Cryptocurrency Mixers (also known as Tumblers)

As the use of cryptocurrencies grows, criminals are increasingly using cryptocurrency mixers, also known as tumblers, to commingle illicit funds with monies from other sources which makes any investigation and potential seizure more difficult for law enforcement.

Background

Cryptocurrency is a type of digital asset based on decentralized distributed ledger technology which relies on cryptography to produce transactions and record them on a public ledger known as a blockchain. Law enforcement often leverages public blockchains, depending on the type of cryptocurrency, to trace criminal transactions from one wallet to another with the goal of identifying the owner(s) when they "cashout"[1] or perform some type of other payment that provides investigative clues. The decentralized nature of cryptocurrency, the use of exchanges in foreign countries, and the employment of peer-to-peer transfers makes it difficult for law enforcement to trace crypto transactions. Depending on the type of cryptocurrency, the movement of funds is only pseudonymous. Consequently, criminals frequently use cryptocurrency mixers to make analyzing the flow of digital assets much more complicated.

What is Cryptocurrency Mixing?

Cryptocurrency mixers are services that help conceal cryptocurrency transactions, making it difficult for law enforcement to trace specific transactions involving certain individuals. Although cryptocurrency transactions are recorded on the blockchain, they are done so using pseudonyms. Depending on the cryptocurrency, this means that certain transaction details like the distributing and receiving wallet addresses and transaction amounts are publicly viewable; however, the identity behind each transaction is not. Users who wish to keep their financial activities even more confidential may look to cryptocurrency mixers to disguise the origin and destination of the funds they transferred. Mixers allow users to commingle funds from various sources which can facilitate illicit activities such as digital money laundering, transnational cybercrime, or terrorist financing.

Centralized vs. Decentralized Mixers

Centralized mixers typically offer their services to interested users using their own websites. These mixers will receive cryptocurrency from one user, and they will return the same amount of cryptocurrency, minus a fee, received from another user of the mixer which helps obscure the financial trail. Using a centralized mixer exposes customers to a higher level of risk since the operator(s) of the mixer could abscond with funds at any time and retain transaction logs that law enforcement could leverage to trace funds back to specific suspects. Additionally, depending on the amount that a given user intends to mix, a centralized mixer may not have a sufficient userbase or adequate cryptocurrency reserves to effectively mix a given transaction. Centralized mixing services may also retain certain sensitive information such as the IP address of their clients.

Decentralized mixing services minimize some of the security and privacy concerns of centralized mixers which benefits criminals who want to further distance themselves from potential law enforcement detection. Decentralized mixers typically facilitate transactions using a peer-to-peer or coordinated method involving customer transactions that are combined and then reallocated individually to each sender. Bitcoin enables this process using the "CoinJoin" protocol which is performed with specific wallet software providers and removes any requirement for users to visit decentralized mixing services websites. Historically, Wasabi and Samourai are two of the most well-known wallet service providers that offered CoinJoin features to users.

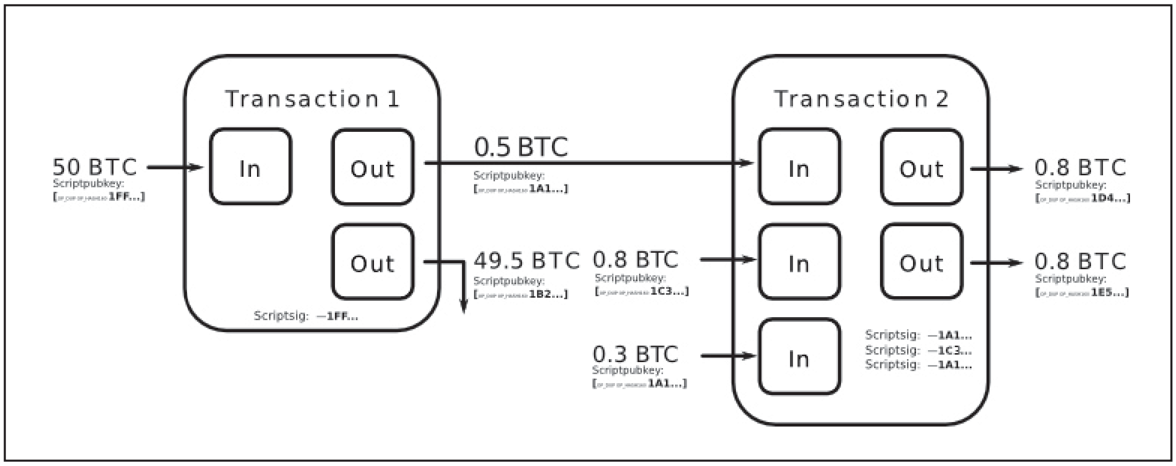
1 A "cashout" or "cashing out" typically refers to the process of converting cryptocurrency into a fiat currency through an exchange or third party money laundering service.

May 2025

Mixers and Criminal Enforcement Actions

It is a crime to operate a mixer with the knowledge that it is processing illicit funds. In April 2024 , the U.S. Department of Justice (DOJ) charged two co-founders of Samourai and seized the service's infrastructure for allegedly facilitating over $2 billion in illegal transactions and for laundering more than $100 million in criminal proceeds.[2] Similarly, on January 7, 2025, the DOJ announced charges against three individuals for their alleged roles in running two popular cryptocurrency mixing services called "Blender.io" and "Sinbad.io."[3]

Furthermore, Wasabi's parent company, zkSnacks, stopped offering CoinJoin services shortly after Samourai was shut down, citing the risk of legal consequences for handling illicit transactions. Other services have emerged to offer CoinJoin features through the Wasabi protocol, with "Kruw.io" becoming the most prolific one. Numerous illicit actors use Kruw.io to launder funds including the Lazarus Group, a North Korean hacking collective also known as APT38 and TraderTraitor which is subject to U.S. and international sanctions. The Lazarus Group has previously used Kruw.io to mix approximately $14.3 million in cryptocurrency stolen by the North Korean regime.[4] The Lazarus Group is currently laundering some proceeds of the $1.5 billion Bybit hack through the Kruw.io service.



2 https://www.justice.gov/usao-sdny/pr/founders-and-ceo-cryptocurrency-mixing-service-arrested-and-charged-money-laundering
3 https://www.justice.gov/archives/opa/pr/operators-cryptocurrency-mixers-charged-money-laundering
4 https://www.fbi.gov/news/press-releases/fbi-identifies-cryptocurrency-funds-stolen-by-dprk

Contact Your Local United States Secret Service Cyber Fraud Task Force
To Report Suspected Cyber or Financial Crimes Involving Cryptocurrency Mixing.