

TRACE-OBSCURING IN THE CRYPTO ECOSYSTEM: CRYPTO MIXERS

Crypto mixers have been developed as tools designed to enhance user privacy by splitting and reassembling transaction data on the blockchain. However, the high level of anonymity provided by these systems facilitates the concealment of the origin of crypto-assets. This, in turn, significantly increases the risks of money laundering of proceeds of crime, obscuring the traceability of funds derived from fraud, and concealing violations of multiple regulatory obligations.

1. What Is a Crypto Mixer?

Crypto mixers are services designed to conceal the origin and ultimate owner of funds by pooling and commingling crypto assets from multiple users and redistributing those assets to new addresses in varying amounts and at different times. This structure is premised on anonymity within the blockchain and allows users to exchange their crypto assets or redirect them to different addresses without linking such transactions to their prior transaction history. In addition, certain mixers seek to obscure the very use of the mixing service itself by varying transaction fees or utilizing multiple withdrawal addresses.

Crypto mixers are generally categorized into two types based on their operational structure: centralized and decentralized mixers:

- **Centralized Mixers:** These are service providers that aggregate users' crypto assets into a single pool and, in return for a specified fee, distribute different crypto assets back to the users, exercising full authority over the process. However, because such providers typically maintain records of transactions and require a high degree of trust in a third party, they carry inherent risks of privacy breaches and data leakage.



- **Decentralized Mixers:** These are non-custodial mixing systems that combine and redistribute user funds through protocols such as *CoinJoin* and similar mechanisms employing zero-knowledge proof techniques. As no records are maintained and transactions are executed through smart contracts, identifying the source of funds becomes significantly more difficult, and a higher level of privacy is achieved compared with centralized mixers.



2. Use of Crypto Mixers in Fraud, Money Laundering, and Cybercrime

Although crypto mixers provide an additional layer of privacy for blockchain transactions, their design, namely, fragmenting transaction histories and reducing the traceability of fund flows, renders them high-risk tools conducive to the concealment of criminal proceeds in the context of fraud, cybercrime, and money laundering. In this regard, malicious actors frequently use mixers to obscure the origin of illicit funds such as hacking proceeds, revenues from narcotics trafficking, ransomware payments, and other unlawful gains. Indeed, cybercriminals also rely on mixers to sever the link between wallets in which they initially receive illicit proceeds and the exit wallets used to transfer such funds to crypto-fiat exchanges, thereby hindering the activation of AML monitoring mechanisms and complicating the detection of fund movements. Europol's findings regarding the *ChipMixer* operation corroborate these assessments, noting that a substantial portion of transactions routed through the mixer were associated with dark-web marketplaces, ransomware groups, illicit goods trafficking, circulation of child exploitation material, and stolen crypto assets.

In addition to money laundering, mixers are used in fraud schemes, particularly investment fraud, unauthorized transfers carried out through social engineering, and exchange hacks, to rapidly “disaggregate” the illicit proceeds and diminish the visibility of their on-chain traces. Mixer use has also become a common intermediary step in ransomware attacks to impede the traceability of the demanded crypto payments, further complicating efforts to track and identify cybercrime-related proceeds.



3. Legal Analysis Under The Financial Action Task Force (the “FATF”), The Financial Crimes Investigation Board (the “FCIB”), and the Turkish Criminal Code (the “TCC”)

Due to the inherent capability of crypto mixers to obscure fund movements, international standard-setters as well as national regulatory and criminal frameworks classify these services as high-risk. In this context, FATF guidance, FCIB regulations, and the provisions of the TCC address the AML/CFT risks and the concealment of criminal proceeds arising from mixer usage from distinct regulatory perspectives.



3.1. Legal Analysis Under the FATF Guidance

According to the FATF guidance, crypto mixers are anonymizing tools that deliberately complicate transaction flows on the blockchain by inserting multiple artificial transactions, thereby making it difficult to trace the origin of transfers. For this reason, mixers are classified among structures that carry a high level of money laundering and terrorist-financing risk. Likewise, the 2019 Risk Base Approach (RBA) Guidance underscores that crypto assets with embedded mixers or tumblers, together with anonymity-enhancing cryptocurrencies, constitute higher-risk activities for crypto-asset service providers (the “CASPs”), given that such products and services reduce transactional transparency and may effectively render customer due-diligence and transaction-monitoring obligations inoperative. In this context, the guidance emphasizes that countries and CASPs should explicitly identify mixer use in their national risk assessments and manage such risks through enhanced customer due diligence, record-keeping, suspicious-transaction reporting, and sanctions-screening measures.

3.2. Legal Analysis Under the FCIB Regulations

Under the FCIB regulations and the compliance guide for CASPs; crypto mixers, being anonymity-enhancing structures designed to obscure the parties to a crypto-asset transfer and the origin of funds, should be evaluated as high-risk activities comparable to transfers conducted through unregistered wallet addresses or through foreign platforms that are not required to share sender/recipient information. Facilitating such structures may trigger, for CASPs, enhanced customer-due-diligence obligations, suspicious-transaction reporting duties, and, where necessary, the initiation of transaction-postponement or asset-freezing processes under Article 19/A, pursuant to Law No. 5549 and its secondary legislation. Additionally, failure to comply may result in administrative sanctions and heightened supervisory risk. For this reason, platforms should adopt a risk-based approach toward mixer-originated or mixer-bound transfers and carefully determine whether to accept, delay, limit, or reject such transactions.



3.3. Legal Analysis Under the TCC

When Article 244 of the TCC, which regulates offenses against information systems, is considered together with Article 283, which criminalizes the laundering of assets derived from an offense, it becomes evident that mixers, by dispersing criminally obtained crypto assets through numerous transactions in a random manner and transferring them to new wallets, create an anonymization mechanism aimed at severing the link between the illicit proceeds and the perpetrator. In this respect, mixers technically facilitate acts of laundering that involve concealing assets derived from an offense, obscuring their origin, or creating the appearance that such assets originate from a legitimate source. Accordingly, given their inherent capability to eliminate the traceability of criminal proceeds, crypto mixers may be viewed both as a method that enables the commission of the laundering offense under the Article 283 of TCC, and as a “concealment tool” that hinders the detection and evidentiary establishment of the underlying crime.



4. International Sanctions: U.S. and OFAC Practices

For crypto asset service providers seeking to operate in the United States, the U.S. Department of Justice’s explicit stance that activities intended to conceal crypto-currency transactions may constitute criminal conduct is of critical importance. Indeed, on October 6, 2021, the Department announced the establishment of the National Cryptocurrency Enforcement Team (NCET) to investigate and prosecute the criminal use of mixers and tumblers. The Financial Crimes Enforcement Network (the “FinCEN”) classifies individuals and entities offering custodial mixing services as money transmitters under the Bank Secrecy Act (BSA), thereby requiring registration with the FinCEN, the implementation of an effective AML/KYC program, and compliance with applicable reporting and record-keeping obligations. In addition, sanctions imposed by the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) are particularly noteworthy.

