TOXIC RECALL ATTACK

UNWINDING JOINMARKET CASE STUDY

OXT RESEARCH

Introduction

Executive Summary

This report aims to help solve a cold case that was never solved. The year is 2015, Bitcoin is still young but gaining in popularity. Reddit is the venue, the /r/bitcoin subreddit is where the alleged victim makes a plea for help

> "On the 9th of February 2015, somebody gained access to an online computer of ours with a BTC wallet holding 445 BTC... transferred those BTC to 5 different wallets... Those BTC were left sitting for roughly 1.5 years, until a few weeks ago when the thieves found out how nice bitcoin mixers are, and started to mix them, leaving nearly no traces..."

The reddit post by u/gridchain concludes with a plea for aid in tracking the allegedly stolen funds. As far as we can tell, no help was provided.

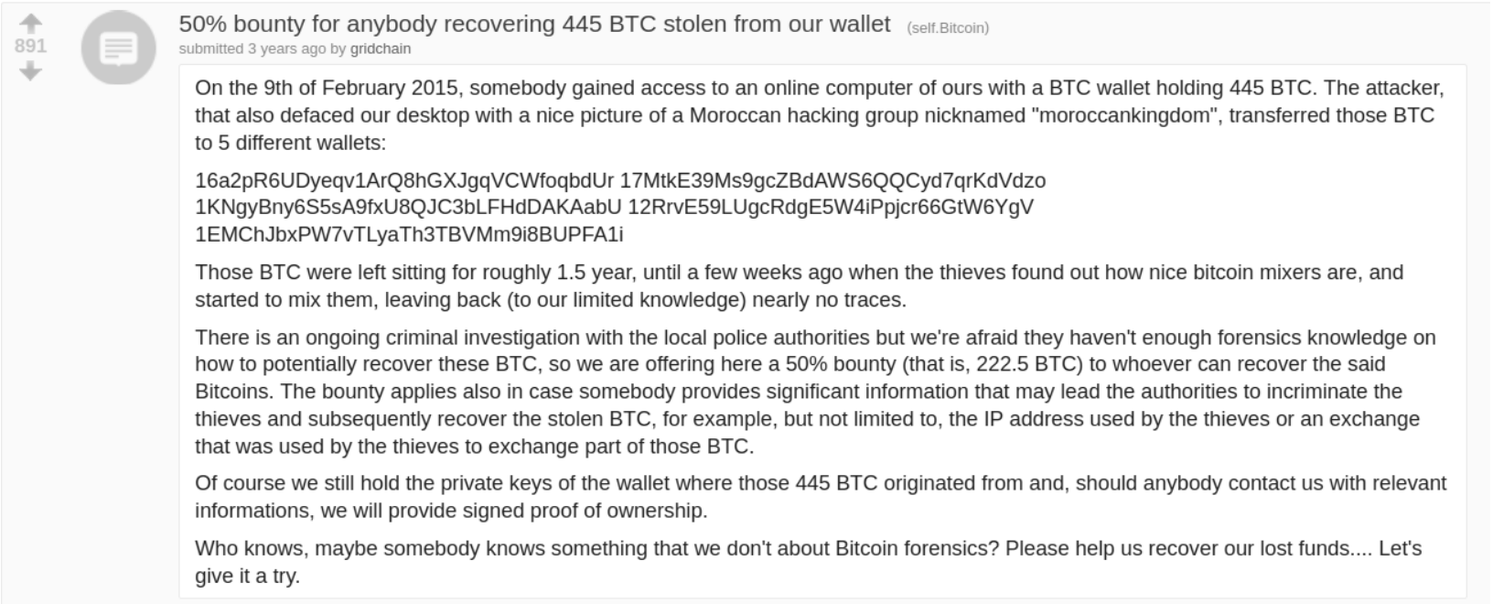

Fig.1 — Screenshot of the Reddit post by /u/gridchain

Scope

In this report we will cover the following:

- The timeline of events that occured during the incident
- An introduction to bitcoin privacy and CoinJoin theory
- An introduction to the Toxic Recall Attack on flawed CoinJoin protocols
- Assessment of likely destinations of the alleged stolen coins

We cannot attest to the validity of the claims of theft in the original post by u/gridchain. However, we have attempted to contact the user with the conclusions of this report to aid in the recovery of the allegedly stolen funds. At the time of publication, we have not received any return communication from the user.

If anyone can aid us in contacting the user, please reach out to us at investigations@oxtresearch.com.

A Timeline of Events

Based on the information provided in the reddit post and some additional background acquired from the blockchain, a rough timeline of the events is provided below.

- **15 January 2015 to 8 February 2015**
  - u/gridchain's web wallet receives approximately 445 BTC in payouts from mining pools and coinbase (miner block reward) transactions to the following cluster: ANON-494272502.
- **9 February 2015**
  - The user's web wallet is allegedly compromised. Funds are removed from the web wallet in a series of 5 transactions to the noted address provided in the reddit post.

Table 1 — Alleged Withdrawal Destination of Stolen Funds

Date Received	Destination Address	Blockheight	Received BTC
09 Feb 2015	16a2pR6UDyeqv1ArQ8hGXJgqVCWfoqbdUr	342641	45.868
09 Feb 2015	17MtkE39Ms9gcZBdAWS6QQCyd7qrKdVdzo	342641	100
09 Feb 2015	1KNgyBny6S5sA9fxU8QJC3bLFHdDAKAabU	342641	100
09 Feb 2015	12RrvE59LUgcRdgE5W4iPpjcr66GtW6YgV	342640	100
09 Feb 2015	1EMChJbxPW7vTLyaTh3TBVMm9i8BUPFA1i	342640	100

- **7 April 2017**
  - After nearly two years of inactivity, the alleged stolen funds are moved for the first time.
  - 45.87 BTC from address [16a2pR...] are transferred via the following TxID (f1609...) and enter their first JoinMarket CoinJoin via TxID (49b5f...).
- **10 April 2017**
  - 400 BTC from the remaining addresses in Table 1 above are transferred via the following TxID (136d7...) and enter their first JoinMarket CoinJoin via TxID (926aa...).
- **2 May 2017**
  - The coins continue mixing and the last of the "unmixed change" associated with both initial mixer deposits is merged into the same CoinJoin transaction via TxID (a85b3...).
- **5 May 2017**
  - u/gridchain posts about the events above on reddit.

Bitcoin Privacy & Mixers

Overview

We have spent a considerable amount of time tracking the movement of coins across both custodial tumblers and non-custodial CoinJoin protocols alike. However, we have yet to cover the basics of bitcoin privacy and why CoinJoins are vital to providing users with a basic level of privacy.

Pseudonymous Bitcoin

Bitcoin transactions spend bitcoins to and from pseudonymous addresses. Rather than a bank account or name tied directly to an identity. Bitcoin addresses offer a powerful, but fragile level of pseudonymous privacy.

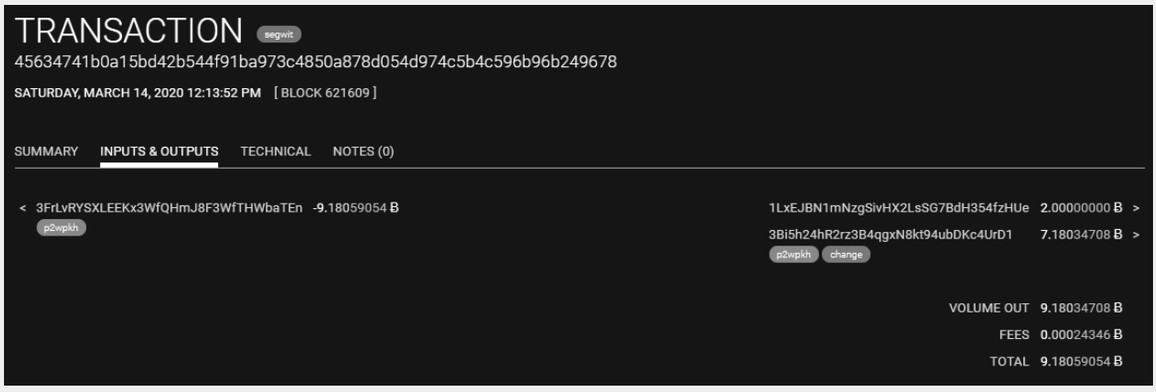

Fig.2 — A Typical Bitcoin Transaction

The Transparent Ledger

In contrast to the traditional finance system, bitcoin's public ledger can be observed by any third party running a full node or with access to a web-based block explorer.

This allows any observer to construct a transaction graph showing the relationship between transaction inputs and outputs over a series of transactions.

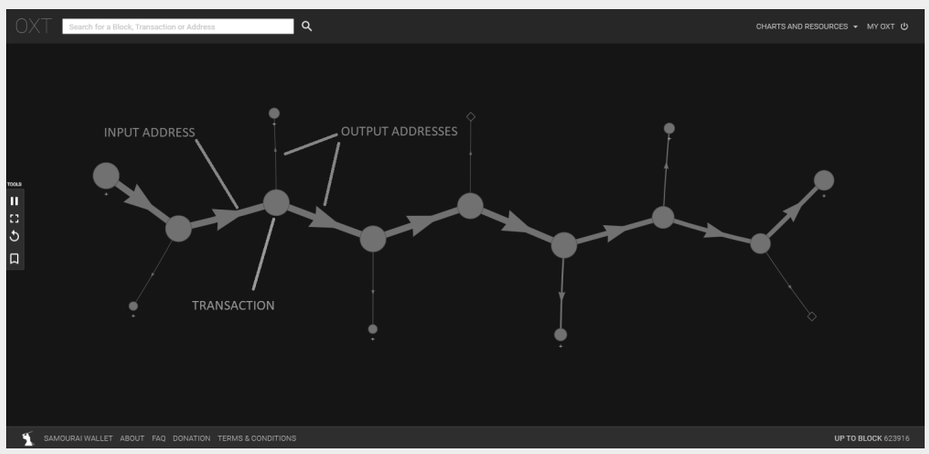

Fig.3 — A Typical Bitcoin Transaction Graph

Heuristics That Damage Bitcoin Transaction Privacy

Additional metadata and heuristics, such as output amounts and wallet fingerprinting, can be leveraged to infer additional information about a bitcoin transaction. Common heuristics include wallet fingerprinting and the round payment heuristic.

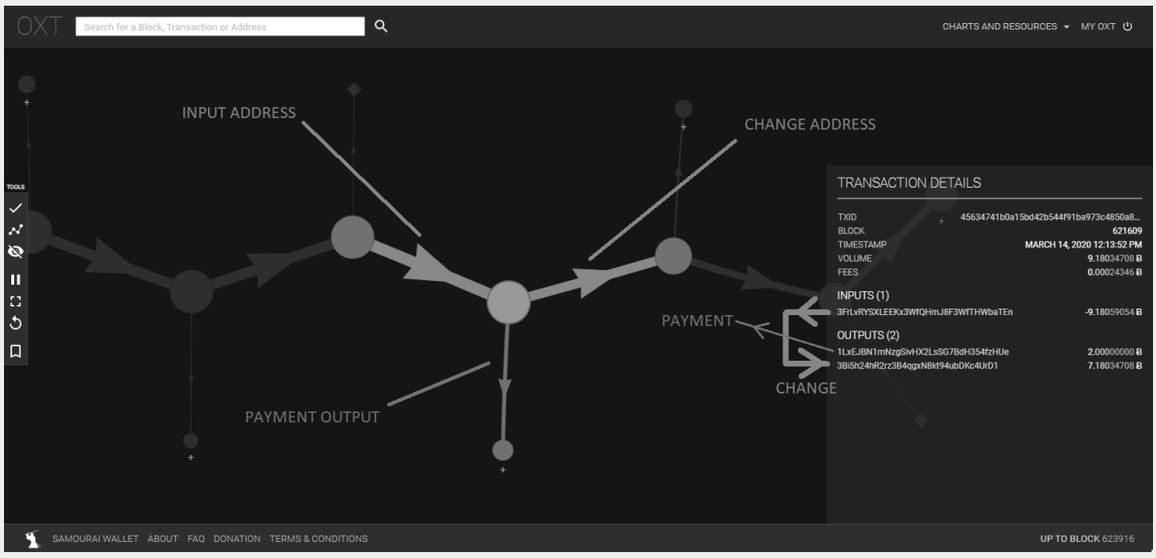

Fig.4 — Wallet Fingerprinting and Round Payment Amount Heuristics

Regardless of the heuristics applied to evaluate bitcoin transactions, a mathematical relationship exists between the inputs and outputs of most bitcoin transactions. These relationships are called deterministic links which indicate a mathematical certainty that a transaction input was used to pay an output.

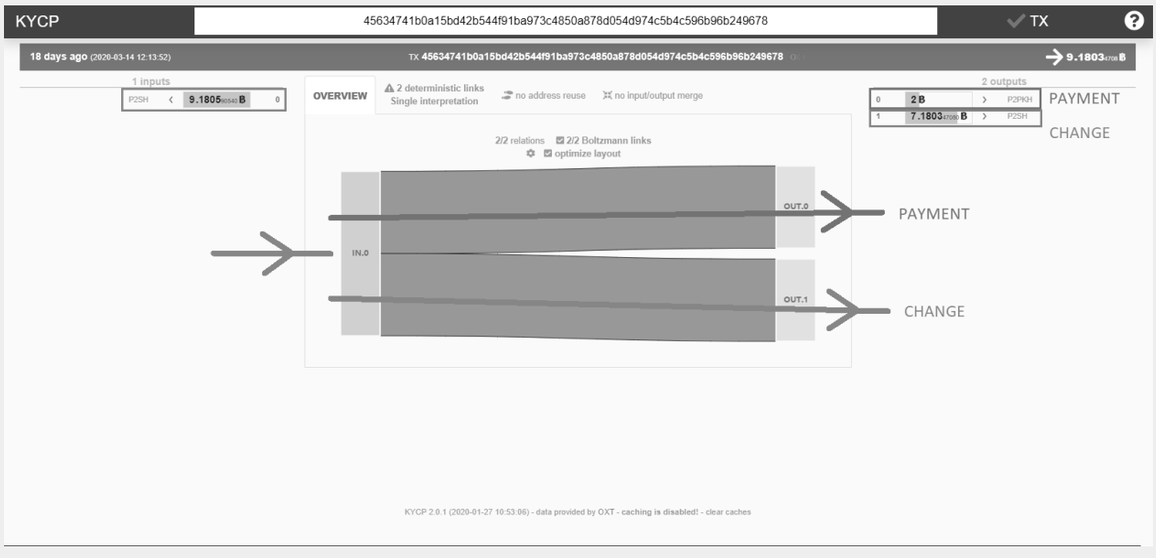

Fig.5 — Deterministic Links Between Inputs and Outputs

CoinJoin and Deterministic Links

In a properly constructed CoinJoin transaction, deterministic links between inputs and outputs are broken, instead creating probabilistic links between inputs and identical outputs.

The presence of deterministic links between inputs and outputs are evaluated based on the CoinJoin sudoku algorithm which has been integrated into the transaction privacy algorithm called Boltzmann.

Boltzmann evaluates CoinJoin transactions for deterministic and probabilistic links between inputs and outputs.

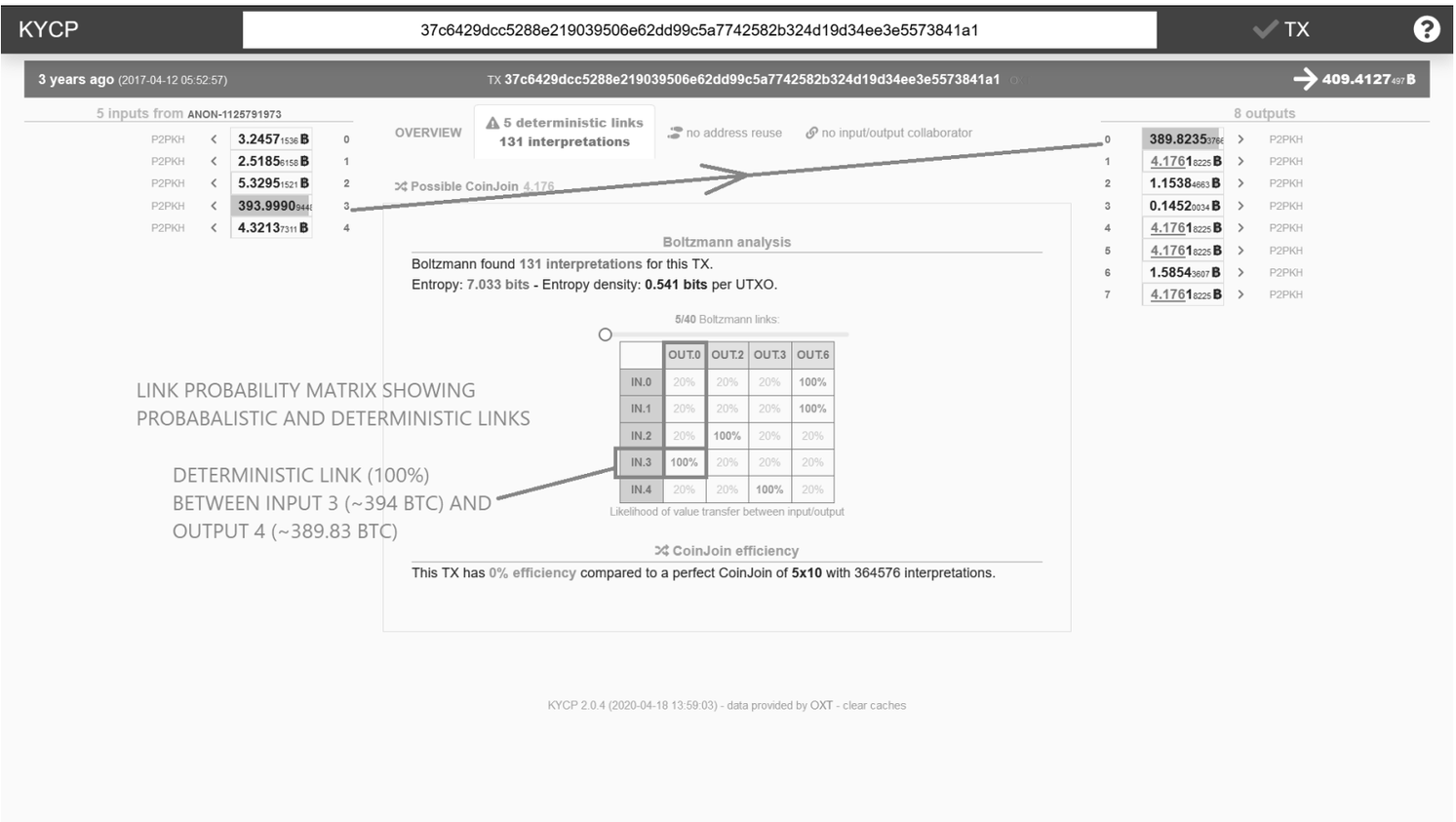

Fig.6 — A CoinJoin Transaction with Deterministic Links for "Unmixed Change" TxID (37c64...)

The JoinMarket CoinJoin shown in Fig. 6 above breaks the deterministic links between transaction inputs and outputs for the identical outputs.

Identical outputs are often described with a simple privacy metric called anonymity set. In this case there are four 4.1761 BTC outputs, so these outputs are assigned an initial anonymity set of four.

Deterministic Links Within a Coinjoin Transaction

The non-identical outputs shown in the example transaction above are deterministically linked (100%) to the transaction inputs. These outputs are sometimes referred to as "unmixed change" and create a "peeling" style transaction graph.

These outputs are directly attributable to an initial mixer deposit and its associated toxic pre-mix history. The most obvious deterministic link in the transaction above is between input 3 (~394 BTC) and output 2 (389.82 BTC). In most cases, deterministic links become obvious when subtracting the mix output denomination from the targeted input.

As described in this report, a transaction graph based attack combines the presence of "unmixed change" and previously seen mix outputs to retroactively attack mixer deposits.

The CoinJoin Coordinator

Coordinator Responsibilities

The privacy afforded by a CoinJoin protocol is dictated by the coordinator algorithm.

If a coordinator does not enforce each item in the list below, it creates the possibility of attacking user privacy through no fault of the user.

No Deterministic Links
Address reuse, a common privacy worst practice should be rejected by the coordinator to preserve all user's privacy.

Sybil resistance fee should be taken prior to mixing. Fees taken directly in a mix transaction result in deterministic links ("unmixed change"). Taking fees outside of the mix allows for an "ideal" CoinJoin with no reliable discernable history and provides the opportunity for free remixing.

Identical Output Denominations and Pool Style Mixing
Non-identical outputs create unique fingerprints for each mix, which can be used as additional leverage in an attack. Users are often required to combine smaller outputs to meet a larger mix output denomination. Identical output denominations and a pool style mixer allow for higher anonymity sets than that obtained with a single mix.

Structural Liquidity Enforcement
New mixer liquidity should be required by the coordinator before triggering a mix. If new liquidity is not enforced, users will continuously remix with the same mix participants.

Limiting "Previously Seen" Mix Outputs
A mix transaction should limit the number of outputs from a previous mix to no more than one. This minimizes the risks of users remixing with the same entities and creates a dispersed transaction graph.

Coins On The Move

Introducing JoinMarket

Now that we have presented the basics of bitcoin transaction and CoinJoin privacy, we can circle back to the mixing of u/gridchain's allegedly stolen coins.

After nearly two years of inactivity, the coins were mixed through JoinMarket. JoinMarket was the first CoinJoin protocol offering a trustless, non-custodial mixing service.

As detailed above, the "unmixed change" outputs within a CoinJoin transaction are deterministically linked to the corresponding inputs. The presence of "unmixed change" creates a "peeling" pattern as mixed output amounts are subtracted from the deterministic links with each subsequent mix.

We have highlighted the unmixed change as it works its way through subsequent CoinJoins. Fully expanding the transaction graph of each CoinJoin reveals a very noisy transaction graph.

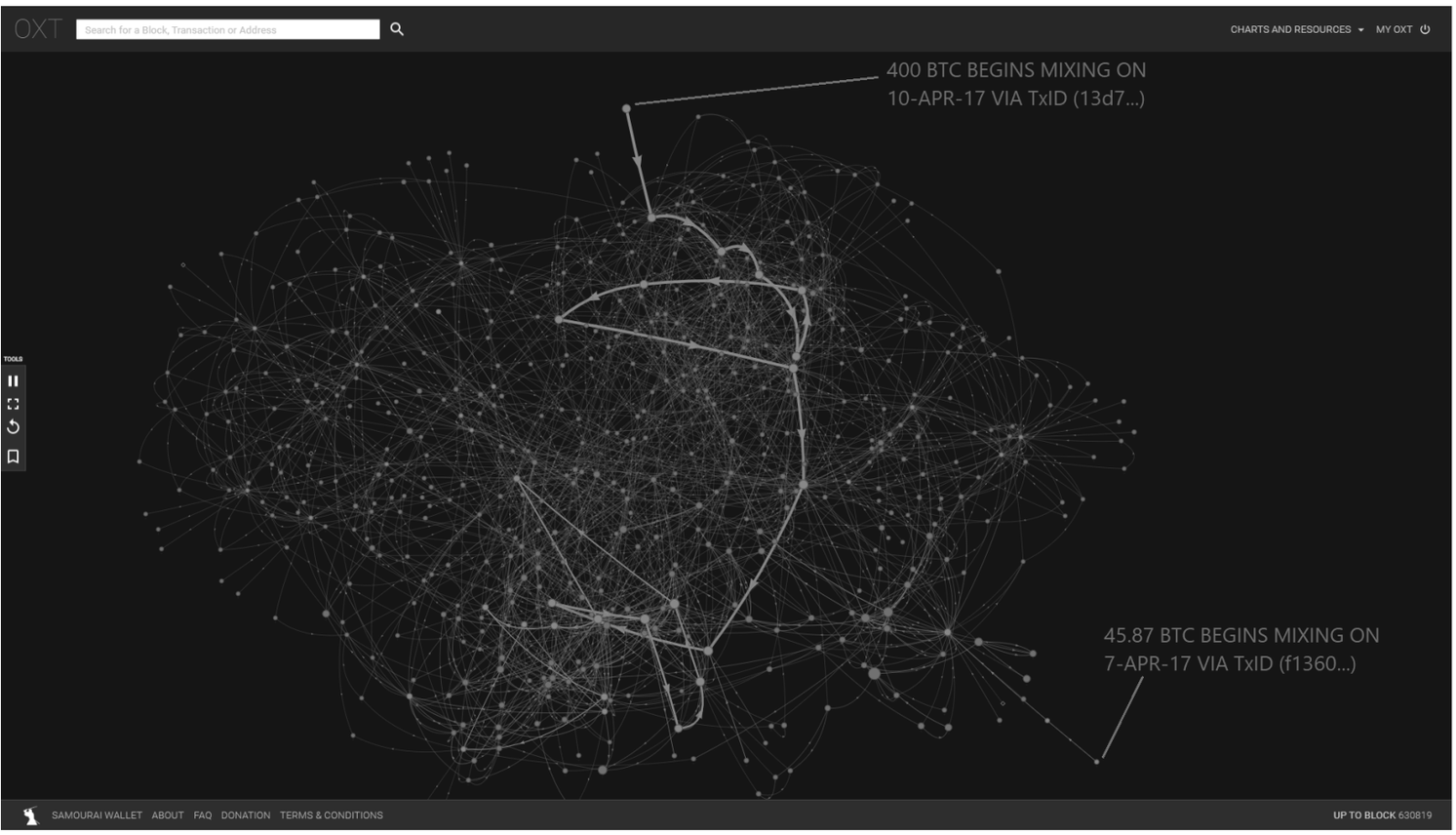

Fig.7 — Complete Transaction Graph Tracing the Path of "Unmixed Change" Through JoinMarket

The peeling pattern presents a unique metadata trail that indicates each initial mix that a user participates in. It's worth noting metadata indicating the first mixing round a user participates in is present in all CoinJoin implementations. However, the presence of "unmixed change" within a CoinJoin transaction creates a target for the attack described in this report.

This metadata becomes more apparent when we filter out the irrelevant transaction graph data. We do this by only expanding the "unmixed change" outputs (orange highlighted lines) from each mix that are attributable to the original mixer deposits (400 BTC and 45.87 BTC).

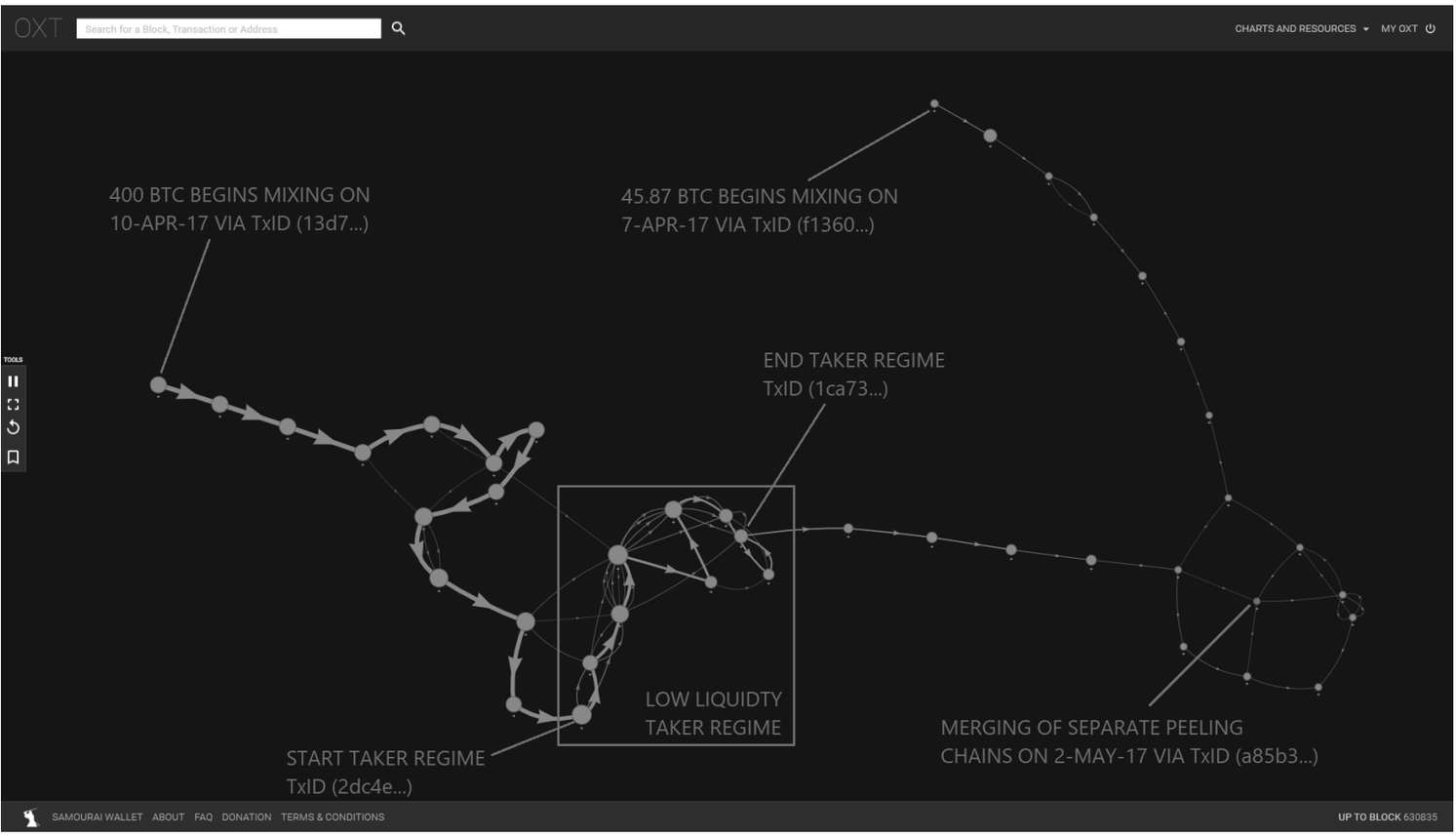

Fig.8 — Isolated Tx Graph Tracing the Path of "Unmixed Change" of Each Mixer Deposit (Tx Graph Bookmark)

Takeaways: Figure 8

- Hiding the unnecessary transaction graph data highlights the separate peeling chains.
- The transaction graph feature on oxt.me automatically reveals outputs (blue lines) that are used as inputs in following transactions.
- Three distinct mixing regimes become apparent in the 400 BTC peeling chain.

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