CHINA AND NORTH KOREA

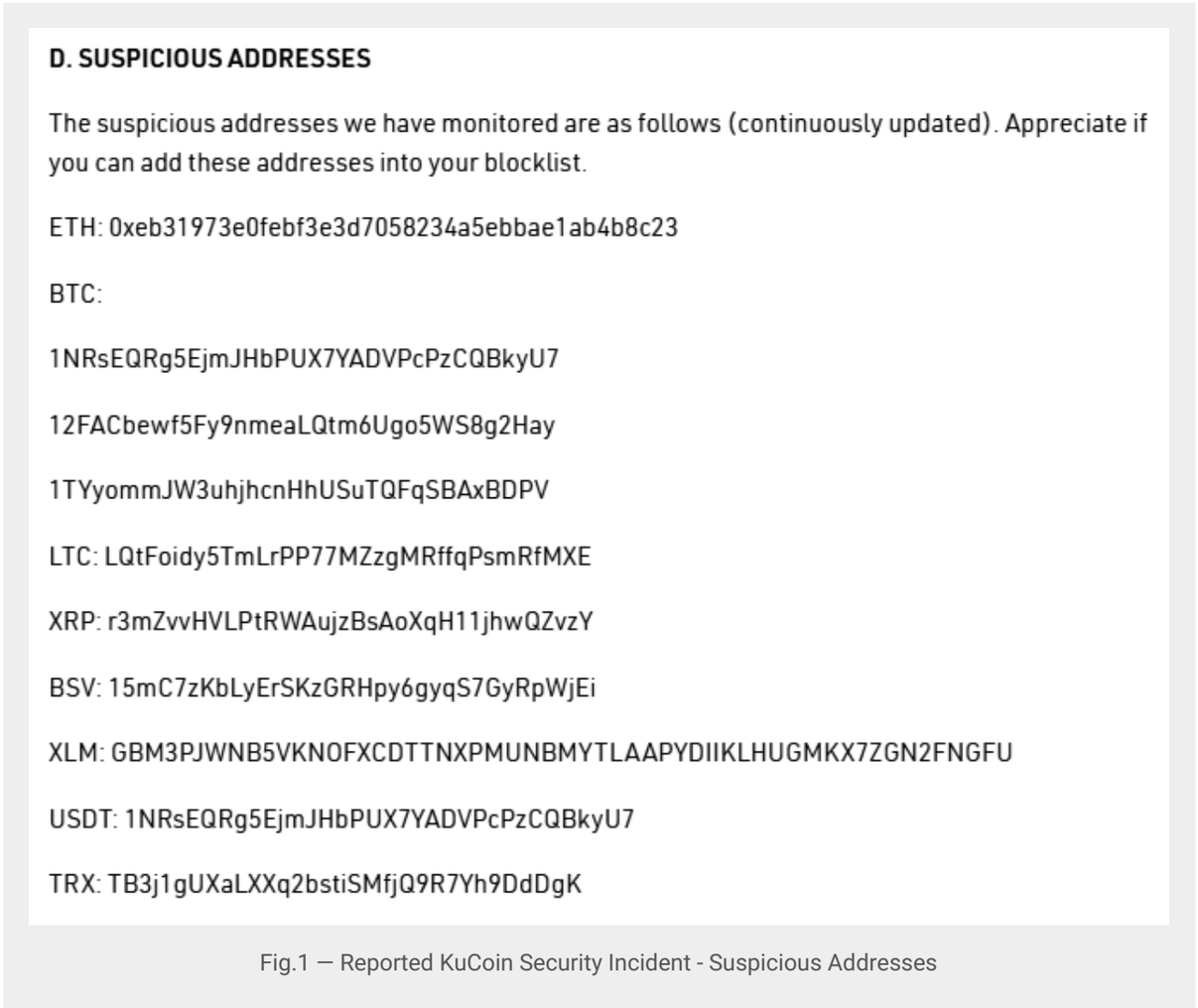
THE KUCOIN HACK

OXT RESEARCH

Introduction

On September 26th 2020, KuCoin, a Hong Kong based cryptocurrency exchange suspended withdraws as part of an on-going "security incident". Shortly after the event, KuCoin revealed their security had been compromised and funds from several crypto hot wallets had been withdrawn to a list of suspicious addresses. The stolen crypto was valued at approximately $280 million at the time of the hack.

1008 BTC, valued at approximately $11 million, was among the reported stolen crypto. These coins remained unspent until late October.



D. SUSPICIOUS ADDRESSES

The suspicious addresses we have monitored are as follows (continuously updated). Appreciate if you can add these addresses into your blocklist.

ETH: 0xeb31973e0febf3e3d7058234a5ebbae1ab4b8c23

BTC:

1NRsEQRg5EjmJHbPUX7YADVPcPzCQBkyU7

12FACbewf5Fy9nmeaLQtm6Ugo5WS8g2Hay

1TYyommJW3uhjhcnHhUSuTQFqSBAxBDPV

LTC: LQtFoidy5TmLrPP77MZzgMRffqPsmRfMXE

XRP: r3mZvvHVLPtRWAujzBsAoXqH11jhwQZvzY

BSV: 15mC7zKbLyErSKzGRHpy6gyqS7GyRpWjEi

XLM: GBM3PJWNB5VKNOFXCDTTNXPMUNBMYTLAAPYDIIKLHUGMKX7ZGN2FNGFU

USDT: 1NRsEQRg5EjmJHbPUX7YADVPcPzCQBkyU7

TRX: TB3j1gUXaLXXq2bstiSMfjQ9R7Yh9DdDgK

Fig.1 — Reported KuCoin Security Incident - Suspicious Addresses

Shortly after the incident, most of the stolen altcoins began spending from the noted addresses. On November 11th, almost 2 months after the incident, a tweet thread from the KuCoin CEO stated that 84% of the stolen cryptocurrency ($235M of $280M) had been recovered.

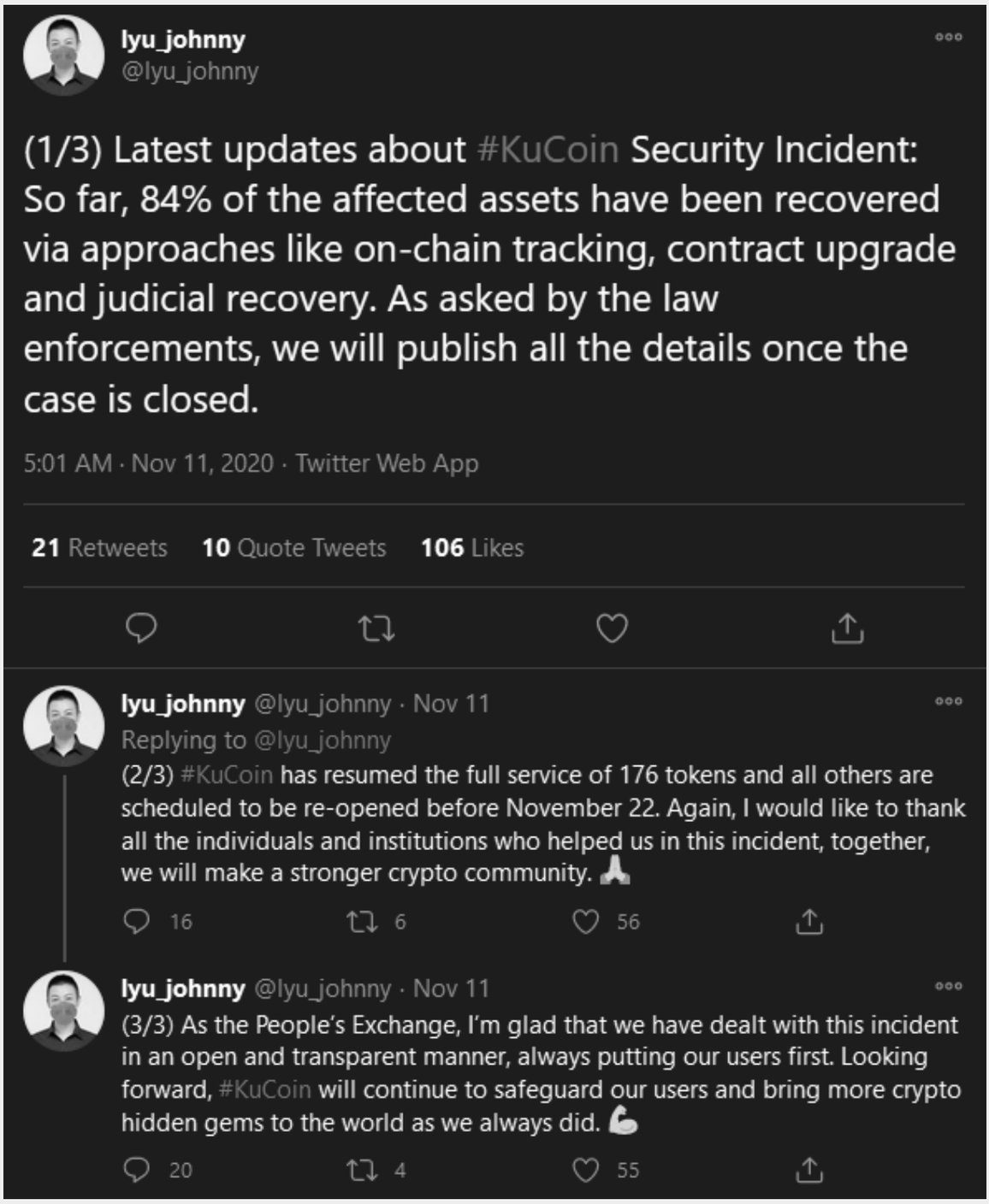


Fig.2 — Recovery Notice Issued by KuCoin's CEO

Specifics on which assets have been recovered are relatively vague. According to a news report by CoinJournal.net, the stolen altcoins seem to make up the bulk of the recovered assets.

> **Based on the reported recovered volumes, the timing of the recovery news, and our observations of the movement of the stolen BTC, we do not believe that the BTC was among the recovered assets.**

Executive Summary

The immediate spending patterns of the stolen BTC have been well documented. Due to the usage of several mixers, the flows and destination of the stolen BTC remains largely undiscussed by the community. In this report, we aim to provide some clarity on the situation by discussing the following:

- Details of the immediate flows of the 1008 stolen BTC.
- Identification of several mixing services used to obfuscate the flows of the stolen BTC.
- Testing and refining a volume and timing analysis for evaluating likely postmix UTXOs attributable to the stolen coins.
- A discussion of the postmix spending patterns of our likely UTXO list.
- Mixing services as only a small part of an elaborate obfuscation scheme.
- Possible attribution of the entities involved in the massive scheme.

The Flow of Stolen BTC

Timeline Overview

A high-level timeline of the flows of the 1008 stolen BTC is provided below:

- **25 September 2020**
  The stolen coins are spent to address [1NRsEQ...] over a series of 9 transactions as a part of the security breach.

- **27 September 2020**
  The 1008 BTC is split into two UTXOs, one for 201 BTC and another for 807 BTC, via TxID (48898).

- **26 - 28 October 2020**
  Approximately 474 BTC are spent to a single address [17vuW7] over a series of transactions. Outputs from this address are later consumed in ChipMixer transactions.

- **30 October - 2 November 2020**
  The remaining roughly 534 BTC are distributed to an "intermediary" wallet receiving to nested P2WPKH addresses.

- **31 October - 3 November 2020**
  The intermediary wallet begins spending to bech32 address formats. All UTXOs are "partially mixed" through Wasabi Wallet CoinJoins.

- **3 November 2020**
  "Unmixed" change outputs and de-anonymized mix outputs begin flowing from Wasabi to apparent "large consolidation transactions" receiving large volumes from nested P2WPKH addresses. For now, we will refer to this as the "Post-Wasabi wallet."

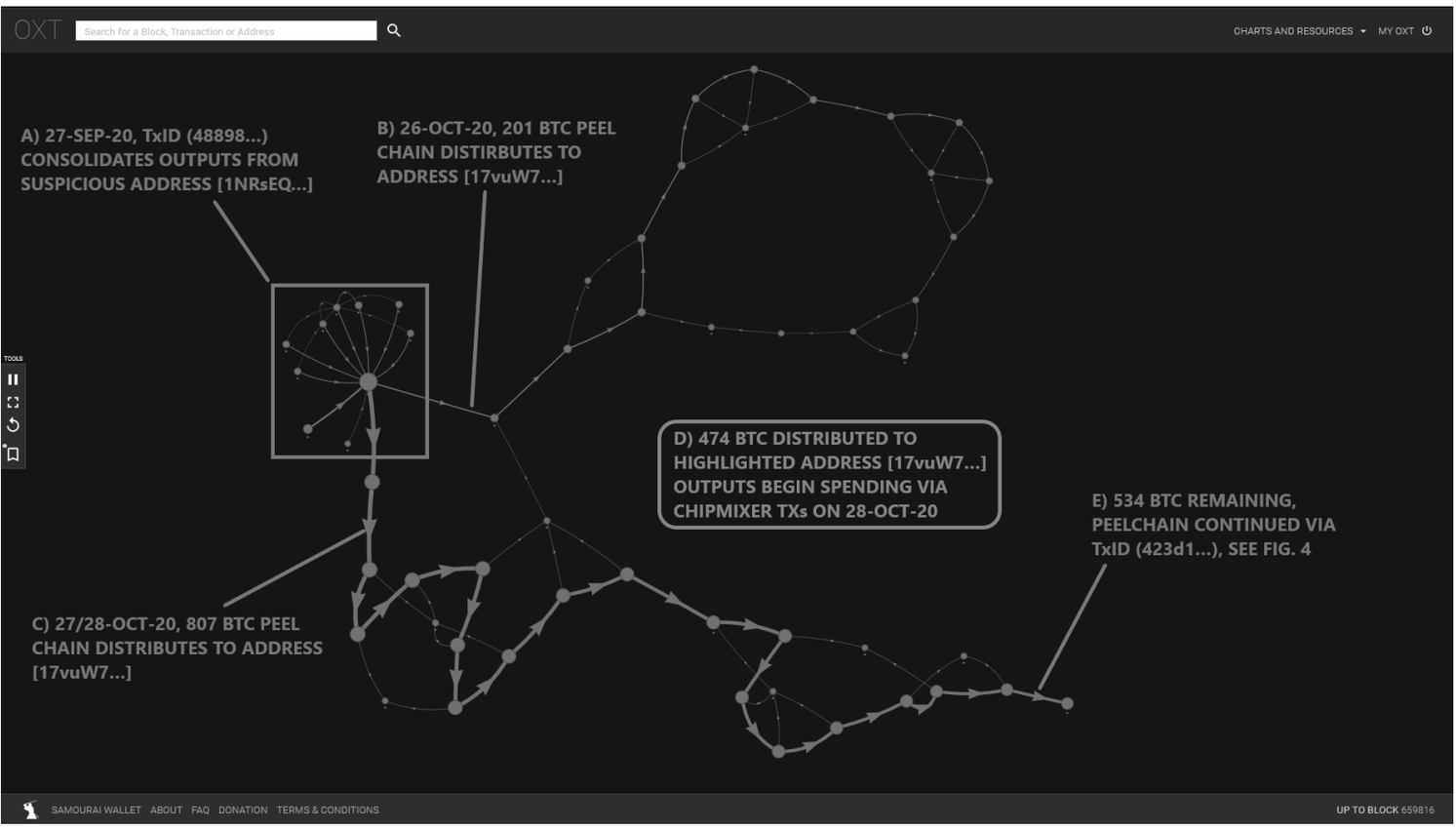


Fig.3 — 474 BTC of Stolen Funds Distributed to ChipMixer - Tx Graph

An example of these flows is illustrated below in Fig. 4. A detailed timeline of these flows including premix distributions to each mixer and tracking of the major Wasabi CoinJoin change outputs can be found in the resource spreadsheet (Tabs 1 and 2).

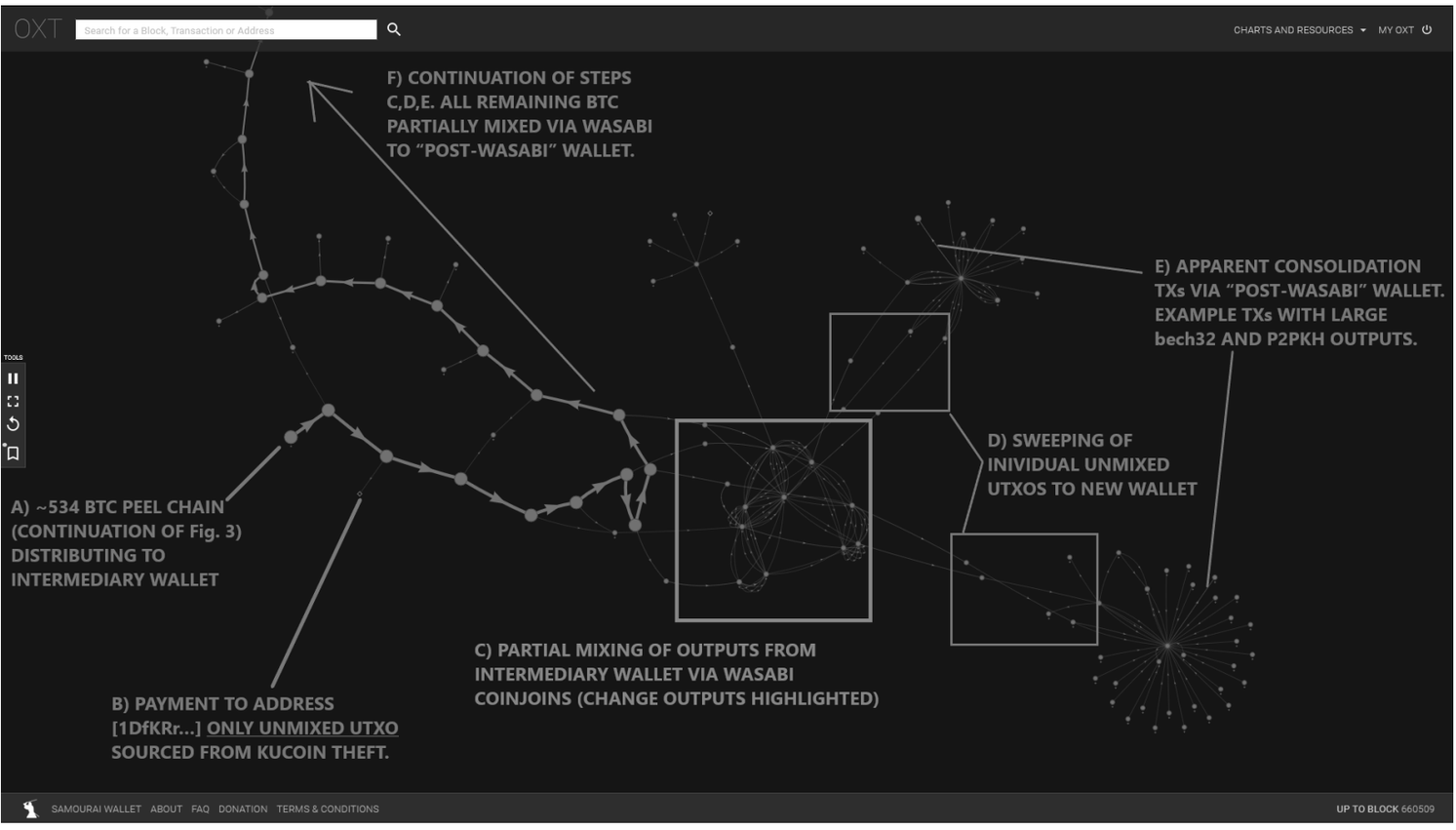


Fig.4 — 534 BTC Peel Chain To Intermediary Wallet, Partial Wasabi Mixing, Large Consolidation Transactions - Tx Graph

Key Takeaways

- The flows from the suspect addresses into the mixing services are deterministic, or mathematically certain.
- We know that 474 BTC were mixed via ChipMixer.
- We know that the remaining 534 BTC were mixed via a different, more complex process. This process needs further investigation, but we begin to explore the possibility that we are observing a second custodial tumbler.

The flows out of the mixing process are not deterministic and offer unique challenges to analysts. In the remainder of this report we develop a series of hypotheses for testing and identification of possible postmix UTXOs attributable to the original KuCoin theft.

We attempt to invalidate each hypothesis in a fashion typical of the scientific method. If the observed data does not invalidate our hypotheses, we continue refining our approach in an effort to develop a "most likely" postmix UTXO list.

Background Knowledge

Wallet Fingerprinting for Refining Flow of Fund Analysis

Bitcoin wallets generate transactions with additional metadata that can be used to "fingerprint" the software (or "wallet") used to create a transaction.

We used wallet fingerprinting to identify the unique wallets used in the flows of the stolen KuCoin BTC displayed in Figures 3 and 4.

Common transaction fingerprint metatdata includes the following:

- Address type used for inputs and outputs.
- Batch spending (indications of service activity) vs. simple spending (indications of single user activity).
- Change output indexes (VOUT 0 vs. VOUT 1) for simple spends.
- Transaction Version Number and Locktime.

Analysts tracking the flow of bitcoins can use transaction fingerprinting to note coins entering a new service or being spent by new wallet software.

In our analysis of the flows of the stolen KuCoin BTC, we noted several unique fingerprints used to construct the transactions involved.

A summary of each wallet, and their unique fingerprints are shown below in Table 1.

Table 1 — Example Wallet Fingerprinting

Wallet	Input Address Type	Output Address Type	Denomination Fingerprint	Version No.	Locktime
Stolen Fund Wallet	P2PKH (1...)	P2PKH (1...)	None	2	Blockheight
ChipMixer	P2PKH (1...)	P2PKH (1...)	"Chips" (0.001, 0.002,... 8.192 BTC)	2	Blockheight
Intermediary Wallet	Nested P2WPKH (3...)	No change, possible self-spend	None	2	0
Wasabi Wallet	bech32 (bc1q...)	bech32 (bc1q...)	Identical outputs (Coinjoin Footprint)	1	0
Post Wasabi Wallet	Nested P2WPKH (3...)	Nested P2WPKH (3...)	None	2	0

Key Takeaways

- **Stolen Fund Wallet Fingerprint** (critical in later part of analysis)
  - P2PKH address types for inputs and "change" outputs
  - Transactions created with a Version No. 2
  - Locktime = current block height
- **ChipMixer**
  - A unique footprint that can be found relatively easily by scanning the blockchain for similar transactions
- **Intermediary Wallet & Post-Wasabi Wallet**
  - The fingerprint of the Intermediary and Post-Wasabi wallet are identical

Custodial Tumblers

Custodial tumblers were among the first privacy techniques employed by BTC users attempting to obfuscate their bitcoin transactions. Recently the term for tumblers, mixers, and coinjoins has become interchangeable. We tend to use "mixer" as a general term to describe both obfuscation techniques. Despite this confusing of terms, there are major differences between custodial tumblers and coinjoins.

The purpose of custodial tumblers is to act as a swap service. Users deposit coins to the tumbler and (hopefully) receive different UTXOs with a new transaction history in return. This swapping process results in a "broken" transaction graph that severs the link between a user's deposits and withdrawals. To prevent users from receiving their original deposits, custodial tumblers keep BTC "reserves" to supply liquidity during times of high demand.

Frequently, users interacting with custodial tumblers are attempting to hide the movement of coins sourced from illicit activities. The swapping nature of custodial tumblers and proximity to inflows from illicit activities means a user may receive "tainted" coins in return for their deposit. "Taint" risk is an inherent risk present in the process of swapping coins with unique attributable histories. In contrast, a true Zerolink CoinJoin provides sufficient plausible deniability against evaluating a UTXOs unique history and therefore its "taint".

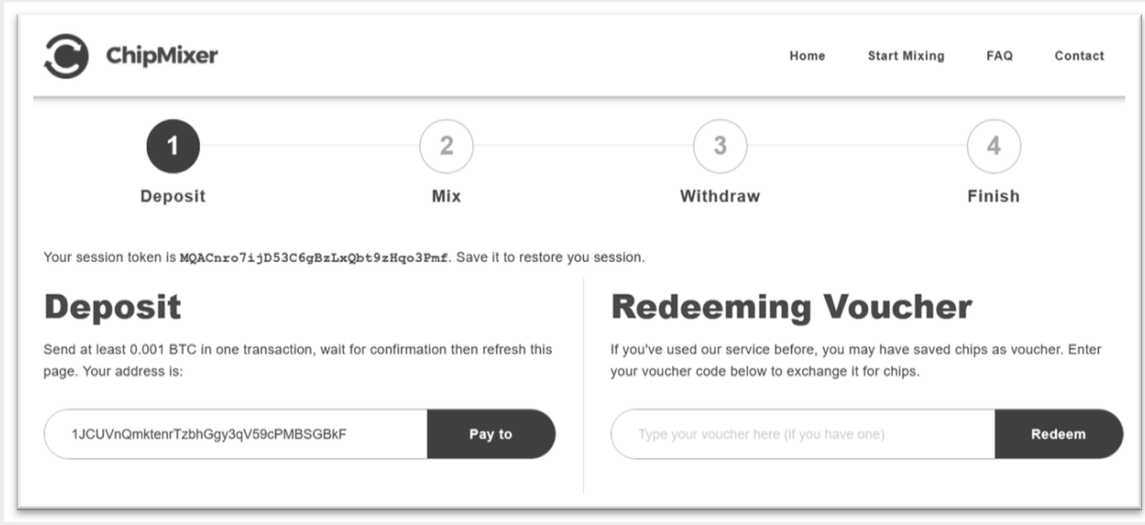


Fig.5 - ChipMixer Workflow Requesting "Deposit" Into the Custodial Tumbler

The "Ideal" Custodial Tumbler

- **Opaque**
  Operates a "shared" wallet, with an internal database.
- **No Links**
  Users deposit funds into the shared wallet and receives "new coins" that are not linked to their original deposit.
- **No Cluster**
  No wallet cluster detected by traditional clustering algorithms.
- **No Footprint**
  Minimal footprint with irregular input and output denominations.
- **No Exit Scam**
  Does not exit scam with user deposited funds.

Attempts to track the swapping of funds across tumblers is heavily reliant on volume and timing analysis.

End of Preview

Going forward updates will be provided through the OXT Research center at research.oxt.me. Given the complexity of this targeted analysis, we are available for consulting to help research teams better understand and evaluate the effects of events like this. Be on the lookout for new features from the OXT Team in the coming months.

OXT research