Coinjoin Workshop

#798768
Zitadelle 2023, Österreich

Agenda

- Crash course
  - Surveillance & Heuristics
  - Best Practices

- Demo

Goals

- Basic understanding of **surveillance mechanisms**

- Basic understanding of **counter measures**

- Form the **foundation** for **further self-study**

- Non-goals
  - Expert knowledge
  - Side chains, anonymity set, dust attacks, timing correlations, taproot, etc.

Who of you has your cell phone turned off?

...

Cross check

Please, turn it off now.

What is Privacy

- **Fundamental** right
- Highly **individual**
- Self-determination
- **Requirement** for a **healthy** and **functioning society**

Bitcoin and Privacy

- **Open** and **transparent** append-only log
- **Not anonymous**, “pseudonymous” at best
- **Your privacy** depends **entirely on your usage**
  - As with security: depends on your threat model

Bitcoin and Privacy

- Surveillance & Heuristics
  - “Chain analysis”
- Best practices

Surveillance & Heuristics

- **Large-scale surveillance** of the bitcoin ecosystem **through data mining**
  - Gathering metadata
  - Wallet **clustering**
  - Traffic analysis (e.g. on public block explorers)
  - Communication eavesdropping (through third parties, e.g. electrum servers)

- **State “sponsored”** industry (by law)
  - Chainalysis, Scorechain, Ciphertrace, GraphSense, etc.

- Heuristics are **probabilistic**: they cannot offer certainty

Surveillance & Heuristics

- Common-input-ownership
- Change address detection
  - Address reuse
  - Unnecessary input heuristic
  - Round amounts heuristic
  - Script type heuristic
  - Exact payment amounts (no change)
- ~~Time-based cluster analysis~~
- ~~Wallet fingerprinting~~

Common-input-ownership

- **Assumption**: All inputs of a transaction are owned by the same entity
- Fundamental **core heuristic**
- **Clustering** of addresses
- Broken by: CoinJoin, PayJoin, Dual-Funded Channel, etc.
  - e.g. First Dual-Funded Channel: https://blockstream.info/tx/91538cbc4aca767cb77aa0690c2a6e710e095c8eb6d8f73d53a3a29682cb7581

Change address detection

- **Assumption**: Change-output can be detected and belongs to the initiating entity
- Set of fundamental **core heuristics**
- **Clustering** of addresses
- “Detection”:
  - “Easy” when address is reused
  - Unnecessary input heuristic
  - Decimal places of outputs
  - Script type heuristics
  - Round amounts heuristic (in sats or fiat)
- Broken by:
  - Change avoidance
  - Multiple change-outputs

Address reuse

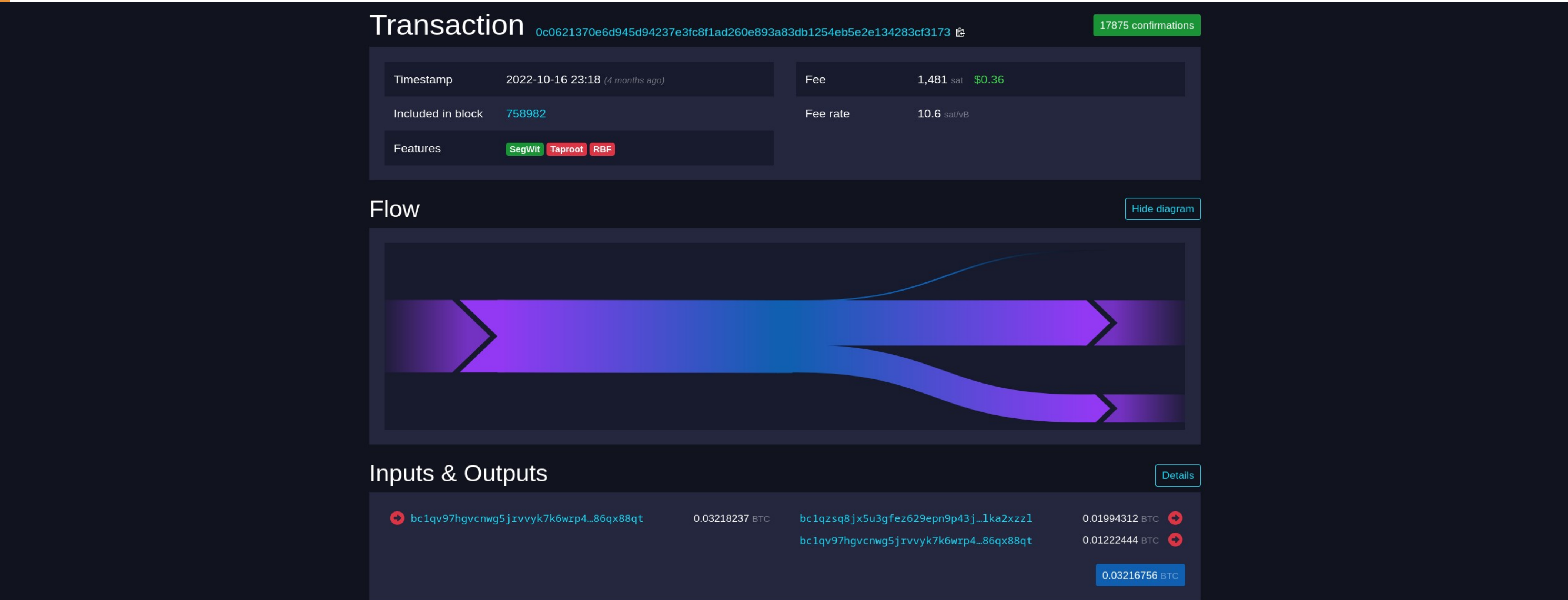
- “**Assumption**” (de facto): Same address controlled by same entity

- Should be **avoided**
  - **Do not hand out** addresses multiple times
  - **Do not send** to already used addresses
  - hint: Can be forced

- (theoretically) broken by:
  - Passing private keys **¯_(ツ)_/¯**
  - Multiple keys can derive same address **¯_(ツ)_/¯**

Address reuse

- 0c0621370e6d945d94237e3fc8f1ad260e893a83db1254eb5e2e134283cf3173



Transaction 0c0621370e6d945d94237e3fc8f1ad260e893a83db1254eb5e2e134283cf3173

17875 confirmations

Timestamp	2022-10-16 23:18 *(4 months ago)*	Fee	1,481 sat $0.36
Included in block	758982	Fee rate	10.6 sat/vB
Features	SegWit ~~Taproot~~ ~~RBF~~		

Flow

Inputs & Outputs

bc1qv97hgvcnwg5jrvvyk7k6wrp4…86qx88qt	0.03218237 BTC	bc1qzsq8jx5u3gfez629epn9p43j…lka2xzzl	0.01994312 BTC
		bc1qv97hgvcnwg5jrvvyk7k6wrp4…86qx88qt	0.01222444 BTC

0.03216756 BTC

Unnecessary input heuristic

- **Assumption**: What need not be spent, stays

- Also called “Optimal change heuristic”
  - **flags the smallest output** as a change address if it is smaller than the smallest input

- Example:

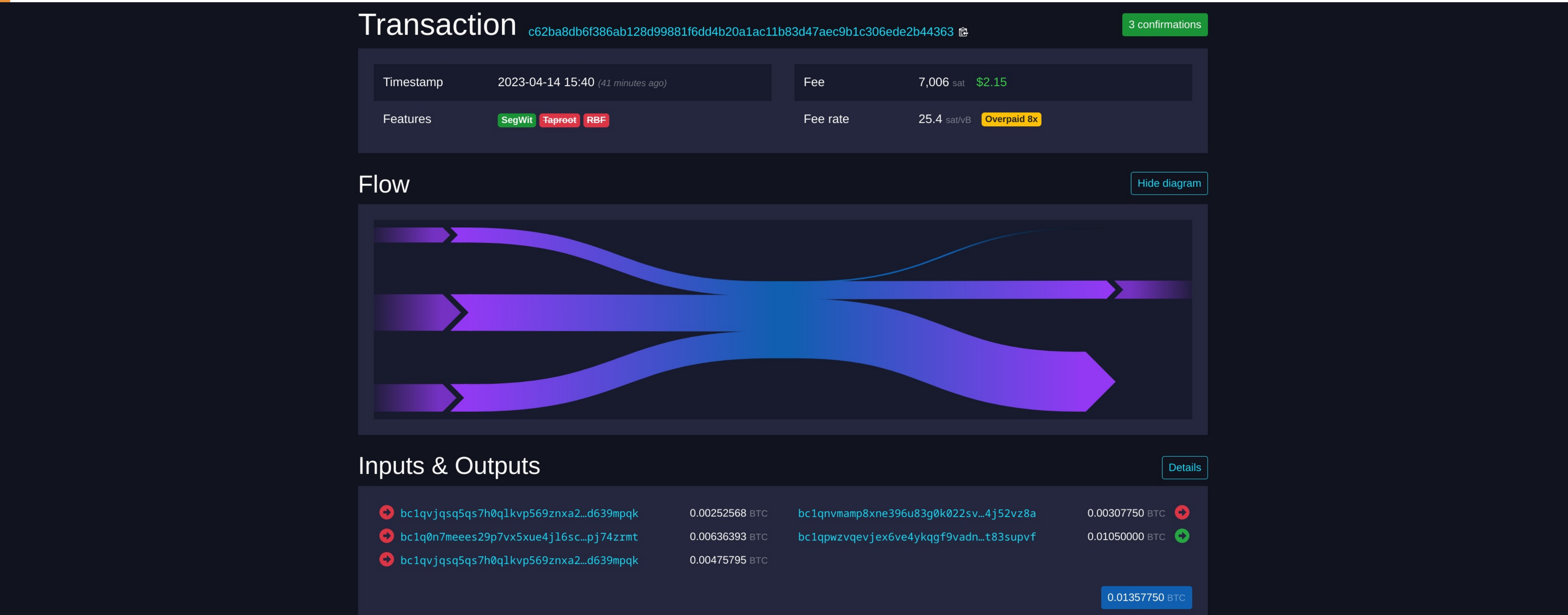
```
In:                 Out:
A (2 btc)  -->  X (4 btc)
A (3 btc)       Y (1 btc)
```

  - Question: Change?

- Broken by:
  - **Add more inputs** until the change output is higher than any input
  - Wallets with coin selection algorithms that **adds unnecessary inputs** (note: can be marked as “abnormal”)

Unnecessary input heuristic

- 49e3e113b43c80a6828510d070872adca5a9549207f998e03f37625df8d0cabe



Transaction c62ba8db6f386ab128d99881f6dd4b20a1ac11b83d47aec9b1c306ede2b44363

Timestamp	2023-04-14 15:40 *(41 minutes ago)*	Fee	7,006 sat $2.15
Features	SegWit ~~Taproot~~ RBF	Fee rate	25.4 sat/vB Overpaid 8x

Flow

Inputs & Outputs

bc1qvjqsq5qs7h0qlkvp569znxa2…d639mpqk	0.00252568 BTC	bc1qnvmamp8xne396u83g0k022sv…4j52vz8a	0.00307750 BTC
bc1q0n7meees29p7vx5xue4jl6sc…pj74zrmt	0.00636393 BTC	bc1qpwzvqevjex6ve4ykqgf9vadn…t83supvf	0.01050000 BTC
bc1qvjqsq5qs7h0qlkvp569znxa2…d639mpqk	0.00475795 BTC		

0.01357750 BTC

Round amounts heuristic

- **Assumption**: Round number outputs are payments

- **Round outputs** as well as **in bitcoin** as **in fiat** (e.g. USD, EUR, etc.)

- Example:

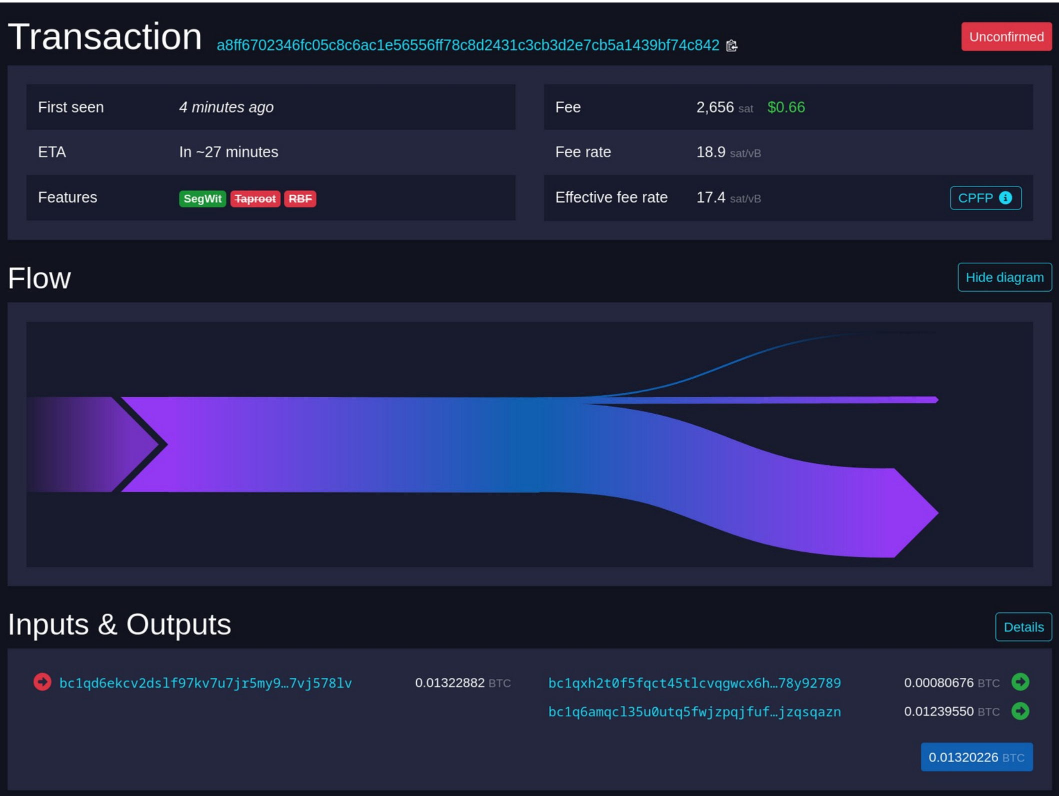
```
In:                         Out:
A (1.11838477 btc) --> X (0.31838477 btc)
                            Y (0.8 btc)
```

  - Question: Change?

- Broken by:
  - Out-of-band payment (e.g. on-chain + lightning)
  - Sometimes clashes with “Optimal change heuristic”
    - (e.g. 2 in + 2 out, but smaller output is round amount in fiat)

Round amounts heuristic

- a8ff6702346fc05c8c6ac1e56556ff78c8d2431c3cb3d2e7cb5a1439bf74c842



Transaction a8ff6702346fc05c8c6ac1e56556ff78c8d2431c3cb3d2e7cb5a1439bf74c842

Unconfirmed

First seen	*4 minutes ago*	Fee	2,656 sat $0.66
ETA	In ~27 minutes	Fee rate	18.9 sat/vB
Features	SegWit ~~Taproot~~ RBF	Effective fee rate	17.4 sat/vB CPFP

Flow

Hide diagram

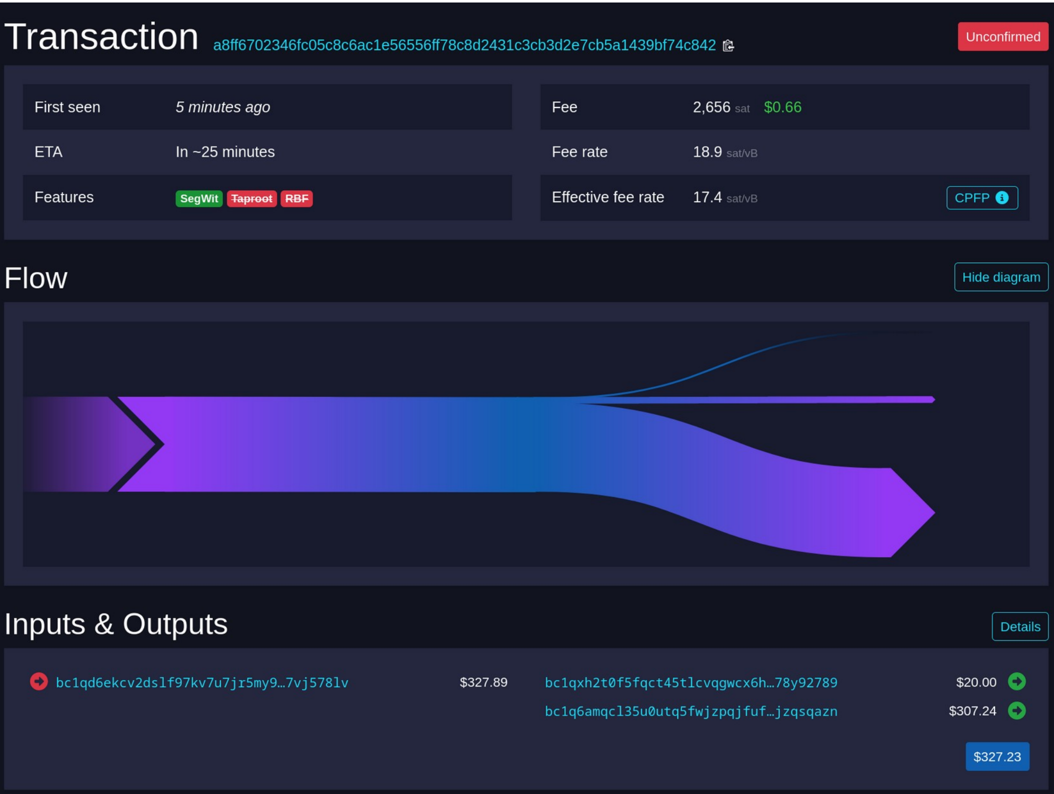
Inputs & Outputs

Details

bc1qd6ekcv2dslf97kv7u7jr5my9…7vj578lv	0.01322882 BTC	bc1qxh2t0f5fqct45tlcvqgwcx6h…78y92789	0.00080676 BTC
		bc1q6amqcl35u0utq5fwjzpqjfuf…jzqsqazn	0.01239550 BTC
			0.01320226 BTC

Round amounts heuristic

- a8ff6702346fc05c8c6ac1e56556ff78c8d2431c3cb3d2e7cb5a1439bf74c842



Transaction a8ff6702346fc05c8c6ac1e56556ff78c8d2431c3cb3d2e7cb5a1439bf74c842

Unconfirmed

First seen	*5 minutes ago*	Fee	2,656 sat $0.66
ETA	In ~25 minutes	Fee rate	18.9 sat/vB
Features	SegWit ~~Taproot~~ RBF	Effective fee rate	17.4 sat/vB CPFP

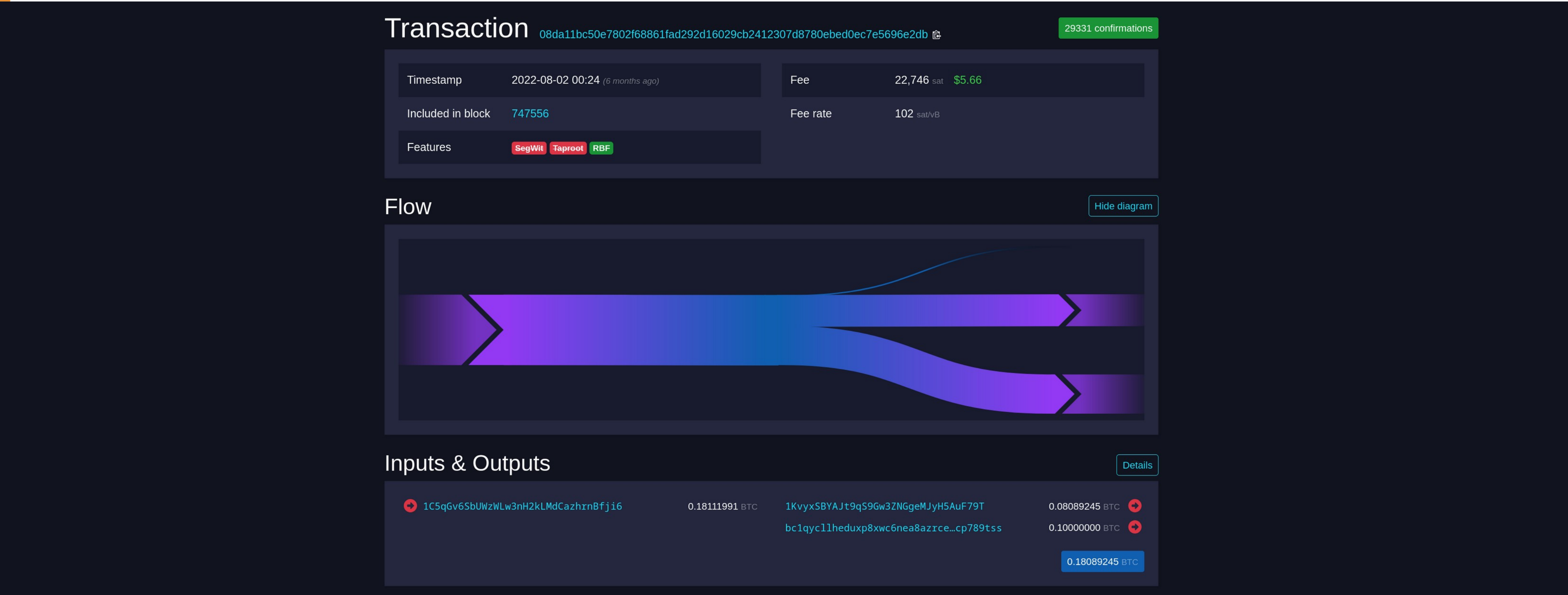
Flow

Inputs & Outputs

bc1qd6ekcv2dslf97kv7u7jr5my9…7vj578lv	$327.89	bc1qxh2t0f5fqct45tlcvqgwcx6h…78y92789	$20.00
		bc1q6amqcl35u0utq5fwjzpqjfuf…jzqsqazn	$307.24
			$327.23

Round amounts heuristic

- 08da11bc50e7802f68861fad292d16029cb2412307d8780ebed0ec7e5696e2db



Transaction 08da11bc50e7802f68861fad292d16029cb2412307d8780ebed0ec7e5696e2db

29331 confirmations

Timestamp	2022-08-02 00:24 *(6 months ago)*	Fee	22,746 sat $5.66
Included in block	747556	Fee rate	102 sat/vB
Features	~~SegWit~~ ~~Taproot~~ RBF		

Flow

Inputs & Outputs

1C5qGv6SbUWzWLw3nH2kLMdCazhrnBfji6	0.18111991 BTC	1KvyxSBYAJt9qS9Gw3ZNGgeMJyH5AuF79T	0.08089245 BTC
		bc1qycllheduxp8xwc6nea8azrce…cp789tss	0.10000000 BTC
			0.18089245 BTC

Script Type Heuristic

- **Assumption**: Change address is of same script type as inputs

- Example:

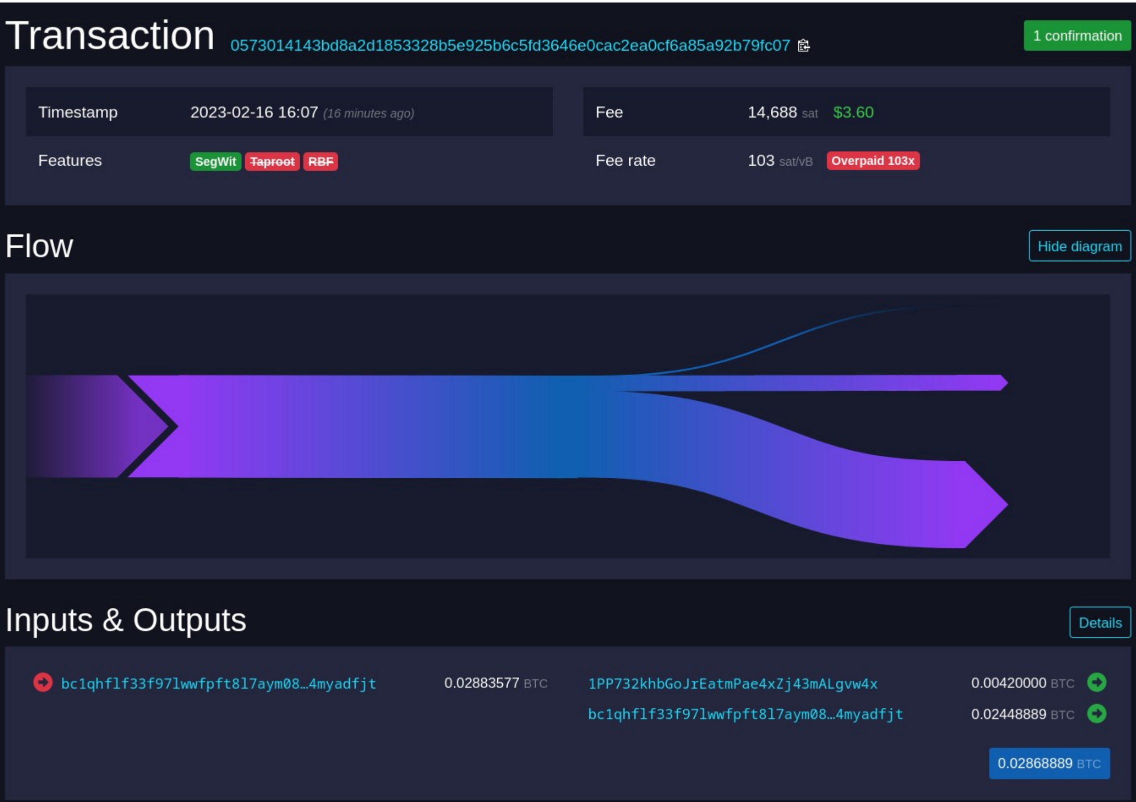
```
In:                    Out:
A (“bc1q..”) --> X (“bc1q..”)
                       Y (“3..”)
```

  - Question: Change?

- Broken by:
  - Self-spend to different script type (e.g. change-output)
  - Wallets using multiple script types ¯_(ツ)_/¯

Script Type Heuristic

- 0573014143bd8a2d1853328b5e925b6c5fd3646e0cac2ea0cf6a85a92b79fc07



Transaction 0573014143bd8a2d1853328b5e925b6c5fd3646e0cac2ea0cf6a85a92b79fc07

Timestamp	2023-02-16 16:07 *(16 minutes ago)*	Fee	14,688 sat $3.60
Features	SegWit ~~Taproot~~ ~~RBF~~	Fee rate	103 sat/vB Overpaid 103x

Flow

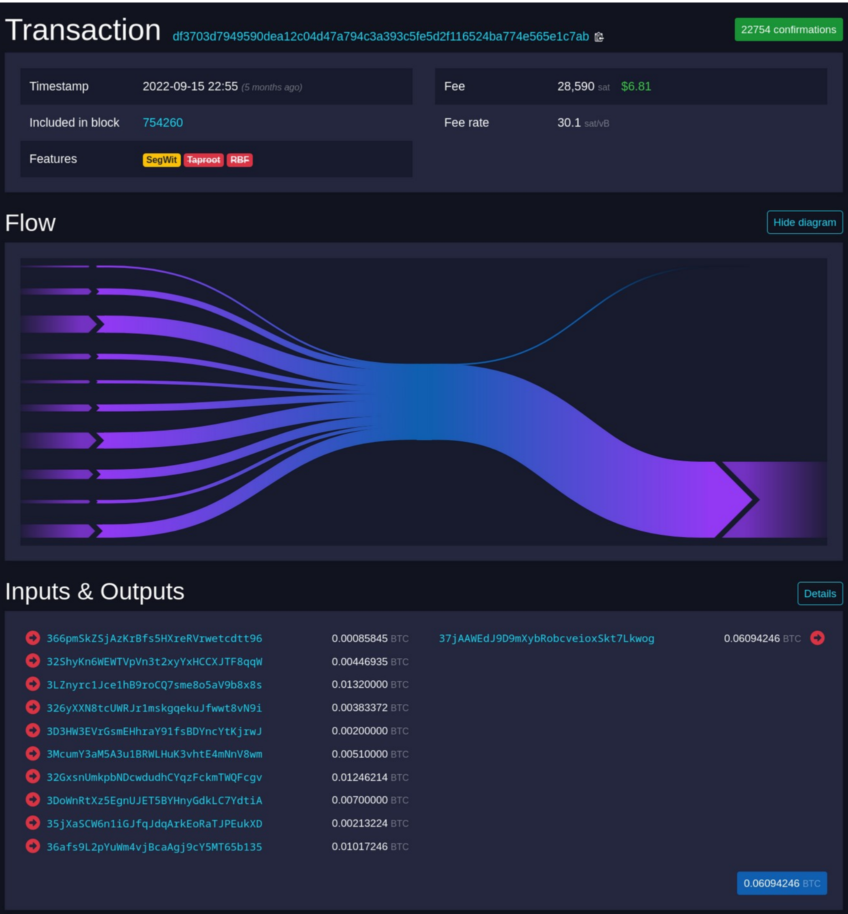
Inputs & Outputs

bc1qhflf33f97lwwfpft8l7aym08…4myadfjt	0.02883577 BTC	1PP732khbGoJrEatmPae4xZj43mALgvw4x	0.00420000 BTC
		bc1qhflf33f97lwwfpft8l7aym08…4myadfjt	0.02448889 BTC
			0.02868889 BTC

Exact payment amounts (no change)

- **Assumption**: coins still controlled by same entity
- **Unlikely** that an output **exactly matches** spending amount
- Possibly **input consolidation** or switching to **new wallet**
- However: **Switching transaction structure** afterwards **reverses assumption**
  - e.g. from “normal payments” to “batching transactions”
- Broken by:
  - Out-of-band payment (e.g. on-chain + lightning)
  - Consolidate to multiple outputs

Exact payment amounts (no change)



Transaction df3703d7949590dea12c04d47a794c3a393c5fe5d2f116524ba774e565e1c7ab

Timestamp	2022-09-15 22:55 *(5 months ago)*	Fee	28,590 sat $6.81
Included in block	754260	Fee rate	30.1 sat/vB
Features	SegWit ~~Taproot~~ ~~RBF~~		

Flow

Inputs & Outputs

366pmSkZSjAzKrBfs5HXreRVrwetcdtt96	0.00085845 BTC	37jAAWEdJ9D9mXybRobcveioxSkt7Lkwog	0.06094246 BTC
32ShyKn6WEWTVpVn3t2xyYxHCCXJTF8qqW	0.00446935 BTC		
3LZnyrc1Jce1hB9roCQ7sme8o5aV9b8x8s	0.01320000 BTC		
326yXXN8tcUWRJr1mskgqekuJfwwt8vN9i	0.00383372 BTC		
3D3HW3EVrGsmEHhraY91fsBDYncYtKjrwJ	0.00200000 BTC		
3McumY3aM5A3u1BRWLHuK3vhtE4mNnV8wm	0.00510000 BTC		
32GxsnUmkpbNDcwdudhCYqzFckmTWQFcgv	0.01246214 BTC		
3DoWnRtXz5EgnUJET5BYHnyGdkLC7YdtiA	0.00700000 BTC		
35jXaSCW6n1iGJfqJdqArkEoRaTJPEukXD	0.00213224 BTC		
36afs9L2pYuWm4vjBcaAgj9cY5MT65b135	0.01017246 BTC		
			0.06094246 BTC

Wallet fingerprinting

- Goal: Figure out **which wallet** software an entity is using
- Transaction construction analysis of clustered addresses
- Input/Output order
  - BIP69: Lexicographical Indexing of Transaction Inputs and Outputs
- Fee estimates
- Coin selection
- etc.

Surveillance & Heuristics

- Conclusion
  - **Know** your threat vectors
  - On-chain analysis **cannot be avoided**
  - Heuristics are **probabilistic**
    - Inherently flawed
    - Can be mitigated/broken

Best practices

- **Self-custody** your coins
- **Do not reuse** addresses
- **Run your own node**
  - **Avoid** public block explorers
- **Minimize** exposure to KYC/third parties
- Use the **Lightning Network**
- Use **Coin Control**
- **CoinJoin** early and often

Self-custody

- Single **most important step**

- “**Not your keys, not your coins**”

- Failure to do so, means you **disclose by default**:
  - amounts
  - timestamps
  - history and future of all your transactions
  - lots and lots of metadata

Run your own node

- **Essential** if you want to preserve privacy

- Information remains under **your control**
  - Otherwise, someone other knows your every move
  - Avoiding public block explorers
    - Source of information for surveillance companies

- **“Not your node, not your rules**”

- **Not:** Do you run a node? But: **How many** nodes do you run?

Do not reuse addresses

- Links to previous transactions

- Bad for privacy of receiver **and** sender

- Never a “change” output
  - See “change detection heuristic”

Minimize exposure to KYC/third parties

- “Trusted third parties are **security holes**”
  - Nick Szabo (2001)

- **Trusting someone else** with your **personal** data

- Mostly **negative** impacts for the **general public**
  - Data will be lost eventually
  - Criminals will always find a way

- Links your **real identity** to your funds
  - Root of all future surveillance mechanisms

Use the Lightning Network

- Increases **transactional privacy**
  - Onion routed; multi-hop; “peer-to-peer”
- **No public record** of individual payments
- **Strong privacy guarantees**; especially for sender
- Hints
  - Purpose of LN is **quick settlements**, **not privacy**
  - Still has On-chain footprints
  - Private channels → Unannounced channels
  - custodial vs. non-custodial (hint: WoS anyone?)

Use Coin Control

- Feature of most wallets
  - aka “UTXO management”
- Mark individual UTXOs for usage in Coin Selection
- Pre/Post-Transaction privacy
- Label your outputs

CoinJoin early and often

- **Construction** of transactions

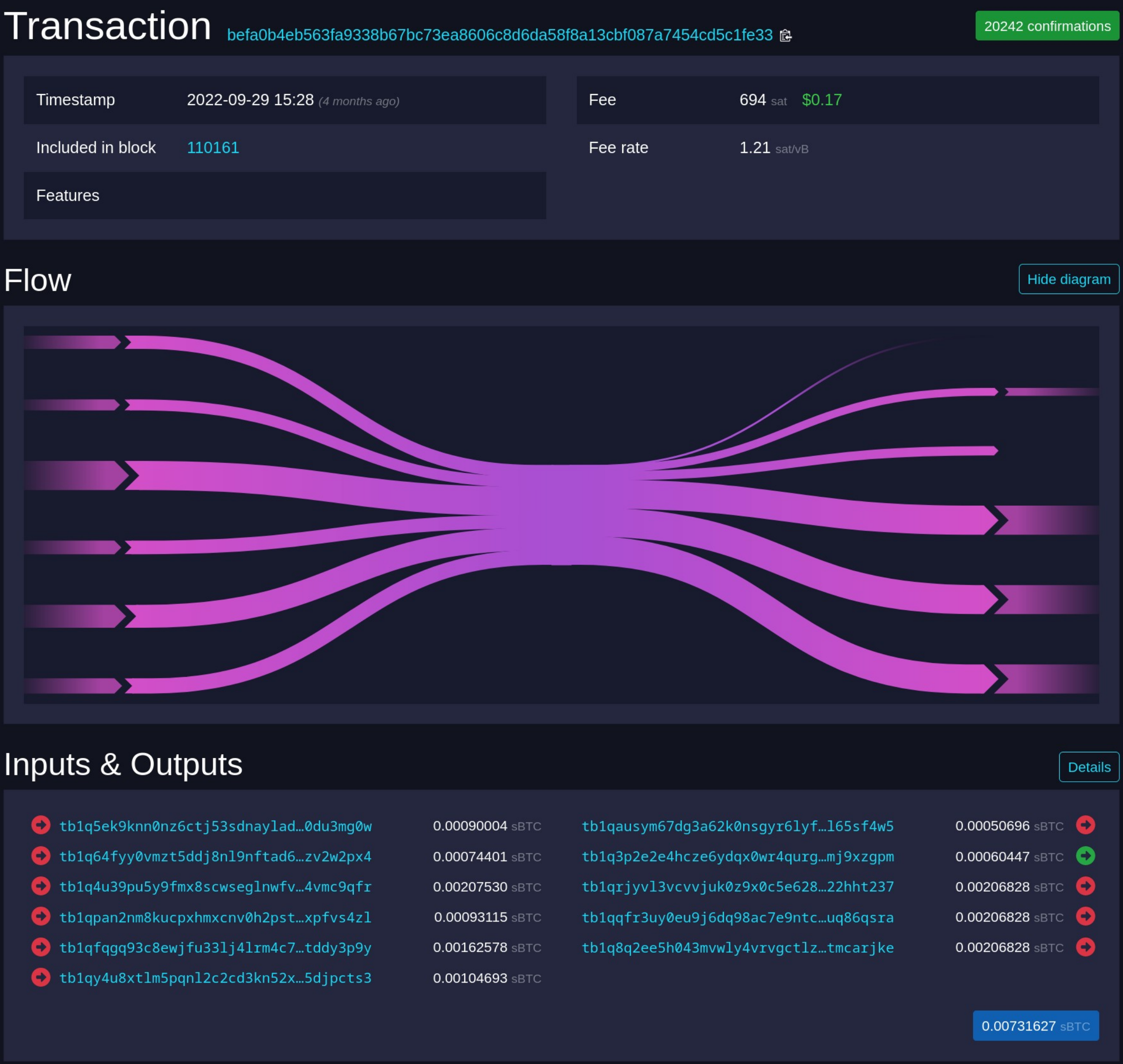
- **Collaboration** between **multiple parties**

- **Breaks** common-input-ownership heuristic

- Multiple implementations
  - Wasabi, Samourai, JoinMarket, etc.

CoinJoin early and often

- Fun fact: Technically, **every transaction is a CoinJoin**
  - Special: transaction with exactly one input
- PayJoin
- Considerations
  - There are **fees** involved with CoinJoins
  - Spending **habits after joins** are very **important**



Transaction befa0b4eb563fa9338b67bc73ea8606c8d6da58f8a13cbf087a7454cd5c1fe33

20242 confirmations

Timestamp	2022-09-29 15:28 *(4 months ago)*	Fee	694 sat $0.17
Included in block	110161	Fee rate	1.21 sat/vB
Features			

Flow

Inputs & Outputs

tb1q5ek9knn0nz6ctj53sdnaylad…0du3mg0w	0.00090004 sBTC	tb1qausym67dg3a62k0nsgyr6lyf…165sf4w5	0.00050696 sBTC
tb1q64fyy0vmzt5ddj8nl9nftad6…zv2w2px4	0.00074401 sBTC	tb1q3p2e2e4hcze6ydqx0wr4qurg…mj9xzgpm	0.00060447 sBTC
tb1q4u39pu5y9fmx8scwseglnwfv…4vmc9qfr	0.00207530 sBTC	tb1qrjyvl3vcvvjuk0z9x0c5e628…22hht237	0.00206828 sBTC
tb1qpan2nm8kucpxhmxcnv0h2pst…xpfvs4zl	0.00093115 sBTC	tb1qqfr3uy0eu9j6dq98ac7e9ntc…uq86qsra	0.00206828 sBTC
tb1qfqgq93c8ewjfu33lj4lrm4c7…tddy3p9y	0.00162578 sBTC	tb1q8q2ee5h043mvwly4vrvgctlz…tmcarjke	0.00206828 sBTC
tb1qy4u8xtlm5pqnl2c2cd3kn52x…5djpcts3	0.00104693 sBTC		

0.00731627 sBTC

Demo

Questions & Answers

- Run your own node.
- Stay humble, stack sats.
- Fix the money, fix the world.