

Tracing Transactions Across Cryptocurrency Ledgers

Haaroon Yousaf, George Kappos and Sarah Meiklejohn

University College London

Bitcoin and anonymity

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Bitcoin and anonymity

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

“...privacy can still be maintained by breaking the flow of information ... keeping public keys anonymous”

“ if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner”

Anonymity defeated

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage
University of California, San Diego George Mason University[†]

An Analysis of Anonymity in the Bitcoin System

Fergal Reid and Martin Harrigan

Structure and Anonymity of the Bitcoin Transaction Graph

Micha Ober^{1,2}, Stefan Katzenbeisser^{1,*} and Kay Hamacher^{1,2,3,*}

The Unreasonable Effectiveness of Address Clustering

Martin Harrigan^{*1} and Christoph Fretter²

Deanonymisation of clients in Bitcoin P2P network

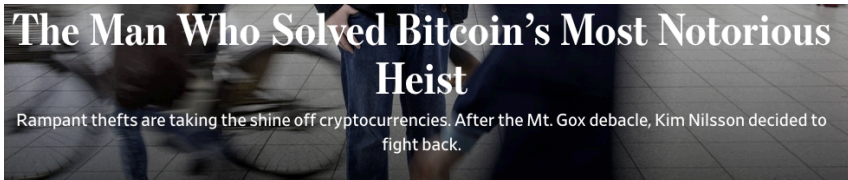
Alex Biryukov
University of Luxembourg
alex.biryukov@uni.lu

Dmitry Khovratovich
University of Luxembourg
dmitry.khovratovich@uni.lu

Ivan Pustogarov
University of Luxembourg
ivan.pustogarov@uni.lu

¹Waterford Institute of Technology
²Elliptic Enterprises Limited, London

On-chain tracking



Kim Nilsson in his Tokyo neighborhood. SHIHO FUKADA FOR THE WALL STREET JOURNAL

By [Justin Scheck](#) and [Bradley Hope](#)

An Empirical Analysis of Anonymity in Zcash

George Kappos, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn
University College London

USENIX Security 2018



Someone moves \$8 million in Bitcoins (BTC) stolen from Binance

CRYPTOS | Jul 09, 10:49 GMT



Malte Möser*, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, and Nicolas Christin

An Empirical Analysis of Traceability in the Monero Blockchain

Privacy Enhancing Technologies 2018

Cross-currency tracking?

How Dirty Money Disappears Into the Black Hole of Cryptocurrency

Journal investigation documents suspicious trades through venture capital-backed ShapeShift

By *Justin Scheck* and *Shane Shifflett*

Sept. 28, 2018 11:49 am ET

WannaCry Hackers Are Using This Swiss Company To Launder \$142,000 Bitcoin Ransoms



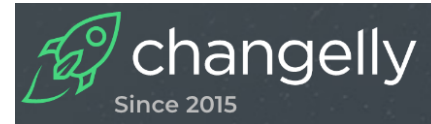
Thomas Brewster Forbes Staff

Security

I cover crime, privacy and security in digital and physical forms.

Cross-currency trading

- ShapeShift (Aug '14), Changelly ('13)
- Cross-currency trading service (lightweight exchange)
- Allow users to interchange multiple coins/tokens
- ShapeShift supporting 32 coins (Aug '19)
- Changelly supporting 107 coins (Aug '19)



Why cross trade?


- Non-custodial (Does not require coins in an account)
- Easy to use
- Potential extra anonymity?
- Single rate charge

How to perform a shift?


1

Choose Which Assets to Trade


Deposit



Bitcoin



Receive



Ether

Quick

Precise

Continue



How to perform a shift?

2

1

Choose Which Assets to Trade

Deposit Receive



 Bitcoin  Ether

Quick Precise

Continue

Instant Rate 1 BTC = 50.39434162 ETH

Deposit Min	Deposit Max	Miner Fees
0.00004341 BTC	0.42079856 BTC	0.0011 ETH


 → 

Your Ether Address (destination address)

Your Bitcoin Refund Address

☐ I agree to the Terms and certify that I am the beneficial owner of the input assets and the destination address.

Reusable Address? ☐

 Congratulations! You'll be earning FOX back on this shift.

Start Transaction


User's destination address

How to perform a shift?

1

Choose Which Assets to Trade

Deposit



Bitcoin

Receive



Ether

Quick



Precise

Continue

2


Instant Rate 1 BTC = 50.39434162 ETH

Deposit Min	Deposit Max	Miner Fees
0.00004341 BTC	0.42079856 BTC	0.0011 ETH

☐ I agree to the Terms and certify that I am the beneficial owner of the input assets and the destination address.

Reusable Address? ☐


 Congratulations! You'll be earning FOX back on this shift.

Start Transaction

3


Order ID: d4f6f17f-6854-4b7b-854c-dd9cdd5e7b0c


Bookmark



Send to this address

3Q1R4a5jJPZHG1nrW4qKLYgRBPJd6UTSgo


Send up to this amount: 0.42144551  Bitcoin

Send AT LEAST this amount: 0.00004341  Bitcoin

Rec. Miner Fee (fast processing): 5.6e-7 BTC


Awaiting Exchange

Order Details

 Deposit

Send up to 0.42144551

3Q1R4a5jJPZHG1nrW4qKLYgRBPJd6UTSgo

 Receive

0x811b4737c1122b31fa8b2d55183c0f549e1ca8e5

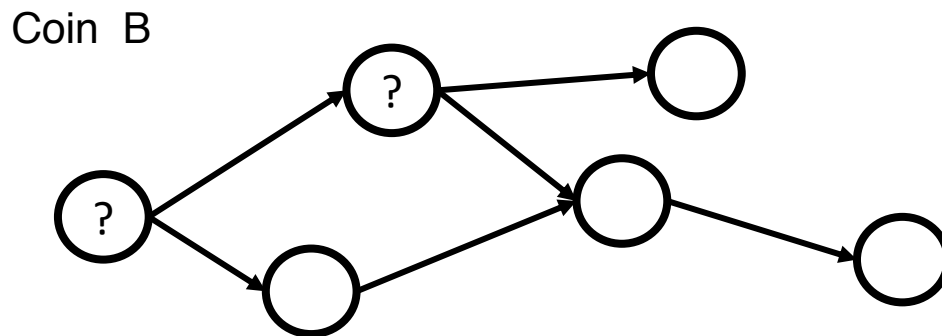
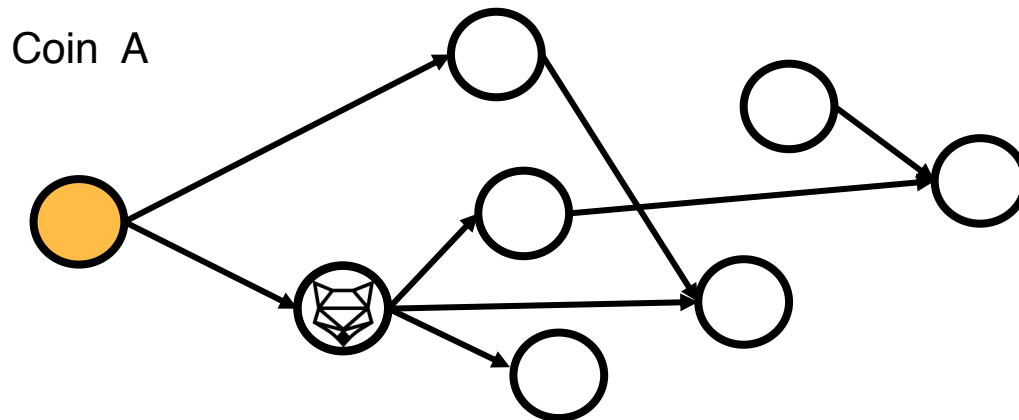
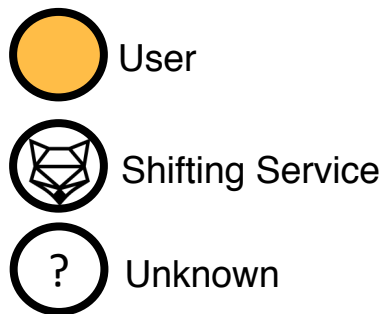
Current Rate

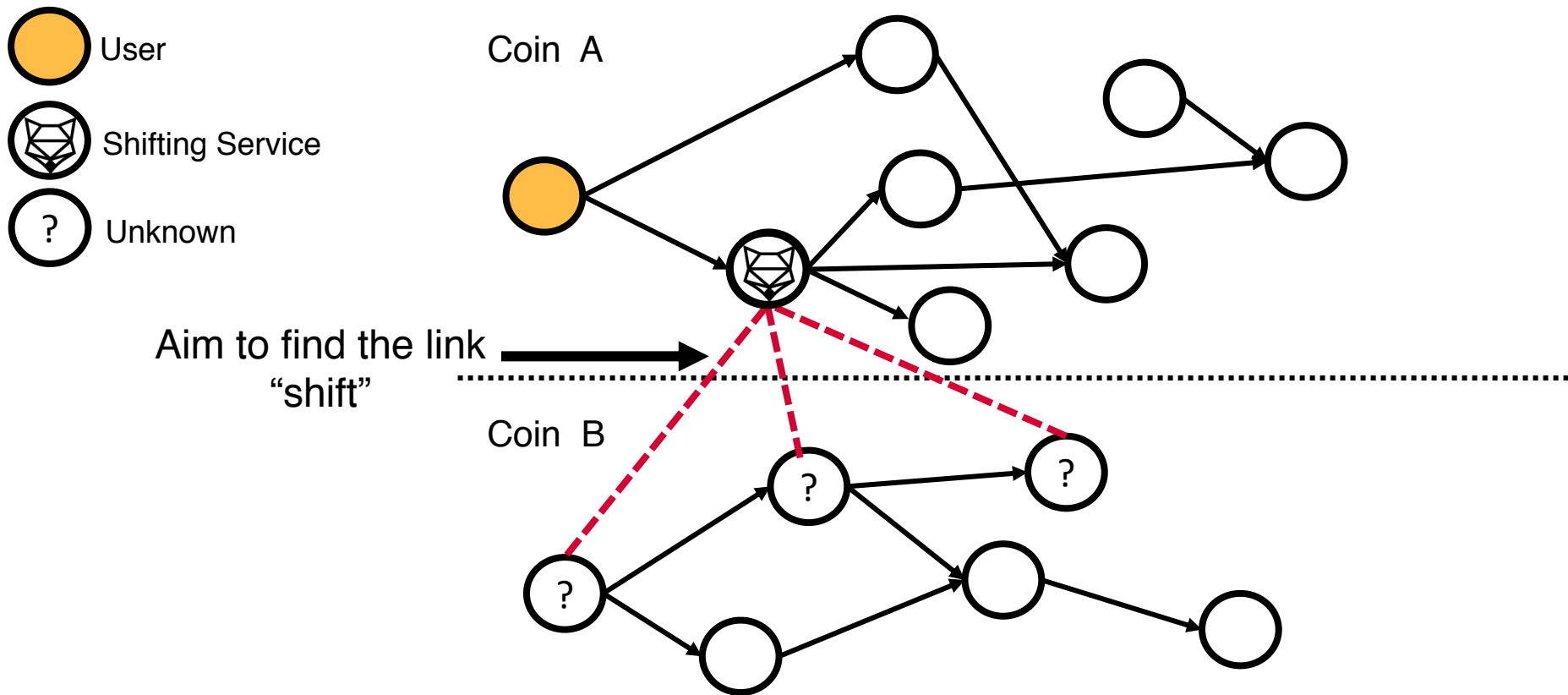
1 BTC = 50.39819179 ETH

Type

Quick

What is cross-chain?





Our contributions

- Blockchain analysis of transactions moving cross-chain
- Created heuristics analysing user behaviours
- Defined a common relationship heuristic identifying major entities (in paper)
- Investigated real world scams which made use of cross-chain transactions (more in paper)
- Analysed how users make use of privacy-coin features

Our contributions

- Blockchain analysis of transactions moving cross-chain
- Created heuristics analysing user behaviours
- Defined a common relationship heuristic identifying major entities (in paper)
- Investigated real world scams which made use of cross-chain transactions (more in paper)
- Analysed how users make use of privacy-coin features

How?

1. Scraped public API for recent transactions

```
0:
  curIn:      "BTC"
  curOut:     "BCH"
  amount:     0.51566669
  timestamp:  1525650476.615
```

<https://shapeshift.io/recenttx>

How?

1. Scraped public API for recent transactions

0:

curIn: "BTC"
curOut: "BCH"
amount: 0.51566669
timestamp: 1525650476.615

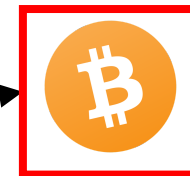
Currency user sent, Input

Currency user wants, Output

Input currency user sent

How?

2. Search and find this input transaction



0:
curIn: "BTC"
curOut: "BCH"
amount: 0.51566669
timestamp: 1525650476.615

34a39ff37b5dc132efc5ede47398b3bd13152e2c2ad464f22776464c3ce1b338

1Q6iXB9ijtFKjpxEyDiB14umZ2X6FZtu15 (0.86487609
 BTC - Output)

→ 1JfZePYHEHkMMThb1uDNC9svbR9PaMIEJn - (Spent)
 0.3491509 BTC

35EgH9XDA2xHhYmuVvU8FYvwZdetFIShs - (Spent)
 0.51566669 BTC
 0.86481759 BTC

Exact value

+/- blocks

Summary

Size	223 (bytes)
Weight	892
Received Time	2018-05-06 23:47:56
Lock Time	Block: 521533

Included In
 Blocks 521534 (2018-05-06 23:50:14 + 2
 minutes)

Inputs and Outputs

Total Input	0.86487609 BTC
Total Output	0.86481759 BTC
Fees	0.0000585 BTC
Fee per byte	26.233 sat/B
Fee per weight unit	6.558 sat/WU
Estimated BTC Transacted	0.3491509 BTC

How?

2. Search and find this input transaction



Summary	
Size	223 (bytes)
Weight	892
Received Time	2018-05-06 23:47:56
Lock Time	Block: 521533
Included In Blocks	521534 (2018-05-06 23:50:14 + 2 minutes)

Inputs and Outputs	
Total Input	0.86487609 BTC
Total Output	0.86481759 BTC
Fees	0.0000585 BTC
Fee per byte	26.233 sat/B
Fee per weight unit	6.558 sat/WU
Estimated BTC Transacted	0.3491509 BTC

How?

3. Confirm this is correct via official API + find the output transaction

<https://shapeshift.io/txstat/<address>>

status: "complete"
 address: "35EgH9XDA2xHhYmuVVrU8FYvwZdetEjSHs"
 withdraw: "13JwaysXv433bqAWdkHiPEFKRHKzYXrtgh"
 incomingCoin: 0.51566669
 incomingType: "BTC"

outgoingCoin: "2.7965838"
 outgoingType: "BCH"
 Transaction:
 "e33779961628f9868cad28c0331a9ccb78f76c90240fc14be1b69075377d82b0"
 transactionURL:
 "<https://explorer.bitcoin.com/bch/tx/e33779961628f9868cad28c0331a9ccb78f76c90240fc14be1b69075377d82b0>"

Output transaction

4c3ce1b338

→ 1JfZePYHEHkMMThb1uDNC9svbR9PaMIEJn - (Spent)
 0.491509 BTC
 35EgH9XDA2xHhYmuVVrU8FYvwZdetEjSHs (Spent)
 0.51566669 BTC

ShapeShift address

0.31759 BTC

How?

3. Confirm this is correct via official API + find the output transaction

```

outgoingCoin: "2.7965838"
outgoingType: "BCH"
Transaction:
"e33779961628f9868cad28c0331a9ccb78f76c90240fc14be1b69075377d82b0"
transactionURL:
"https://explorer.bitcoin.com/bch/tx/e33779961628f9868cad28c0331a9ccb78f76c90240fc14be1b69075377d82b0"
    
```

Output transaction

ShapeShift

Hash

e33779961628f9868cad28c0331a9ccb78f76c90240fc...

qqzcxfu76u47md5ufs6h29kypsr5a... 2.81189142 BCH

Fee

0.00000226 BCH (1.004 sat/B - 225 bytes)

2018-05-07 12:54 AM

qqv4fcu0s5afq9i785ytqkx78ux4x... 2.79658380 BCH

qru0mxurz747ugf3em9cfnrmcelc... 0.01530536 BCH

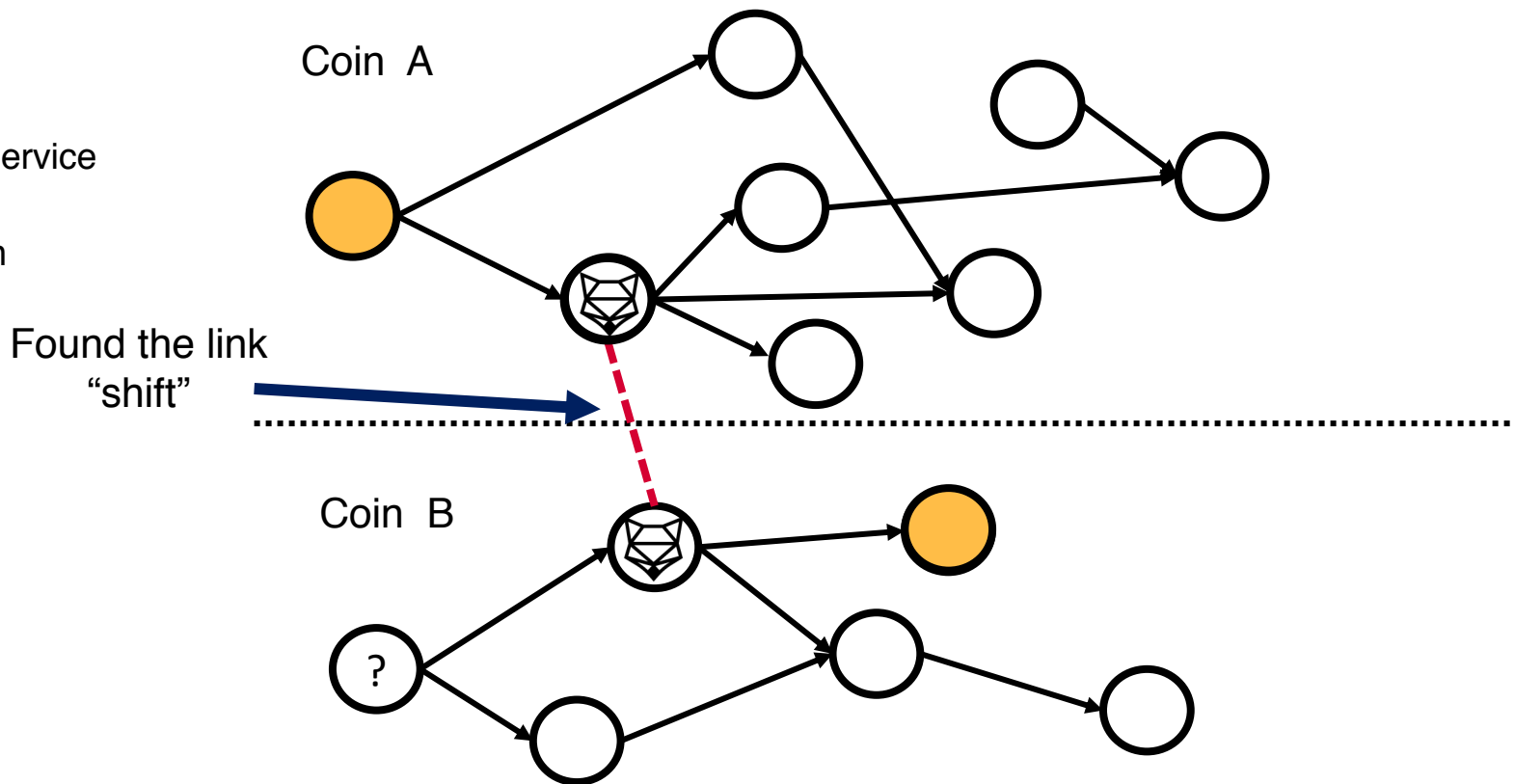
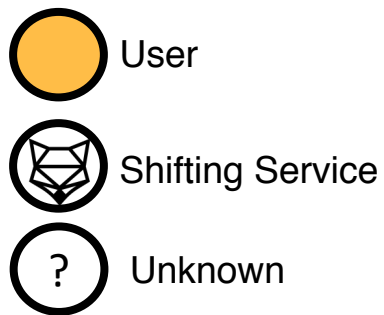
2.81188916 BCH

Recipient

How summary

1. Scrape public API for transactions
2. Search and find the input transaction
3. Confirm this is correct via the API and obtain output transaction

Linked cross-chain



Our contributions

- Blockchain analysis of transactions moving cross-chain
- Created heuristics analysing user behaviours
- Defined a common relationship heuristic identifying major entities (in paper)
- Investigated real world scams which made use of cross-chain transactions (more in paper)
- Analysed how users make use of privacy-coin features

Results

- Scraped ShapeShift public API ~13 months
- 2.8 million shifts total
- Parsed blockchain data from full nodes
- Top 8 currencies - 2.3 million shifts

Currency

Ethereum

Bitcoin

Litecoin

Bitcoin Cash

Dogecoin

Dash

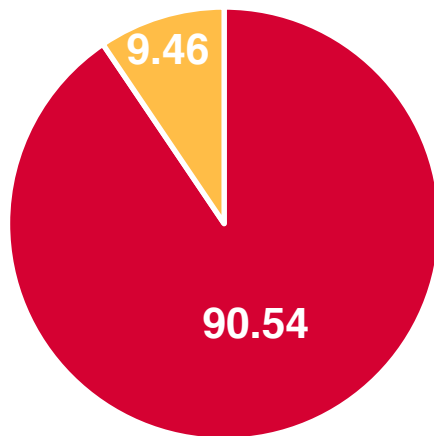
Ethereum Classic

Zcash

Cross-chain activity

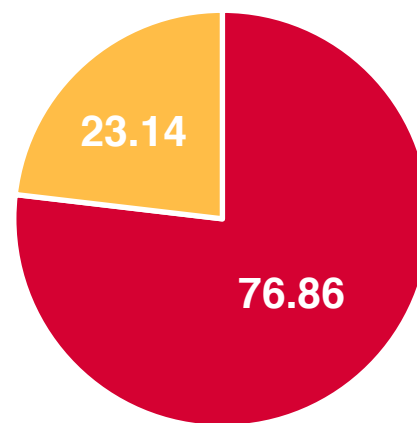
- Traced 1.3M transactions cross-chain
- Corresponding input and output transactions

Best Case (Zcash)



■ Traced ■ Not traced

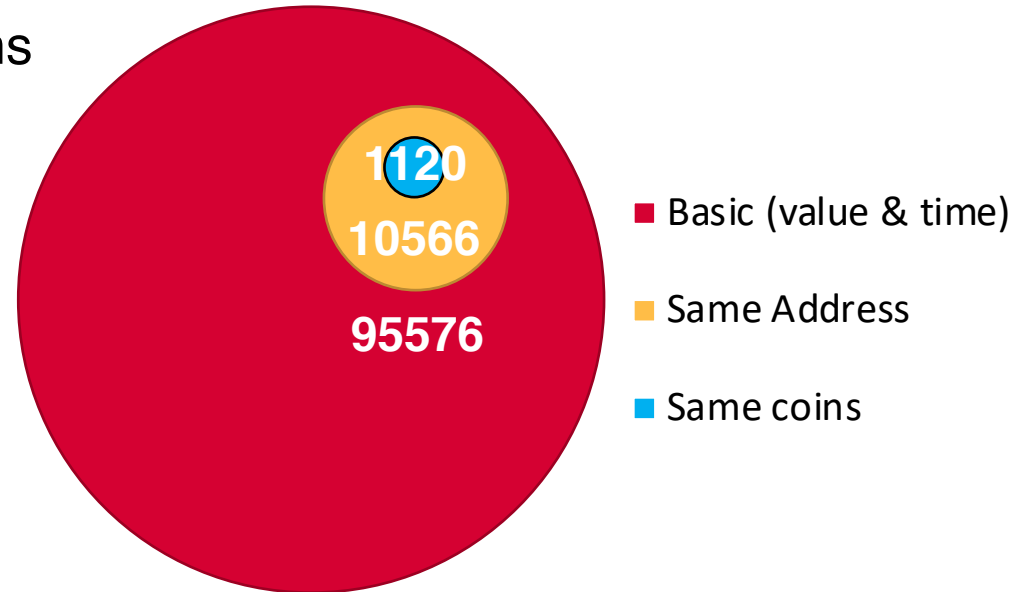
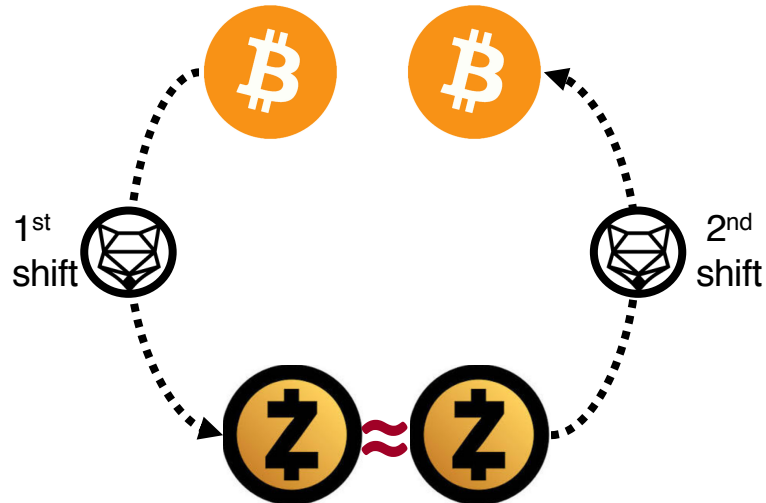
Worst Case (Bitcoin)



■ Traced ■ Not traced

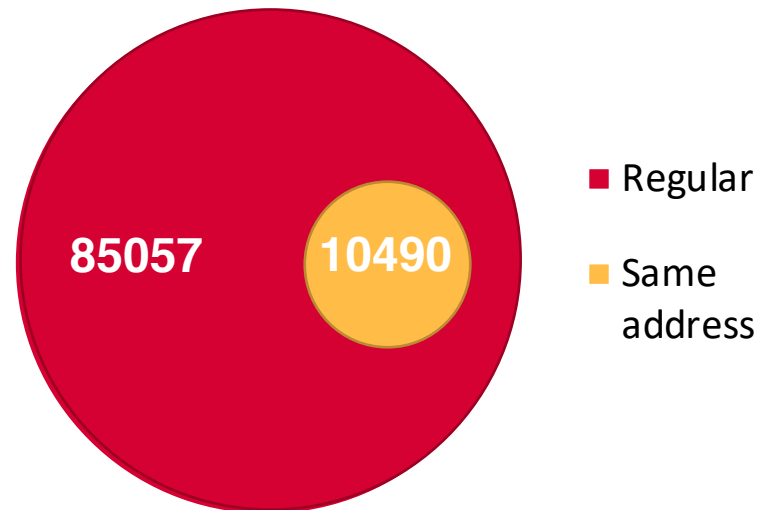
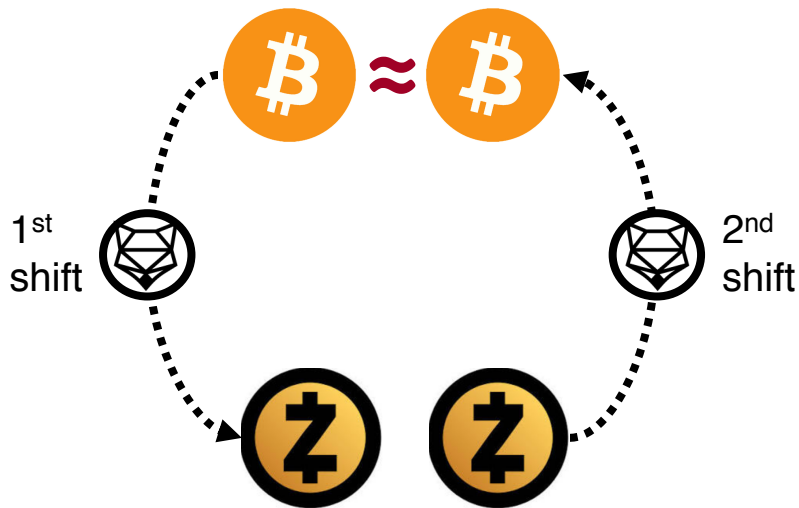
U-turn

- Two shifts, close proximity in time and value
- Use the same coin or address between shift
- Follows movement of user coins



Round-trip

- Two shifts, close proximity in time and value
- 1st shift value similar to 2nd shift or return to the same input address
- Advantage over U-turn: identity of initiator is known

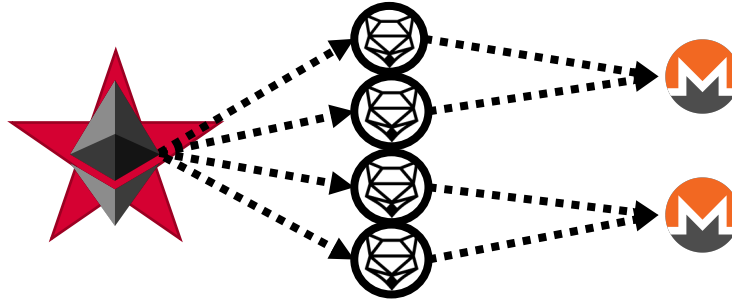


Our contributions

- Blockchain analysis of transactions moving cross-chain
- Created heuristics analysing user behaviours
- Defined a common relationship heuristic identifying major entities (in paper)
- Investigated real world scams which made use of cross-chain transactions (more in paper)
- Analysed how users make use of privacy-coin features

Case study: Starscape Capital Scam

- Investment firm promised **50% return** in cryptocurrency arbitrage fund
- Raised 2000 ETH in January 2018 (2.2M USD)
- **Disappeared**
- 192 transactions (total) – 109 shifted to Monero (465 ETH)
- 2x Monero addresses that received shifted coins



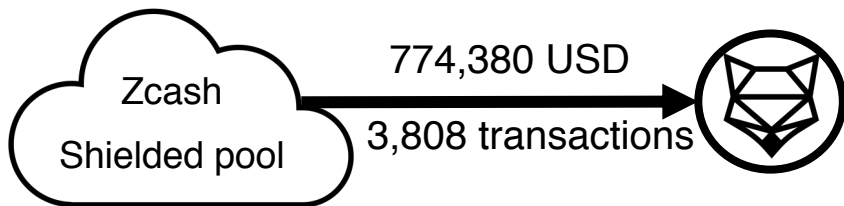
Our contributions

- Blockchain analysis of transactions moving cross-chain
- Created heuristics analysing user behaviours
- Defined a common relationship heuristic identifying major entities (in paper)
- Investigated real world scams which made use of cross-chain transactions (more in paper)
- Analysed how users make use of privacy-coin features

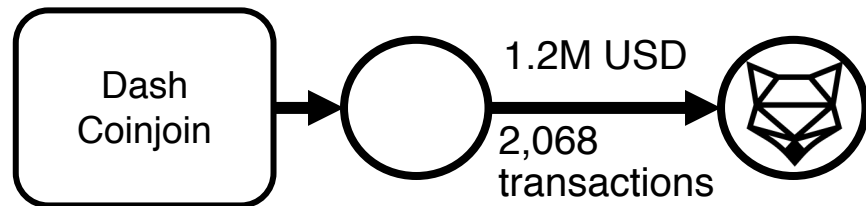
Case study: Anonymity coins

- Zcash: Shielded pool, privacy feature that hides values + address
- Dash: Coinjoin, privacy feature that mixes transactions with other users
- Significant total volume from both of these coins however...

Pool funds sent to ShapeShift



Coinjoin funds sent to ShapeShift



Case study: Anonymity coins

- ...we find usage that does not provide anonymity
- Dash U-turns
 - Same coins - 5.6%
 - Same address - **64.6%**
- Zcash U-turns
 - Same coins - **28.7%**
 - Same address - **54.2%**

Our contributions

- Blockchain analysis of transactions moving cross-chain
- Created heuristics analysing user behaviours
- Defined a common relationship heuristic identifying major entities (in paper)
- Investigated real world scams which made use of cross-chain transactions (more in paper)
- Analysed how users make use of privacy-coin features

THANK YOU QUESTIONS?

Authors are supported by the EU H2020 TITANIUM project under grant agreement number 740558.

