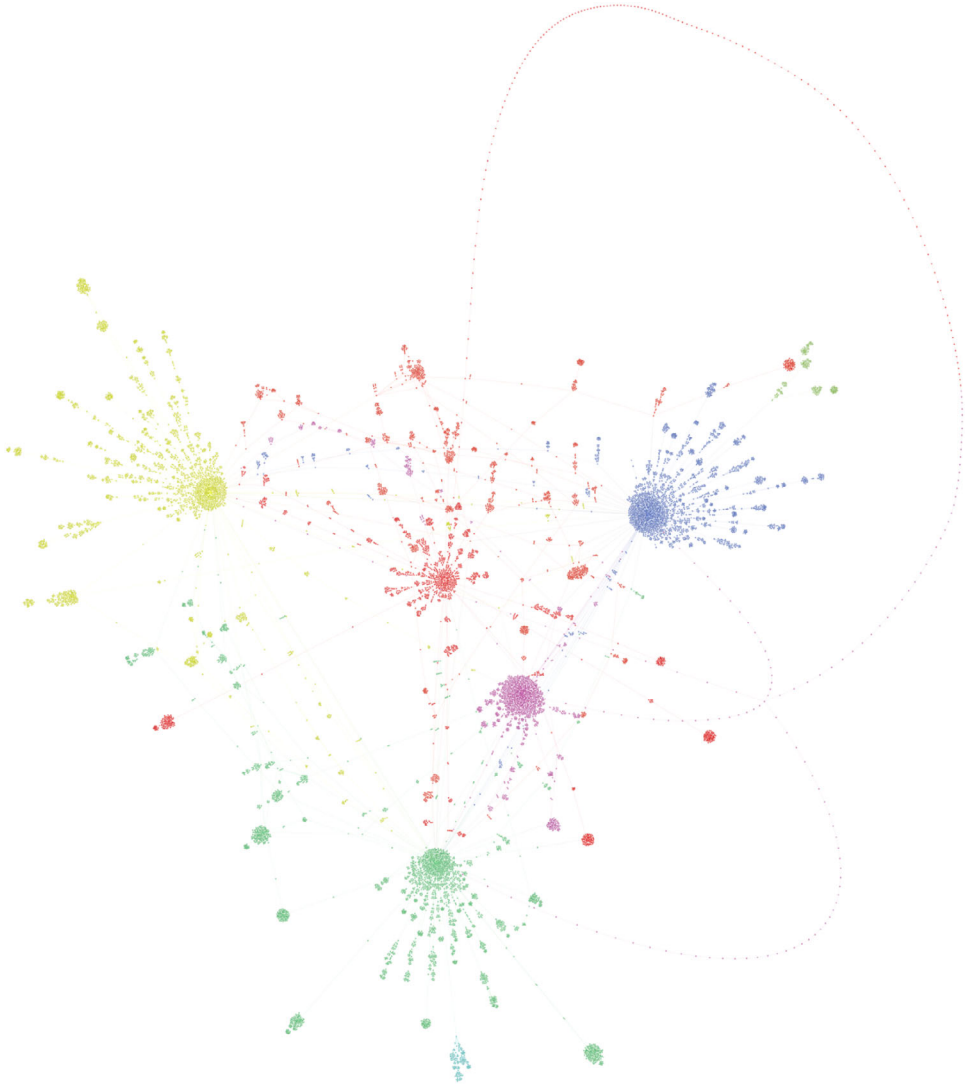

FIGURE 7 | Sample of created communities (aggregation addresses) in BitcoinFog [64].

clusters of aggregating addresses, which shows that the mixer is resilient to the taint analysis attack. Following the generation of these aggregating addresses, funds underwent a process of division into several smaller transactions, and these were subsequently subdivided until they reached their designated destination addresses.

4.2.4 | DarkLaunder, Bitlaunder, and CoinMixer

According to the evaluation conducted by Balthasar et al., in their 2017 study, these particular services were identified as the least effective mixing services at the time of assessment [66]. The authors chose to examine them together due to their belief that these services were likely under common ownership and displayed striking similarities in their operations and attributes. Consequently, an analysis of these services can offer valuable insights into the pitfalls that mixing services should steer clear of in order to attain a higher level of anonymity.

First problem of these mixers comes from that they require users to create account for having access to the mixer. Furthermore, they stored this user information alongside the IP addresses associated with transaction requests, as well as comprehensive transaction details in their database. What exacerbates this concern is the vulnerability of their websites, making it relatively simple for potential attackers to gain access to this stored data.

Moving on to their obfuscating techniques, they employed an aggregation approach akin to several other services. However, a significant drawback was the aggregation addresses were static for a long time, which led to a concentration of the mixing process and made it discernible to potential attackers. Additionally, these services encountered a scarcity of participants, resulting in notably small anonymity set size and poor obfuscating permutations. In summary, these services exhibited exceedingly low levels of security and privacy, rendering them illustrative examples of common pitfalls to be noticed when implementing a secure mixer.

4.2.5 | Helix

Helix, a cryptocurrency tumbler, gained prominence within the dark web community due to its affiliation with the creators of the

renowned dark web search engine, Grams. The developers assert that Helix utilizes innovative proprietary technology to not only cleanse Bitcoins but also generate entirely new ones untouched by the darknet's transactions. This service was introduced to the public in June 2014. It is worth noting, however, that Helix's founder later pleaded guilty to a conspiracy charge involving the laundering of approximately $300 million. The potential consequences for this individual may include a 20-year prison sentence and a fine of either $500,000 or twice the value of the assets involved in the illicit transaction, as indicated in the references [67, 68].

Helix is accessible only using Tor, and it utilizes random time delays for mixing to achieve anonymity. It takes 2.5% of the transaction value as a mixing fee, and only allows withdrawals of 0.02 BTC or more.[1] Based on the assessment of Balthasar et al. [66], Helix also uses an aggregating method to accumulate funds into an address, and then distribute them to the recipients using a peeling chain. However, their observation shows that wallets and withdrawals of multiple customers are present on the same transaction, or very close to each other, thus it is easy to identify them. In short, although linking senders to recipients is a hard challenge in Helix, it is easy to verify that their transactions were passed from a mixer, by performing a taint analysis.

4.2.6 | AlphaBay

AlphaBay was a darknet market operating from the year 2014, a year after the Silk Road market was busted in 2013. In 2017, this platform was forcefully terminated, and its principal administrator was arrested [69]. However, this service was relaunched in August 2021 by the self-described co-founder of the AlphaBay. Prior to its 2017 shutdown, AlphaBay's management utilized a mixer to obscure the origins of the market's financial transactions. Since Alphabay had approximately 400,000 users in 2017, a significant proportion of users employed the mixer for their monetary transactions. Consequently, the mixer had a large mixing anonymity set, making it an interesting subject for studying with the potential to yield valuable insights about its operation mechanism. Balthasar et al. [66] assessed this mixing service by creating 35 different transactions to this mixer, and found three main clusters of aggregated funds, which shows that although this mixer had a multitude of users, it did not use a large number of clusters and its mixing transactions can be found easily by performing a taint analysis. This mixer also used other third-party mixing services like Helix, in order to make the mixing process more anonymous. Also, it utilizes random delays between creating mixing transactions to prevent any time-based mixing detection.

4.2.7 | MixTum

MixTum [70], established in 2018, claims to have a separate pool of Bitcoin from cryptocurrency stock exchanges such as Binance, OKEex, and DigiFinex, which is used to obfuscate users' funds with external coins from exchanges. Shojaeinasab et al. [26] have assessed the mixing mechanism of MixTum, revealing its similarity to typical mixers in aggregating incoming funds into an aggregation address and subsequently distributing them through a peeling chain. Furthermore, this platform ensures privacy enhancement by avoiding the aggregation of transactions from a single address into a common aggregation address, and also leveraging fee and delay randomization.

Additionally, MixTum furnishes users with a PGP-signed guarantee letter containing details about the mixing process, and its PGP fingerprint is publicly accessible on its website. This provision enables users to validate any concerns or complaints regarding improper mixing of funds from the service. This method is similar to MixCoin [25] guarantee letter, with the distinction that MixCoin signs its guarantee letter using its Bitcoin private key instead of a PGP fingerprint.

4.2.8 | CryptoMixer

In 2016, CryptoMixer [71] was introduced as a Tor-accessible Bitcoin mixing service. This service functions by aggregating user funds into aggregation addresses, followed by their distribution to recipients using peeling chains [26]. Additionally, CryptoMixer offers a guarantee letter, akin to the concept introduced in the MixCoin paper [25], signed using the mixer's private key. This feature allows users to publish their complaints from the mixer using a valid evidence. Moreover, CryptoMixer provides customizable obfuscation options, including the number of input and output addresses, mixing delay, and service fee. Furthermore, upon sending funds to the mixer, users are assigned a unique identification code. This code ensures that a user's coins are not mixed with those from previous transactions in subsequent dealings. It is worth noting, however, that there is a lack of documented information regarding CryptoMixer's operational details [66]. Most recently, CryptoMixer has been used by North Korean hackers to launder $1.4 billion stolen from the Bybit exchange which is regarded as one of the largest thefts in the history [72], highlighting the continued appeal of this service to high-profile attackers despite being a centralized.

4.2.9 | Blender

In 2017, Blender [73] was introduced as a centralized mixing service, and it employed several techniques, such as tailored mixing fees, mixing delays, and distinctive mixing codes, much like CryptoMixer, to establish a level of anonymity. Furthermore, Blender required that the input address and at least one of its output addresses be of the P2SH[2] type. This mixer's mixing process is claimed to resemble MixTum and CryptoMixer, involving the consolidation of input funds into aggregation addresses and the utilization of peeling chains to distribute mixed funds to recipients [26].

4.2.10 | ChipMixer

Established in 2017, ChipMixer quickly gained popularity as a top-notch mixing service. However, in March 2023, the FBI seized the operation for processing over $3 billion in illegal transactions [74]. ChipMixer operates by utilizing units known as "chips."

Users deposit their funds into the mixer and receive "chips" of a pre-specified value, consisting of bitcoins from various people. The "chip" is basically just BTC in a new address for which the participants are provided the private key, and chips are always created before a user deposits their funds into the mixer. Interestingly, Mixing fees are completely donation-based in this system, with a "Pay What You Want" strategy, contributing to its popularity as a free mixing service. Between 2017 and 2020, ChipMixer is estimated to have laundered about 53,000 bitcoins [75].

As the chips are fungible, tracing the funds in this system is a challenging task. Researchers like Pakki et al. [75] and Wu et al. [21] examined this service by making several transactions through it. Their findings suggest that the service pools funds into a few aggregation addresses divides the funds into many interchangeable addresses (chips), and then employs multi-path mixing to distribute these chips to users.

4.2.11 | Wasabi Wallet

Wasabi Wallet [76] is a publicly available Bitcoin wallet designed for desktop computers, emphasizing user privacy and security. It incorporates a trustless mixing technique, akin to the CoinJoin method. When users initiate transactions within this wallet, Wasabi executes a CoinJoin transaction, generating distinct groups of funds with varying denominations. Subsequently, funds from these generated groups are transferred to the intended recipients [21]. The transaction cost for utilizing Wasabi consists of the standard mining fee plus an additional 0.3% fee. Notably, Wasabi Wallet was also used besides CryptoMixer service by the North Korean hackers responsible for laundering $1.4 billion stolen assets from the Bybit exchange [72], underscoring its usage by major cybercriminals due to its anonymity features.

4.2.12 | ShapeShift

ShapeShift [78], founded by Erik Voorhees in 2014, is a cryptocurrency exchange platform that emphasizes privacy. It allows users to trade different cryptocurrencies without revealing their identities, making it suitable for exchanging various cryptocurrencies across different blockchain networks. However, although this service was not designed for a mixing purpose, it can be used for cross-chain mixing due to its provided coin exchanging anonymity. To illustrate, as reported by the Wall Street Journal, this service has been linked to facilitating at least $9 million in money laundering activities over several years [79]. Consequently, in response to mounting pressure from governments and media outlets, ShapeShift applied the know-your-customer (KYC) policy and it mandates account creation for accessing its services. Also, ShapeShift stated that they utilize anti-money laundering methods in their system, and rejected the mentioned accused report.

Figure 8 illustrates an example of using this service as a mixer. First, Alice sends 3 BTC to ShapeShift and receives 127.11 Ether in Ethereum later. Since these chains are totally different from each other, there is not any direct link between senders and

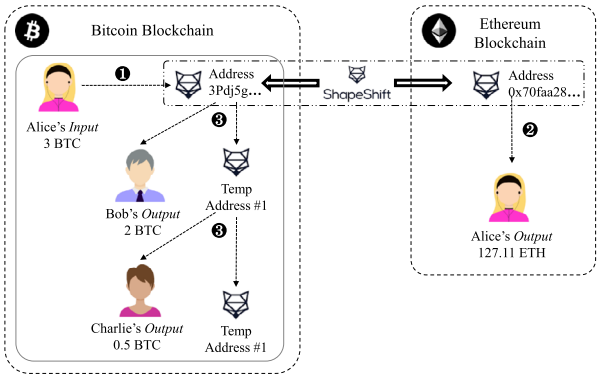

FIGURE 8 | Overview of ShapeShift's mixing process [21].

receivers, and Alice can use the exchanged Ethers as a mixed fund. Afterwards, the Bitcoin sent by Alice will be organized as a peeling chain to distribute Bitcoins to other users (e.g. Bob and Charlie in this figure) who swap other cryptocurrencies for Bitcoin [21].

4.2.13 | Bitmix

Bitmix.bz [80] was introduced in 2017, and currently serves mixing for Bitcoin, Dash, and Litecoin. This service claimed to utilize several methods like dust-attack prevention, randomized fees and delays, and guarantee letters in order to achieve anonymity. The mixing mechanism of this service is almost like most of the previous described services; aggregating funds into some addresses, then using a peeling chain for funds distribution [21].

4.2.14 | Sudoku Wallet

Sudoku Wallet was announced in 2019 within the bitcointalk forum. The service is a single-use wallet that outputs private keys rather than on-blockchain transactions. As the creators described, the mixing fees are randomized from 0.5% to 1% plus the CoinJoin fee and there is not any database and no log is saved in their system. Furthermore, they asserted that this service performs CoinJoin transactions using its incoming funds and sends them to newly generated addresses. Afterwards, the private keys of the corresponding addresses are given to the users to spend them [81].

Although the creators of this service explained their mixing protocol, the interaction of Pakki et al. [75] with this mixer showed different results from the creators' claim. After transacting 3 times with the mixer and analysing transactions using the Chainalysis tool, they did not identify any evidence of CoinJoin transactions. Also, the mixing fees of their transactions were inconsistent, as one of them had a mixer fee of 0 BTC while another had a fee of 90%. Consequently, it can be inferred that this mixer does not offer enough safety and reliability, besides its poor implementation.

4.2.15 | JoinMarket

JoinMarket [82] is a decentralized peer-to-peer (P2P) mixing service designed to connect users seeking to engage in CoinJoin

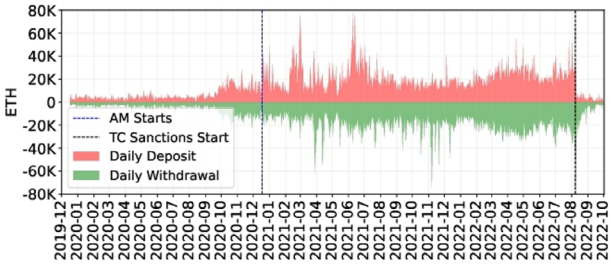

FIGURE 9 | Daily transactions in TC ETH pools. There was a panic exit when the OFAC sanctions were announced [77].

transactions. This platform consisted of two primary participant categories: market makers and market takers. Market makers are responsible for crafting CoinJoin transactions, while market takers are individuals seeking to mix their funds. Takers pay a fee to makers which works as an incentive, and notably, all actions within the system occur without reliance on any centralized authority. JoinMarket is remarkable within the Bitcoin network as one of the scarce decentralized mixing services, widely adopted by users seeking to obfuscate the origins of their funds.

4.2.16 | Tornado Cash

Tornado Cash is an open-source software project on the Ethereum network launched in December 2019 [83], stands as the predominant mixer within the Ethereum ecosystem. When a user wishes to blend their assets, they transfer their tokens into the Tornado Cash smart contract. The funds are secured using a Merkle tree cryptographic commitment scheme, hiding both the amount and source of the funds. Later, when taking funds out of the Tornado pool, a withdrawer proves the ownership of a commitment without revealing which specific commitment is being spent by using zero-knowledge proofs. This provides unlinkability between the deposited and withdrawn funds.

In August 2022, the United States Department of the Treasury's Office of Foreign Assets Control (OFAC) imposed sanctions on Tornado Cash due to its involvement in laundering a sum exceeding $7 billion [84]. After that, OFAC added the Tornado Cash website and addresses used this mixer to the "Specially Designated Nationals And Blocked Persons" list, thereby prohibiting U.S. citizens from engaging in any transactions involving the Tornado Cash website or addresses listed in the sanctions. Afterwards, the rate of using Tornado Cash dropped significantly for more than 77%, as depicted in Figure 9. It is noteworthy that a subset of Tornado Cash users have tried to diffuse banning from OFAC to other addresses by performing a dusting attack. Wang et al. conducted an assessment of the OFAC's sanctions' effects on ZKP-based mixers [77].

However, in a landmark decision on 26 November 2024, the U.S. Fifth Circuit Court of Appeals overturned the Treasury Department's sanctions against Tornado Cash. The court ruled that the OFAC had exceeded its authority by sanctioning the platform's immutable smart contracts, which it determined do not constitute "property" under the International Emergency Economic Powers Act [85, 86]. This new rule challenges the limits of U.S. sanctions authority on open-source code, and also could potentially impact other privacy tools and related lawsuits in the cryptocurrency space. However, the possibility of a government appeal and potential Supreme Court review leaves the long-term implications of this ruling uncertain.

4.2.17 | Post-Tornado Cash Services

After OFAC imposed sanctions on Tornado Cash, several new services emerged as alternative mixing solutions, such as RailGun [87], Cyclone [88], zkBob [89], and Typhoon Cash [90]. However, these services generally suffer from insufficient liquidity, and as of the time of this research, no Ethereum mixing service has been able to match Tornado Cash's pre-sanctions liquidity. Recently, Tornado Cash won a court case challenging the sanctions imposed against it. The Fifth Circuit Court of Appeals ruled that OFAC had exceeded its authority by sanctioning Tornado Cash, as its immutable smart contracts do not qualify as property under federal law. This ruling may have significant implications for the future of Ethereum mixing services. Given the limited popularity of these alternatives and the lack of frequent technical improvements compared to Zether and Tornado Cash, we do not provide a detailed discussion of these services in this paper. Interested readers are encouraged to refer to the Elliptic report on Tornado Cash alternative solutions [91] for more information. Additionally, Barbereau et al. analysed the taxonomy of Ethereum mixing services, particularly post-sanctions options like RailGun and zkBob, as documented in their work [92].

Table 3 outlined functionalities utilized by real-world mixing services, and as depicted, most services are centralized. A repetitive pattern in most services involves using aggregation techniques to accumulate funds into a designated address and using a peeling chain to distribute these funds to individual users. This approach is favoured over alternatives such as swapping, diverging from what is typically observed in academic frameworks. Also, third-party blinding has not been used by services, and it is clear that mixer entities do not want to blind themselves from the mixing information of their users. Moreover, Since forcing users to deposit coins only in a specific denomination to achieve fungibility is not desirable for most users, this functionality is not used by any service. However, a solution for users to heighten the obfuscation for their mixed funds is to fragment their output transactions to align with the average funds sent to the mixer by all users [64]. In addition, it is worth noting that several services may use off-chain transactions in platforms like payment channel networks, but it is a challenging task for an external observer to ascertain the utilization of off-chain transactions, as they occur in a separate layer distinct from the main Bitcoin network transactions.

4.3 | Comparison Between Academic and Real-World Services

By examining the data in Tables 2 and 3, it is clear that academia and market display considerable differences, which are mostly attributable to their different goals for the creation of mixing services. In the context of Bitcoin mixing services, since the Bitcoin scripting language is not Turing-Complete, it is necessary to construct mixers in a higher layer of the Bitcoin network.

TABLE 3 | Functionalities employed by all mixing services available in market.

	Birth date	Active?	Centralized	Swapping	Aggregating	Peeling chain	Splitting	Chain hopping	Random fee	Random delay	3rd-party blinding	Off-chain	Input fungibility	Disconnected fund flow	Address freshness	TEE	ZKP
BitcoinFog	2013	✗	✓	✗	✓	✓	—	✗	✓	—	✗	—	✗	—	✓	✗	✗
BitLaundry	2013	✗	✓	✗	✓	—	—	✗	✗	✗	✗	—	✗	—	✓	✗	✗
Blockchain.com	2013	✗	✓	✗	✓	—	✓	✗	✗	—	✗	—	✗	✓	—	✗	✗
DarkLaunder	2015	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	—	✗	✗	✗	✗	✗
Bitlaunder	2015	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	—	✗	✗	✗	✗	✗
CoinMixer	—	—	✓	✗	✓	✓	✗	✗	✗	✗	✗	—	✗	✗	✗	✗	✗
Helix	2017	✗	✓	—	✓	✓	—	✗	✗	✓	✗	—	✗	✗	—	✗	✗
Alphabay	2017	✓	✓	✗	✓	✓	—	✗	✗	✓	✗	—	✗	✗	—	✗	✗
MixTum	2018	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	—	✗	✗	✓	✗	✗
CryptoMixer	2016	✓	✓	✗	✓	✓	—	✗	✓	✓	✗	—	✗	✗	✓	✗	✗
Blender	2017	✓	✓	✗	✓	✓	—	✗	✓	✓	✗	—	✗	✗	✓	✗	✗
ChipMixer	2017	✗	✓	✗	✓	—	✓	✗	a.	✓	✗	—	✗	✗	✓	✗	✗
Wasabi Wallet	2018	✓	✓	✓	✗	✗	✓	✗	✗	—	✗	—	✗	✗	—	✗	✗
ShapeShift	2014	✓	✓	✓	✗	✓	✗	✓	—	—	✗	—	✗	✓	✓	✗	✗
Bitmix.bz	2017	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	—	✗	✗	✓	✗	✗
Sudoku Wallet	2019	✗	✓	—	—	—	—	✗	✓	✓	✗	—	✗	—	—	✗	✗
Join-Market	2017	✓	✗	✓	✗	✗	✗	✗	a.	a.[a]	n.a.	✗	✗	✗	a.	✗	✗
Tornado Cash	2019	✓	✗	✗	✗	✗	✗	✗	✗	a.[a]	n.a.	✗	✗	✗	n.a.	✗	✓

[a]Since performing a CoinJoin transaction in Join-Market and withdrawing money from Tornado Cash can be done whenever users choose to, users can add random delays by their own.

Notably, most academic endeavours have focused on developing decentralized mixing approaches to achieve the fundamental objective of cryptocurrencies, which is to minimize regulatory control exerted by centralized entities. Various techniques such as multi-round digital signing (e.g. CoinJoin [41], CoinShuffle [42]) and joint-address-creation (e.g. CoinParty [45], SecureCoin [47]) have been applied within decentralized mixing frameworks to achieve this objective.

Even in centralized approaches, there have been novel innovations for blinding the centralized mixer party from having any information about associations between inputs to outputs, by leveraging cryptographic schemes like Blind Signature which were used in TumbleBit [28] and BSC [35]. Moreover, Obscuro [62] suggested utilizing trusted-execution-environment (explained in Section 3) to monitor the mixing workflow which is performed by a mixer entity.

However, in practical mixing services found in real-world applications, most of the methods discussed in academic papers have not been fully implemented. As outlined earlier, these services generally aggregate funds into an address and then distribute them using a peeling chain [21, 26, 64, 66]. This approach is commonly used perhaps because it is a well-established and straightforward technique to implement. Furthermore, there hasn't been any significant attack on this method that can link inputs and outputs to each other. Additionally, a mixer can effortlessly add its own supply funds to the aggregation addresses, enhancing the anonymity pool. These steps are easy to develop by the services, and there's no need for complex implementations, resulting in a widespread and common method to use in mixing services. Also, centralized services tend to avoid blinding themselves from the mixing data, and we haven't come across any service employing blinding techniques to obscure sender-recipient relationships.

Nevertheless, despite this gap, several services have adopted academic methods to assure their users of their reliability and enhance the security of their mixing process. Specifically, the MixCoin guarantee letter [25] has been incorporated into multiple mixers, and some services have integrated features like fee and delay randomization to prevent attackers from identifying mixing transactions based on fee or time patterns.

To talk about other services that use alternative methods (rather than aggregating), some services like Wasabi Wallet [76] act as an intermediary responsible for collecting mixing transactions from users and executing a CoinJoin transaction (which is decentralized in its nature) in a centralized manner. Conversely, JoinMarket [82] introduced a decentralized P2P network, enabling participants to generate CoinJoin transactions in a decentralized way. Additionally, leveraging anonymous cryptocurrency exchanges for cross-chain mixing shows promise, leaving no trace of mixing association due to the isolation among different chains.

Regarding all these observations, in our investigation, it was evident that a majority of Bitcoin users opted for centralized mixers as opposed to decentralized alternatives, primarily due to their user-friendliness, intuitive interface, streamlined operations, and the absence of a requirement for advanced technical knowledge.

Besides all these inferences, things are totally different when it comes to turing-complete-based cryptocurrencies. In such cryptocurrencies like Ethereum, there is no need to setup a mixing framework at a higher layer of the cryptocurrency network, and mixing algorithms can be directly coded and executed in a smart contract, without the need for any centralized intermediary. This feature gives smart contract developers a wider range of options to create untraceable mixing solutions, resulting in introducing advanced mixing methods like zero-knowledge proofs in Tornado Cash [83] or ring signatures in Möbius [36], all fully decentralized. To the date of this publication, Tornado Cash remains the most popular service of its kind, though its usage has been significantly dropped by more than 77% after OFAC sanctions enforced [8, 77, 84]. Given these features of turing-complete cryptocurrencies, employing centralized mixing frameworks in these networks seems almost pointless.

5 | Possible Attacks on Mixing Services

Mixing services exist to ensure transaction anonymity, aiming to protect both senders and receivers from being identified at any point in the mixing process. Here we introduce 6 most common attacks within the context of mixing services, which can be performed by a mixer, mixing participants, or any third party who stands outside of the mixing process:

- **Sybil attack**: A common method to undermine mixing protocols is for an attacker to represent a significant portion of the participants. The larger this deceptive Sybil group, the higher the likelihood that the chosen mixing parties will include the attacker. Essentially, the attacker aims to dominate the system to decrease the anonymity set for others. In pairwise mixing protocols, a Sybil attacker can determine the fund's destination paired with any address. Protocols such as DarkWallet, SharedCoin, and CoinShuffle are vulnerable to cost-free Sybil attacks since they don't charge participants, and creating addresses (or Sybil identities) in Bitcoin and similar virtual currencies is free.
- **DoS attack**: DarkWallet, SharedCoin, and CoinShuffle don't charge users to join their mix pool, making them vulnerable to denial-of-service (DoS) attacks. An attacker can create multiple identities, each with a unique IP and Bitcoin address, and add them to the mix pool for free. If chosen, the attacker simply doesn't sign the transaction, disrupting the mix. If they create enough identities, they can hinder most transactions without any loss. CoinJoin and its variants, including CoinShuffle, conduct the entire mix in one step and can't impose an upfront fee. Any potential fee would require a different, yet-unproposed protocol. Likewise, Barber et al.'s fair exchange protocol [38] doesn't have participation fees, allowing an attacker to disrupt the exchange without any cost.
- **Coin stealing attack**: This type of attack predominantly occurs through untrusted centralized mixing services that steal user-submitted coins. While some services attempt to mitigate this risk by employing guarantee letters to reassure users about their trustworthiness (like the MixCoin guarantee letter, introduced in Section 4.1.2), this approach does not

provide an absolute guarantee of protection against such attacks.

- **Trojan attack**: This attack mirrors the Sybil attack, with the attacker actively participating in the mixing process. By transacting with the services, they can trace the mixing pattern and unveil the mixing procedure. Possessing both the sender and receiver addresses allows the attacker to easily discern the transaction pattern. This attack poses the most substantial threat to mixing services as it can expose the entire mixing process, pinpoint mixing transactions, identify related addresses, and uncover those utilizing the mixing services. Several studies have leveraged this attack method to demystify the operations of leading mixing services in the industry [26, 66, 75, 93]
- **Intersection attack**: The intersection attack focuses on tracking frequent activity by specific wallets either owned by one participant or exhibiting distinct patterns. For instance, in systems like CoinJoin and CoinShuffle, partner peer information is logged on the public blockchain. This allows even non-participating attackers to exploit the vulnerability. In terms of paralleling anonymous communication methods, every attacker in these protocols acts as a global passive observer.
- **ML-based attacks**: In the realm of mixing transactions, a comprehensive and trusted dataset remains elusive. Nonetheless, the WalletExplorer platform offers categorized data for various transaction types, notably for mixing services such as BitcoinFog, Helix, and Bitlaunder [94]. This platform sources its labels predominantly from user submissions and extensive forum analyses, subsequently expanding label classifications based on shared input addresses heuristic deanonymization attacks. In a separate endeavour, Blockstream.info has disseminated a dataset, structured utilizing their proprietary CoinJoin detection methodology and an established method for SharedCoin detection [95]. The reliability of these datasets, however, remains a subject of debate. Various studies have embarked on experimental pursuits and deep learning-based attacks, yet many confront challenges rooted in the lack of verifiable data [96–99]. Also, De Silva et al. proposed a deep reinforcement learning model to identify the safe and anonymous patterns for interacting with mixing services for users, with a focus on the Tornado Cash mixing service [100]. In addition, Du et al. proposed a graph neural network approach for breaking the anonymity of the Tornado Cash mixing service on the Ethereum network, while offering a gathered dataset on real mixing transactions on Tornado Cash [101].

6 | Proposing an Evaluation Framework to Assess Mixing Services

The paper identifies the most significant functionalities that mixing services utilize to conceal themselves behind blockchain transactions and maintain anonymity. In this section, we introduce an evaluation mechanism, along with specific metrics and criteria, to assess various mixing services and explore their vulnerabilities. To this end, the authors examine various attacks designed to reveal information behind cryptocurrency transactions and undermine anonymity.

In the wake of examining the major challenges posed by attacks on mixing services, we can establish a set of criteria for robust mixing services. Our assessment emphasizes both resilience to attacks and the capacity to obscure cryptocurrency transactions. After introducing various evaluation criteria, Table 4 presents an assessment of both academic and real-world mixing solutions. The assessment is based on their operational mechanisms, which are discussed in Section 4.

Prior to this study, Feng et al. conducted a thorough evaluation of mixing services, employing a comprehensive methodology that examined the effectiveness of protocols in fully anonymizing user identities, the involvement of centralized authorities in the mixing process, and the application of service fees [19]. Nevertheless, while their criteria established a robust framework for evaluating the effectiveness and security of mixing services in preserving user anonymity and protecting transactions, it did not encompass all facets of mixing services. The criteria set out in this document aim to provide an all-encompassing assessment of mixing services, as discussed in academic literature and observed in real-world applications, across both Ethereum and Bitcoin platforms.

- **Centralization concerns**: Centralized tumblers are potential targets for cyber-attacks, legal inquiries, or subpoenas. Compromised records from these services can lead to transaction de-anonymization.
- **Unlinkability**: For the highest standard of privacy, it's essential that the connection between the sender and the receiver be entirely severed. A fully unlinkable service ensures that taint analysis or similar techniques cannot be traced back to either party, solidifying anonymity. Within this context, we can categorize services into 2 different types, fully disconnected and correlated to pool size. The second type means that the higher pool size, resulted in a higher anonymization ratio, while in the first type, senders and receivers are completely disconnected from each other.
- **Liquidity**: High liquidity ensures that there are always sufficient funds for mixing, which can prevent delays and improve the anonymity set. Low liquidity mixers might pose the risk of having transactions stalled or linked due to insufficient participants. As the liquidity can be measured only in real-world mixing services, and some of the available data from mixers' liquidities are from several years ago, we mark those services that have enough funds to avoid linking senders to recipients as "high," and others as "low."
- **Anonymity set size**: The size of an anonymity set is pivotal when assessing the resilience of a mixing service, representing the aggregate of participants or inputs in a specific mixing event. An expansive anonymity set obfuscates the discernment of a coin's flow, while a limited set delineates transaction pathways, potentially undermining user privacy. This metric retains its significance across both traditional and contemporary mixing services. Prominent traditional services like CoinShuffle and CoinJoin fundamentally depend on the

TABLE 4 | The evaluation of all mixing solutions proposed in academia and market.

	Centralization	Unlinkability	Liquidity	Anonymity set size	Log storing	Random delay	Random fee	Mixing fee?	Auditable	Address reusing?	Cross-chain mixing	Sybil/DoS resistance	Coin stealing r	Front-running resistance
CoinJoin	✗	Cor. pool size	—	Limited to Tx size	✗	a.	No fee	✗	✓	✗	✗	✗	✓	n.a.
CoinShuffle	✗	Cor. pool size	—	Limited to Tx size	✗	a.	No fee	✗	✓	✗	✗	✗	✓	n.a.
Xim	✗	Fully disconnected	—	Participants count	✗	a.	✗	✓	✓	✗	✗	✓	✓	n.a.
CoinParty	✗	Cor. pool size	—	Participants count	✗	a.	No fee	✗	✓	✗	✗	✗	✗	n.a.
SecureCoin	✗	Cor. pool size	—	Participants count	✗	a.	a.	✓	✓	✗	✗	✓	✓	n.a.
Möbius	✗	Cor. pool size	—	Max 24 users	✗	a.	n.a.	✗	✓	n.a.	✗	✓	✓	✓
AMR	✗	Cor. pool size	—	Up to Merkle tree size	✗	a.	n.a.	✗	✓	n.a.	✗	✓	✓	✓
MixEth	✗	Cor. pool size	—	Participants count	✗	a.	n.a.	✗	✓	n.a.	✗	✓	✓	✓
Zether	✗	Cor. pool size	—	Anonymity set count	✗	a.	n.a.	✗	✓	n.a.	✗	✓	✓	✓
Mixcoin	✓	Dep. implementaion	—	Participants count	✗	a.	✓	✓	✓	✗	✗	✓	Guarantee Letter	n.a.
BlindCoin	✓	Dep. implementaion	—	Participants count	✗	a.	✓	✓	✓	✗	✗	✓	Guarantee Letter	n.a.
TumbleBit	✓	Fully disconnected	—	Participants count	✗	a.	a.	✓	✓	✗	✗	✓	✓	n.a.
$A^2L^{+/UC}$	✓	Fully disconnected	—	Participants count	✗	a.	a.	✓	✓	✗	✗	✓	✓	n.a.
BSC	✓	Fully disconnected	—	Participants count	✗	a.	a.	✓	✓	✗	✗	✓	✓	n.a.
Obscuro	✓	Dep. implementaion	—	Participants count	✗	a.	a.	✓	✓	✗	✗	✓	✓	n.a.

(Continues)

TABLE 4 | (Continued)

	Centralization	Unlinkability	Liquidity	Anonymity set size	Log storing	Random delay	Random fee	Mixing fee?	Auditable	Address reusing?	Cross-chain mixing	Sybil/DoS resistance	Coin stealing r	Front-running resistance
BitcoinFog	✓	Cor. pool size	High	High participants	No signup req.	—	✓	✓	✗	✗	✗	✓	✗	n.a.
BitLaundry	✓	Cor. pool size	Low	Low participants	No signup req.	✗	✗	✓	✗	✗	✗	✓	✗	n.a.
Blockchain.com	✓	Cor. pool size	High	High participants	Signup req.	—	✗	✓	✗	—	✗	✓	✗	n.a.
DarkLaunder	✓	Cor. pool size	Low	Low participants	No signup req.	✗	✗	✓	✗	✓	✗	✓	✗	n.a.
Bitlaunder	✓	Cor. pool size	Low	Low participants	No signup req.	✗	✗	✓	✗	✓	✗	✓	✗	n.a.
CoinMixer	✓	Cor. pool size	Low	Low participants	No signup req.	✗	✗	✓	✗	✓	✗	✓	✗	n.a.
Helix	✓	Cor. pool size	High	High participants	No signup req.	✓	✗	✓	✗	—	✗	✓	✗	n.a.
Alphabay	✓	Cor. pool size	High	High participants	No signup req.	✓	✗	✓	✗	—	✗	✓	✗	n.a.
MixTum	✓	Cor. pool size	High	High participants	No signup req.	✓	✓	✓	✗	✗	✗	✓	Guarantee Letter	n.a.
CryptoMixer	✓	Cor. pool size	High	High participants	No signup req.	✓	✓	✓	✗	✗	✗	✓	Guarantee Letter	n.a.

(Continues)

TABLE 4 | (Continued)

	Centralization	Unlinkability	Liquidity	Anonymity set size	Log storing	Random delay	Random fee	Mixing fee?	Auditable	Address reusing?	Cross-chain mixing	Sybil/DoS resistance	Coin stealing r	Front-running resistance
Blender	✓	Cor. pool size	High	High participants	No signup req.	✓	✓	✓	✗	✗	✗	✓	✗	n.a.
ChipMixer	✓	Cor. pool size	High	High participants	No signup req.	✓	a.	✗	✗	✗	✗	✓[a]	✗	n.a.
Wasabi Wallet	✓	Cor. pool size	High	Limited to Tx size	No signup req.	—	✗	✓	✓	—	✗	✓	✗	n.a.
ShapeShift	✓	Fully disconnected	High	n.a.	Signup req.	—	—	✓	✗	✗	✓	✓	✓	n.a.
Bitmix.bz	✓	Fully disconnected	—	High participants	No signup req.	✓	✓	✓	✗	✗	✗	✓	Guarantee Letter	n.a.
Sudoku Wallet	✓	—	Low	Low participants	No signup req.	✓	✓	✓	✗	—	✗	✓	✓	n.a.
Join-Market	✗	Cor. pool size	High	Limited to Tx size	No signup req.	a.	a.	✗	✓	✗	✗	✓	✓	n.a.
Tornado Cash	✗	Cor. pool size	High	Max 2^{20}[b]	No signup req.	a.	✗	✗	✓	n.a.	✗	✓	✓	✓

Rows' colours stand as blue: decentralized academic, orange: centralized academic, green: centralized real-world, and pink: decentralized real-world.

[a]Although mixing fee is donation-based in ChipMixer, its is resilient to these types of attack due to its high liquidity.

[b]This value is corresponded to the maximum size of the Tornado Cash's Merkle tree [104].

integrity of their anonymity sets. In the domain of modern mixers, certain attack vectors have illuminated a paradox. Even as these services generate addresses randomly for each mixing request, there remains a necessity to consolidate funds into a restricted number of addresses to facilitate mixing operations. The inputs tied to these consolidation, or "sweeper," transactions inherently influence the size of the anonymity set.

- **Log storing**: Certain centralized mixing services retain mixing logs within their database, which leads to a security risk as sensitive mixing data, such as sender details, recipients, and transaction amounts, could potentially be exposed from the mixing service database. As there is not any reliable data about this metric on services, and nothing can be concluded without accessing to the implementation behind each tumbler, we mark those services who require users to signup before mixing as Signup Required (Signup Req.), since it can be an evidence that they store users' information in their database, which is a security risk. However, it is recommended to use TOR browser for mixing, in order to prevent mixer server from linking the IP addresses to the corresponding crypto addresses.
- **Cost of mixing (mixing fee)**: The economic viability of using a mixer is crucial for widespread adoption. Services that offer competitive fees while maintaining robust security and privacy features are likely to be preferred. Moreover, an unpredictable fee structure might aid in obfuscation.
- **Auditability**: Some users may prefer services that have undergone third-party audits, ensuring that the underlying code and mechanisms are sound and free of vulnerabilities.
- **Address reusing**: The redirection of mixed coins to initial addresses or address clusters linked to a user's identity can vitiate the mixing process, thereby reintroducing traceability. Note that this metric is not applicable for smart-contract-based cryptocurrencies, due to their account-based nature.
- **Cross-chain mixing**: As the cryptocurrency ecosystem grows, the ability for a mixer to support transactions between different blockchains (cross-chain transactions) can be a valuable feature. It can help users obscure their tracks even further by moving funds between different cryptocurrencies.
- **Sybil/DoS attack resistance**: In scenarios where an adversary populates a tumbler with a majority of its own addresses, the integrity of the anonymity set is compromised, thereby facilitating the tracing of coins (Sybil attack). Moreover, the efficacy of a tumbler can be compromised if a significant portion of its users are colluding or have established identities. In most cases, leveraging mixing fees can be a good obstacle for both Sybil and DoS attacks.
- **Coin stealing attack resistance**: When a third-party takes the responsibility to perform mixing, there is a great potential for them to steal the given funds by avoiding sending them the corresponding recipients. This scenario is more likely to happen in terms of centralized services, and several mixers have used mixing guarantee letters, introduced by MixCoin paper [25].
- **Trojan/intersection attack resistance**: A mixer's effectiveness is compromised when it uses predictable or discernible transaction mixing patterns. Such patterns, like uniform mixing amounts, and timely patterns, are vulnerable to taint analysis. This vulnerability becomes particularly evident when adversaries deploy Trojan or intersection attacks, potentially exposing the mixing pattern. Several studies have highlighted successful attacks on prominent Bitcoin services [26, 44, 64, 75, 93]. We assess two important factors in terms of pattern obfuscating: Fee and delay randomization, as discussed in Section 3. In terms of mixing structure, since the structure of most real-world services has been revealed by prior attacks, we do not discuss them in the table. However, it is vital for a service to be resistant to these types of attacks, and employing dynamic mixing methods can be an innovative way to reach this milestone.
- **Regulatory compliance**: Depending on the jurisdiction, mixing services might be subject to regulations. Ensuring compliance can prevent potential legal complications for both the service providers and their users. As an example, ShapeShift [78] employed a know-your-customer policy after being accused of money laundering, which resulted in lower anonymity and more traceability for its users. Due to the lack of reliable data about this metric for most services (except ShapeShift), we don't depict this metric in the table. Nevertheless, Those services that require users to sign up before mixing, are suspected to regulatory compliance.
- **Front-running resistance**: Front-running is one of the main challenges in terms of smart-contract-based cryptocurrencies like Ethereum. When talking about mixing, some actions like depositing funds alter the state of the mixing contract, while other actions like withdrawing funds have to rely on the state of the contract to form the cryptographic proofs, which grant them to withdraw their funds. Therefore, if there are multiple concurrent deposit actions issued to the contract, some withdrawing actions will get invalidated by those transactions that modify the state of the contract, and this process can be happened unintentionally by ordinary users, or deliberately by malicious ones [49, 102, 103]. Discussing mentioned smart-contract based methods (Möbius, AMR, MixEth, and Tornado Cash), front-running is not applicable in Möbius because of the nature of ring signature scheme [48], not applicable in MixEth due to its shuffling mechanism, and also not cost-efficient in AMR and Tornado Cash [49, 83]. Also, Zether places conflicting transactions in a pending state, and execute them only after resolving the conflicts to prevent potential front-running situations.

As illustrated in the evaluation Table 4, our analysis is based on pre-defined criteria and offers a comprehensive overview of the current mixing service landscape. Contrary to real-world applications where centralized services dominate, academic research mainly focuses on decentralized solutions. This academic inclination matches user preferences for enhanced privacy and reduced risk from regulatory intervention.

Centralized services come with their own set of inherent risks, including the potential for fraudulent activities and theft of funds, as highlighted in the "Coin Stealing Resistance" criterion of our evaluation table. On the flip side, most academic solutions are largely immune to such vulnerabilities, with CoinParty being a notable exception.

A significant security vulnerability emerges when a mixing service links multiple peeling chains together through aggregation transactions. In a peeling chain, transactions are divided into smaller parts, which are then distributed to their final destinations. However, as transactions near the end of the peeling chain, the remaining amounts often become too small to be further divided. Some services input these residual amounts into an aggregation transaction, which serves as the starting point for the next peeling chain [26].

By doing so, a traceable link is created between the two separate peeling chains. This linkage could potentially allow an attacker to correlate all transactions related to a particular service, thereby undermining the anonymity of users. In essence, transactions from different chains could be combined into one large cluster, which could be analysed collectively to identify patterns or isolate individual users.

Another crucial issue revolves around the transparency of the underlying algorithm. Services that disclose their algorithms not only gain more user trust but also invite community contributions. Those solutions using turing-complete smart contract technology are naturally more credible, due to their auditable and decentralized nature. Comparing early assessments, like the one by Novetta in 2015, with recent reports from CypherTrace and Chainalysis, reveals a noticeable increase in the adoption of mixing services [7, 8, 93]. However, sanctions on services like Tornado Cash have led to a shift towards other centralized alternatives [8].

Clearly, each service has its own strengths and drawbacks, and a user who wishes to mix her funds should choose the most appropriate mixer based on her important evaluation metrics. Also, an innovative approach to achieve higher anonymity is to utilize various mixing services in several consecutive rounds, which is referred to as multi-round mixing.

7 | Regulatory Compliance and Legal Challenges

Evaluating mixing services requires a thorough consideration of regulatory compliance and potential legal implications, particularly for centralized services. The regulatory landscape for cryptocurrencies and their ancillary services, including mixers, is complex and varies significantly across different jurisdictions. In the United States, for instance, cryptocurrency mixing services are subject to Financial Crimes Enforcement Network (FinCEN) regulations, which classify them as money service businesses (MSBs). This classification mandates the implementation of comprehensive anti-money laundering (AML) and counter-terrorism financing (CTF) measures, including rigorous know your customer (KYC) protocols [105].

These regulatory requirements aim to prevent the misuse of cryptocurrency platforms for money laundering and other illicit activities. However, they also present significant challenges to the core objective of mixing services: enhancing user privacy and transactional anonymity. The recent hack of the Bybit exchange underscores this tension. In February 2025, North Korean hackers exploited vulnerabilities in Bybit's security systems, stealing approximately $1.5 billion in digital assets. The stolen funds were laundered through various methods, including centralized and decentralized exchanges and mixing services such as Cryptomixer(centralized) and Wasabi Wallet (centralized), highlighting the challenges in tracing illicit transactions and the need for robust AML compliance [106]. Therefore, the design and operation of mixing services must balance enhancing privacy with adhering to regulatory standards aimed at preventing their use for illicit purposes [107].

Furthermore, the global nature of cryptocurrencies necessitates international cooperation and the harmonization of regulatory frameworks to effectively manage and mitigate risks associated with digital financial transactions. Varying regulatory approaches across countries add a layer of complexity for mixing services operating on a global scale. These differences arise from how jurisdictions classify and oversee cryptocurrencies—some treat them as commodities, others as securities, property, or even as prohibited assets. For instance, while the European Union has introduced a comprehensive framework through Markets in Crypto-Assets Regulation (MiCA) [108] to regulate crypto markets uniformly, the United States maintains a fragmented, multi-agency system that differs in technical regulatory policies compared to the Europe [109]. In contrast, countries like China have imposed outright bans on cryptocurrency trading, mining, and mixing services [110]. Such divergent approaches create legal uncertainty for platforms operating across borders, making it difficult to establish a single compliance strategy. This issue also enables regulatory arbitrage, allowing entities to shift operations to countries with looser oversight, thereby undermining coordinated enforcement efforts. Therefore, a robust understanding of international compliance requirements and the implementation of adaptable frameworks that satisfy multiple jurisdictions without compromising core functionalities is essential, without harming both the crypto industry and also the investors [111].

Incorporating a regulatory compliance framework into the evaluation criteria for mixing services underscores the importance of legal and ethical considerations in their operation. It also serves as a critical reminder that, while striving to enhance privacy and security, mixing services must ensure they do not become conduits for financial malfeasance. This dual responsibility is paramount to maintaining the legitimacy and sustainability of mixing services amidst evolving regulatory landscapes.

Recent legal developments further illuminate the complexities in this domain. In November 2024, a U.S. appeals court overturned the Treasury Department's sanctions against Tornado Cash, a privacy tool on the Ethereum blockchain. The court ruled that Tornado Cash's smart contracts could not be considered property, and thus fell outside the scope of the sanctions. This decision highlights the challenges regulators face in addressing decentralized technologies and emphasizes the need for clear legal frameworks that distinguish between technology platforms and their users' actions [112].

Subsequently, mixing services face a host of regulatory challenges that vary significantly across jurisdictions, largely due to disparate legal frameworks governing cryptocurrencies and varying interpretations of permissible activities related to anonymity-enhancing technologies. These challenges can be broadly categorized into several key areas:

- **Anti-money laundering compliance**: Many jurisdictions require entities operating as financial intermediaries to comply with AML regulations. Mixing services, particularly centralized ones, may fall under these regulations as they handle and transfer funds on behalf of users. AML compliance typically involves implementing systems to monitor and report suspicious activities, as well as conducting KYC procedures to verify customer identities. This poses operational challenges in maintaining user anonymity while complying with legal requirements.
- **Uncertainty and variability of laws**: The legal status of cryptocurrencies and related services, such as mixing, remains undefined or in flux in many regions. This uncertainty poses significant challenges, as mixing services may struggle to operate legally without risking sudden regulatory changes that could render their operations illegal or subject them to new compliance requirements.
- **Cross-border regulatory challenges**: As digital services, mixing platforms often operate across borders, serving an international user base. This exposes them to a complex patchwork of regulations that may conflict or overlap. This cross-border aspect complicates compliance efforts and increases the risk of legal liabilities in multiple countries.
- **Risk of sanctions and legal actions**: In jurisdictions with strict regulations against money laundering and terrorism financing, mixing services that fail to comply with regulatory demands might face severe penalties, including fines, sanctions, or even criminal charges against their operators. The example of the mixer service "Helix," which was linked with darknet marketplaces, illustrates potential legal repercussions.
- **Technological and operational constraints**: Adhering to regulatory requirements often means that mixing services must implement robust technological solutions to monitor transactions and user activities. These requirements can impose significant operational costs and technical challenges, especially for services striving to balance compliance with the privacy assurances promised to users.

Overall, mixing services must navigate a complex array of regulatory environments that vary by jurisdiction and evolve as digital currencies gain prominence and regulatory bodies adjust their frameworks. This dynamic regulatory landscape requires mixing services to be highly adaptable, often necessitating a proactive approach to compliance and legal strategy to mitigate legal challenges and ensure sustainable operations.

8 | Open Problems and Research Challenges

The digital frontier of cryptocurrencies, now expanded by the advent of mixing services, marks a significant leap in financial innovation, yet presents unparalleled challenges, particularly in the context of tracing fraudulent transactions and activities. Traditionally, tracking money laundering transactions within a single cryptocurrency ecosystem has been achievable to a certain extent through strategies such as Trojan attacks, ML-based strategies, or Sybil attacks. However, the emergence of cross-chain mixing activities significantly undermines these efforts.

For instance, when dirty money undergoes a series of complex transformations encompassing multiple cryptocurrencies and DeFi solutions, tracing it becomes exponentially difficult. It begins with a Bitcoin mixing service, morphing into Ether via anonymous exchanges, only to be further intertwined with other cryptocurrencies through platforms like Uniswap before it eventually resurfaces as fiat currency. This complex process poses a considerable obstacle in pinpointing the transitional phases where money changes hands and forms.

Moreover, an impending issue surfaces when the money to be laundered originates from fiat currency. The complex network created by combining this phase with cross-chain mixing methods creates an almost untraceable path, amplifying the challenges of monitoring and enforcement. This lack of a fully trackable chain from the path before ramp-on point to ramp-off, combined with the complicated techniques associated with mixing services, constructs a virtually impenetrable shield against current tracking techniques.

In research, a significant issue is the lack of detailed data about mixing services, which makes it difficult to improve machine-learning attack strategies. Without this crucial data, researchers are unable to create and enhance methods that could possibly lead to major breakthroughs in combating money laundering through cryptocurrencies.

Looking forward, a promising avenue of research is to conceptualize a mixing framework that stands resilient against Trojan attacks that are proficient at identifying patterns in transaction flows. Such a framework might hinge on the execution of off-chain transactions, safeguarded by groundbreaking encryption methodologies, zero-knowledge proofs, and trusted-execution-environments, fostering both innovation and security in cryptocurrency transactions.

Additionally, dynamic mixing can serve as an effective solution to prevent Trojan attacks while enhancing the security and anonymity of the mixing process. In essence, dynamic mixing involves using multiple mixing methods in conjunction with each other to make the mixing process look more complicated from the outside, thus hindering attackers from detecting the mixing pattern through their interactions with the service.

However, working towards this goal is not easy due to the complex nature of the problem, and it demands careful planning to maintain both decentralization and security. Furthermore, embracing the prospect of interdisciplinary research, which merges the strengths of various domains such as cryptography, machine learning, and policy formulation, can create a robust platform to address these open problems. The nexus of these fields could pave the way for innovative solutions that are both secure and preserve the fundamental principles of cryptocurrencies.

In addition to the risks posed by fungible cryptocurrencies, an emerging area for future investigation is the money laundering vulnerabilities associated with non-fungible tokens (NFTs). NFTs combine the pseudonymity and international accessibility of crypto-assets with the subjective pricing systems often seen in the fine art market [113, 114]. This blend of characteristics creates a complex challenge for anti-money laundering frameworks,

as the highly variable and subjective pricing of NFTs provides opportunities for value manipulation, making them particularly susceptible to illicit financial activities.

Conclusively, as the landscape of cryptocurrencies evolves, it requires a proactive approach in addressing the imminent challenges and fostering an environment that nurtures innovation while upholding the principles of security and privacy. Finding an optimal pathway that facilitates advancements in technology while maintaining strict regulations poses a formidable challenge, yet stands as a vital undertaking for the community in the coming years.

9 | Conclusion

In this comprehensive study, the authors have introduced a novel evaluation framework for blockchain-based mixing services, marking the first instance where such criteria have been systematically defined and applied. The manuscript provides an in-depth analysis that bridges academic theories and real-world applications, making it both a tutorial for beginners and a resource for experts to identify the strengths and weaknesses of each solution, as well as potential attack methods. This study has rigorously analysed 32 mixing services implementations and has gone beyond theoretical discussions by conducting real-world attacks to reveal the operational mechanisms of existing black-box mixing services.

A key finding highlights the prevalent use of a conventional set of techniques—such as aggregation, peeling chains, and the integration of random delays and fees—in current real-world mixing services. These findings contrast sharply with the innovative and diverse methods that have been theorized in academic circles.

Regulatory compliance and potential legal implications are particularly relevant for centralized mixing services, casting doubt on their long-term sustainability. Additionally, the absence of dynamic mixing strategies, which would combine multiple techniques, represents a significant shortfall in augmenting both the security and anonymity aspects of blockchain transactions.

Furthermore, the manuscript underscores the need for mixing services that are compatible across multiple blockchain platforms, a challenge that also presents a significant opportunity for future innovation. Overcoming the technical barriers to achieving cross-chain mixing would catalyse further advancements in this rapidly growing domain.

Consequently, the study emphasizes the need for closer integration between academic research and industry practices to nurture a blockchain ecosystem that is not only secure but also robustly anonymous.

Author Contributions

Alireza Arbabi: conceptualization, formal analysis, investigation, visualization, writing – original draft, writing – review & editing. **Ardeshir Shojaeinasab:** conceptualization, methodology, validation, writing – original draft, writing – review & editing, supervision, project administration. **Homayoun Najjaran:** writing – review & editing, supervision.

Acknowledgements

Alireza Arbabi and A.-SArdeshir Shojaeinasab contributed equally to this work. We would like to express our sincere gratitude to Dr. Behnam Bahrak for his invaluable help and contribution to this work. Without his guidance and support, this research would not have been possible.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

Data sharing not applicable—no new data generated, or the article describes entirely theoretical research.

Endnotes

[1] This data was captured in 2016

[2] P2SH: Pay-to-Script-Hash

References

1. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (2008), accessed January 12, 2025, https://bitcoin.org/bitcoin.pdf.

2. Y. Sompolinsky and A. Zohar, "Secure High-Rate Transaction Processing in Bitcoin," in *Financial Cryptography and Data Security: 19th International Conference* (Springer, 2015), 507–527.

3. A. Ghosh, S. Gupta, A. Dua, and N. Kumar, "Security of Cryptocurrencies in Blockchain Technology: State-of-Art, Challenges and Future Prospects," *Journal of Network and Computer Applications* 163 (2020): 102635.

4. J. Wu, J. Liu, Y. Zhao, and Z. Zheng, "Analysis of Cryptocurrency Transactions From a Network Perspective: An Overview," *Journal of Network and Computer Applications* 190 (2021): 103139.

5. N. Christin, "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace," in *Proceedings of the 22nd International Conference on World Wide Web* (ACM, 2013), 213–224.

6. S. Bistarelli, M. Parroccini, F. Santini, et al., "Visualizing Bitcoin Flows of Ransomware: Wannacry One Week Later," in *Italian Conference on Cybersecurity (ITASEC)* (2018), 1–8.

7. C. Inc., "Cryptocurrency Crime and Anti-Money Laundering Report," https://ciphertrace.com/crime-and-anti-money-laundering-report-march-2023/.

8. "Chainalysis Crypto Crime Report," https://go.chainalysis.com/2023-crypto-crime-report.html (2023).

9. D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and Prisma Group, "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: the Prisma Statement," *Annals of Internal Medicine* 151, no. 4 (2009): 264–269.

10. A. Gaikwad, "Overview of Blockchain," *International Journal for Research in Applied Science and Engineering Technology* 8, no. 6 (2020): 2268–2270.

11. S. King and S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency With Proof-of-Stake" (2012), accessed December 21, 2024, https://peercoin.net/assets/paper/peercoin-paper.pdf.

12. National Institute of Standards and Technology, "Secure Hash Standard (SHS)" (2012), accessed February 3, 2025, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

13. A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of Clients in Bitcoin P2P Network," in *Proceedings of the 2014 ACM SIGSAC*

Conference on Computer and Communications Security (ACM, 2014), 15–29.

14. A. Kumar, D. Choudhary, M. Raju, D. K. Chaudhary, and R. Sagar, "Combating Counterfeit Drugs: A Quantitative Analysis on Cracking Down the Fake Drug Industry by Using Blockchain Technology," in *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (IEEE, 2019), 174–178.

15. V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform" (2014), accessed January 27, 2020, https://ethereum.org/en/whitepaper/.

16. F. Schär, "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets," *Federal Reserve Bank of St. Louis Review* 103, no. 1 (2021): 37–54.

17. J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments" (2016), accessed January 8, 2025, https://lightning.network/lightning-network-paper.pdf.

18. U. Fiege, A. Fiat, and A. Shamir, "Zero Knowledge Proofs of Identity," in *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing* (1987), 210–217.

19. Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A Survey on Privacy Protection in Blockchain System," *Journal of Network and Computer Applications* 126 (2019): 45–58.

20. M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," *IEEE Communications Surveys & Tutorials* 20, no. 4 (2018): 3416–2018.

21. L. Wu, Y. Hu, Y. Zhou, et al., "Towards Understanding and Demystifying Bitcoin Mixing Services," in *Proceedings of the Web Conference 2021* (2021), 33–44.

22. T.-H. Chang and D. Svetinovic, "Improving Bitcoin Ownership Identification Using Transaction Patterns Analysis," *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50, no. 1 (2018): 9–2018.

23. M. Harrigan and C. Fretter, "The Unreasonable Effectiveness of Address Clustering," in *2016 International IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress* (IEEE, 2016), 368–373.

24. Y. Gong, K. P. Chow, S. M. Yiu, and H. F. Ting, "Analyzing the Peeling Chain Patterns on the Bitcoin Blockchain," *Forensic Science International: Digital Investigation* 46 (2023): 301614.

25. J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for Bitcoin With Accountable Mixes," in *18th International Conference on Financial Cryptography and Data Security* (Springer, 2014), 486–504.

26. A. Shojaeinasab, A. P. Motamed, and B. Bahrak, "Mixing Detection on Bitcoin Transactions Using Statistical Patterns," *IET Blockchain* 3, no. 3 (2022): 136–148.

27. L. Valenta and B. Rowan, "Blindcoin: Blinded, Accountable Mixes for Bitcoin," in *Financial Cryptography and Data Security: FC 2015 International Workshops* (Springer, 2015), 112–126.

28. E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg, "TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub," in *Network and Distributed System Security Symposium* (NDSS, 2017), 1–15.

29. J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," (2016).

30. "Raiden Network Official Webpage," accessed: July 17 2024, https://raiden.network/.

31. F. Zhang and H. Zhang, "SOK: A Study of Using Hardware-Assisted Isolated Execution Environments for Security," in *Proceedings of the Hardware and Architectural Support for Security and Privacy 2016* (ACM, 2016), 1–8.

32. I. Anati, S. Gueron, S. Johnson, and V. Scarlata, "Innovative Technology for CPU Based Attestation and Sealing," in *Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy* (ACM, 2013), 1–7.

33. F. McKeen, I. Alexandrovich, A. Berenzon, C. V. Rozas, H. Shafi, V. Shanbhogue, and U. R. Savagaonkar, "Innovative Instructions and Software Model for Isolated Execution," in *HASP '13: Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy* (ACM, 2013), 1–10.

34. ARM Limited, "Security Technology Building a Secure System Using Trustzone Technology" (2009), accessed December 14, 2024, https://developer.arm.com/documentation/PRD29-GENC-009492C.

35. E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions," in *International Conference on Financial Cryptography and Data Security* (Springer, 2016), 43–60.

36. S. Meiklejohn and R. Mercer, "Möbius: Trustless Tumbling for Transaction Privacy" (2018), accessed January 31, 2019, https://eprint.iacr.org/2018/1048.pdf.

37. K. M. Alonso, "Zero to Monero" (2020), accessed January 9, 2023, https://www.getmonero.org/library/Zero-to-Monero-2-0-0.pdf.

38. S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to Better—How to Make Bitcoin a Better Currency," in *16th International Conference on Financial Cryptography and Data Security* (Springer, 2012), 399–414.

39. M. C. K. Khalilov and A. Levi, "A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems," *IEEE Communications Surveys & Tutorials* 20, no. 3 (2018): 2543–2018.

40. E. Tairi, P. Moreno-Sanchez, and M. Maffei, "A 2 l: Anonymous Atomic Locks for Scalability in Payment Channel Hubs," in *2021 IEEE Symposium on Security and Privacy (SP)* (IEEE, 2021), 1834–1851.

41. G. Maxwell, "Coinjoin: Bitcoin Privacy for the Real World" https://bitcointalk.org/index.php?topic=279249 (2013), accessed January 25, 2021, https://bitcointalk.org/index.php?topic=279249.0.

42. T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coinshuffle: Practical Decentralized Coin Mixing for Bitcoin," in *19th European Symposium on Research in Computer Security on Computer Security-ESORICS 2014* (Springer, 2014), 345–364.

43. N. Glaeser, M. Maffei, G. Malavolta, P. Moreno-Sanchez, E. Tairi, and S. A. K. Thyagarajan, "Foundations of Coin Mixing Services," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (ACM, 2022), 1259–1273.

44. G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybil-Resistant Mixing for Bitcoin," in *Proceedings of the 13th Workshop on Privacy in the Electronic Society* (ACM, 2014), 149–158.

45. J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, "Coinparty: Secure Multi-Party Mixing of Bitcoins," in *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy* (ACM, 2015), 75–86.

46. I. Ingemarsson and G. J. Simmons, "A Protocol to Set Up Shared Secret Schemes Without the Assistance of a Mutually Trusted Party," in *Workshop on the Theory and Application of of Cryptographic Techniques* (Springer, 1990), 266–282.

47. M. H. Ibrahim, "Securecoin: A Robust Secure and Efficient Protocol for Anonymous Bitcoin Ecosystem", accessed February 7, 2025, https://arxiv.org/abs/1604.00517.

48. R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in *7th International Conference on the Theory and Application of Cryptology and Information Security Advances in Cryptology—ASIACRYPT 2001* (Springer, 2001), 552–565.

49. D. V. Le and A. Gervais, "Amr: Autonomous Coin Mixer With Privacy Preserving Reward Distribution," in *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies* (ACM, 2021), 142–155.

50. "AAVE: The Money Market Protocol", accessed December 11, 2024, https://aave.com/.

51. "Compound. https://compound.finance/", accessed February 5, 2025 https://compound.finance/.

52. I. A. Seres, D. A. Nagy, C. Buckland, and P. Burcsi, "Mixeth: Efficient, Trustless Coin Mixing Service for Ethereum" (2019), accessed December 20, 2024, https://eprint.iacr.org/2019/236.pdf.

53. C. A. Neff, "A Verifiable Secret Shuffle and Its Application to E-Voting," in *Proceedings of the 8th ACM Conference on Computer and Communications Security* (ACM, 2001), 116–125.

54. B. Bünz, S. Agrawal, M. Zamani, and D. Boneh, "Zether: Towards Privacy in a Smart Contract World," in *International Conference on Financial Cryptography and Data Security* (Springer, 2020), 423–443.

55. D. Chaum, "Blind Signature System," in *Advances in Cryptology: Proceedings of Crypto* (Springer, 1983), 153–153.

56. L. Aumayr, O. Ersoy, A. Erwig, et al., "Generalized Bitcoin-Compatible Channels" (2020), accessed January 16, 2025, https://eprint.iacr.org/2020/476.pdf.

57. R. Canetti, "Universally Composable Security: A New Paradigm for Cryptographic Protocols," in *Proceedings 42nd IEEE Symposium on Foundations of Computer Science* (IEEE, 2001), 136–145.

58. H. Xie, S. Fei, Z. Yan, and Y. Xiao, "Sofitmix: A Secure Offchain-Supported Bitcoin-Compatible Mixing Protocol," *IEEE Transactions on Dependable and Secure Computing* 20, no. 5 (2022): 4311–2022.

59. M. Minaei, P. Chatzigiannis, S. Jin, et al., "Unlinkability and Interoperability in Account-Based Universal Payment Channels," in *International Conference on Financial Cryptography and Data Security* (Springer, 2023), 367–384.

60. Z. Ge, J. Gu, C. Wang, Y. Long, X. Xu, and D. Gu, "Accio: Variable-Amount, Optimized-Unlinkable and Nizk-Free Off-Chain Payments via Hubs," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (ACM, 2023), 1541–1555.

61. C. Decker and R. Wattenhofer, "A Fast and Scalable Payment Network With Bitcoin Duplex Micropayment Channels," in *17th International Symposium on Stabilization, Safety, and Security of Distributed Systems, SSS 2015* (Springer, 2015), 3–18.

62. M. Tran, L. Luu, M. S. Kang, I. Bentov, and P. Saxena, "Obscuro: A Bitcoin Mixer Using Trusted Execution Environments," in *Proceedings of the 34th Annual Computer Security Applications Conference* (ACM, 2018), 692–701.

63. J. Carlyle, T. Malene, C. Manai, N. Shah, G. Thomas, and R. Willis, "Obscuro Whitepaper" (2022), accessed January 24, 2025, https://obscu.ro/obscuro-whitepaper.pdf.

64. M. Moser, "Anonymity of Bitcoin Transactions" (2013), accessed February 4, 2018, https://mmoser.github.io/publications/anonymity-of-bitcoin-transactions.pdf.

65. U. D. of Justice, "Individual Arrested and Charged With Operating Notorious Darknet Cryptocurrency "Mixer"" (2021) accessed: September 29 2023, https://justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer.

66. T. de Balthasar and J. Hernandez-Castro, "An Analysis of Bitcoin Laundry Services," in *Secure IT Systems: 22nd Nordic Conference, NordSec 2017* (Springer, 2017), 297–312.

67. "Operator of Helix Bitcoin "Mixer" Pleads Guilty" (2021), accessed: September 09 2023, https://wsj.com/articles/operator-of-helix-bitcoin-mixer-pleads-guilty-11629328791.

68. M. Prathap, "Operator of Helix Bitcoin "Mixer" Pleads Guilty" (2021), accessed: September 09 2023, https://businessinsider.in/investment/news/bitcoin-mixing-service-helix-pleads-guilty-to-laundering-300-million-will-forfeit-over-4400-bitcoins/articleshow/85482090.cms.

69. "Alphabay Crime Report" (2017), accessed: September 09 2023, https://bitcointalk.org/index.php?topic=2040756.0.

70. "Mixtum Webpage" (2018), accessed: September 09 2023, https://mixtum.io/.

71. "Cryptomixer Webpage", https://cryptomixer.ltd/ (2016) accessed: September 09 2023, https://cryptomixer.io/.

72. Elliptic Research, "The Largest Theft in History – Following the Money Trail From the Bybit Hack," (2025), accessed February 24 2025, https://www.elliptic.co/blog/bybit-hack-largest-in-history.

73. "Blender webpage" (2017), accessed September 09 2023, https://blendor.io/.

74. "Chipmixer Seizure Report," (2019), accessed September 09 2023, https://justice.gov/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3.

75. J. Pakki, Y. Shoshitaishvili, R. Wang, T. Bao, and 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* (Springer, 2021), 117–146.

76. "Wassabi Wallet Github Page" (2018), accessed September 09 2023, https://github.com/zkSNACKs/WabiSabi/.

77. Z. Wang, S. Chaliasos, K. Qin, et al., "On How Zero-Knowledge Proof Blockchain Mixers Improve, and Worsen User Privacy," in *Proceedings of the ACM Web Conference 2023* (ACM, 2023), 2022–2032.

78. "Shapeshift Webpage" (2014), accessed September 09 2023, https://shapeshift.io.

79. "How Dirty Money Disappears Into the Black Hole of Cryptocurrency" (2018), accessed September 29 2023, https://wsj.com/articles/how-dirty-money-disappears-into-the-black-hole-of-cryptocurrency-1538149743.

80. "Bitmix Webpage" (2017), accessed September 29 2023, bitmix.bz.

81. "Soduku Wallet Publication Announcement Page" (2019), accessed September 29 2023, https://bitcointalk.org/index.php?topic=5194344.0.

82. "Joinmarket Official Repository" (2017), accessed September 29 2023, https://github.com/JoinMarket-Org/joinmarket-clientserver.

83. A. Pertsev, R. Semenov, and R. Storm, "Tornado Cash Privacy Solution Version 1.4" (2019), accessed December 13, 2024, https://tornado.cash/Tornado%20cash%20privacy%20solution%201.4.pdf.

84. "Tornado Cash Seizure Report" (2022), accessed September 29 2023, https://home.treasury.gov/news/press-releases/jy0916.

85. The Record by Recorded Future, "Tornado Cash: Crypto Mixer Judge Overturns Sanctions" (2024), accessed December 25 2024, https://therecord.media/tornado-cash-crypto-mixer-judge-overturns-sanctions.

86. Morgan Lewis, "Fifth Circuit Rejects OFAC's Tornado Cash Sanctions" (2024), accessed December 25 2024, https://www.morganlewis.com/pubs/2024/12/fifth-circuit-rejects-ofacs-tornado-cash-sanctions#_ftnref2.

87. "Railgun Webpage," accessed September 29 2023, https://www.railgun.org/.

88. "Cyclone Webpage," accessed September 29 2023, http://www.cyclone.xyz/.

89. "Zkbob Webpage" accessed September 29 2023, https://www.zkbob.com/.

90. "Typhoon Cash Webpage" accessed September 29 2023, https://typhoon.cash/.

91. Elliptic Inc., "Tornado Cash Alternatives Report" (2022), accessed January 18, 2025, https://www.elliptic.co/resources/tornado-cash-alternatives.

92. T. J. BARBEREAU, E. Ermolaev, M. Brennecke, E. Hartwich, and J. Sedlmeir, "Beyond a Fistful of Tumblers: Toward a Taxonomy of Ethereum-Based Mixers," in *44th International Conference on Information Systems* (AIS Library, 2023), 1–17.

93. Novetta Security Co., "Survey of Bitcoin Mixing Services: Tracing Anonymous Bitcoins" (2015), accessed January 28, 2018, https://www.novetta.com/wp-content/uploads/2015/06/Tracing-Anonymous-Bitcoin.pdf.

94. "WalletExplorer," accessed September 29 2023, https://walletexplorer.com/.

95. Blockstream.info, "Bitcoin Coin Mixing Data Set With Rule-Based Label" (2023), accessed September 29 2023, https://github.com/sxwxs/BitcoinCoinMixingDataSetWithRuleBasedLabel.

96. L. Nan and D. Tao, "Bitcoin Mixing Detection Using Deep Autoencoder," in *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)* (IEEE, 2018), 280–287.

97. J. Wu, J. Liu, W. Chen, H. Huang, Z. Zheng, and Y. Zhang, "Detecting Mixing Services via Mining Bitcoin Transaction Network With Hybrid Motifs," *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 52, no. 4 (2021): 2237–2021.

98. X. Sun, T. Yang, and B. Hu, "LSTM-TC: Bitcoin Coin Mixing Detection Method With a High Recall," *Applied Intelligence* 52, no. 1 (2022): 780–793.

99. J. Wu, D. Lin, Q. Fu, et al., "Towards Understanding Asset Flows in Crypto Money Laundering Through the Lenses of Ethereum Heists," *IEEE Transactions on Information Forensics and Security* 19 (2023): 1994–2009.

100. R. De Silva, W. Guo, N. Ruaro, I. Grishchenko, C. Kruegel, and G. Vigna, "GuideEnricher: Protecting the Anonymity of Ethereum Mixing Service Users With Deep Reinforcement Learning," in *33rd USENIX Security Symposium (USENIX Security 24)* (ACM, 2024), 3549–3566.

101. H. Du, Z. Che, M. Shen, L. Zhu, and J. Hu, "Breaking the Anonymity of Ethereum Mixing Services Using Graph Feature Learning," *IEEE Transactions on Information Forensics and Security* 19 (2023): 616–631.

102. B. Bünz, S. Agrawal, M. Zamani, and D. Boneh, "Zether: Towards Privacy in a Smart Contract World," in *International Conference on Financial Cryptography and Data Security* (Springer, 2020), 423–443.

103. S. Eskandari, S. Moosavi, and J. Clark, "Sok: Transparent Dishonesty: Front-Running Attacks on Blockchain," in *Financial Cryptography and Data Security: FC 2019 International Workshops, VOTING and WTSC* (Springer, 2020), 170–189.

104. "Tornado Cash Official Repository" (2019), accessed September 29 2023, https://github.com/tornadocash/tornado-core.

105. C. Chainalysis, "Money Laundering and Cryptocurrency: Trends and New Techniques for Detection and Investigation", accessed January 19, 2025, https://www.chainalysis.com/reports/.

106. Associated Press, "North Korea Behind the $1.5B Bybit Crypto Hack, FBI Says" (2025), accessed December 22, 2024, https://apnews.com/article/1.5b-bybit-hack-north-korea-fbi.

107. C. Chainalysis, "The 2024 Crypto Crime Report" (2024), accessed January 29, 2025, https://go.chainalysis.com/2024-Crypto-Crime-Report.html.

108. J. Dilevsky, "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and Amending Directive (eu) 2019/1937" (2022), accessed February 15, 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0593.

109. P. Radanliev, "Review and Comparison of US, EU, and EK Regulations on Cyber Risk/Security of the Current Blockchain Technologies: Viewpoint From 2023," *The Review of Socionetwork Strategies* 17, no. 2 (2023): 105–2023.

110. Reuters, "China Debates How to Handle Criminal Crypto Cache" (2025), accessed April 20 2025, https://www.reuters.com/world/china/china-debates-how-handle-criminal-crypto-cache-2025-04-15/.

111. P. Radanliev, "The Rise and Fall of Cryptocurrencies: Defining the Economic and Social Values of Blockchain Technologies, Assessing the Opportunities, and Defining the Financial and Cybersecurity Risks of the Metaverse," *Financial Innovation* 10, no. 1 (2024): 1.

112. Reuters, "Court Overturns u.s. Sanctions Against Cryptocurrency Mixer Tornado Cash" (2024), accessed January 6, 2025, https://www.reuters.com/legal/court-overturns-us-sanctions-against-cryptocurrency-mixer-tornado-cash-2024-08-30/.

113. A. Mosna and G. Soana, "Nfts and the Virtual Yet Concrete Art of Money Laundering," *Computer Law & Security Review* 51 (2023): 105874.

114. R. Tewari and B. P. Pande, "Transforming Digital Ownership: The Role of NFTs in Shaping Virtual Economies and Market Dynamics," *IET Blockchain* 5, no. 1 (2025): e70010.