ANONYMITY IN CRYPTO MIXERS: TRACING CRYPTO ASSETS

1. Exit from Mixers: Fund Flows on the Blockchain

Crypto mixers are online services that aggregate crypto assets belonging to multiple users into a single pool and subsequently redistribute those assets to different addresses, in varying amounts and at different time intervals, with the aim of weakening the link between the transaction history and the ultimate recipient of the assets. In practice, this structure results in making the identification of the source of funds, particularly those derived from criminal activity, more difficult. Nevertheless, due to the inherently irreversible and transparent nature of the blockchain, the relevant transactions continue to be recorded on the blockchain.

At this stage, the fundamental question is whether the use of mixers renders the tracing of crypto assets entirely impossible. In practice, mixers complicate the flow of funds and slow down tracing processes; however, this does not mean that crypto asset tracing comes to an end. Owing to the public nature of the blockchain, transaction records continue to exist on the chain and may be analyzed when appropriate tools are employed. In particular, the limited liquidity of mixers makes it difficult to effectively dilute high-value transactions, and technical data obtained as a result of law enforcement interventions targeting mixer infrastructures may allow past transactions to be examined retrospectively.

In this context, although mixers significantly limit traceability, it cannot be said that crypto asset movements become entirely invisible. Accordingly, mixers should be regarded not as tools providing absolute anonymity, but rather as mechanisms that make the direct and rapid tracing of fund flows more difficult.

2. Technical Tracing Methods: Are Mixers an Endless Black Hole?

Following the entry of crypto assets into mixer services and their subsequent exit from such services, the traceability of the relevant funds on the blockchain stems from the public and immutable nature of blockchain records. Blockchains preserve the sending and receiving history of an asset at the level of each individual transaction, and these records cannot be deleted and may be examined using specific methods. This transparent structure forms the technical foundation of crypto forensic analyses aimed at tracing fund movements, even where tools such as mixers are used to complicate fund flows. In this context, tracing methods rely on sophisticated algorithms that assess not only transaction histories, but also transaction patterns and the linkages between addresses.

Among the technical tools used for post-mixer tracing are address clustering and transaction graph analysis. Address clustering statistically evaluates user behaviors and transaction patterns in order to determine whether multiple addresses are likely controlled by the same individual or entity, thereby enabling the identification of linkages between addresses emerging from mixers and subsequent transfers. Transaction graph analysis, in this respect, maps the flow of funds between addresses in a graphical form, creating structural models that facilitate the tracing of funds. These methods represent standard techniques employed by forensic analytics firms and law enforcement authorities to transform blockchain data into traceable pathways.

Nevertheless, tracing mixed funds is more complex than basic fund flow monitoring and requires advanced methods. For example, techniques such as the Lowest Intermediate Balance Rule *(LIBR)* assist in analyzing how assets entering a mixer wallet are distributed to different addresses, which assets are likely to remain traceable, and which balances may be considered potentially clean. Under such methods, probable tracing paths of funds are calculated by using data such as the balances of incoming and outgoing transactions to and from the mixer pool, transaction timelines, and transfer weights. Accordingly, it becomes possible to trace, step by step, the movements made to new addresses outside the mixer. Collectively, these technical tools and analytical methods demonstrate that funds do not become entirely invisible after exiting a mixer system.

Although mixers may obscure transaction patterns and thereby impede tracing efforts, the transparency of blockchain data, together with advanced graph and heuristic techniques, enables links between the original input addresses and newly created addresses associated with post mixer transactions to be re-established or at a minimum, significantly narrowed with a high degree of probability. Notably, post mixer tracing activities do not necessarily aim to establish a one to one correspondence between a specific input and a specific output; rather, they focus on conducting a risk based assessment of address clusters and transactional ecosystems through which the funds circulate. In this context, technical tracing methods are employed both in digital forensic investigations and in compliance processes, including AML frameworks, to assess the effectiveness of mixer usage and, where appropriate, to obtain evidentiary value.

3. Identifying Suspicious Addresses and Risk Assessment

AML compliance programs require systematic risk assessment processes to identify high risk fund movements on crypto asset platforms and to implement appropriate mitigating measures. In this context, crypto addresses that enter into or exit from crypto mixers may be classified as high risk by AML compliance tools, as a transaction history involving mixers makes it more difficult to associate the funds with a legitimate source. Compliance software analyzes inter address relationships at both micro and macro levels to determine whether funds have a mixer nexus and flags addresses with a mixer history as high risk transaction indicators within regulatory risk typologies. Such risk labeling is of critical importance for crypto asset service providers *(CASPs)* in fulfilling their compliance obligations and in adhering to the risk based approach mandated by AML regulations.

The effectiveness of AML compliance systems is not limited to identifying address histories; it also enables the automated detection of suspicious activity and the triggering of necessary compliance measures through transaction risk scoring modules and integrated KYC and KYT processes. KYT systems monitor on chain transactions in real time and generate immediate alerts where a transaction involves a mixer history or other high risk indicators; these alerts are designed to allow the platform to automatically suspend the transaction, request additional information, or freeze the relevant funds. Similarly, while KYC processes verify user identity, users associated with funds that have a mixer linked high risk history may be subject to additional compliance measures, such as Enhanced Due Diligence. This risk focused approach forms part of the proactive monitoring framework required by AML and CFT standards and strengthens crypto platforms' obligations to comply with both internal policies and international regulatory requirements.

4. Forensic and Criminal Enforcement Against Mixers

In the context of combating mixers that facilitate the concealment of crypto assets, it has become increasingly evident in recent years that forensic and criminal sanctions are being applied in a concrete manner. In this regard, on May 6, 2022, the U.S. Treasury Department's Office of Foreign Assets Control *(OFAC)* designated a Bitcoin mixer for its use in laundering approximately USD 620 million in crypto assets obtained through a blockchain network attack carried out by a cybercrime group linked to North Korea.

Following this, on August 8, 2022, OFAC imposed sanctions on an Ethereum-based mixer, stating that the service had been used, since 2019, to obfuscate the trail of more than USD 7 billion in crypto assets and that a significant portion of these funds was linked to cybercrime and actors subject to international sanctions. These sanctions were expanded to cover not only the mixer service itself but also the associated smart contract addresses, thereby prohibiting transactions involving those addresses under U.S. law.

Another recent and striking example concerns the Bitcoin Fog mixer. In the case heard before the Federal Court in Washington, D.C. in March 2024, convictions were rendered for facilitating money laundering, conspiracy to commit money laundering, and operating an unlicensed money transmitting business; the individual operating the mixer was sentenced to more than 12 years' imprisonment, and forfeiture was ordered in respect of crypto assets worth millions of dollars. Similarly, it is observed that international law enforcement cooperation plays a critical role in the fight against mixers. In December 2025, an operation carried out by the federal authorities in Switzerland and Germany, coordinated by the European Union Agency for Law Enforcement Cooperation *(Europol)*, resulted in the shutdown of the large-scale Bitcoin mixer *Cryptomixer.io*; infrastructure identified as having been used to conceal transactions linked to ransomware and cybercrime proceeds was seized, along with Bitcoin valued at EUR 25 million and more than 12 terabytes of data.