AUG 6, 2021 • 11 MIN READ • UNDERSTANDING BITCOIN PRIVACY

Understanding Bitcoin Privacy with OXT — Part 2

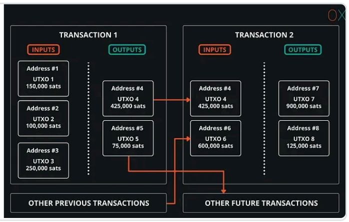
Introduction

Now that we have presented the basic concepts in Part 1, we can move on to the core concepts that underpin chain analysis by expanding our analyses to include “external” transaction data.

Understanding Bitcoin Privacy with OXT — Part 1

Introduction Awareness of Bitcoin’s value proposition for censorship resistant payments took off in 2011 with the launch of Silk Road and...

OXT ErgoBTC • OXT Research



Specifically, Part II will focus on two of the most important tools underpinning chain analysis:

1. The transaction graph
2. The common input ownership heuristic (aka wallet clustering)

External Transaction Data

External transaction data can be used to improve confidence in change detection (weaken transaction privacy) by leveraging additional information and patterns.

External transaction data includes any information not strictly limited to the information included in an individual transaction by the bitcoin protocol. Examples include:

- address reuse over multiple transactions
- co-spending from multiple addresses in the same transaction (wallet clustering)
- multi-sig scripts (which are only revealed after a UTXO is spent)
- wallet fingerprinting over a series of transactions

- off-chain data such as outputs spent to labelled clusters and IP addresses of nodes broadcasting a transaction
- volume, timing, and other transaction pattern recognition analysis

Transaction Graph Analysis

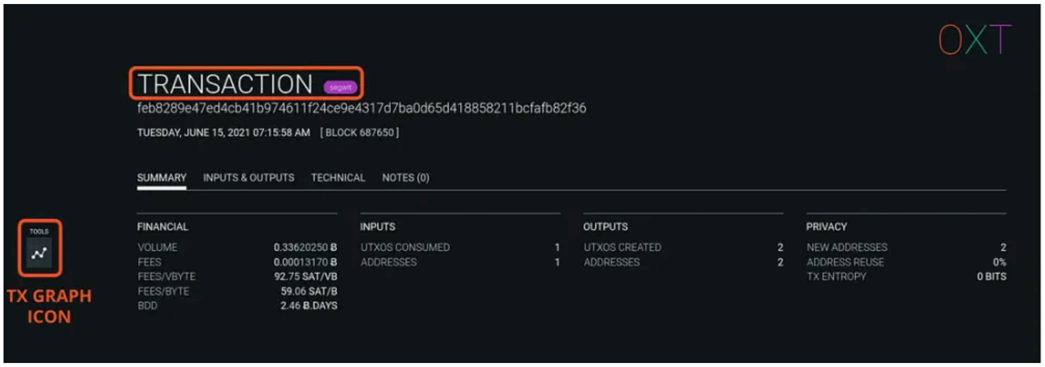
Transaction graphs are the simplest way to show the relationship of inputs and outputs across multiple transactions.

OXT's transaction graph is a Directed Acyclic Graph (DAG). DAG graphs are used to map the relationship between two different objects. In the case of bitcoin, the transaction graph maps the relationship between UTXOs and transactions.

OXT Transaction Graph Basics

The transaction graph is best understood through interaction, but before we get started we will introduce some of the functionality of the OXT transaction graph.

1. To access the transaction graph, navigate to the **TRANSACTION** tab on OXT by imputing or clicking a transaction ID (TxID) of interest.
2. Click the **TX GRAPH ICON** icon on the tool bar on the left side of the screen.



TRANSACTION

feb8289e47ed4cb41b974611f24ce9e4317d7ba0d65d418858211bcfafb82f36

TUESDAY, JUNE 15, 2021 07:15:58 AM [BLOCK 687650]

FINANCIAL		INPUTS		OUTPUTS		PRIVACY	
VOLUME	0.33620250 B	UTXOS CONSUMED	1	UTXOS CREATED	2	NEW ADDRESSES	2
FEES	0.00013170 B	ADDRESSES	1	ADDRESSES	2	ADDRESS REUSE	0%
FEES/VBYTE	92.75 SAT/VB					TX ENTROPY	0 BITS
FEES/BYTE	59.06 SAT/B						
BDD	2.46 B.DAYS						

Fig 2.1 — OXT Transaction Page and Navigation to TxGraph

The starting transaction will be displayed. Transactions are presented as vertices (circles) on the graph. Vertices represent a change in the UTXO Set by showing a new relationship between UTXOs consumed and created by a transaction.

Single clicking the transaction will select the transaction, change its color from blue to green, and display additional options on the toolbar (left side of screen).

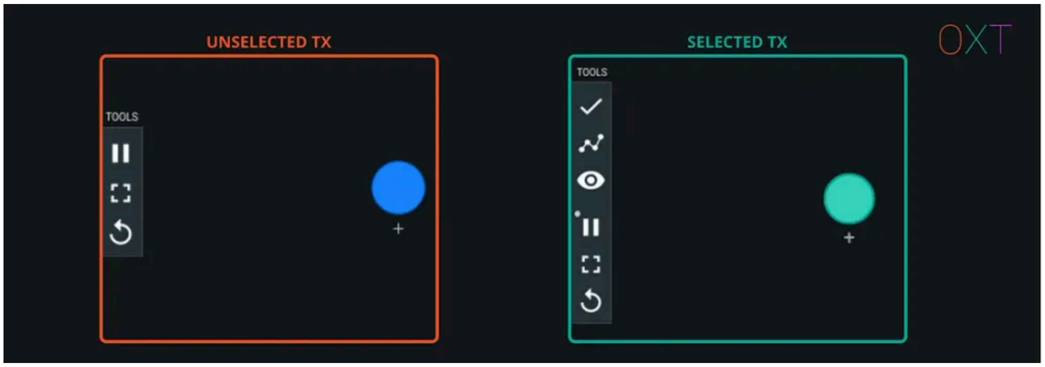
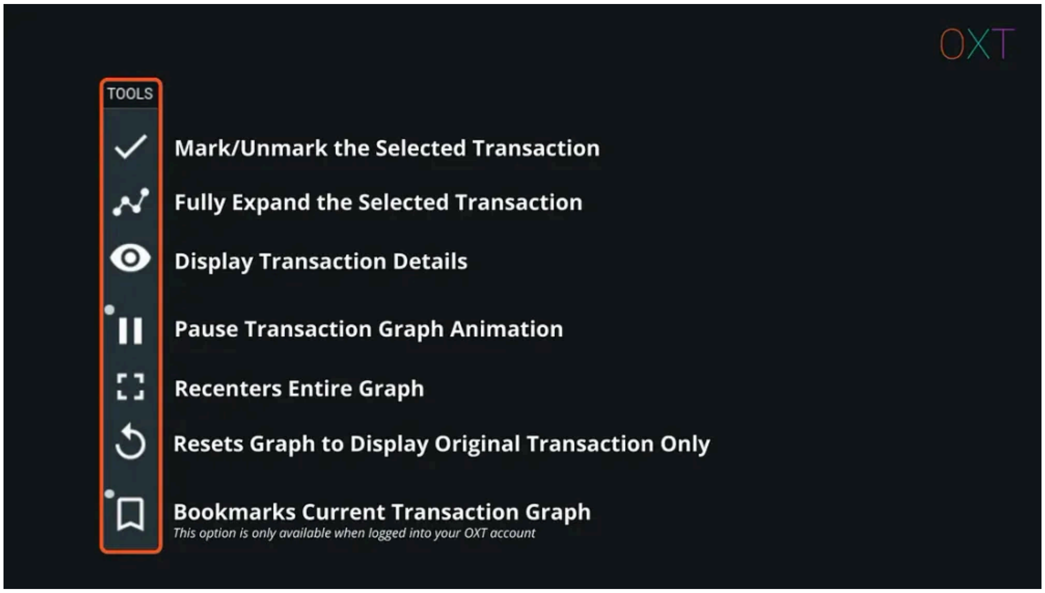


Fig 2.2 — Initial TxGraph with Select and Toolbar

The tool bar icons perform the following actions:



- ✓ Mark/Unmark the Selected Transaction
- Fully Expand the Selected Transaction
- Display Transaction Details
- Pause Transaction Graph Animation
- Recenters Entire Graph
- Resets Graph to Display Original Transaction Only
- Bookmarks Current Transaction Graph
  This option is only available when logged into your OXT account

Fig 2.3 — TxGraph Toolbar Actions

Double click the transaction to fully expand all transaction UTXOs. The UTXOs are displayed as “edges” (lines) with arrows indicating if the UTXO is an input (pointing toward the transaction) or output (pointing away from the transaction). The graph will also display the transaction creating the inputs or consuming the outputs. If the output is unspent, an unfilled diamond will be displayed on the end of the UTXO.

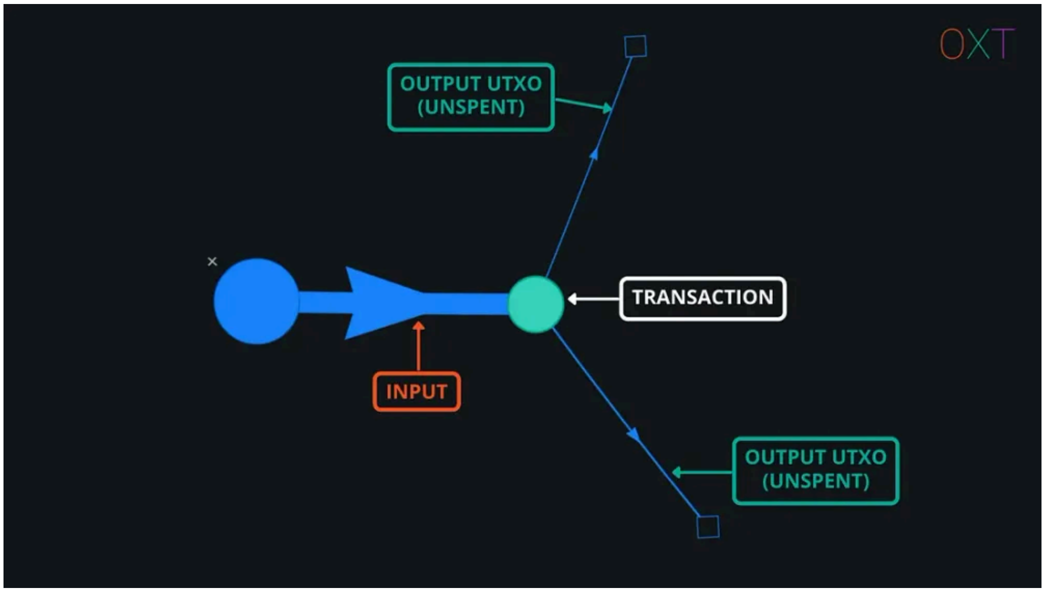
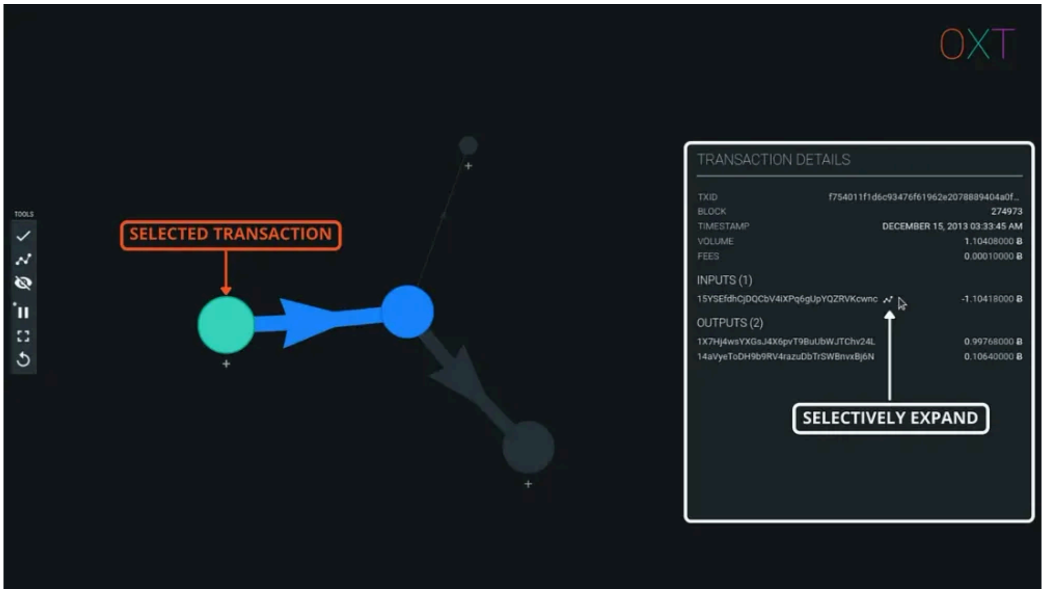


Fig 2.4 — Fully Expanded Transaction

Double-clicking or fully expanding a transaction can make your transaction graph noisy and difficult to read. To minimize clutter, we suggest selectively expanding UTXOs. To selectively expand UTXOs, select the transaction and open the Transaction Details window. The transaction inputs and outputs can be selectively expanded by hovering the mouse to the right of the address text and selecting the visible Expand Tx Graph.



TRANSACTION DETAILS

TXID	f754011f1d6c93476f61962e2078889404a0f...
BLOCK	274973
TIMESTAMP	DECEMBER 15, 2013 03:33:45 AM
VOLUME	1.10408000 Ƀ
FEES	0.00010000 Ƀ

INPUTS (1)

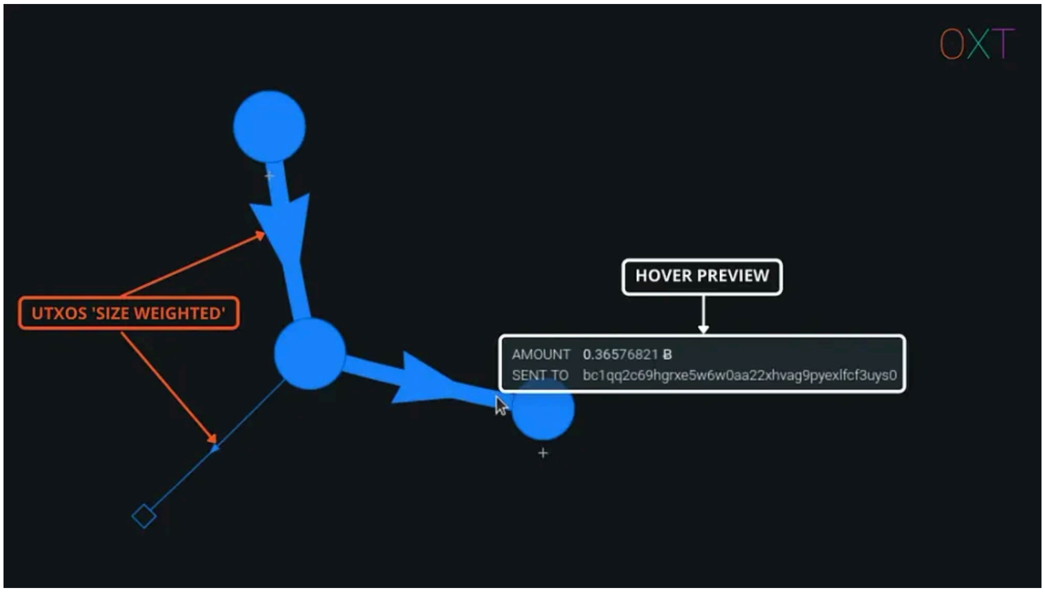
15YSEfdhCjDQCbV4iXPq6gUpYQZRVKcwnc	-1.10418000 Ƀ

OUTPUTS (2)

1X7Hj4wsYXGsJ4X6pvT9BuUbWJTChv24L	0.99768000 Ƀ
14aVyeToDH9b9RV4razuDbTrSWBnvxBj6N	0.10640000 Ƀ

Fig 2.5 — Selective UTXO Expansion

On the graph, hovering the mouse over an input or output will display additional information about the object of interest, without the need for expanding the transaction details tab.



AMOUNT 0.36576821 Ƀ
SENT TO bc1qq2c69hgrxe5w6w0aa22xhvag9pyexlfcf3uys0

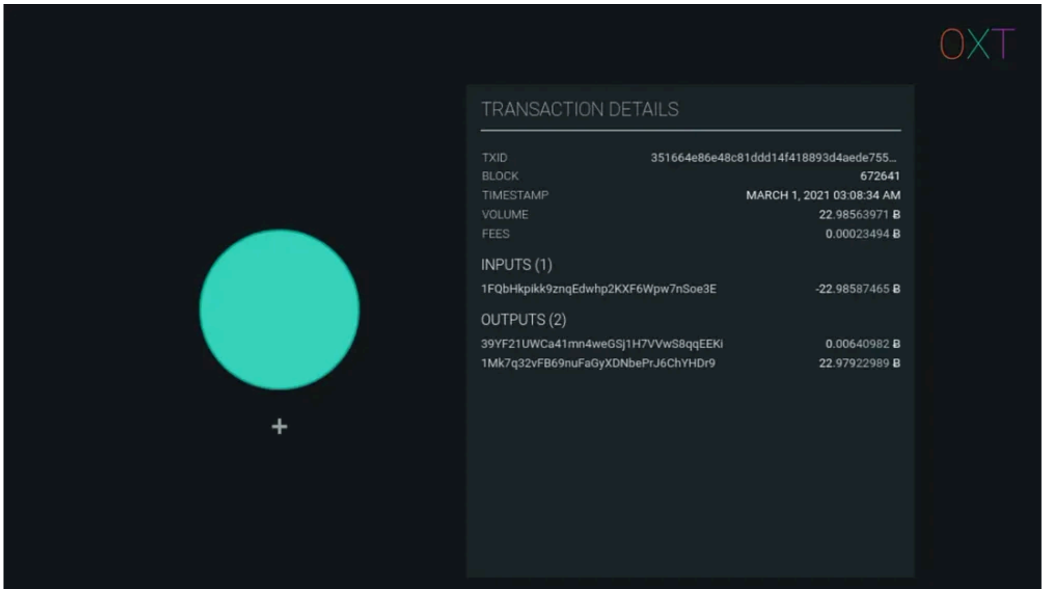
Fig 2.6 — Tx Graph Line Weight and Preview

OXT's transaction graph will also help to process some additional information automatically. Transactions and UTXOs will be "weighted" on a relative basis based on their BTC volumes. This can be very helpful for change detection and illustration of "peel chains", which we will discuss in further detail below.

OXT Peel Chain Transaction Graph Example

A simple transaction graph example is presented below.

1. Navigate to the hyperlink of the transaction page and expand the transaction graph.
2. Select the transaction with a single click.
3. Open the transaction details window by clicking the respective icon on the left toolbar.



TRANSACTION DETAILS

TXID 351664e86e48c81ddd14f418893d4aede755...
BLOCK 672641
TIMESTAMP MARCH 1, 2021 03:08:34 AM
VOLUME 22.98563971 Ƀ
FEES 0.00023494 Ƀ

INPUTS (1)

1FQbHkpikk9znqEdwhp2KXF6Wpw7nSoe3E -22.98587465 Ƀ

OUTPUTS (2)

39YF21UWCa41mn4weGSj1H7VVwS8qqEEKi 0.00640982 Ƀ
1Mk7q32vFB69nuFaGyXDNbePrJ6ChYHDr9 22.97922989 Ƀ

Fig 2.7 — Selected Transaction and Transaction Details

4. Double click the starting transaction to expand all inputs and outputs.
5. Zoom out using the mouse scroll wheel and re-orient the graph with the oldest transactions in your preferred order (ie. left to right) by clicking and dragging the transactions in the preferred orientation.

The two outputs present us with a question to answer if we are going to attempt to track the activity of the wallet creating the transaction.

Which output do we follow?

If we apply the different script heuristic, we identify the second output as change.

6. Double click the next transaction that spends the second output from the original transaction.
7. Repeat the process for change identification using the heuristics presented in Part I. Expand two more transactions using this process.

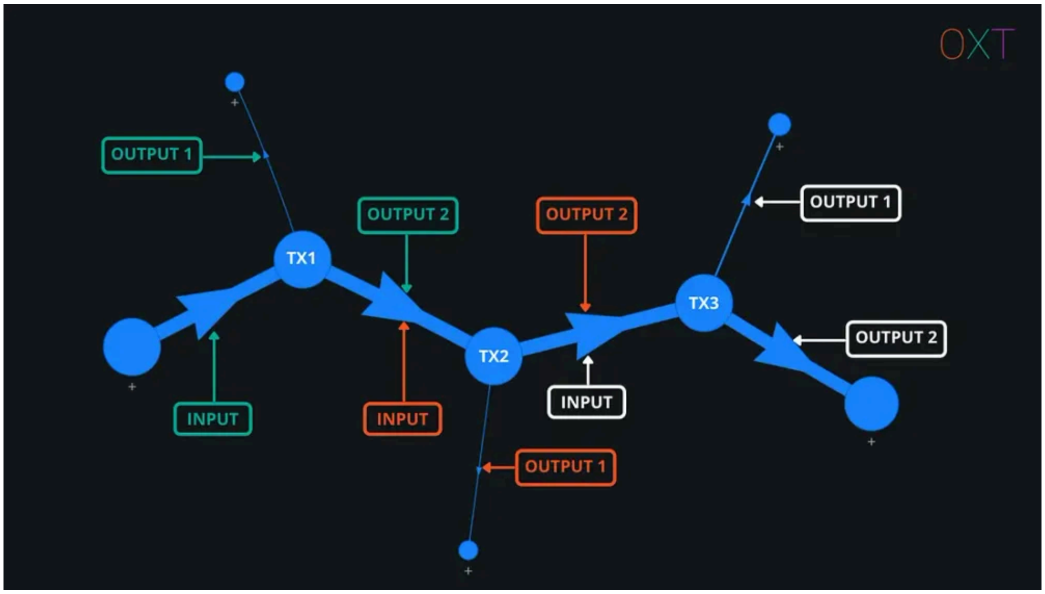


Fig 2.8 — Peel Chain Example (Tx Graph Bookmark)

Afterwards, the graph should look similar to the image in Fig 2.8 above. To add additional emphasis on the change UTXOs, the change UTXOs can be marked and highlighted in orange using the left toolbar button. A transaction graph showing a series of simple spends from the same wallet is commonly referred to as a "peel chain".

Chain surveillance firms attempt to frame peel chains as a form of suspicious activity related to "structuring or money laundering." Though as we described in part 1, approximately 50% of bitcoin transactions are simple spends with 1 input and 2 outputs, in other words entirely normal behavior.

For our purposes, a peel chain is the simple process of tracking a single wallet's activity over multiple transactions.

Wallet Fingerprinting and Transaction Graph Interpretation

As you continue interacting with the example peel chain, additional patterns indicative of a consistent wallet fingerprint will become apparent. Including the following:

1. The largest output, shown by OXT's automatic line weight feature makes the change outputs readily apparent.
2. The change outputs are always paid to P2PKH addresses.
3. The change outputs are always the second of the two outputs.
4. Not shown on the graph, but also worth noting are the consistent transaction version number (2) and lock-time (0) throughout the graph. To see this information, click the transaction ID in the transaction detail window to navigate to the TRANSACTION page. Then select the the TECHNICAL tab to display the transaction version number and lock-time.
5. Expanding the previous or future spending history of this transaction graph will reveal more transactions with the same pattern.

Each of these patterns can be used to describe the behavior of the observed wallet software. Generalization of observed wallet behavior is referred to as wallet fingerprinting, which leverages the following patterns:

1. Input and output address scripts
2. Change UTXO position consistency
3. Version number and lock-time

Combining the above patterns can give an analyst high confidence in their interpretation of change outputs. We confirmed these change interpretations by interacting with the service responsible for this transaction activity. The example peel chain shows activity from a well-known custodial tumbler payout mechanism. Explore the graph source by backtracking from the provided transaction to find coins related to an exchange hack.

In the next section, we will discuss how transaction graph analysis can be improved further by using wallet clustering and monitoring outputs for spends to centralized services.

Wallet Clustering — Common Input Ownership Heuristic

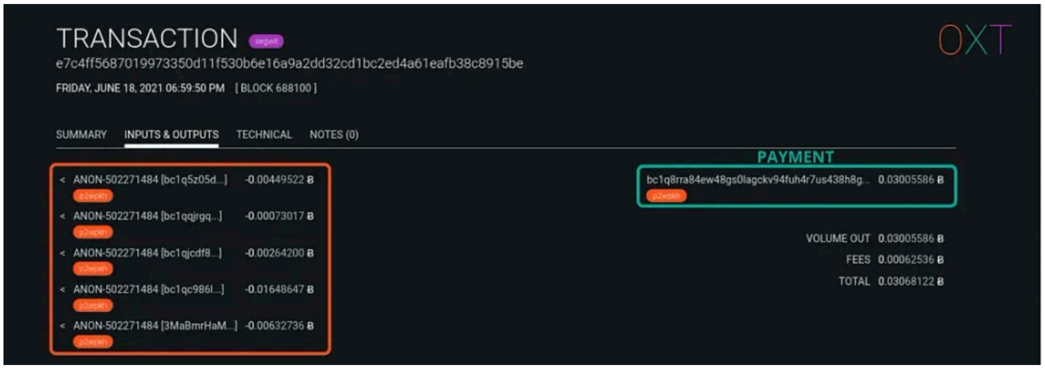
The remaining critical chain analysis tool is referred to as “wallet clustering”. Clustering aggregates addresses based on their co-spending patterns and assumptions about normal wallet software behavior.

Most bitcoin wallets today are hierarchical deterministic wallets. They generate a single master private key which is used to derive child private/public keys and the associated addresses.

Wallet software typically creates a new address automatically for each received payment (UTXO received). If a single UTXO or address balance is not adequate for making a payment, a wallet will include additional UTXOs/addresses controlled by different private keys/addresses as necessary to spend the desired amount. Most wallets do this automatically without user input.

Because of this normal wallet functionality and bitcoin's private/public key cryptography backing, an analyst can ***assume*** that each address used as an input to a transaction, is controlled by the same private key or wallet software.

The assumption that each input to a transaction is controlled by the same wallet is called the common input ownership heuristic (CIOH) or more simply, the merged input heuristic.



TRANSACTION
e7c4ff5687019973350d11f530b6e16a9a2dd32cd1bc2ed4a61eafb38c8915be
FRIDAY, JUNE 18, 2021 06:59:50 PM [BLOCK 688100]

< ANON-502271484 [bc1q5z05d...] -0.00449522 Ƀ
< ANON-502271484 [bc1qqjrgq...] -0.00073017 Ƀ
< ANON-502271484 [bc1qjcdf8...] -0.00264200 Ƀ
< ANON-502271484 [bc1qc986l...] -0.01648647 Ƀ
< ANON-502271484 [3MaBmrHaM...] -0.00632736 Ƀ

bc1q8rra84ew48gs0lagckv94fuh4r7us438h8g... 0.03005586 Ƀ

VOLUME OUT 0.03005586 Ƀ
FEES 0.00062536 Ƀ
TOTAL 0.03068122 Ƀ

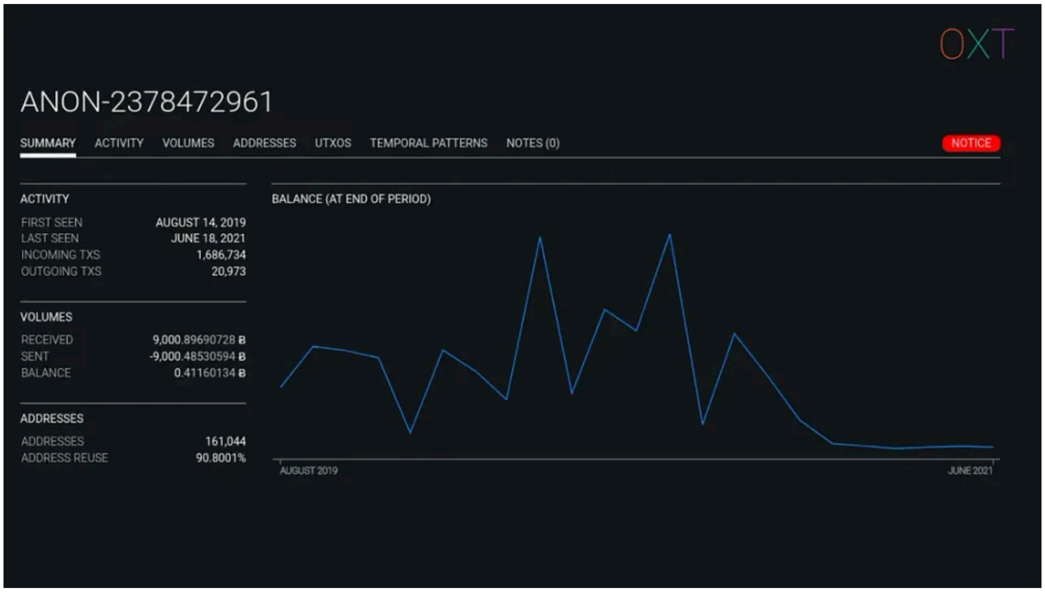
Fig 2.9 — CIOH and Cluster Example

Like all heuristics there are specific scenarios where the CIOH does not hold true. The breakdowns in the CIOH tend to revolve around specially constructed privacy enhancing transactions. We will cover the special scenarios where the CIOH is broken and how OXT handles these exceptions in a later part of this series.

The ANONs — OXT's Clustering Scheme

Separate addresses that are assumed controlled by the same wallet are usually given a wallet cluster ID by analysis software. Due to bitcoin's pseudonymous nature a wallet cluster may be representative of a single user or centralized service's activity.

But without additional information, the wallet remains "anonymous" in that it has not been attributed to any real world entity activity. As a result, OXT gives each new cluster an ANON prefix followed by an index number.



ANON-2378472961

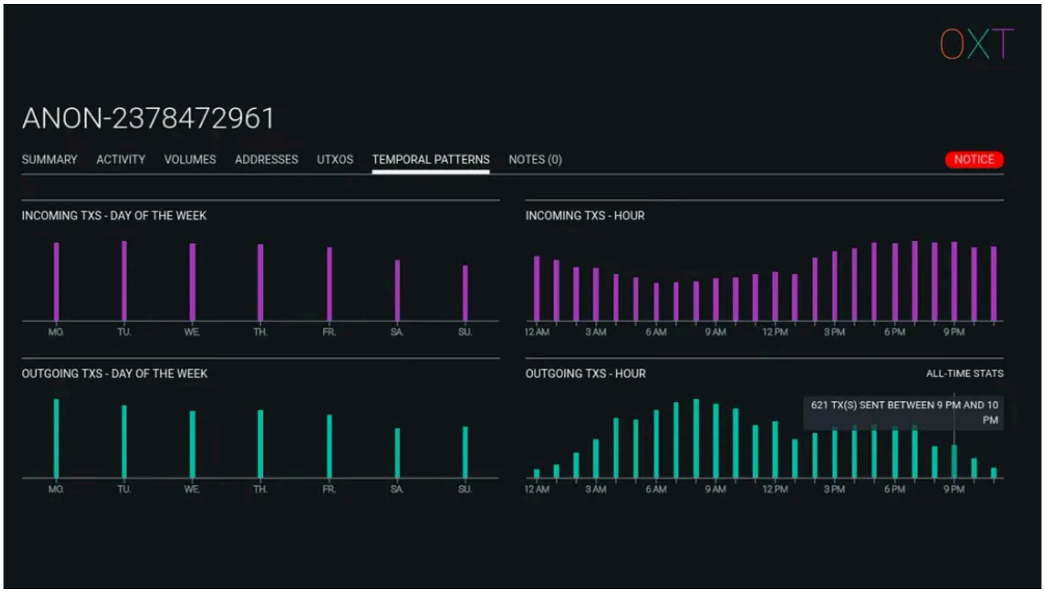
ACTIVITY	
FIRST SEEN	AUGUST 14, 2019
LAST SEEN	JUNE 18, 2021
INCOMING TXS	1,686,734
OUTGOING TXS	20,973
VOLUMES	
RECEIVED	9,000.89690728 Ƀ
SENT	-9,000.48530594 Ƀ
BALANCE	0.41160134 Ƀ
ADDRESSES	
ADDRESSES	161,044
ADDRESS REUSE	90.8001%

Fig 2.10 — ANON Wallet Cluster Example

OXT calculates several cluster types of cluster activity including:

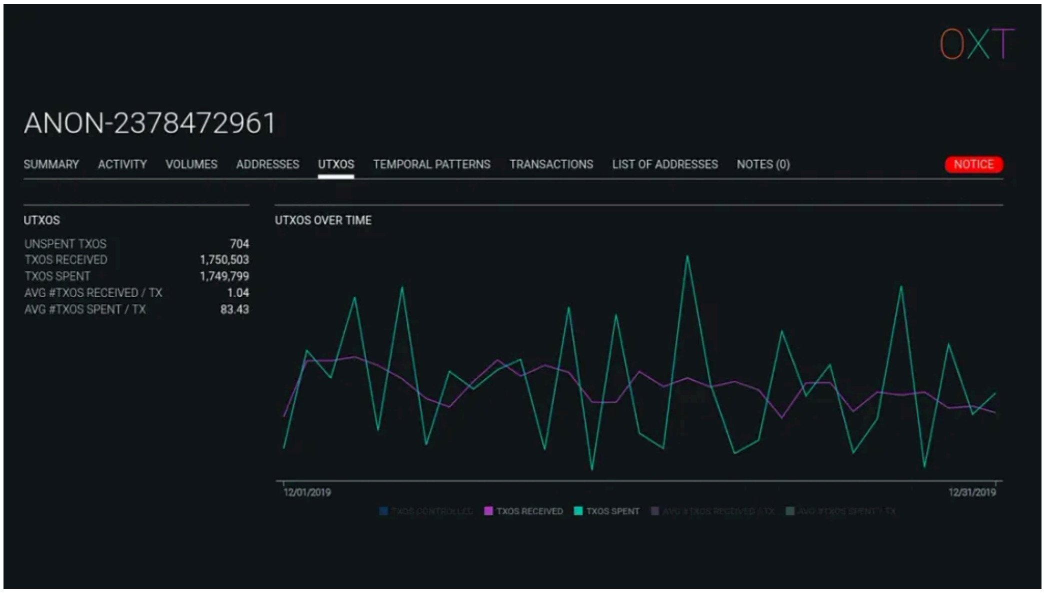
- A summary of general activity (balance, number of transactions, active dates, number of addresses)
- Plots of monthly and daily transaction activity, BTC volumes sent and received, UTXOs sent and received, and address stats
- A temporal pattern of cluster activity by day of the week and hours
- A notes section where OXT users can add notes on possible attribution or context for interacting with an unknown cluster during an investigation.

OXT's general cluster stats are viewable without an account. However, with a free OXT account (no email required), a user can access additional features. When logged in, cluster statistics including daily balance, daily volumes, transaction lists, address lists, and more are accessible.



ANON-2378472961

Fig 2.11 — ANON Wallet Cluster Temporal Patterns



ANON-2378472961

UTXOS

UNSPENT TXOS	704
TXOS RECEIVED	1,750,503
TXOS SPENT	1,749,799
AVG #TXOS RECEIVED / TX	1.04
AVG #TXOS SPENT / TX	83.43

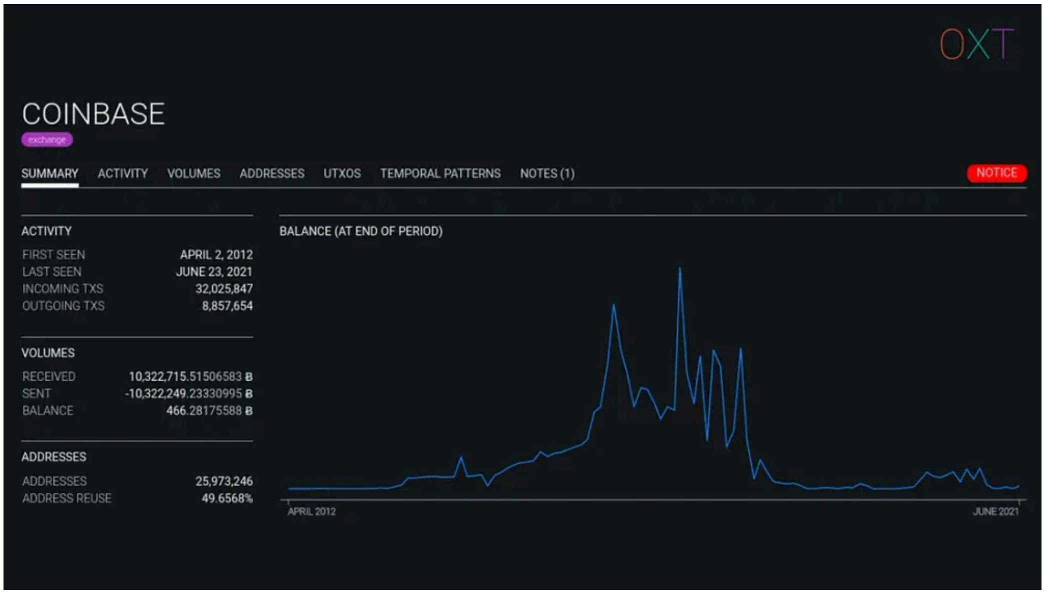
Fig 2.12 — ANON Wallet Cluster UTXO Activity Tab

Cluster Attribution — ANON to Labeled Service

Using the CIOH, OXT will keep track of a wallet cluster's on-chain activity. To attribute the wallet cluster to a specific service requires interacting with the service.

An analyst can create an account with a service and send BTC to a deposit address provided by the service. From there, the analyst can monitor the spending of their deposit UTXO. When spent the analyst can attribute the address and its co-spent addresses to the corresponding cluster ID.

Alternatively, an analyst can use opensource intelligence techniques to search for publicly available information posted by service users. Deposit and withdrawal addresses can be commonly found in social media posts. This publicly available data can also be used to attribute a wallet cluster to a centralized service.



COINBASE

ACTIVITY

FIRST SEEN	APRIL 2, 2012
LAST SEEN	JUNE 23, 2021
INCOMING TXS	32,025,847
OUTGOING TXS	8,857,654

VOLUMES

RECEIVED	10,322,715.51506583 Ƀ
SENT	-10,322,249.23330995 Ƀ
BALANCE	466.28175588 Ƀ

ADDRESSES

ADDRESSES	25,973,246
ADDRESS REUSE	49.6568%

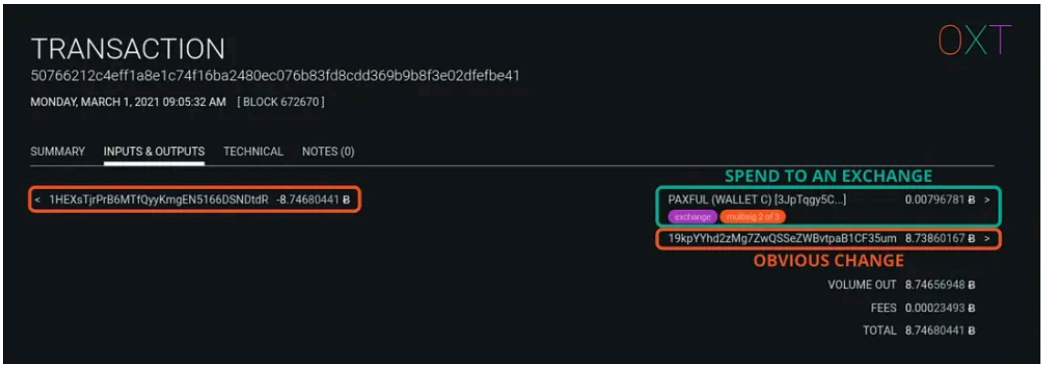
Fig 2.13 — Labelled Cluster Example

Applying External Transaction Data To Change Detection

Additional information including wallet fingerprinting, output spending timing, and output clustering can be applied to change detection interpretation.

The most damaging to transaction privacy is when a simple spend is made to a wallet cluster that has been identified as a centralized service.

When a simple spend is made to a centralized service, all change detection ambiguity is lost. The output to the centralized service is clearly the payment. The only remaining output is the obvious change output. An example from the future spending of the peel chain example above is shown below.



TRANSACTION

50766212c4eff1a8e1c74f16ba2480ec076b83fd8cdd369b9b8f3e02dfefbe41

MONDAY, MARCH 1, 2021 09:05:32 AM [BLOCK 672670]

< 1HEXsTjrPrB6MTfQyyKmgEN5166DSNDtdR -8.74680441 Ƀ

SPEND TO AN EXCHANGE

PAXFUL (WALLET C) [3JpTqgy5C...] 0.00796781 Ƀ >

19kpYYhd2zMg7ZwQSSeZWBvtpaB1CF35um 8.73860167 Ƀ >

OBVIOUS CHANGE

VOLUME OUT 8.74656948 Ƀ

FEES 0.00023493 Ƀ

TOTAL 8.74680441 Ƀ

Fig 2.14— Exchange Payments in Simple Spend Example

The most crucial aspect of the CIOH isn't necessarily how it is used to target individual user privacy, but how wallet clustering among centralised services negatively and significantly effects the privacy of the the bitcoin network transaction graph.

A significant portion of bitcoin's economic activity is immediately from or to a centralised service which has a major centralisation effect on the overall bitcoin network transaction graph.

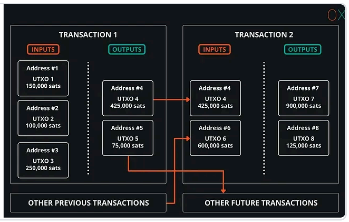
Review

In Parts 1 and 2 we introduced the fundamentals of chain analysis including change detection, transaction graph analysis, and the common input ownership heuristic.

Understanding Bitcoin Privacy with OXT — Part 1

Introduction Awareness of Bitcoin's value proposition for censorship resistant payments took off in 2011 with the launch of Silk Road and...

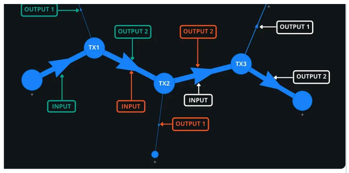
OXT ErgoBTC • OXT Research



Understanding Bitcoin Privacy with OXT — Part 2

Introduction Now that we have presented the basic concepts in Part 1, we can move on to the core concepts that underpin chain analysis by…

OXT ErgoBTC • OXT Research



Change detection consists of a series of heuristics used to determine a likely transaction change output. A transaction graph analysis can quickly and visually illustrate these heuristic interpretations to track the activity of a single user. Additional data including wallet clustering by the common input ownership heuristic can be used to improve confidence in change detection. Attributing a wallet cluster to a user or centralized service activity requires additional off chain data tying a suspect address and spending activity to the noted service.

In the following section we will introduce the concepts used to defeat chain analysis and make user tracking more difficult.

Part 3 covers core concepts of improving bitcoin's privacy including:

1. Randomized wallet fingerprinting for defeating change detection.
2. UTXO flows and the fundamental link between inputs and outputs.
3. How equal output coinjoins address the issue of deterministic flows.
4. Transaction entropy
5. How payjoin defeats the common input ownership heuristic

Understanding Bitcoin Privacy with OXT — Part 3

Introduction With the foundational concepts of chain analysis introduced in Part 1 and Part 2, Part 3 will discuss the methods for…

OXT ErgoBTC • OXT Research

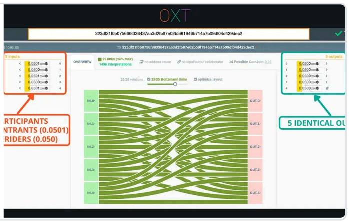
Part 4 discusses:

1. Analyses needing a "starting point"
2. The privacy implications of sending and receiving payments
3. How existing privacy techniques can mitigate many of the issues discussed throughout the guide.

Understanding Bitcoin Privacy with OXT — Part 4

Introduction So far this guide has introduced the basics concepts used by chain analysis and the concepts used to undermine chain analysis…

OXT ErgoBTC • OXT Research



Published by:

You might also like...

AUG 11	Understanding Bitcoin Privacy with OXT — Part 4	10 min read
AUG 09	Understanding Bitcoin Privacy with OXT — Part 3	10 min read
AUG 04	Understanding Bitcoin Privacy with OXT — Part 1	10 min read

Sign up

Powered by Ghost

Subscribe