AUG 11, 2021 • 10 MIN READ • UNDERSTANDING BITCOIN PRIVACY

Understanding Bitcoin Privacy with OXT — Part 4

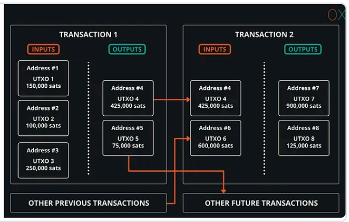
Introduction

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

Previous parts in this series

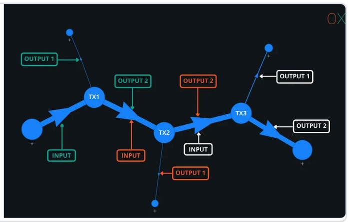
Understanding Bitcoin Privacy with OXT — Part 1
Introduction Awareness of Bitcoin's value proposition for censorship resistant payments took off in 2011 with the launch of Silk Road and...

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



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

It is unlikely that users reading this are looking to become "experts" in chain analysis, but a fundamental understanding of the tools and concepts used to attack their privacy will allow them to better protect their privacy.

In this section we will introduce the real world implications of sending and receiving transactions on user privacy. From there we will present specific privacy enhancing technologies that can be used to maintain privacy when interacting with bitcoin.

Lost On Chain — Starting Points And Breaking Pseudonymity

Bitcoin is pseudonymous by default. Without additional information tying user activity to on-chain activity, an analysis has no "starting point" for tracking related bitcoin network activity.

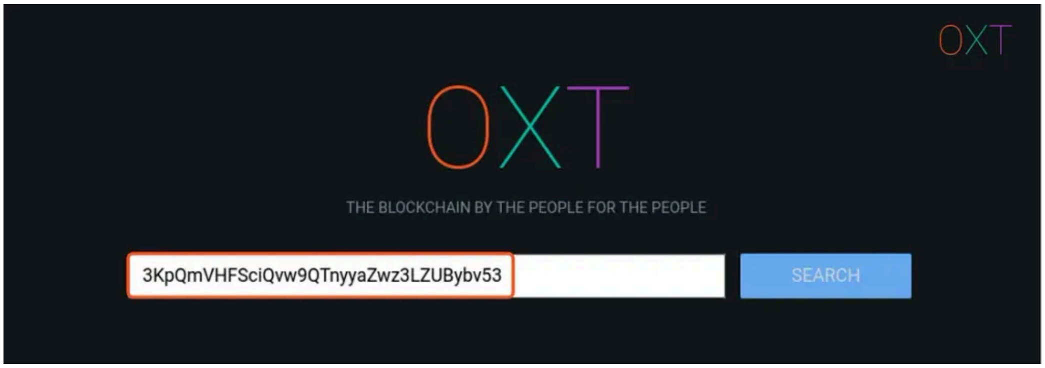
Starting points typically include users willingly disclosing addresses they control. Provided addresses are typically for receiving payment. Starting points can also be obtained from information provided by third parties, such as the information sharing agreements between surveillance firms and exchanges.

For beginner analysts, some "context" is usually necessary for performing an analysis. That valuable context often comes from analysis of their own transactions. Users evaluating their own transaction history via a third party block explorer are encouraged to use a VPN or Tor browser to prevent linking of their IP address with their transaction information.

OXT Workflow — Addresses As Starting Points

Most users query block explorers by entering an address as a starting point. When querying OXT with an address as a starting point, the associated transaction information will not automatically be displayed. Users should follow the steps below to navigate to the transaction graph.

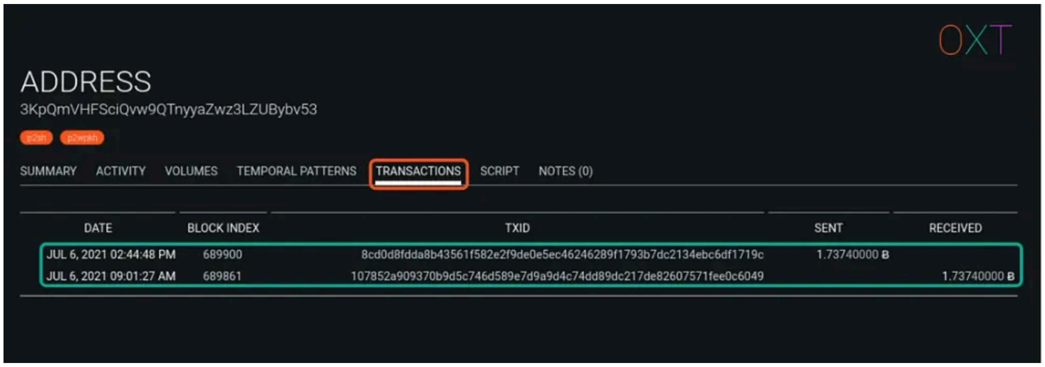
1. Log in to your OXT account. Accounts are free and do not require any personally identifiable information for creation.
2. Enter the desired address into the search bar.



3KpQmVHFSciQvw9QTnyyaZwz3LZUBybv53

Fig 4.1 OXT Workflow Address Query

3. Navigate to the `TRANSACTION` tab

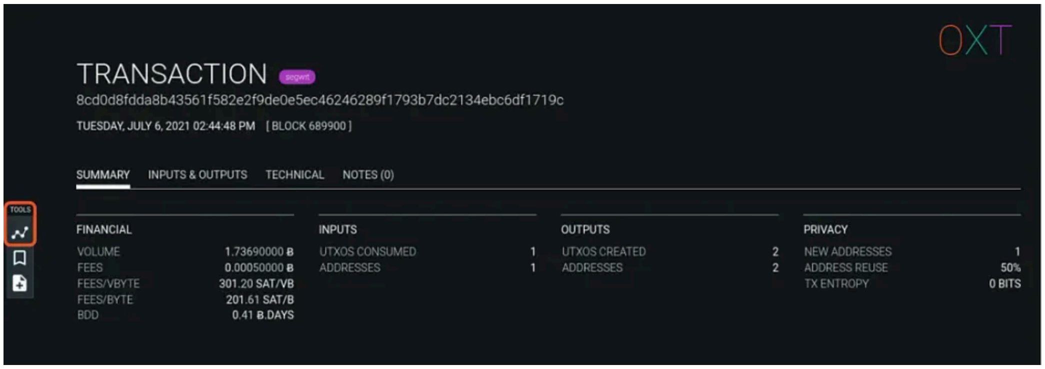


ADDRESS
3KpQmVHFSciQvw9QTnyyaZwz3LZUBybv53

DATE	BLOCK INDEX	TXID	SENT	RECEIVED
JUL 6, 2021 02:44:48 PM	689900	8cd0d8fdda8b43561f582e2f9de0e5ec46246289f1793b7dc2134ebc6df1719c	1.73740000 B	
JUL 6, 2021 09:01:27 AM	689861	107852a909370b9d5c746d589e7d9a9d4c74dd89dc217de82607571fee0c6049		1.73740000 B

Fig 4.2 OXT Workflow Address — Transaction Tab

4. Select the desired transaction. Users should note that a starting address may have received multiple payments. If the address has received multiple transactions, they will have to select the desired transaction based on volume and timing of the transactions.
5. From there the Transaction Page will be opened.



TRANSACTION
8cd0d8fdda8b43561f582e2f9de0e5ec46246289f1793b7dc2134ebc6df1719c
TUESDAY, JULY 6, 2021 02:44:48 PM [BLOCK 689900]

FINANCIAL		INPUTS		OUTPUTS		PRIVACY	
VOLUME	1.73690000 B	UTXOS CONSUMED	1	UTXOS CREATED	2	NEW ADDRESSES	1
FEES	0.00050000 B	ADDRESSES	1	ADDRESSES	2	ADDRESS REUSE	50%
FEES/VBYTE	301.20 SAT/VB					TX ENTROPY	0 BITS
FEES/BYTE	201.61 SAT/B						
BDD	0.41 B.DAYS						

Fig 4.3 OXT Workflow Transaction Page and Graph Tool

6. Open the transaction graph to begin the financial flow evaluation.

Note: If users already have the desired transaction ID, they can avoid logging into OXT and navigate directly to the transaction page for accessing the transaction graph. Revisit Part II for additional details on interacting with the transaction graph.

Analysis Directions — UTXO History And Future Spending

Analysts presented with a starting transaction and UTXO can pursue two investigation “directions”.

They can search for the “source” of funds by evaluating the past history of the target UTXO. Source evaluation for transaction chains with a single input are fairly simple to perform, because there is no “decision” to be made in evaluating which input UTXO path to follow. However, multi-input transactions present analysts with multiple sources to evaluate.

Analysts can also search for the “destination” of future spends from the associated UTXO by applying the change detection heuristics presented in Part I and external transaction data presented in Part II.

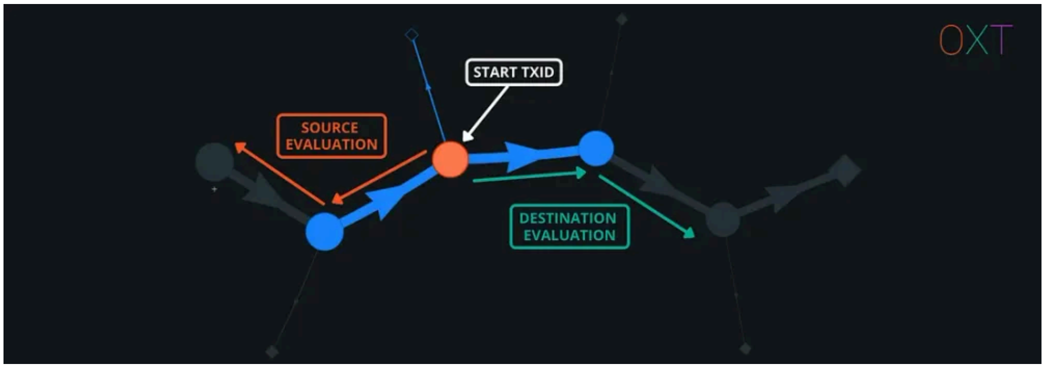


Fig 4.5 Investigation Direction — Source & Destination

Note: UTXO flows should not be tracked across custodial services. It is highly unlikely that a deposit UTXO will be used to payout to the entity making the deposit.

Privacy Implications Of Sending And Receiving Payments

When sending or receiving a payment, users necessarily reveal some of their UTXO set to their counterparty. For naively managed UTXOs, this may reveal a users ***entire*** wallet balance to a counterparty.

Disclosing wealth for making payments is an unfortunate side effect of bitcoin’s transparency. The negative implications of this disclosure to counterparties should be obvious, particularly for simple spends.

In addition, payments made by a sender allow for a recipient to assess the senders past transaction history. Payments also allow a sender to evaluate a recipients future spending of their received payment.

The techniques discussed below are designed to mitigate the negative side effects of bitcoin’s transparency.

Samourai Wallet Privacy Enhancing Transactions

Much of chain analysis is based on the following core concepts:

- analysts needing a starting point
- the issues of the transaction graph
- change detection
- clustering separate addresses by the common input ownership heuristic

In Part I and II we introduced the core concepts of chain analysis. Part III presented the concepts used to undermine these techniques.

The OXT team works with the Samourai Wallet developers to test and create techniques that mitigate the privacy shortcomings we have introduced so far. These techniques are discussed below.

Stealth Addresses — Denying a Start Point

Chain analysts need a starting point when attempting to track an entity's on chain activities. This typically means linking a target's online activity with an address they have posted for receiving payments or donations. From this address an analyst can evaluate a user's activity including received payments, total address balance, and spending patterns.

User's frequently share addresses for receiving payments. The shared addresses are the same addresses that appear on the blockchain and are searchable via any block explorer.

Instead of exchanging a direct address for receiving payment, users can exchange "stealth addresses". Stealth addresses are based on concepts derived from the Diffe-Hellman key exchange, a critical cryptographic concept that underpins TLS/SSL, one of the most important forms of cryptography used in internet secure communications.

Samourai Wallet's stealth address implementation is based on the BIP 47 Proposal by the Open Bitcoin Privacy Project. BIP 47 reusable payment codes allow a sender to: create an unlimited amount of unique bitcoin addresses for payment to the intended recipient without the recipient needing to be online.

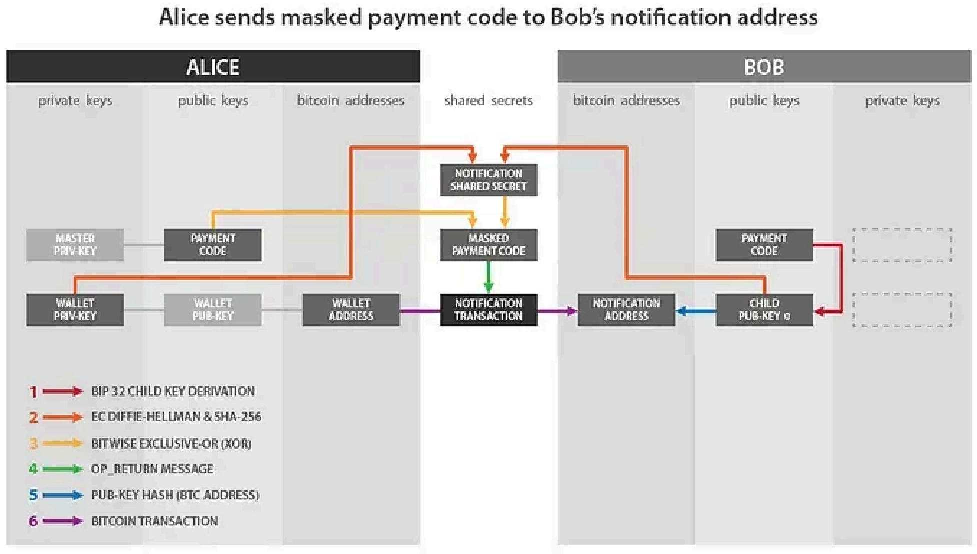


Fig 4.6 V1 BIP47 Payment Code Architecture (BIP 47 Github**)**

Reusable payment codes deprive analysts of a "free" starting point on the bitcoin block chain. More information on Samourai Wallet's reusable payment code can be found here.

Coin Control — UTXO Segregation

Combining inputs from multiple sources in future spends can allow payment senders to evaluate the transaction histories of additional UTXOs combined with their spent UTXO.

To mitigate this privacy leak, users can practice “coin control”. Broadly coin control consists of several steps.

- Labelling received payment UTXOs. At a minimum labelling should include the sender and reason for payment.
- “Marking Do Not Spend”. To prevent a wallet from accidentally including a UTXO in a future payment, UTXOs can be made inactive for inclusion in future spends.
- Sending Individual (Selective UTXO Activation). UTXOs can be selectively spent.

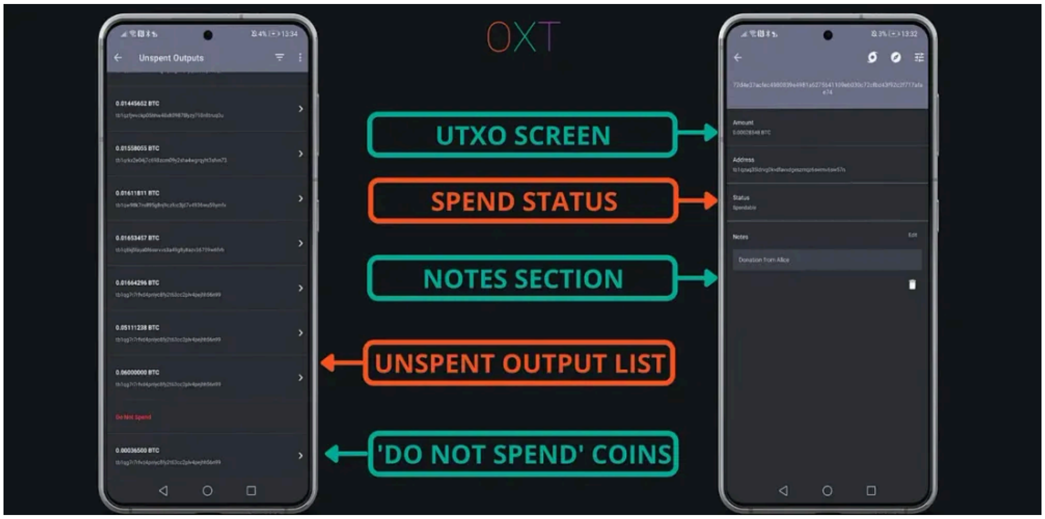


Fig 4.7 Samourai Wallet Coin Control

When payments are made, users should also get in the habit of labelling their change UTXOs. When a label is added to a single UTXO, Samourai Wallet will automatically label any other UTXOs (change outputs) from the same spend with the same label.

Ricochet — Adding Distance

Ricochet is a simple tool that automatically adds “hops”, or dummy transactions between an origin UTXO and payment destination. Ricochet transactions do not obfuscate source of funds or break the transaction graph. However, these transactions put distance between a payment destination and previous UTXO histories.

Source of fund evaluation for transactions with a single input are relatively easy to perform, but adding “hops” requires a receiving entity to evaluate history beyond the immediate incoming UTXO. Transaction graph traversal analyses are simple to perform, but expanding incoming UTXO history evaluation implies additional doubt based on the “UTXO Ownership Model” which increases chances for false positives.

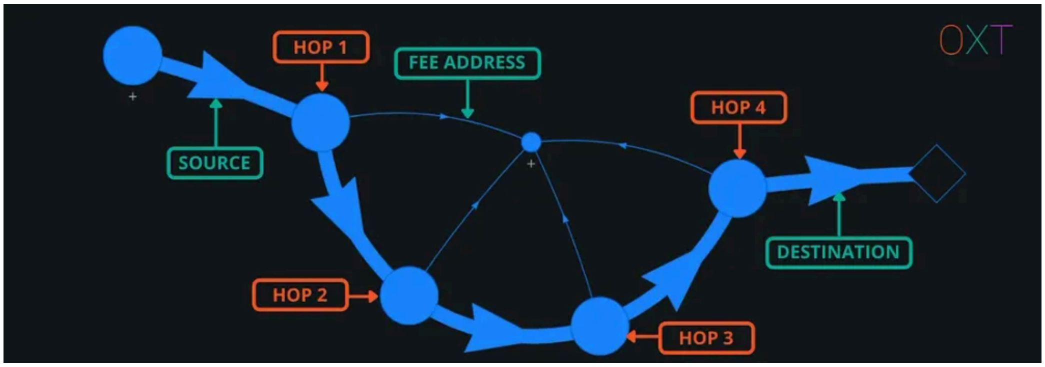


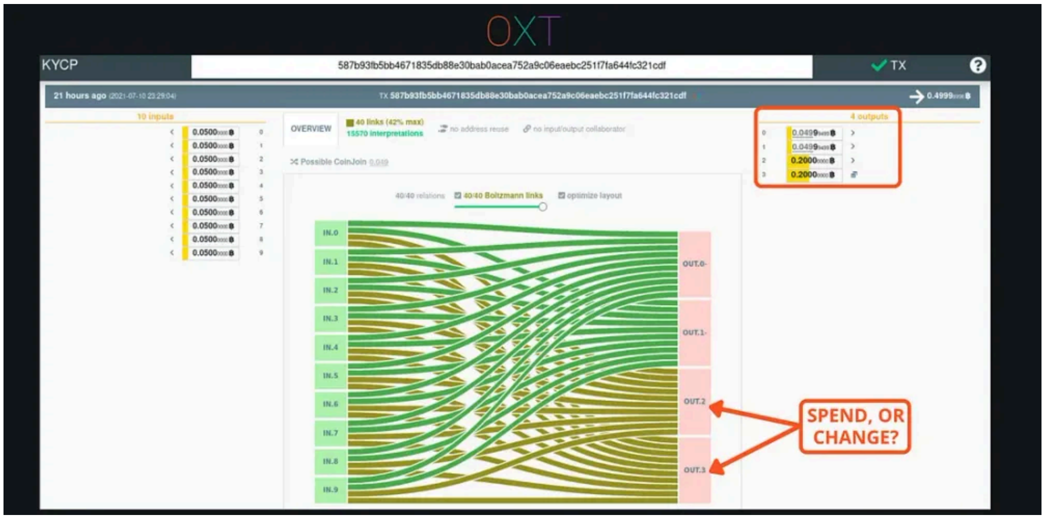
Fig 4.8 Example Ricochet Transaction (TxID)

The current version of ricochet includes four extra hops. A more "dynamic" ricochet with a variable number of hops is planned in future updates. More information on ricochet can be found here.

STONEWALL and STONEWALLx2 — Payments Made Safe

STONEWALL and STONEWALLx2 use the same coin selection algorithm to create transactions with coinjoin properties. STONEWALL is a simulated coinjoin that uses inputs from an individual wallet. STONEWALLx2 is a "true" coinjoin that uses inputs from 2 collaborating users/wallets.

Using the same algorithm means these transactions have identical on-chain footprints, and are indistinguishable to outside observers. As a result, analysts must consider the possibility that any STONEWALL transaction is a "true" coinjoin.



587b93fb5bb4671835db88e30bab0acea752a9c06eaebc251f7fa644fc321cdf ✓ TX

21 hours ago (2021-07-10 23:29:04) TX 587b93fb5bb4671835db88e30bab0acea752a9c06eaebc251f7fa644fc321cdf → 0.4999 ₿

10 inputs

0.0500 ₿	0
0.0500 ₿	1
0.0500 ₿	2
0.0500 ₿	3
0.0500 ₿	4
0.0500 ₿	5
0.0500 ₿	6
0.0500 ₿	7
0.0500 ₿	8
0.0500 ₿	9

40 links (42% max) 15570 interpretations no address reuse no input/output collaborator

Possible CoinJoin 0.019

40/40 relations ☑ 40/40 Boltzmann links ☑ optimize layout

4 outputs

0	0.0499 ₿
1	0.0499 ₿
2	0.2000 ₿
3	0.2000 ₿

Fig 4.9 Example Stonewall Transaction (TxID)

The STONEWALL algorithm is an extension of the transaction properties aimed at defeating simple spend change detection heuristics such as like-type output scripts and randomized change output position.

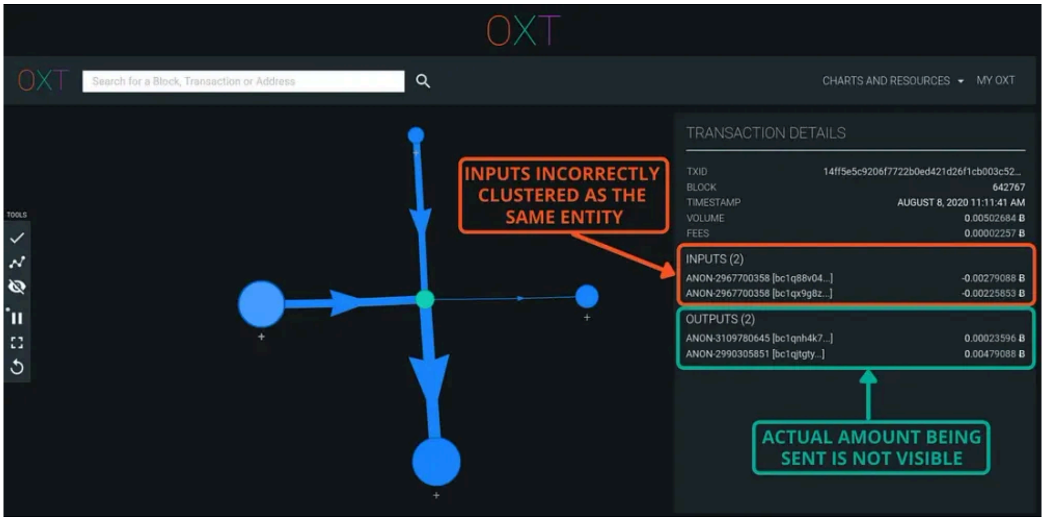
Due to their coinjoin properties, stonewall transactions are capable of defeating the round output payment heuristic interpretation that cannot be defeated by a simple spend.

Stonewall defeats these heuristics by creating transactions with a “dummy” output equal to the intended payment amount.

STONEWALL’s are true payments, that still include deterministic links for their “change” UTXOs. Because a STONEWALL can be a two-wallet coinjoin, a transaction counterparty cannot be sure which change UTXOs belong to the transaction sender responsible for making the payment and which change UTXO belongs to the coinjoin collaborator.

Stowaway — Breaking the CIOH

As we described in Part III, payjoin transactions undermine the common input ownership heuristic. If a single UTXO does not have a sufficient balance to make the desired payment amount, wallet software will include additional inputs as needed to meet the desired amount. Analysts can potentially incorrectly assume the inputs these transactions are controlled by the same wallet.


OXT
OXT
Search for a Block, Transaction or Address
CHARTS AND RESOURCES
MY OXT
TOOLS
INPUTS INCORRECTLY CLUSTERED AS THE SAME ENTITY
ACTUAL AMOUNT BEING SENT IS NOT VISIBLE

TRANSACTION DETAILS

TXID 14ff5e5c9206f7722b0ed421d26f1cb003c52...
BLOCK 642767
TIMESTAMP AUGUST 8, 2020 11:11:41 AM
VOLUME 0.00502684 Ƀ
FEES 0.00002257 Ƀ

INPUTS (2)
ANON-2967700358 [bc1q88v04...] -0.00279088 Ƀ
ANON-2967700358 [bc1qx9g8z...] -0.00225853 Ƀ

OUTPUTS (2)
ANON-3109780645 [bc1qnh4k7...] 0.00023596 Ƀ
ANON-2990305851 [bc1qjtgty...] 0.00479088 Ƀ

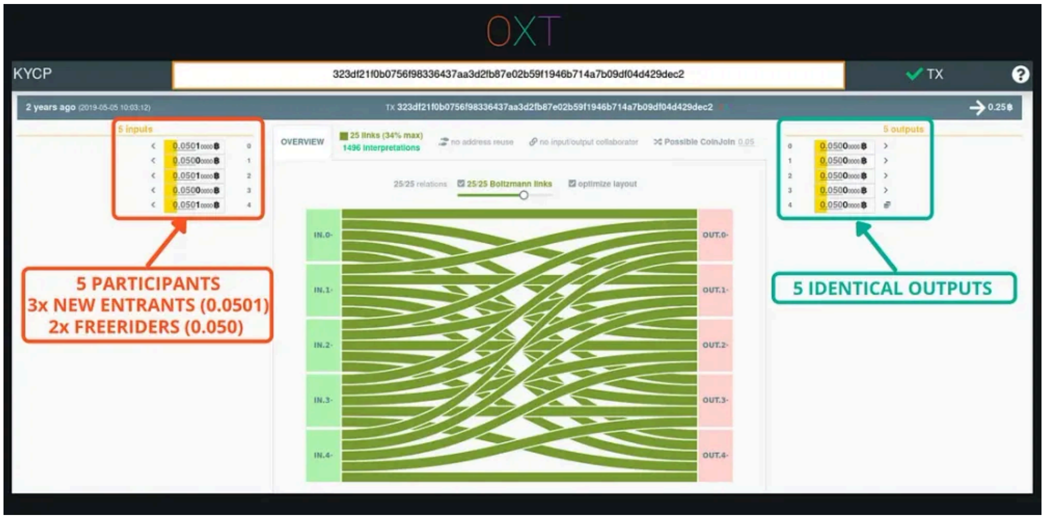
Fig 4.10 Example Stonewall Transaction (TxID)

Payjoins typically have no indistinguishable on chain fingerprint. By including inputs from the transaction sender and payment recipient, two wallets are used to construct the transaction. This undermines the CIOH and creates a “false cluster”. As a consequence of the recipient contributing inputs to the transaction payjoin, the true transaction payment amount is also hidden.

Whirlpool Coinjoin — Creating Forward Privacy

Payment senders can track the future spending of their payment UTXO and potentially obtain additional information about their counterpatry’s wallet composition. To maintain their privacy, payment recipients can coinjoin to break the link between their payment receipt and future spending. In otherwords, sending UTXOs received as payment through a coinjoin establishes forward privacy.

Whirlpool is the only 100% entropy zerolink coinjoin implementation. Whirlpool coinjoins do not include “unmixed change” outputs within the coinjoin transaction that can be used to continue to track user activity.



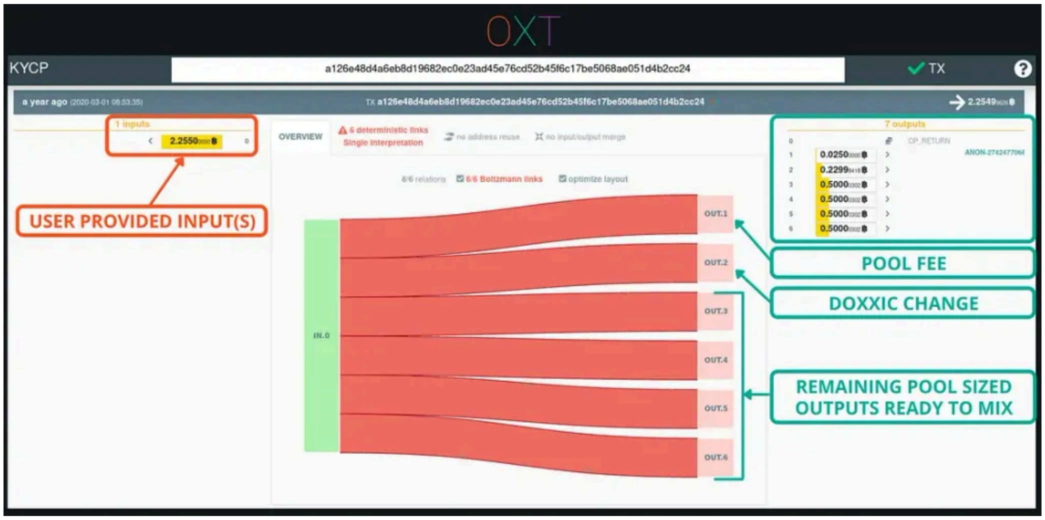
KYCP 323df21f0b0756f98336437aa3d2fb87e02b59f1946b714a7b09df04d429dec2 ✓ TX

2 years ago (2019-05-05 10:03:12) TX 323df21f0b0756f98336437aa3d2fb87e02b59f1946b714a7b09df04d429dec2 → 0.25 ฿

Fig 4.11 Whirlpool Transaction (TxID)

The Whirlpool transaction process begins with the Tx0 which pays the coordinator fee, creates premix UTXOs that are equal to the pool denomination plus miner fees, and a segregated change UTXO.

Inputs to a Tx0 should be selected with care to avoid linking UTXOs from different sources. Combining multiple inputs sources reveals common ownership. The change UTXO should also be handled with care so as to not directly link any future spending activity.



KYCP a126e48d4a6eb8d19682ec0e23ad45e76cd52b45f6c17be5068ae051d4b2cc24 ✓ TX

a year ago (2020-03-01 08:53:35) TX a126e48d4a6eb8d19682ec0e23ad45e76cd52b45f6c17be5068ae051d4b2cc24 → 2.2549 ฿

Fig 4.12 Example Tx0 Transaction (TxID)

After coinjoining and breaking the links between their original (premix) UTXOs and postmix UTXOs, payment recipients can be confident that any payment senders will not be able to reliably follow the future spending of their payment UTXO.

Review

Bitcoin maintains basic user privacy with its pseudonymous nature by not linking real world identities and activities on the blockchain.

At the protocol level, bitcoin transactions send bitcoin to and from transparent addresses for transparent amounts. This transparency has lead to a proliferation of block chain analysis. The bulk of what is considered chain analysis involves payment change detection, transaction graph analysis, and use of the common input ownership heuristic for “wallet clustering”.

While many of these techniques rely on heuristics, applying external transaction data such as address reuse and outputs to or from centralized services can significantly undermine the ambiguity of simple bitcoin transactions.

Wallet software can include randomized fingerprinting and like-type address outputs to maintain ambiguity of simple spends. Even with these tools, the on-chain flows of bitcoin remain “traceable” and deterministic. Properly constructed equal output coinjoins remain the best way for breaking deterministic links and introducing plausible deniability into the transaction graph.

It is likely that the typical user reading this guide is not looking to become an expert in chain analysis. Rather they are looking to improve their privacy when sending and receiving payments. The act of sending and receiving payments necessarily reveals UTXO set information about a sender’s wallet to a payment recipient. As a result, payment senders and receivers are able to evaluate the respective past and future spending of these known UTXOs, which can reveal additional information about their counterparty.

Users armed with knowledge of chain analysis are better prepared for evaluating the implications of spending and receiving and can begin to take steps to protect their privacy.

Those steps include: not linking blockchain activities to an online persona, avoiding address reuse, segregating UTXOs with different histories, establishing forward privacy with coinjoin, and using the advanced spending tools previously discussed to undermine chain analysis heuristics.

Knowledgeable use of these techniques can allow users to obtain a basic level of privacy they may be accustomed to in the traditional finance system.

Closing

A general bitcoin privacy and OXT guide has been requested by many readers. Our hope is that this provides you with a starting point for continuing to expand your understanding of bitcoin privacy.

Armed with additional knowledge and context from this guide, long term readers are encouraged to revisit our previous research reports. Particularly the previously included transaction graphs.

Feedback, comments, and requests for additional guides are welcome.

Thanks for reading and stay safe.

- The OXT Research Team

Published by:

You might also like...

AUG 09	Understanding Bitcoin Privacy with OXT — Part 3	10 min read
AUG 06	Understanding Bitcoin Privacy with OXT — Part 2	11 min read
AUG 04	Understanding Bitcoin Privacy with OXT — Part 1	10 min read

Sign up

Powered by Ghost

Subscribe