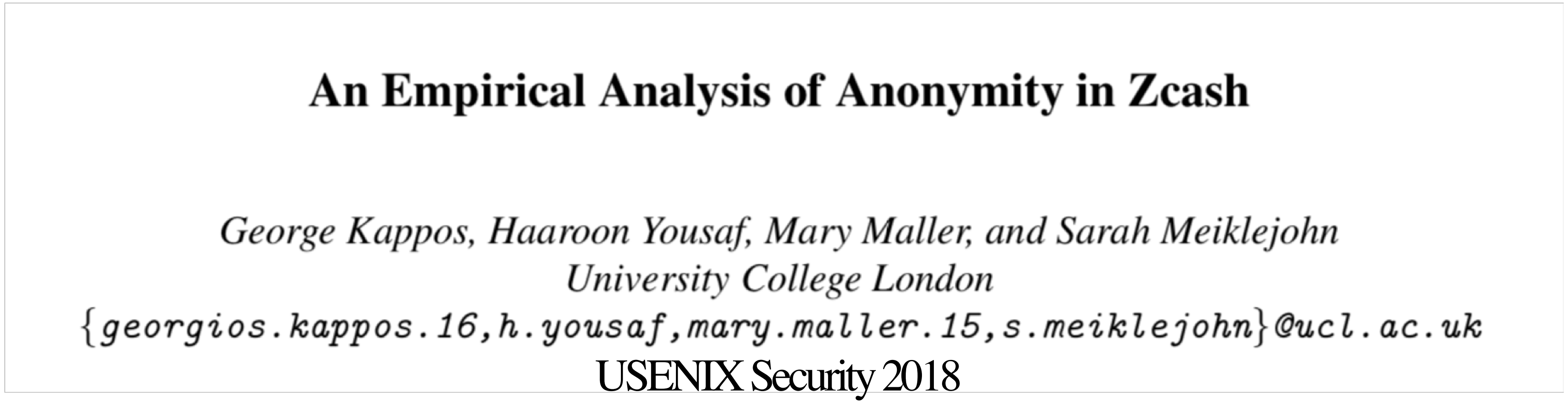


An Empirical Analysis of Anonymity in Zcash

George Kappos, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn
University College London
{georgios.kappos.16,h.yousaf,mary.maller.15,s.meiklejohn}@ucl.ac.uk

USENIX Security 2018

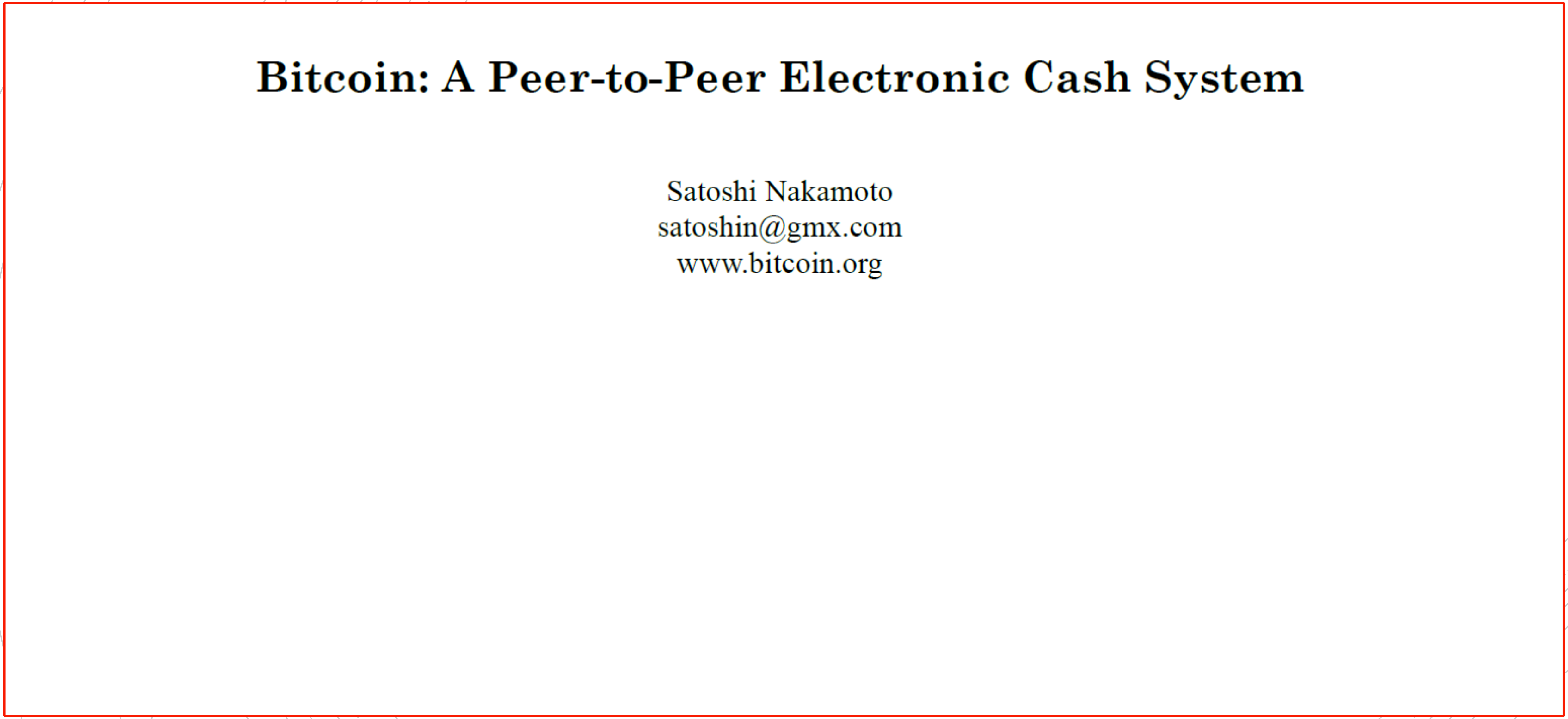
Tracing transactions in Zcash

George Kappos, Haaroon Yousaf

Motivation

- WikiLeaks (2011) Bitcoin is “secure and anonymous…cannot be easily traced back to you”
- Rise in bitcoin anonymity attacks, researchers using practises from graph theory and network analysis to track transactions
- De-anonymising mixing services
- Major tagging and clustering

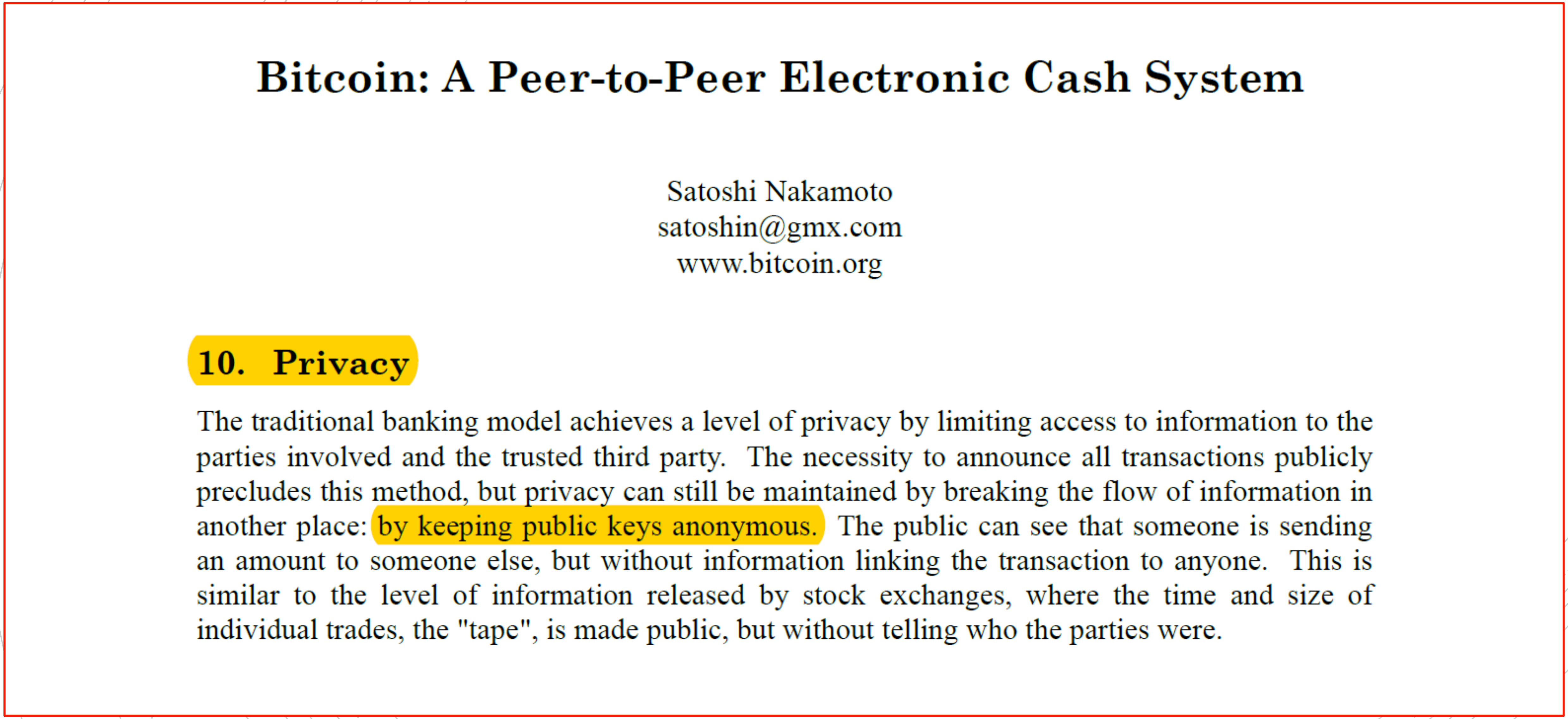
Anonymity(?) in cryptocurrencies



Bitcoin: A Peer-to-Peer Electronic Cash System

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

Anonymity(?) in cryptocurrencies



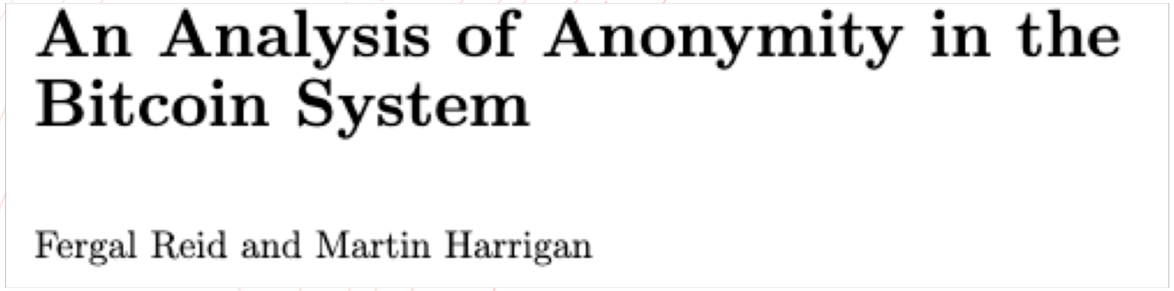
Bitcoin: A Peer-to-Peer Electronic Cash System

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

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

Proved to not be that effective…



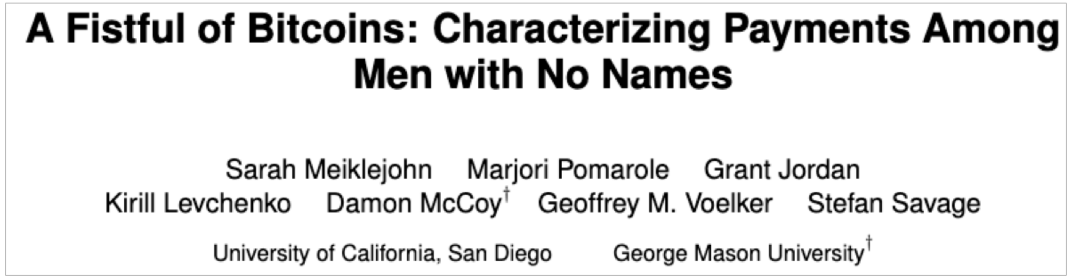
An Analysis of Anonymity in the Bitcoin System

Fergal Reid and Martin Harrigan

Proved to not be that effective…

An Analysis of Anonymity in the Bitcoin System

Fergal Reid and Martin Harrigan



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[†]

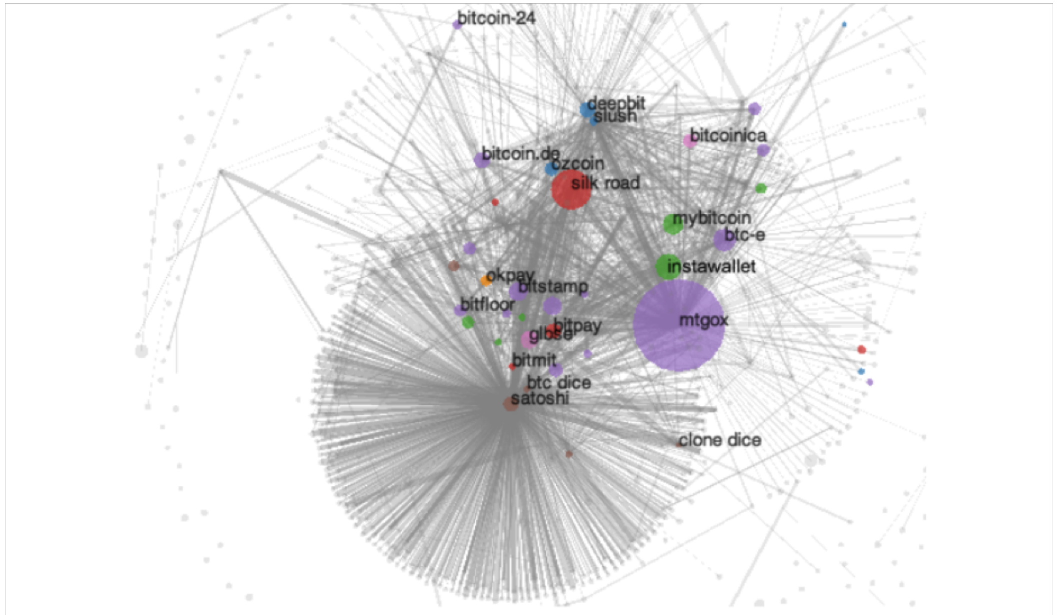
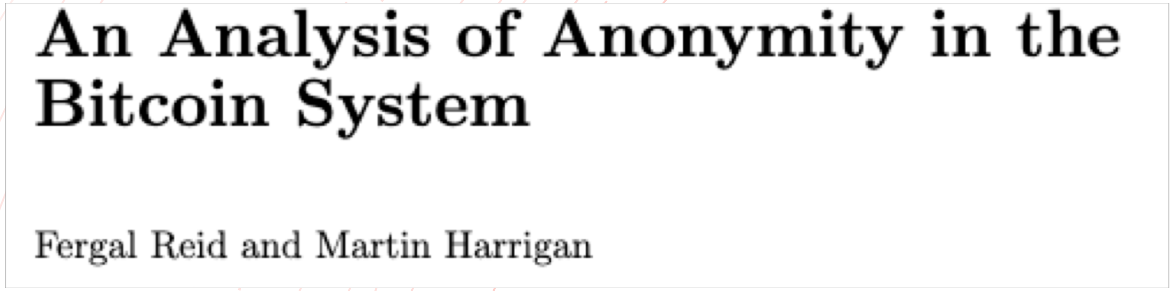


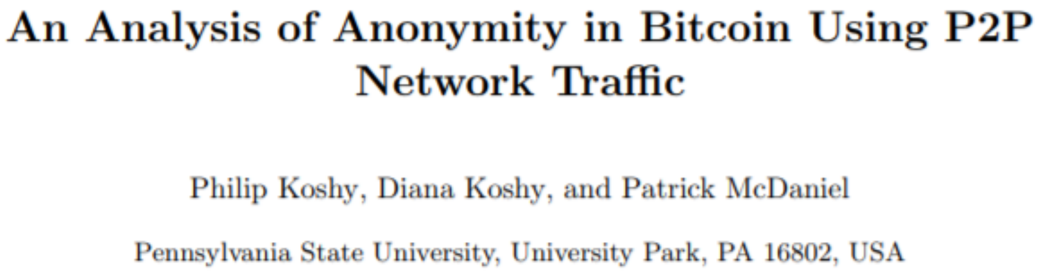
Figure 6: A visualization of the user network. The area of the cluster represents the external incoming value; i.e., the bitcoins received from other clusters but not itself, and for an edge to appear between two nodes there must have been at least 200 transactions between them. The

Proved to not be that effective…



An Analysis of Anonymity in the Bitcoin System

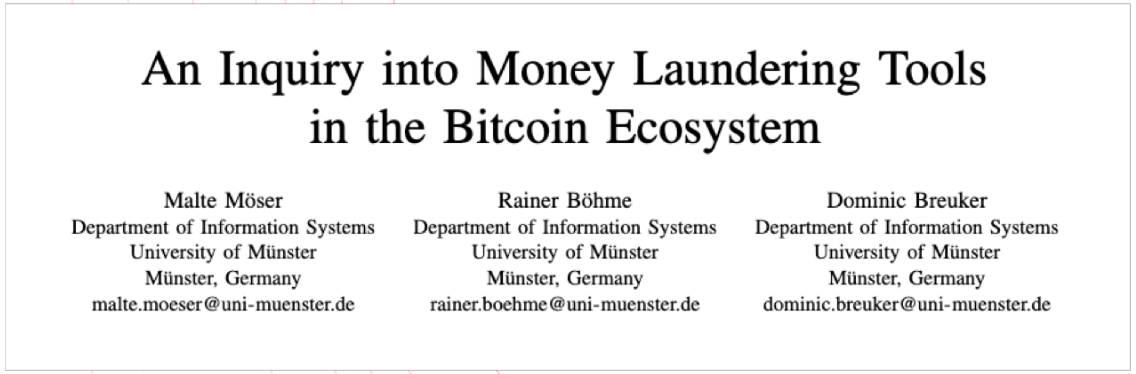
Fergal Reid and Martin Harrigan



An Analysis of Anonymity in Bitcoin Using P2P Network Traffic

Philip Koshy, Diana Koshy, and Patrick McDaniel

Pennsylvania State University, University Park, PA 16802, USA

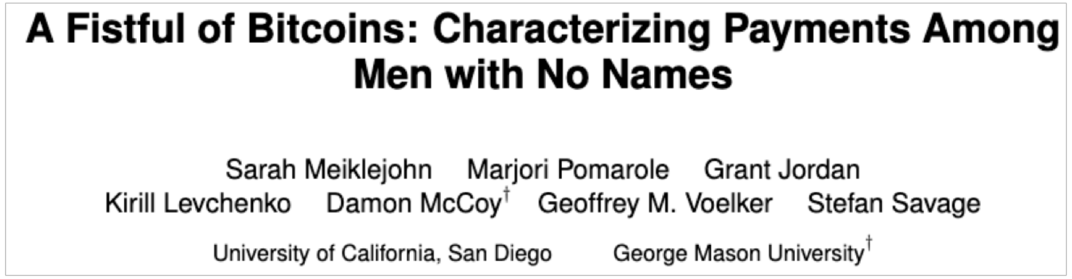


An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem

Malte Möser
Department of Information Systems
University of Münster
Münster, Germany
malte.moeser@uni-muenster.de

Rainer Böhme
Department of Information Systems
University of Münster
Münster, Germany
rainer.boehme@uni-muenster.de

Dominic Breuker
Department of Information Systems
University of Münster
Münster, Germany
dominic.breuker@uni-muenster.de



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[†]

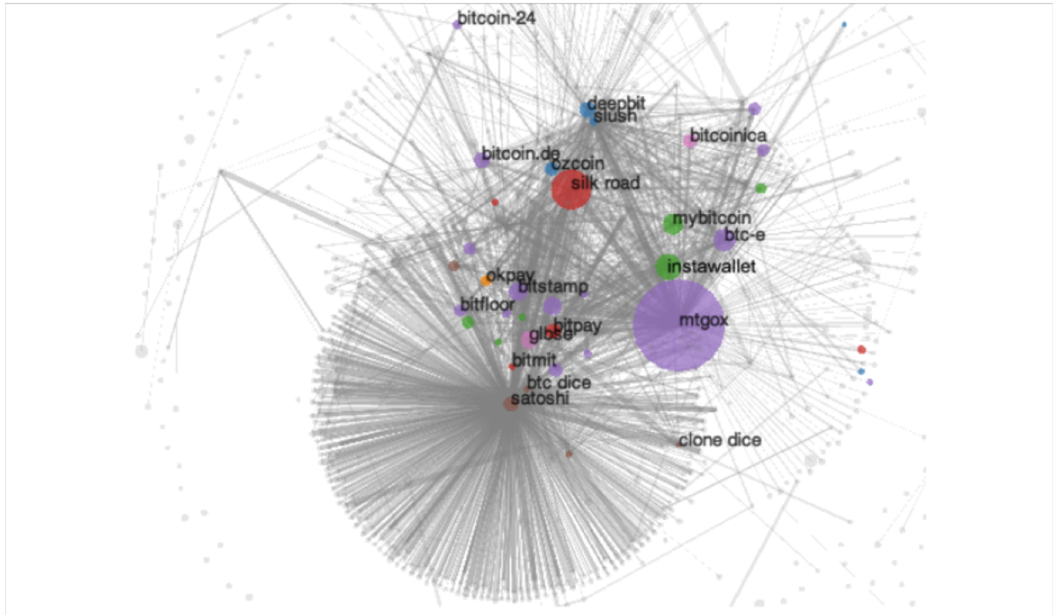
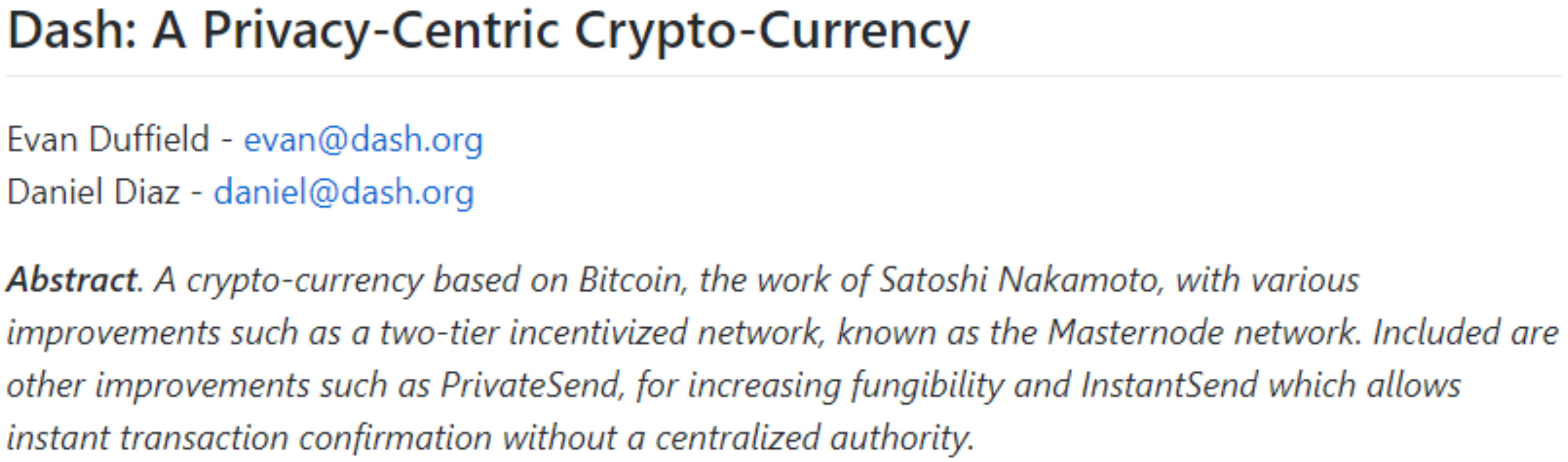


Figure 6: A visualization of the user network. The area of the cluster represents the external incoming value; i.e., the bitcoins received from other clusters but not itself, and for an edge to appear between two nodes there must have been at least 200 transactions between them. The

Some better approaches – DASH



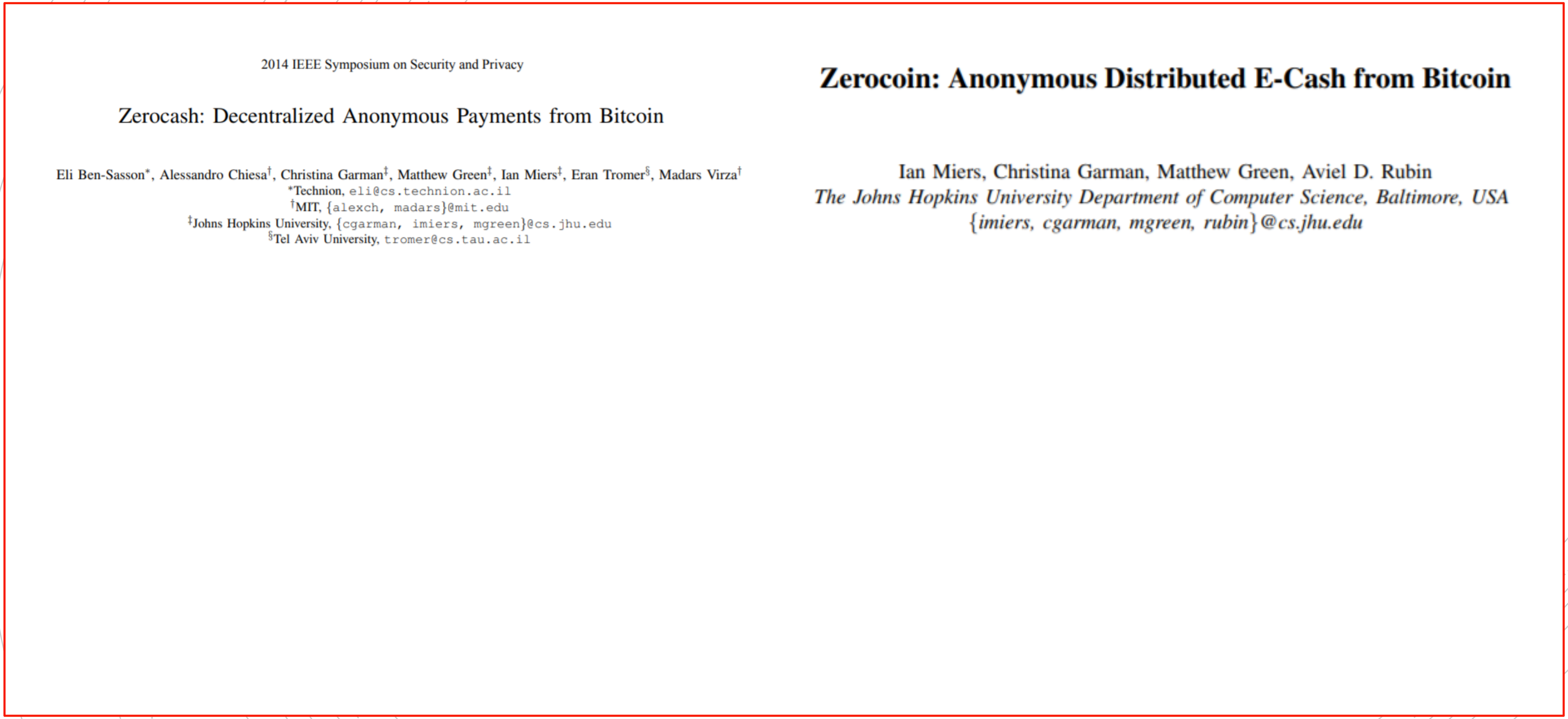
Dash: A Privacy-Centric Crypto-Currency

Evan Duffield - evan@dash.org
Daniel Diaz - daniel@dash.org

Abstract. *A crypto-currency based on Bitcoin, the work of Satoshi Nakamoto, with various improvements such as a two-tier incentivized network, known as the Masternode network. Included are other improvements such as PrivateSend, for increasing fungibility and InstantSend which allows instant transaction confirmation without a centralized authority.*

- Dash is based on CoinJoin transactions
- CoinJoin suffers from availability problems

Zcash



2014 IEEE Symposium on Security and Privacy

Zerocash: Decentralized Anonymous Payments from Bitcoin

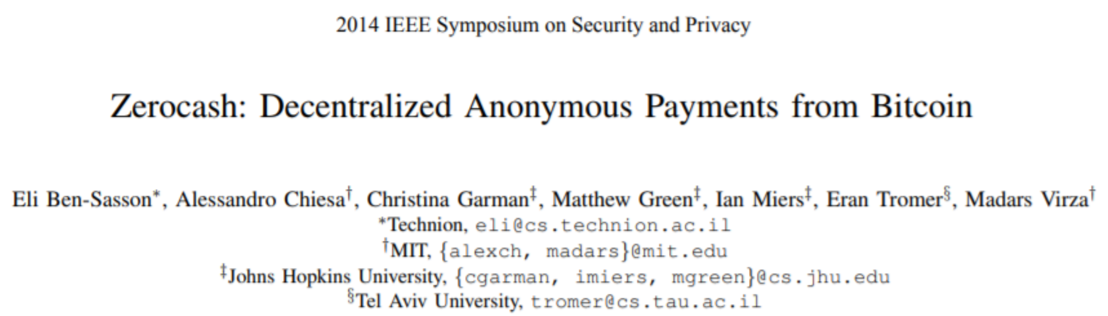
Eli Ben-Sasson[*], Alessandro Chiesa[†], Christina Garman[‡], Matthew Green[‡], Ian Miers[‡], Eran Tromer[§], Madars Virza[†]
[*]Technion, eli@cs.technion.ac.il
[†]MIT, {alexch, madars}@mit.edu
[‡]Johns Hopkins University, {cgarman, imiers, mgreen}@cs.jhu.edu
[§]Tel Aviv University, tromer@cs.tau.ac.il

Zerocoin: Anonymous Distributed E-Cash from Bitcoin

Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin
The Johns Hopkins University Department of Computer Science, Baltimore, USA
{imiers, cgarman, mgreen, rubin}@cs.jhu.edu

Zcash

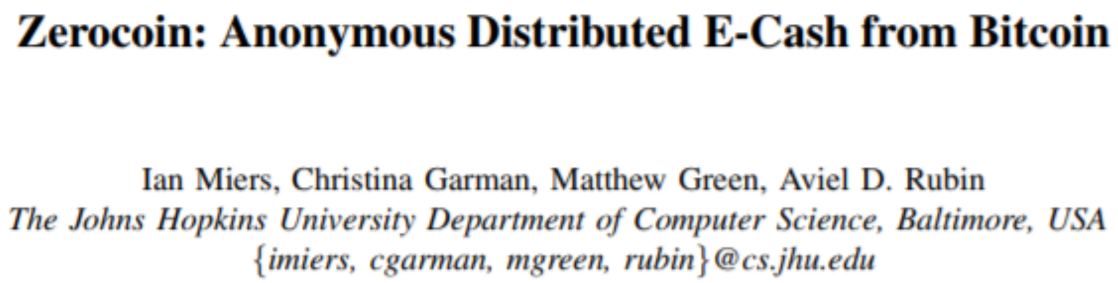
What is Zcash?



2014 IEEE Symposium on Security and Privacy

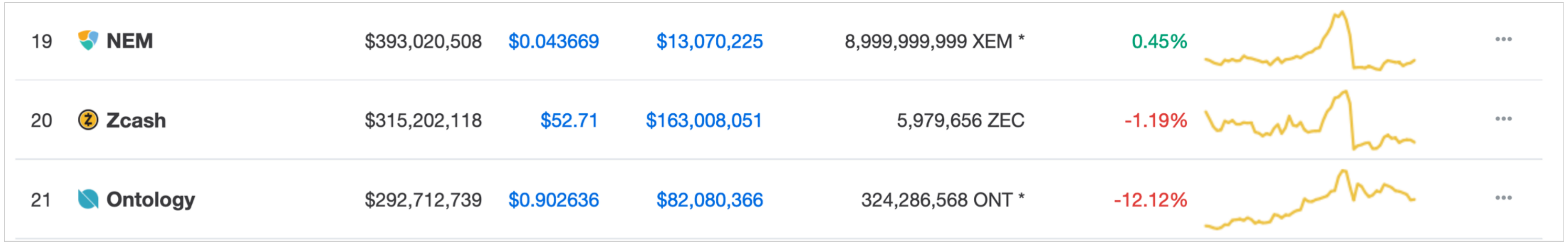
Zerocash: Decentralized Anonymous Payments from Bitcoin

Eli Ben-Sasson[*], Alessandro Chiesa[†], Christina Garman[‡], Matthew Green[‡], Ian Miers[‡], Eran Tromer[§], Madars Virza[†]
[*]Technion, eli@cs.technion.ac.il
[†]MIT, {alexch, madars}@mit.edu
[‡]Johns Hopkins University, {cgarman, imiers, mgreen}@cs.jhu.edu
[§]Tel Aviv University, tromer@cs.tau.ac.il



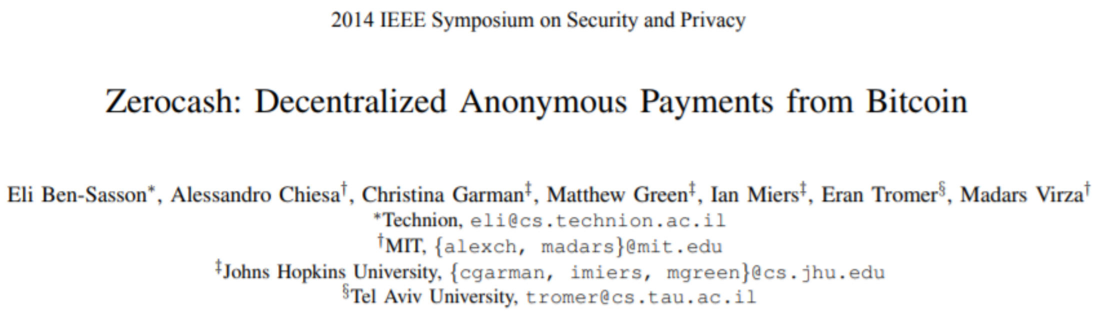
Zerocoin: Anonymous Distributed E-Cash from Bitcoin

Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin
The Johns Hopkins University Department of Computer Science, Baltimore, USA
{imiers, cgarman, mgreen, rubin}@cs.jhu.edu



19	NEM	$393,020,508	$0.043669	$13,070,225	8,999,999,999 XEM *	0.45%	•••
20	Zcash	$315,202,118	$52.71	$163,008,051	5,979,656 ZEC	-1.19%	•••
21	Ontology	$292,712,739	$0.902636	$82,080,366	324,286,568 ONT *	-12.12%	•••

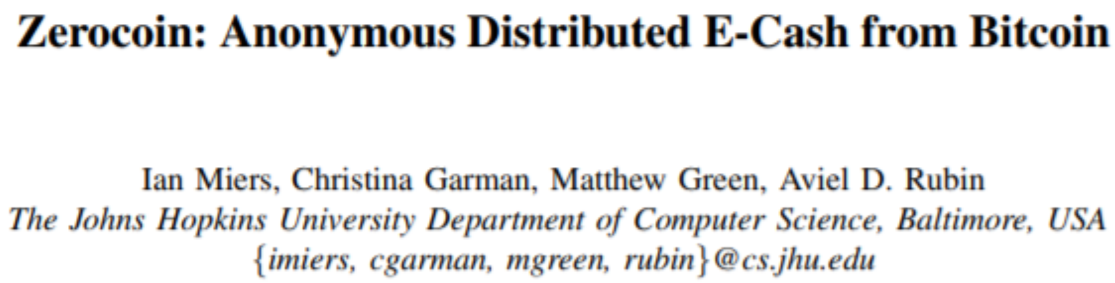
Zcash



2014 IEEE Symposium on Security and Privacy

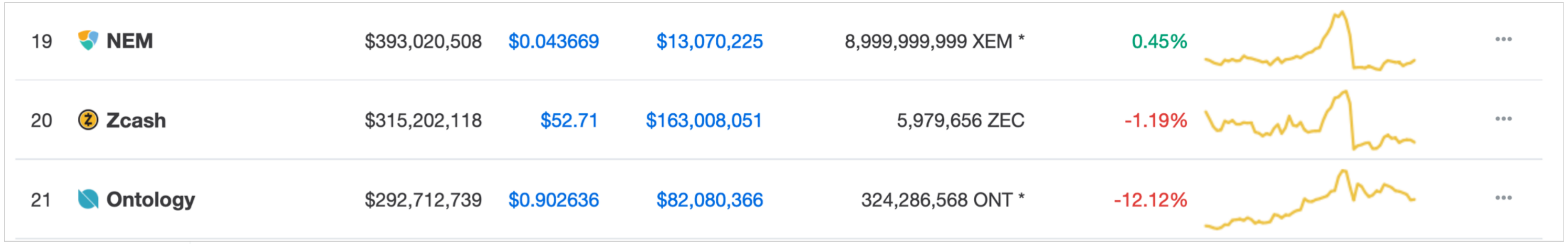
Zerocash: Decentralized Anonymous Payments from Bitcoin

Eli Ben-Sasson[*], Alessandro Chiesa[†], Christina Garman[‡], Matthew Green[‡], Ian Miers[‡], Eran Tromer[§], Madars Virza[†]
[*]Technion, eli@cs.technion.ac.il
[†]MIT, {alexch, madars}@mit.edu
[‡]Johns Hopkins University, {cgarman, imiers, mgreen}@cs.jhu.edu
[§]Tel Aviv University, tromer@cs.tau.ac.il

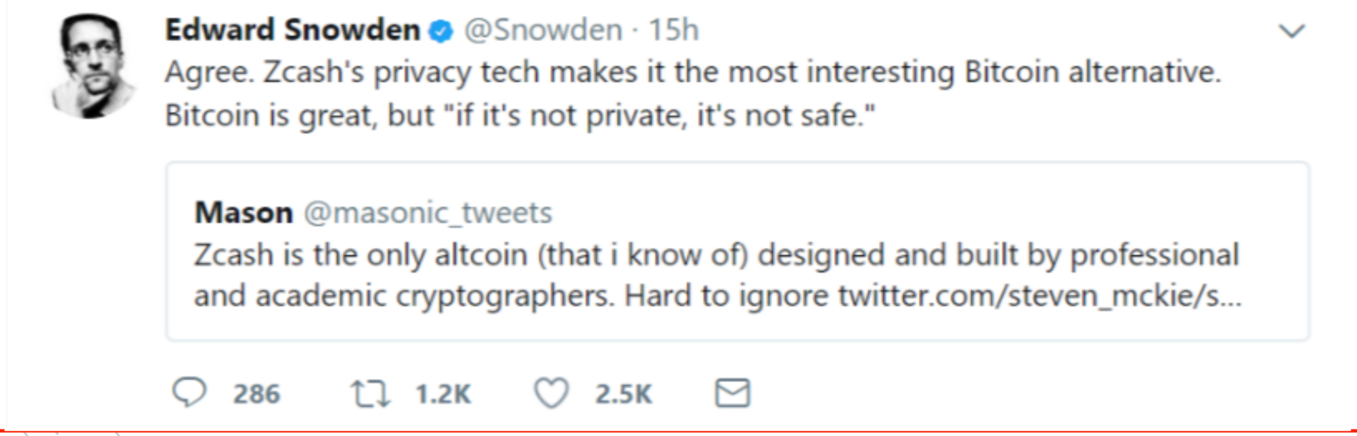


Zerocoin: Anonymous Distributed E-Cash from Bitcoin

Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin
The Johns Hopkins University Department of Computer Science, Baltimore, USA
{imiers, cgarman, mgreen, rubin}@cs.jhu.edu



19	**NEM**	$393,020,508	$0.043669	$13,070,225	8,999,999,999 XEM *	0.45%	···
20	**Zcash**	$315,202,118	$52.71	$163,008,051	5,979,656 ZEC	-1.19%	···
21	**Ontology**	$292,712,739	$0.902636	$82,080,366	324,286,568 ONT *	-12.12%	···

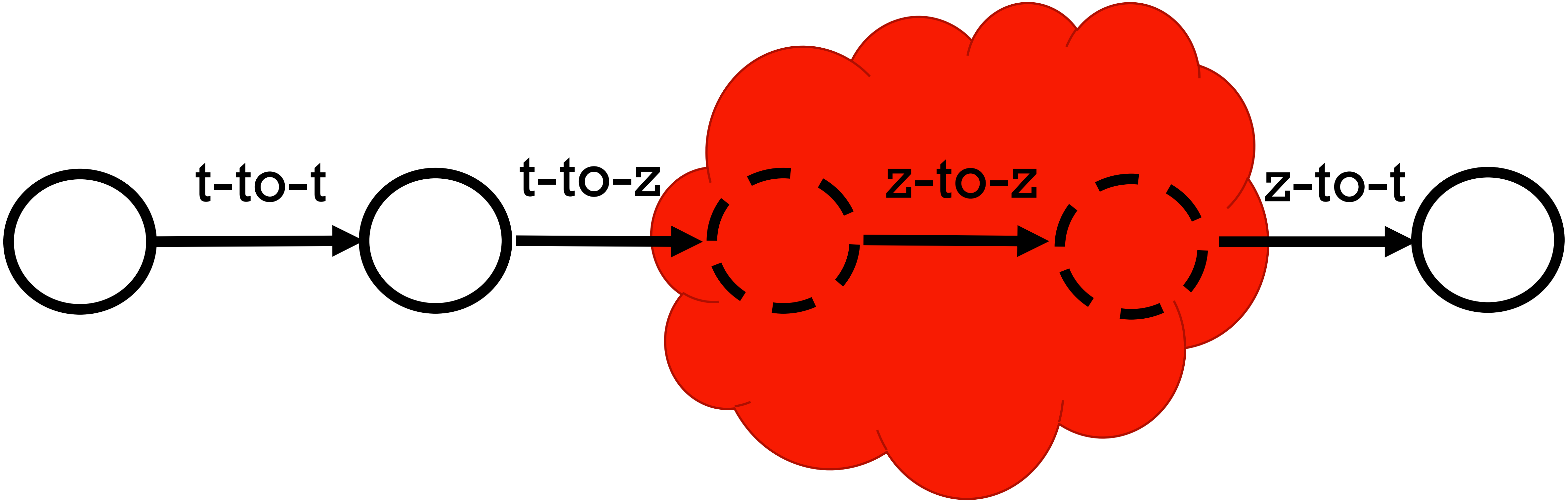


Edward Snowden @Snowden · 15h

Agree. Zcash's privacy tech makes it the most interesting Bitcoin alternative. Bitcoin is great, but "if it's not private, it's not safe."

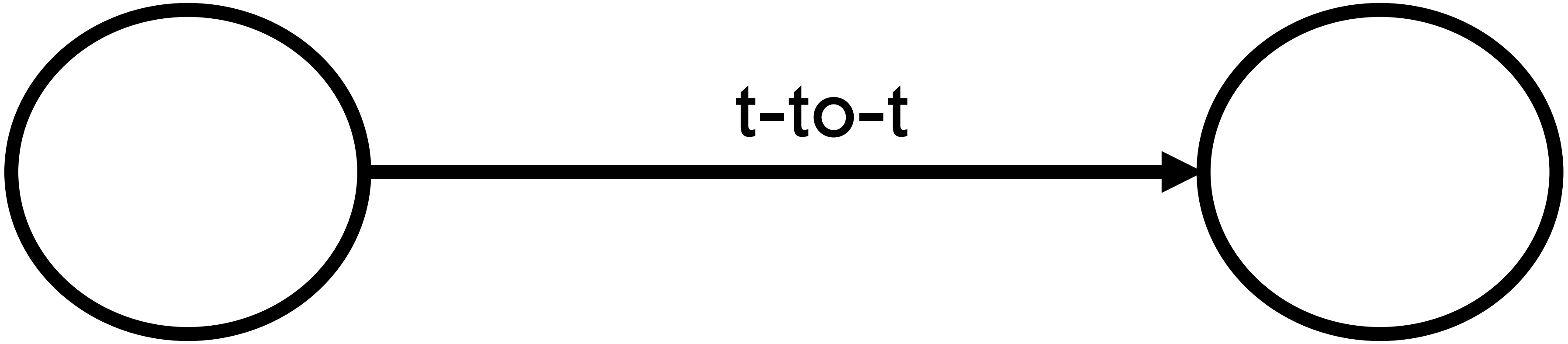
> **Mason** @masonic_tweets
> Zcash is the only altcoin (that i know of) designed and built by professional and academic cryptographers. Hard to ignore twitter.com/steven_mckie/s...

Types of transactions



The set of all z-addresses makes up the shielded pool

Types of transactions - Transparent



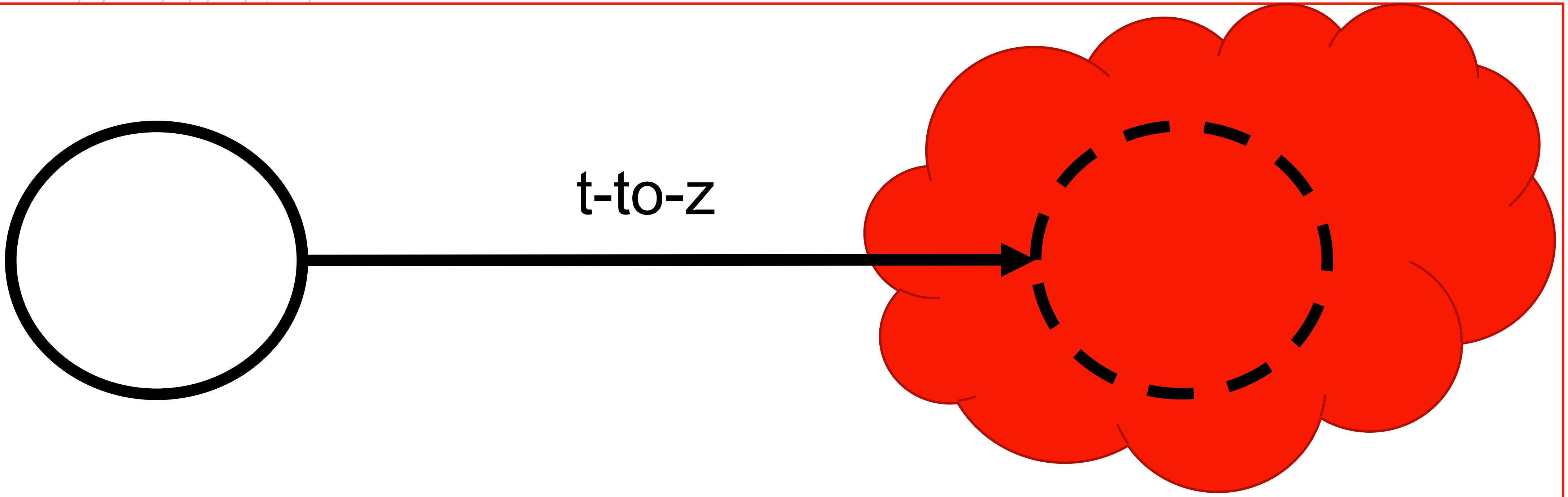
t-to-t

t1YC7abTbqPnen6UGcqvS5hVqXrzh14evvA
1 ZEC

t1ENZOabfdfbFRn67UGcqvS5hSERzh24e2Sa
0.9999 ZEC

Received Time	Fri 23 Feb 2019 11:01:31 GMT
Included in Block	420420
Inputs / Outputs	1/1

Types of transactions - Shielded



t16Eo7gEffPnen6UH4frOn5hV54r4h13edvA

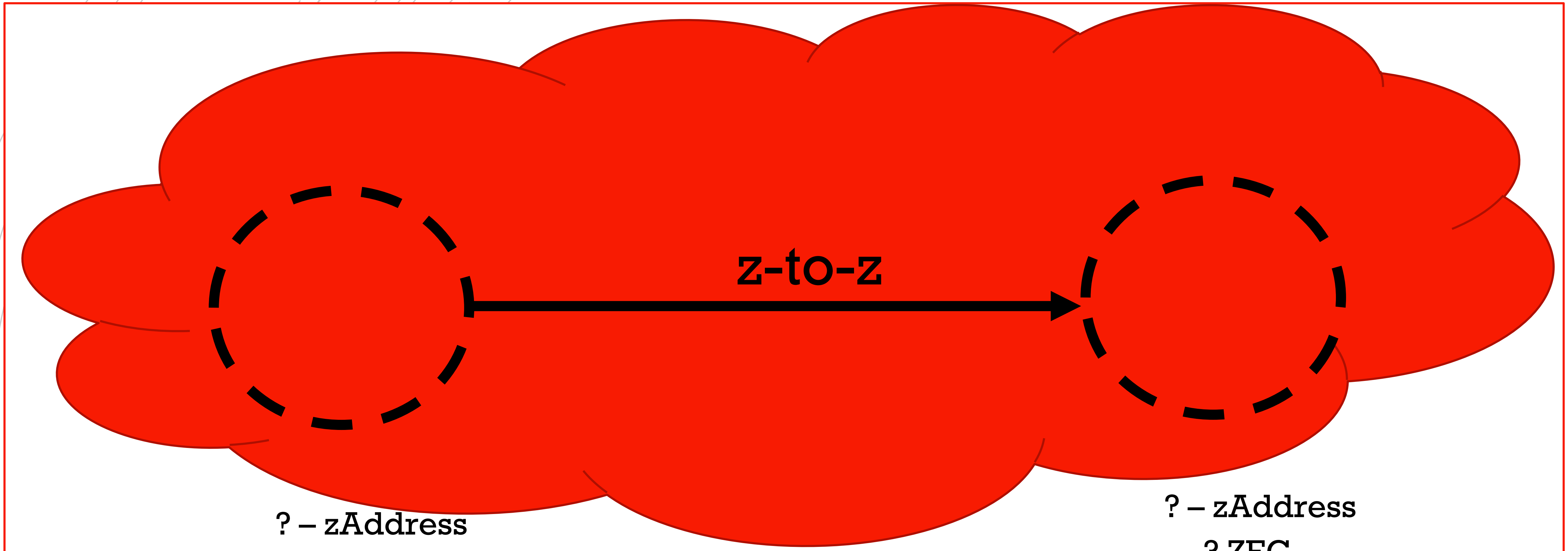
1 ZEC

? – zAddress

1 ZEC

Received Time	23 Feb 2017 13:01:31 GMT
Included in Block	100001
Inputs / Outputs	1/?

Types of transactions - Private



z-to-z

? – zAddress

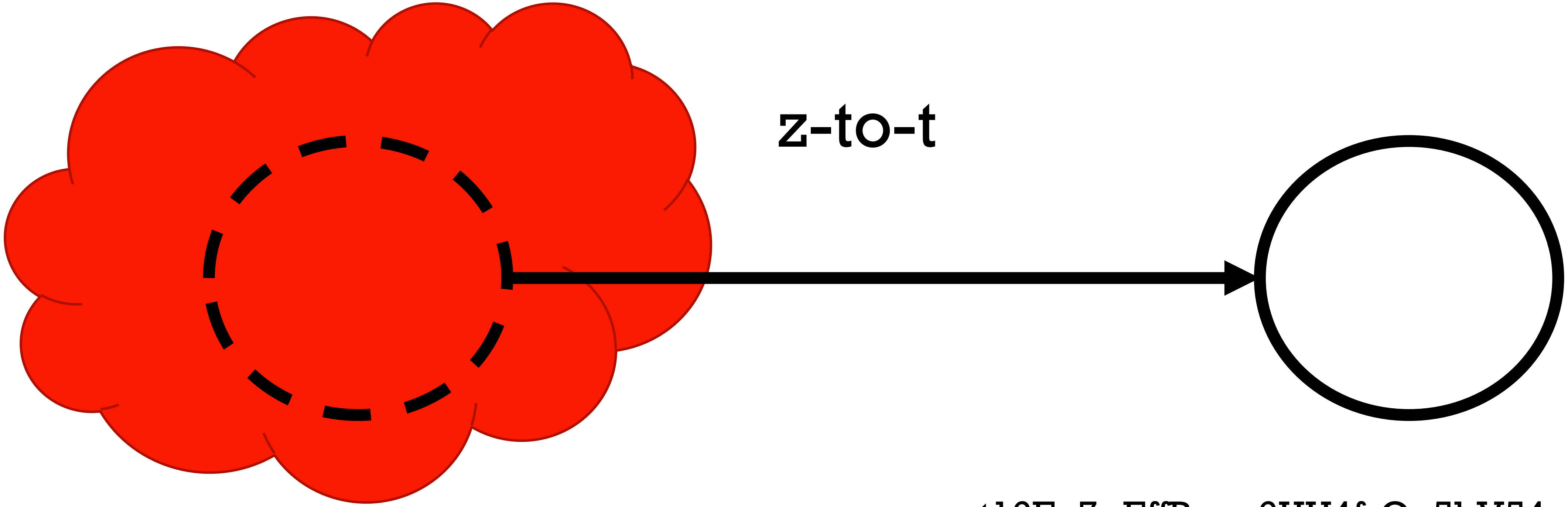
? ZEC

? – zAddress

? ZEC

Received Time	23 Feb 2019 14:01:31 GMT
Included in Block	133707
Inputs / Outputs	?/?

Types of transactions - Deshielded



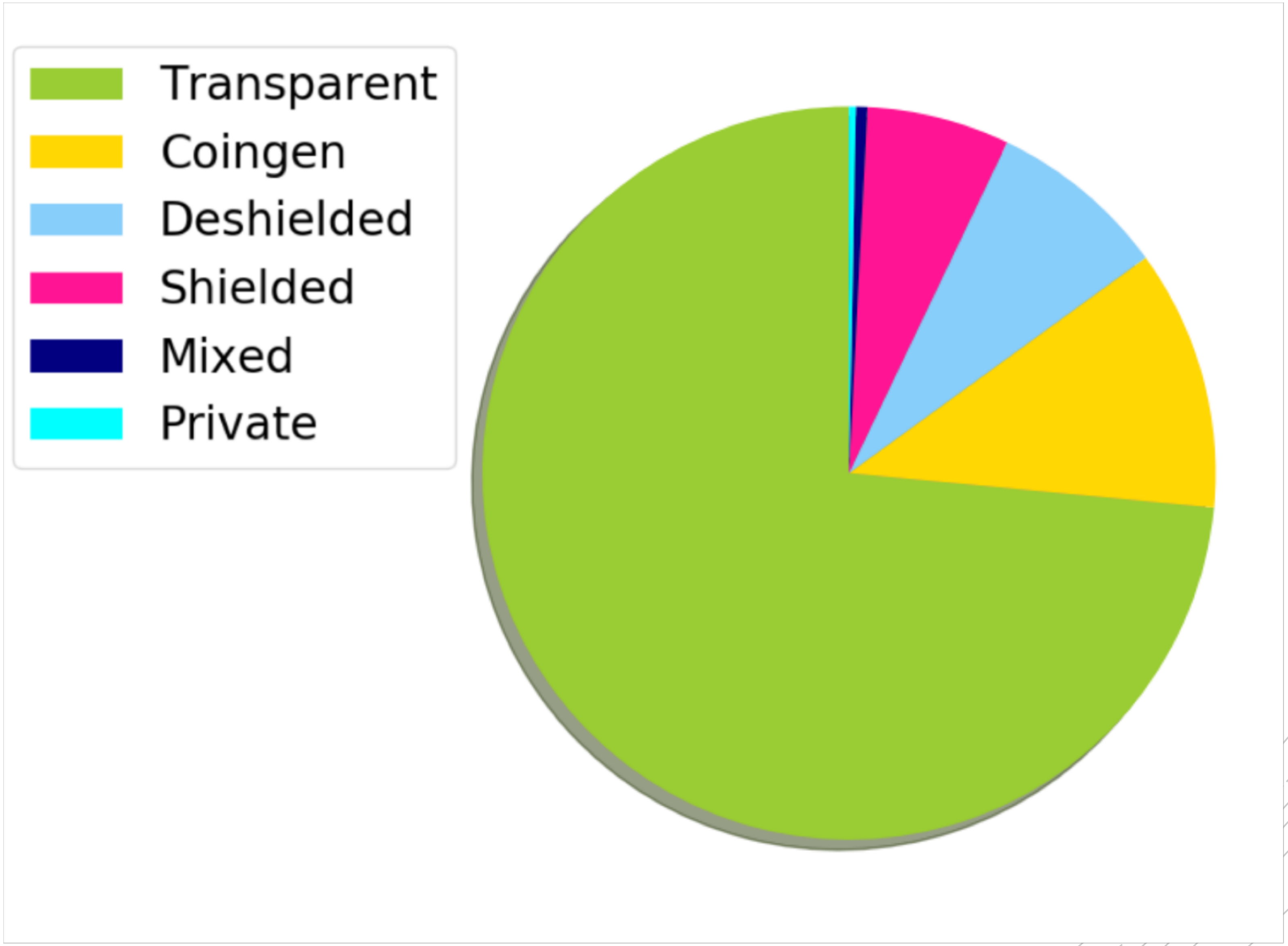
? – zAddress
? ZEC

t16Eo7gEffPnen6UH4frOn5hV54r4h13edvA
1 ZEC

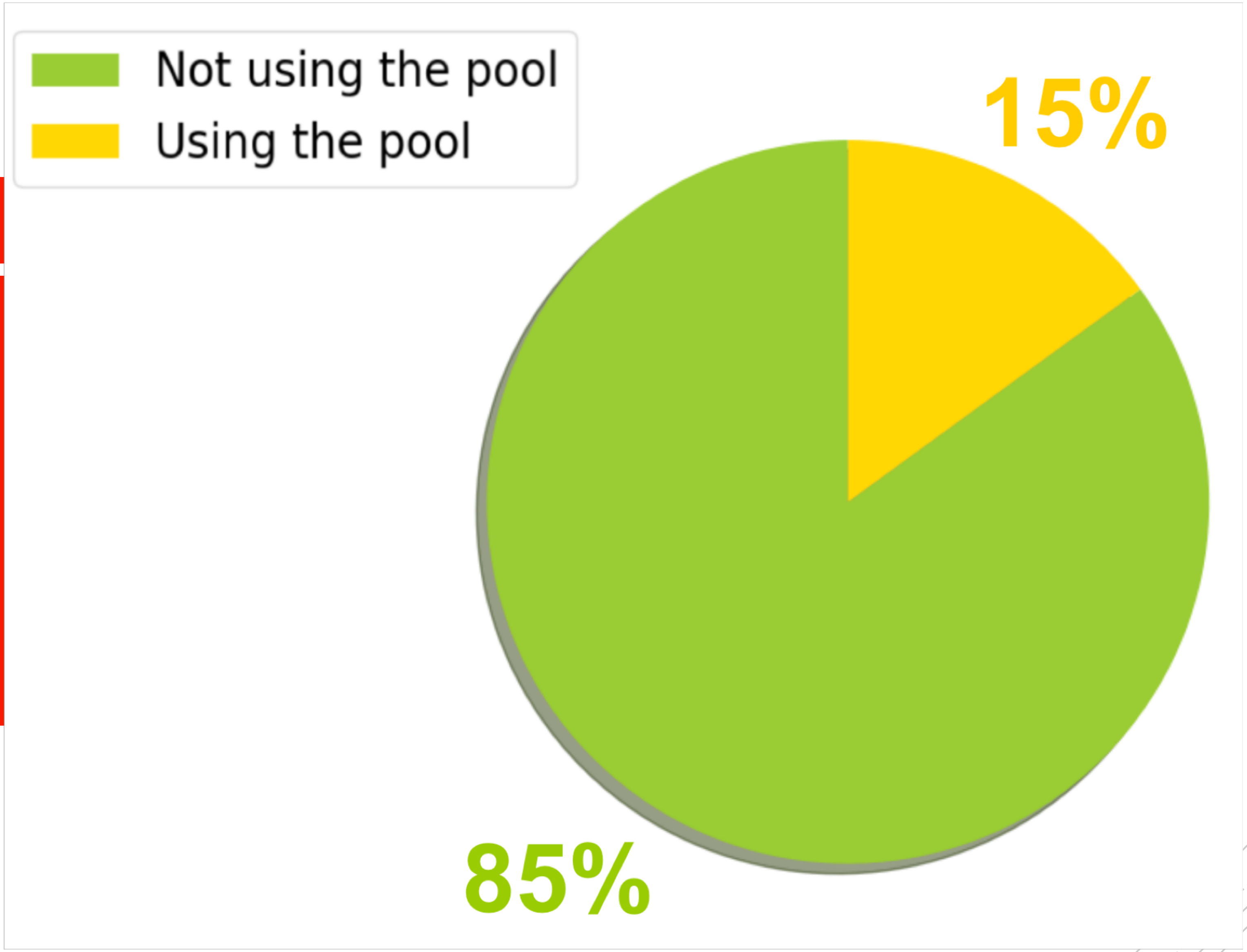
Received Time	Fri 24 Feb 2019 13:37:31 GMT
Included in Block	404040
Inputs / Outputs	?/1

What types of transactions are most prevalent?

Interactions in Zcash

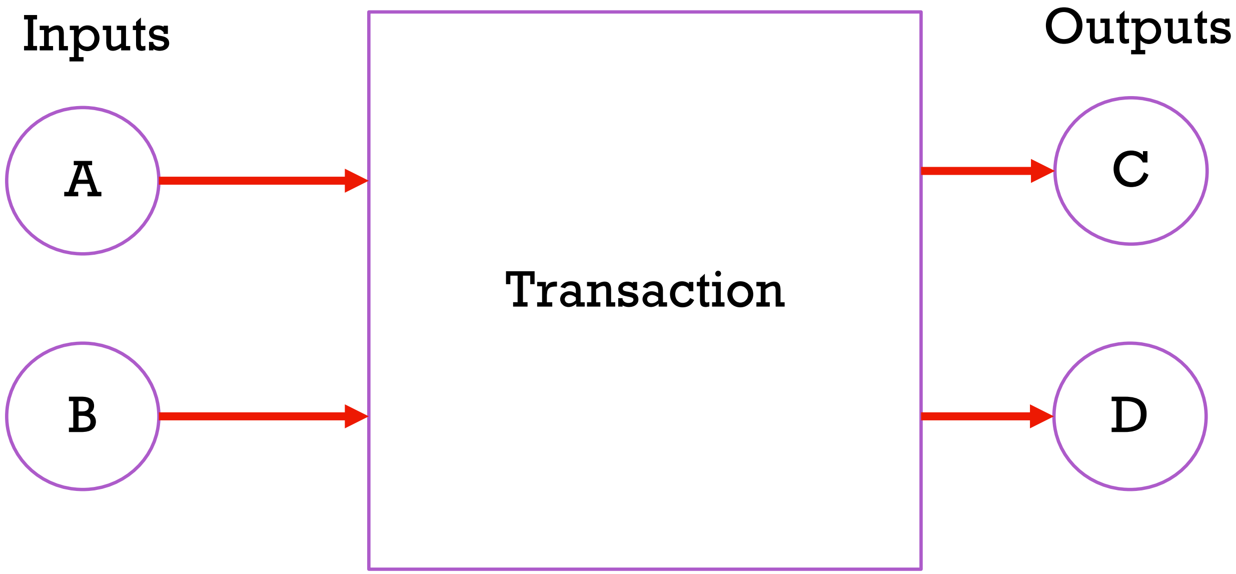


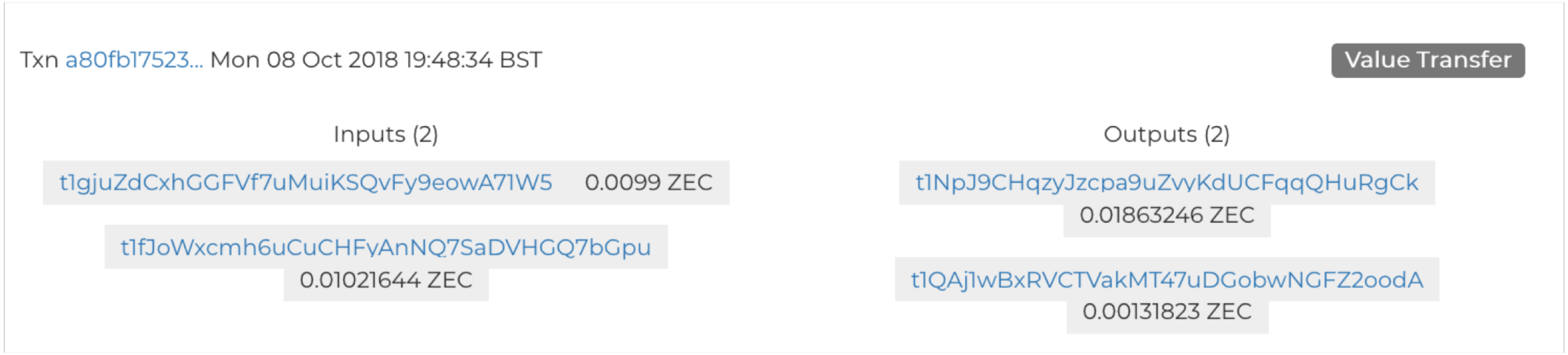
Interactions in Zcash



Most users do transparent, lets try to cluster them?

Address Clustering

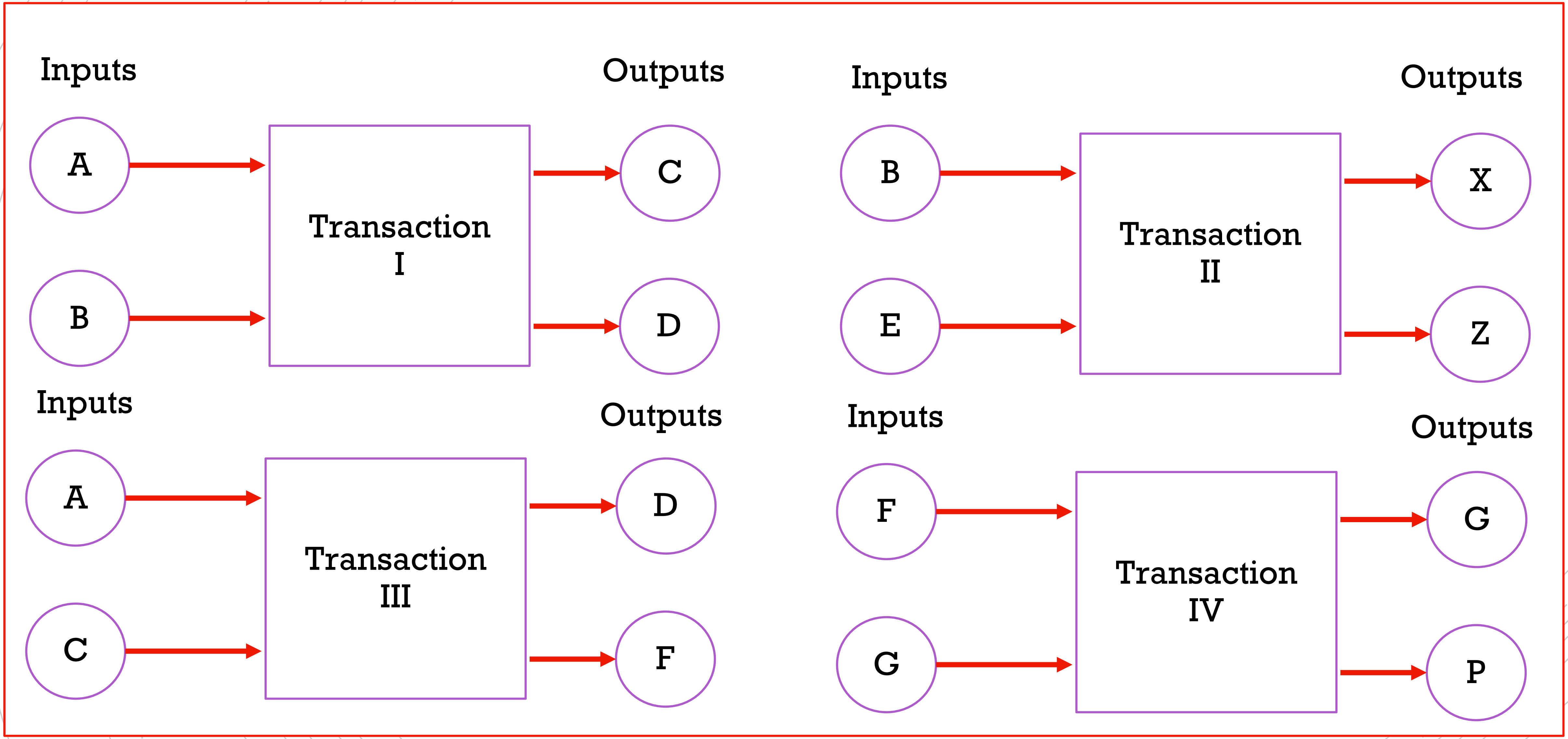



Txn a80fb17523... Mon 08 Oct 2018 19:48:34 BST

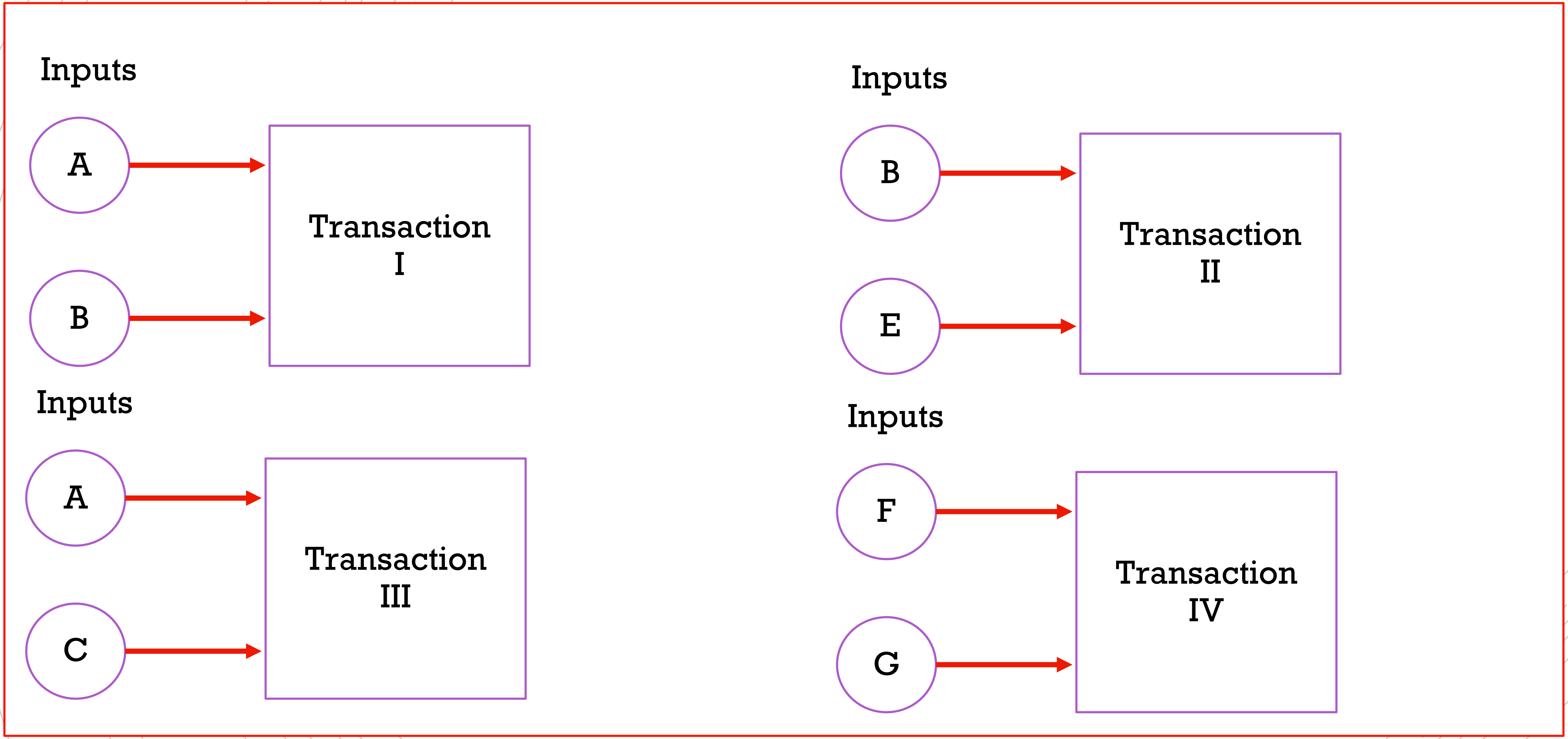
Value Transfer

Inputs (2)	Outputs (2)
t1gjuZdCxhGGFVf7uMuiKSQvFy9eowA71W5 0.0099 ZEC	t1NpJ9CHqzyJzcpa9uZvyKdUCFqqQHuRgCk 0.01863246 ZEC
t1fJoWxcmh6uCuCHFyAnNQ7SaDVHGQ7bGpu 0.01021644 ZEC	t1QAj1wBxRVCTVakMT47uDGobwNGFZ2oodA 0.00131823 ZEC

Address Clustering



Address Clustering



Inputs

A

B

Transaction I

Inputs

B

E

Transaction II

Inputs

A

C

Transaction III

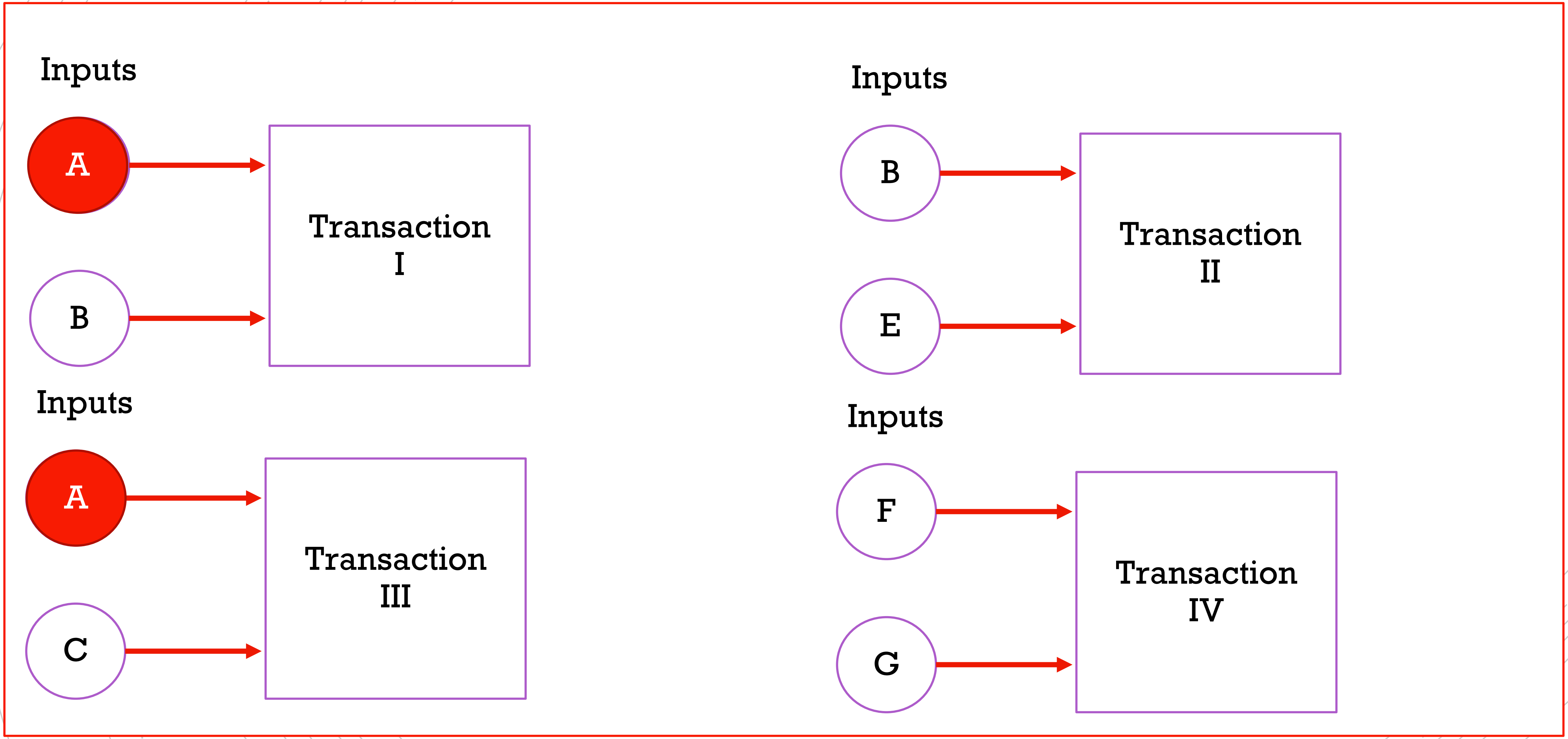
Inputs

F

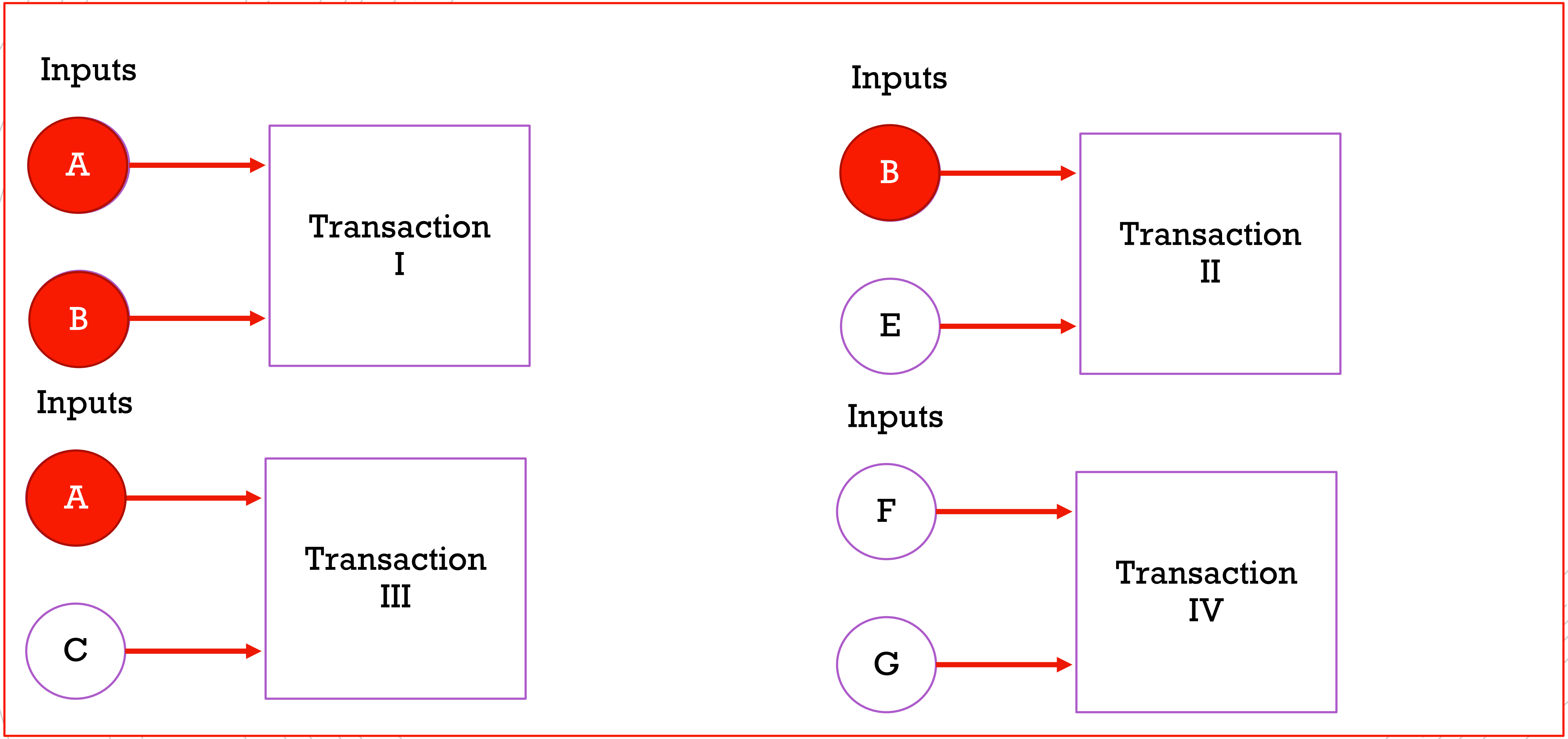
G

Transaction IV

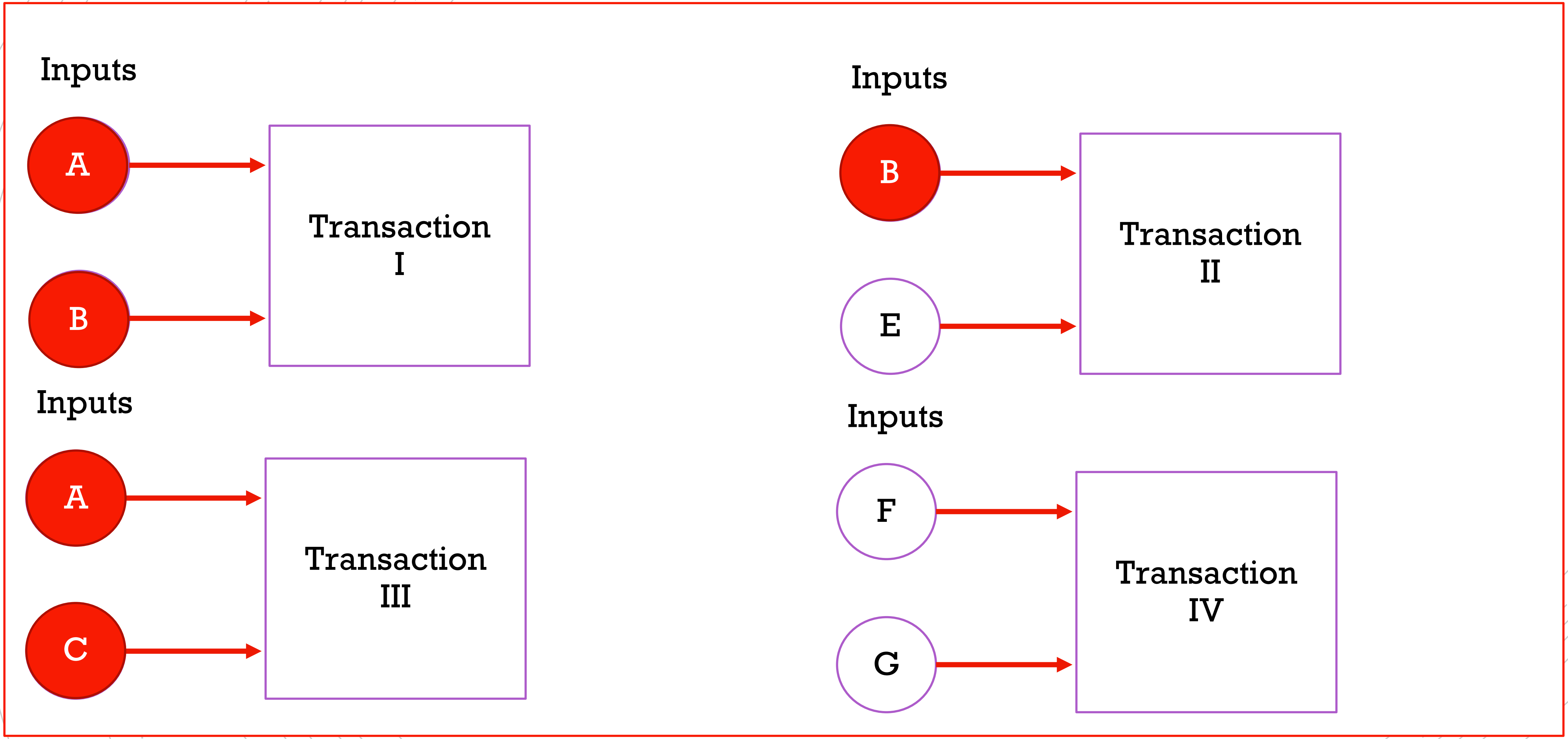
Address Clustering



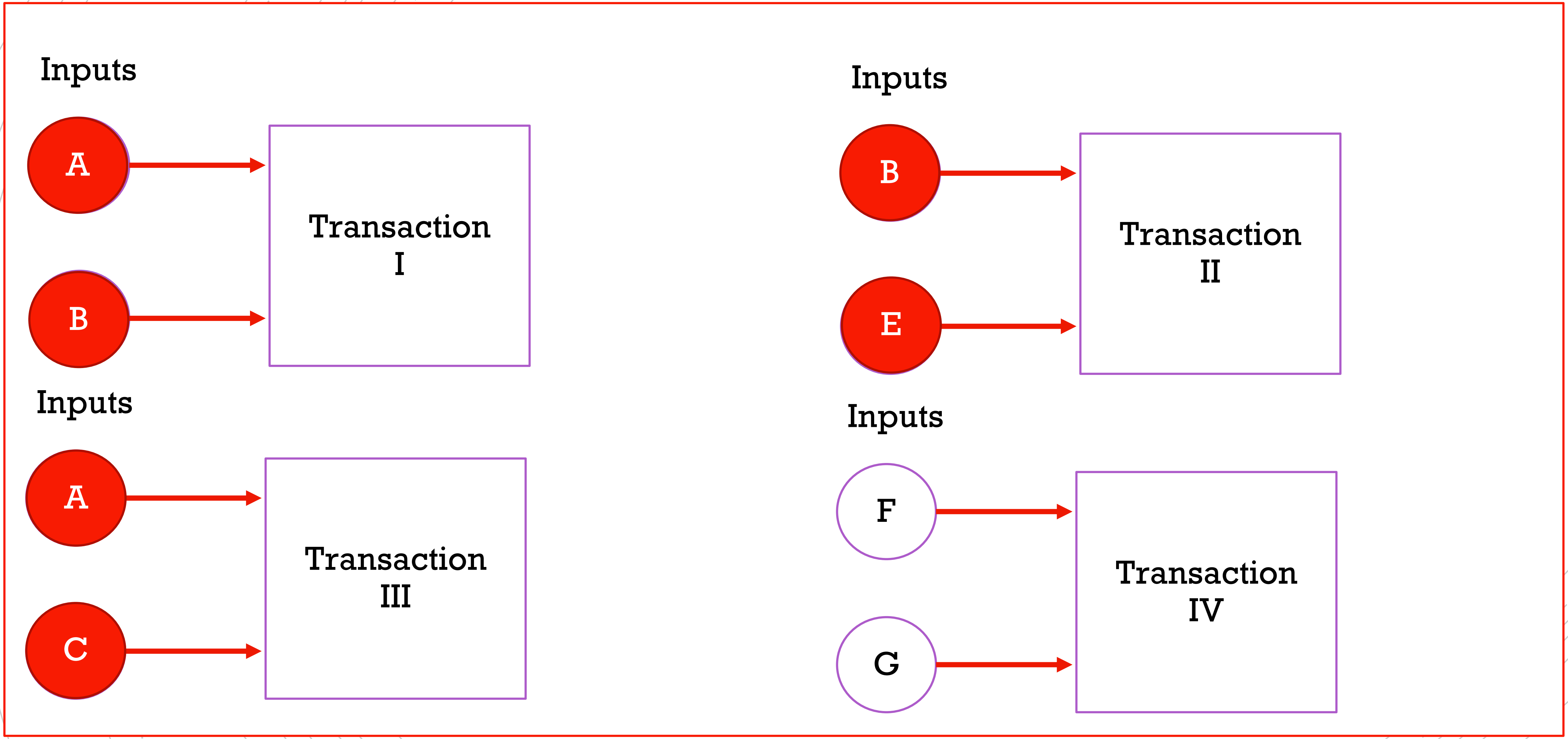
Address Clustering



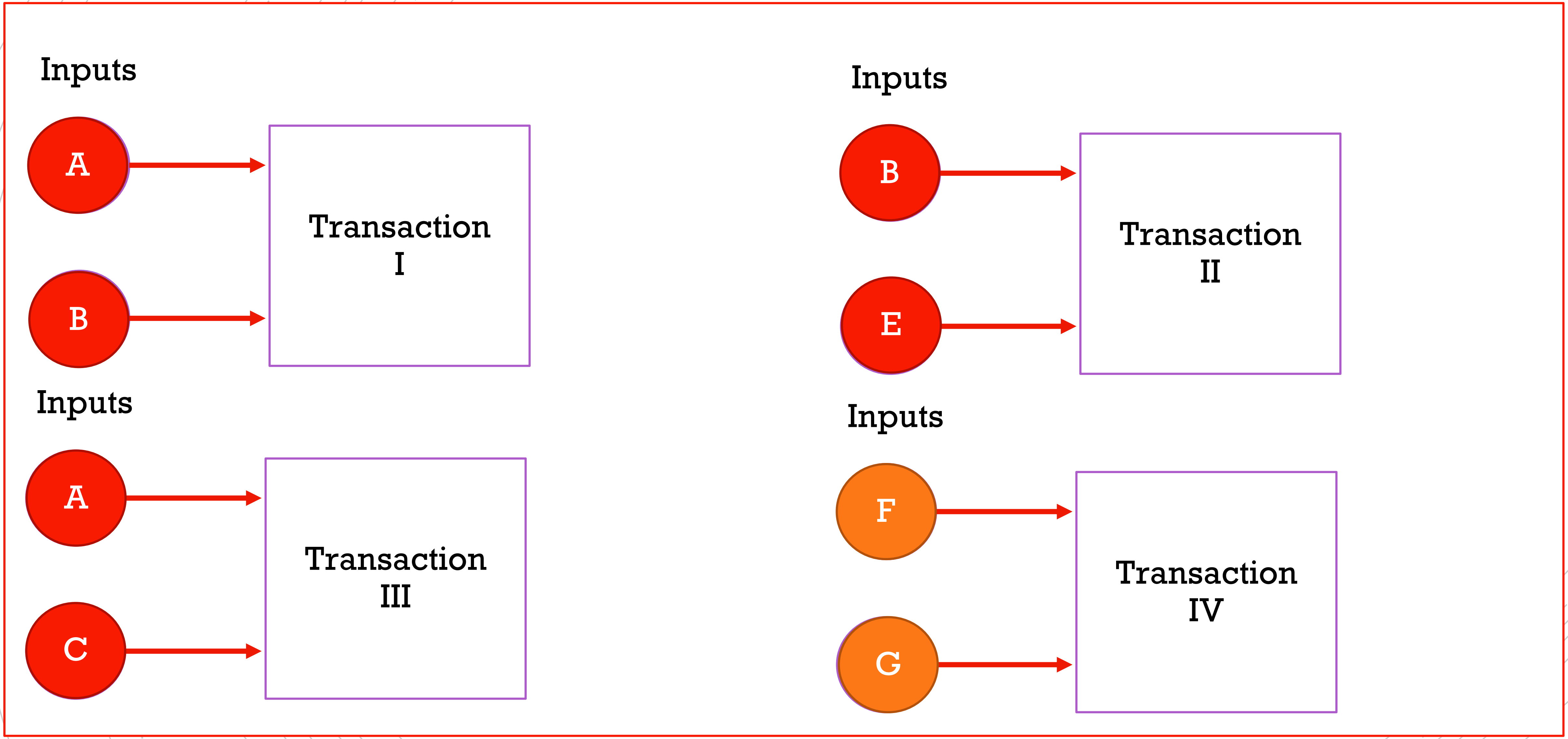
Address Clustering



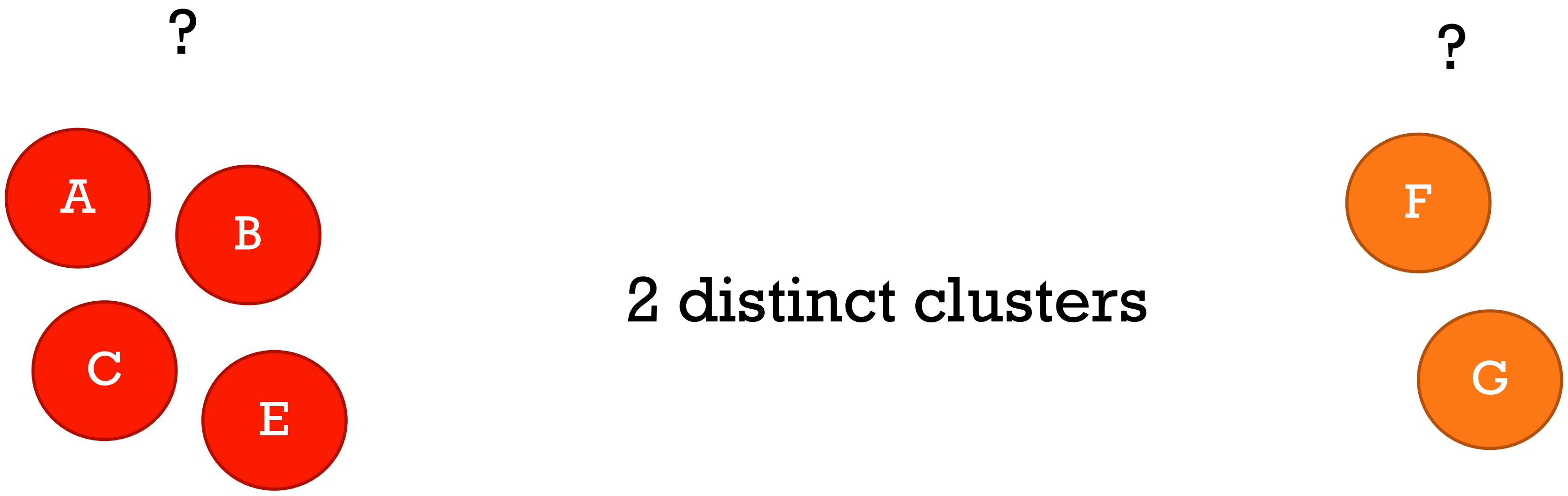
Address Clustering



Address Clustering

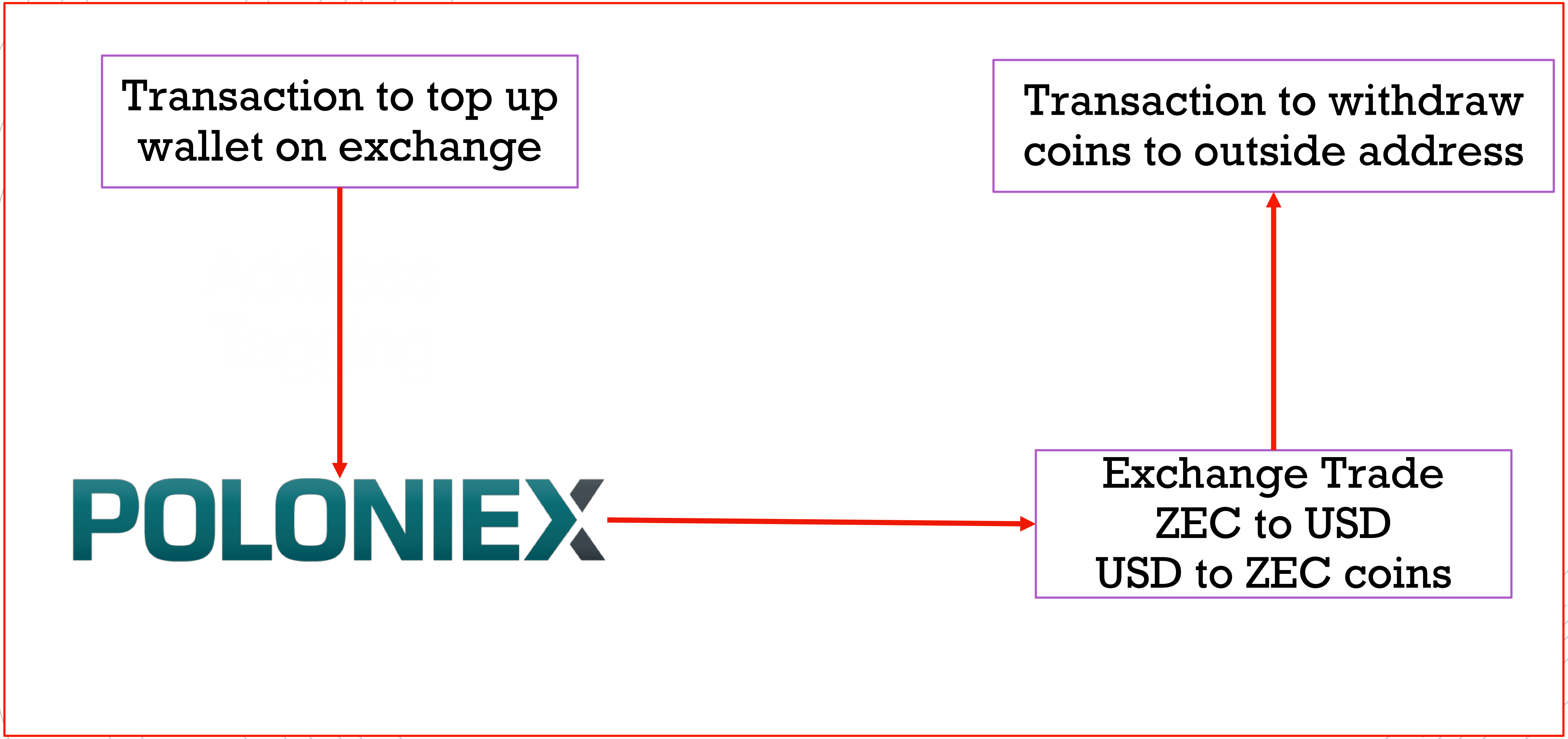


Address Clustering



2 distinct clusters

Address Tagging

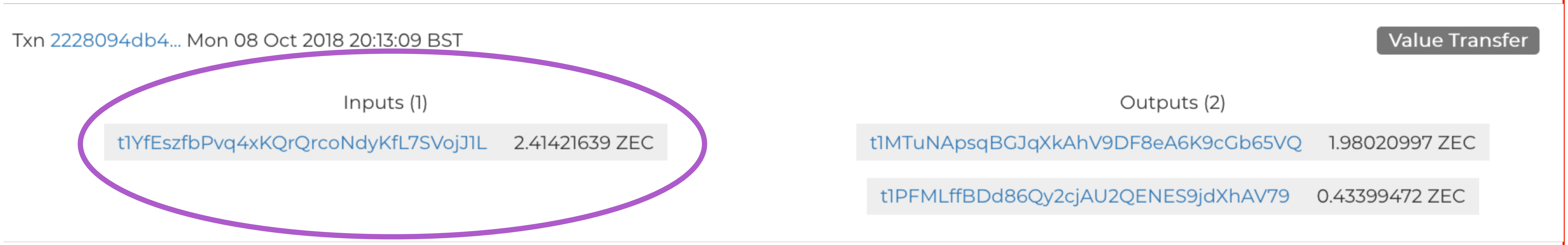


Transaction to top up wallet on exchange

Exchange Trade
ZEC to USD
USD to ZEC coins

Transaction to withdraw coins to outside address

Address Tagging



Txn 2228094db4... Mon 08 Oct 2018 20:13:09 BST

Value Transfer

Inputs (1)

t1YfEszfbPvq4xKQrQrcoNdyKfL7SVojJ1L 2.41421639 ZEC

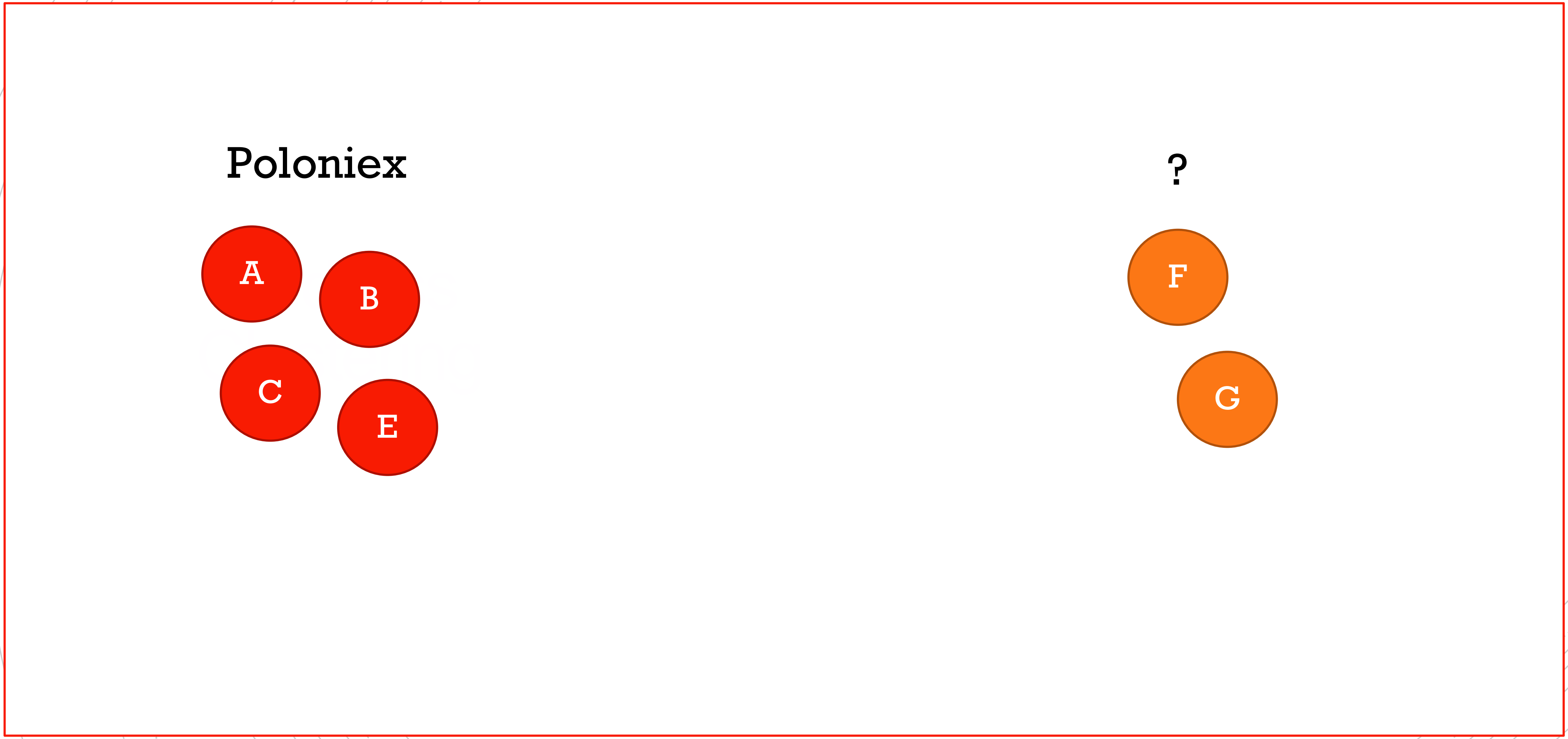
Outputs (2)

t1MTuNApsqBGJqXkAhV9DF8eA6K9cGb65VQ 1.98020997 ZEC

t1PFMLffBDd86Qy2cjAU2QENES9jdXhAV79 0.43399472 ZEC

- Check to see which cluster this address belongs to, that cluster is tagged

Address Tagging



Poloniex

A

B

C

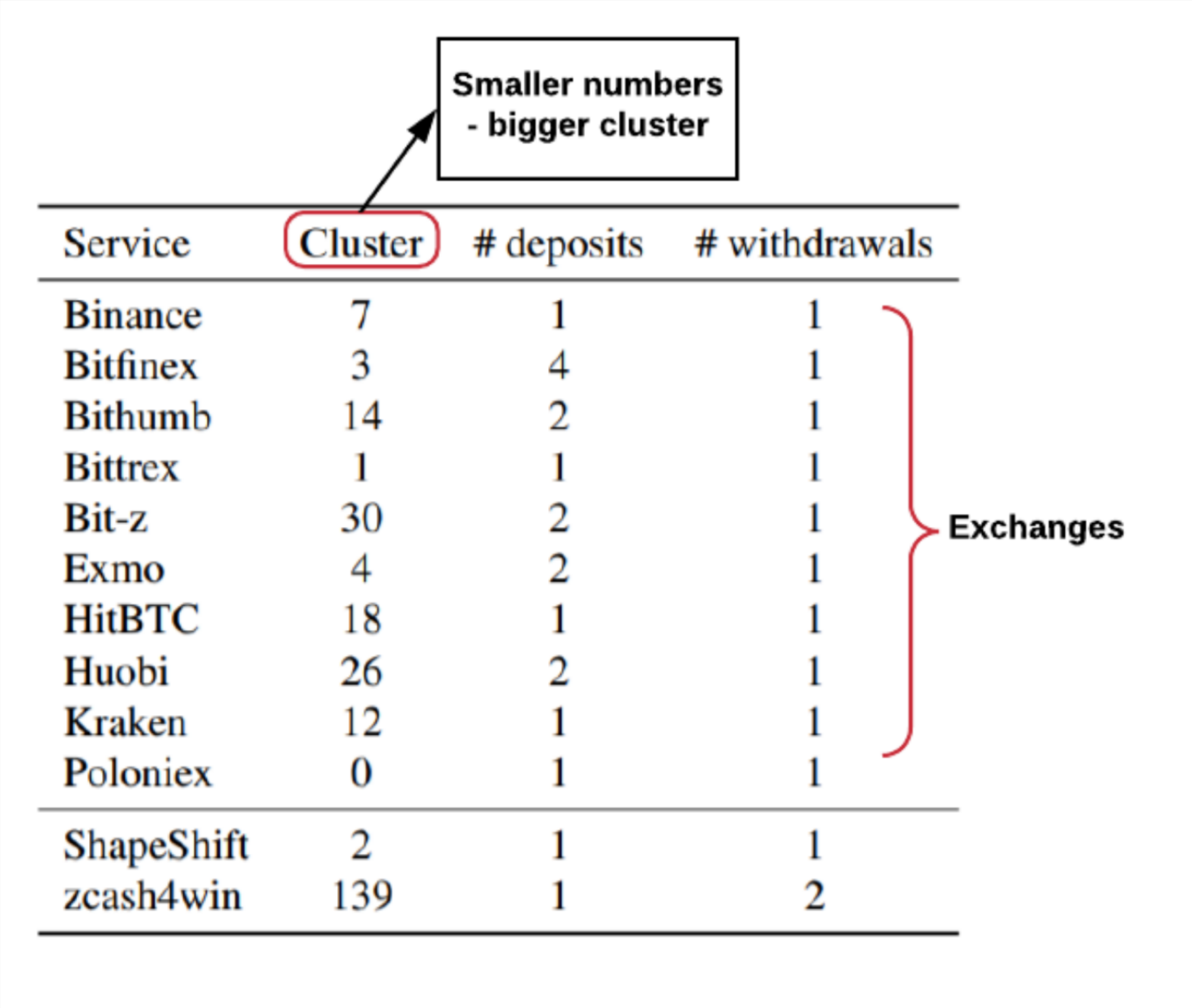
E

?

F

G

Transparent transactions (t-to-t)



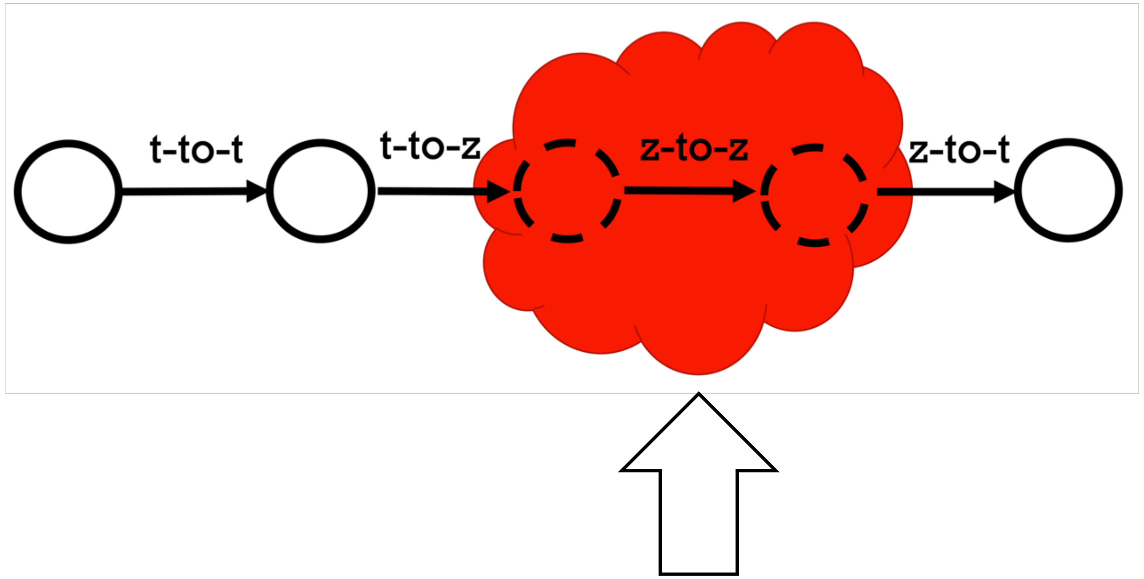
Smaller numbers - bigger cluster

Service	Cluster	# deposits	# withdrawals
Binance	7	1	1
Bitfinex	3	4	1
Bithumb	14	2	1
Bittrex	1	1	1
Bit-z	30	2	1
Exmo	4	2	1
HitBTC	18	1	1
Huobi	26	2	1
Kraken	12	1	1
Poloniex	0	1	1
ShapeShift	2	1	1
zcash4win	139	1	2

Exchanges

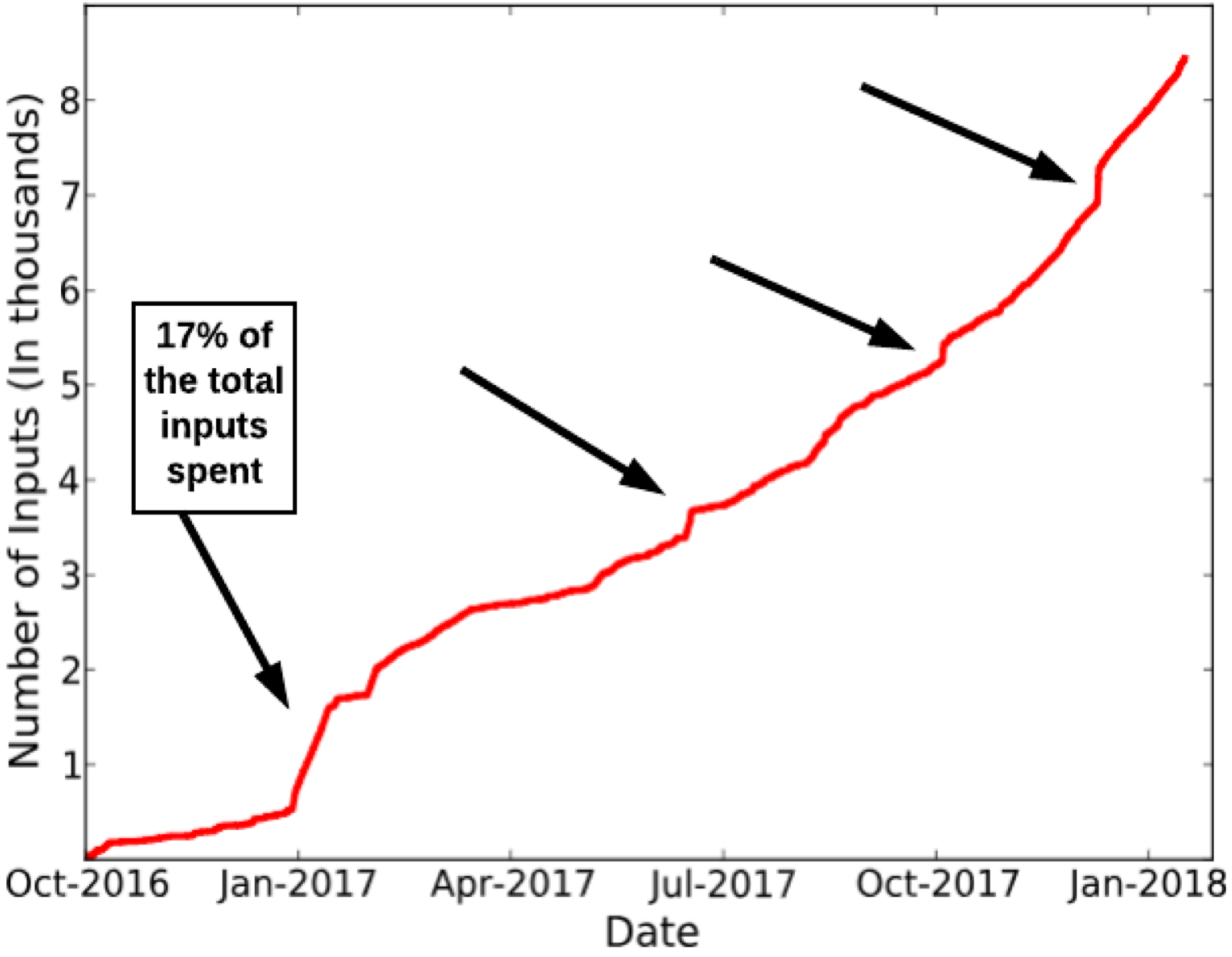
- Top five clusters accounted for 11.21% of all transactions
- 97,549 clusters with more than 1 address
- ShapeShift had received over 1.1M ZEC

Private transactions (z-to-z)



- Less than 1% of the total transactions
- Underlying cryptography is still secure
- No obvious de-anonymization techniques

Maybe the same users?



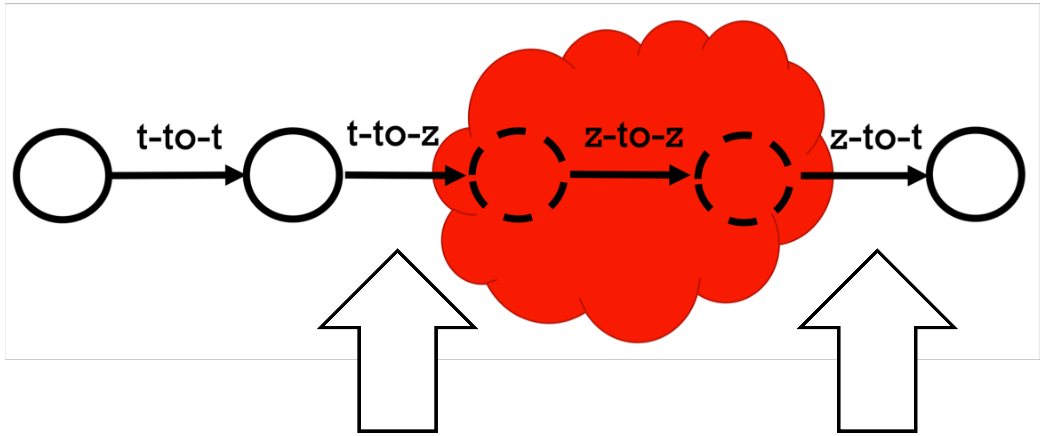
17% of the total inputs spent

Shielded and de-shielded transactions (t-to-z and z-to-t)

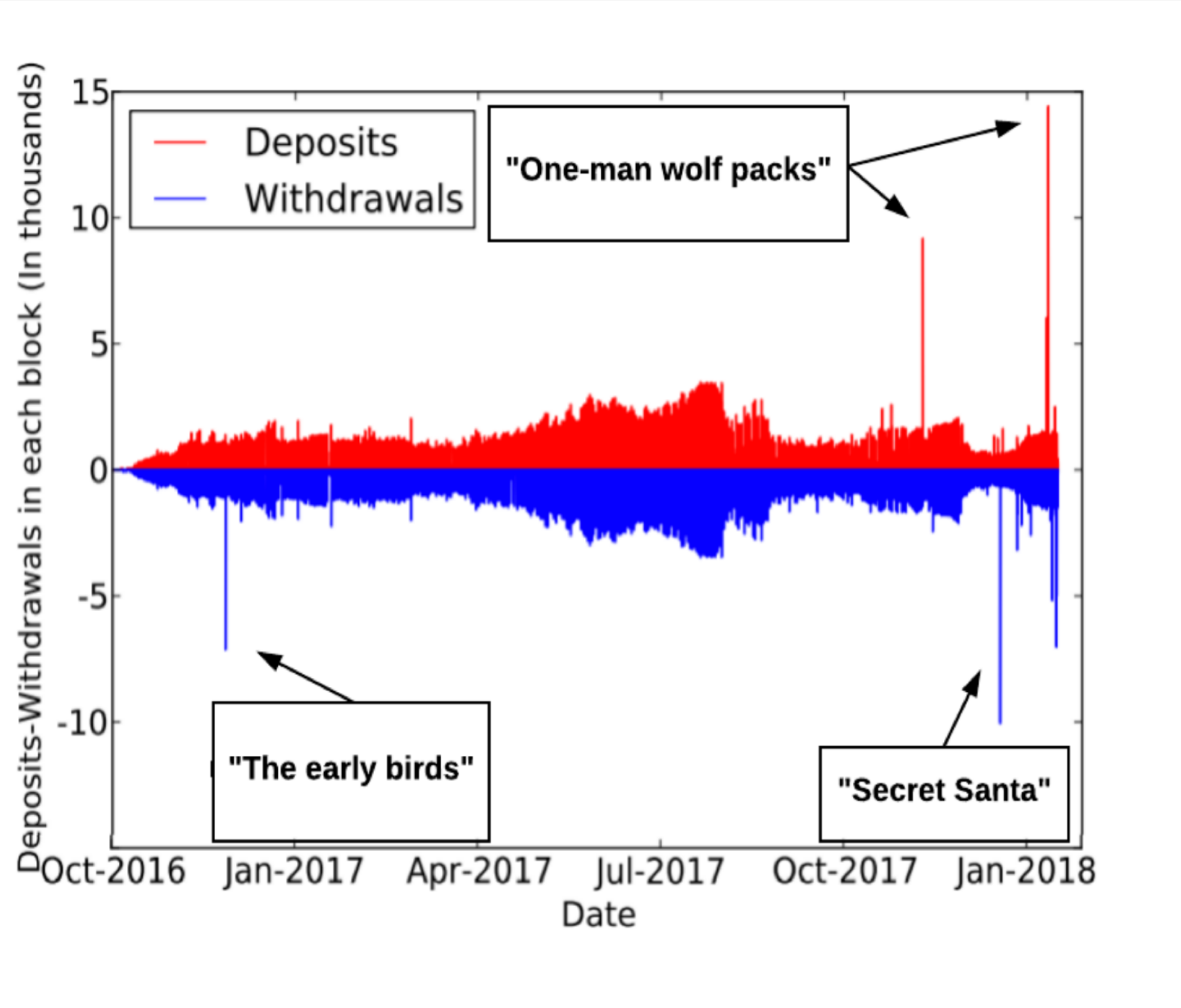
- Miners
  - Come in 2 flavours, independent and mining pools
  - They get 10 ZEC from each block mined
  - They can be trivially identified as the recipients of coin generations

- Founders
  - They get 2.5 ZEC from each block mined
  - Their addresses are publicly known

- Others
  - Individual users, exchanges, wallets, etc.

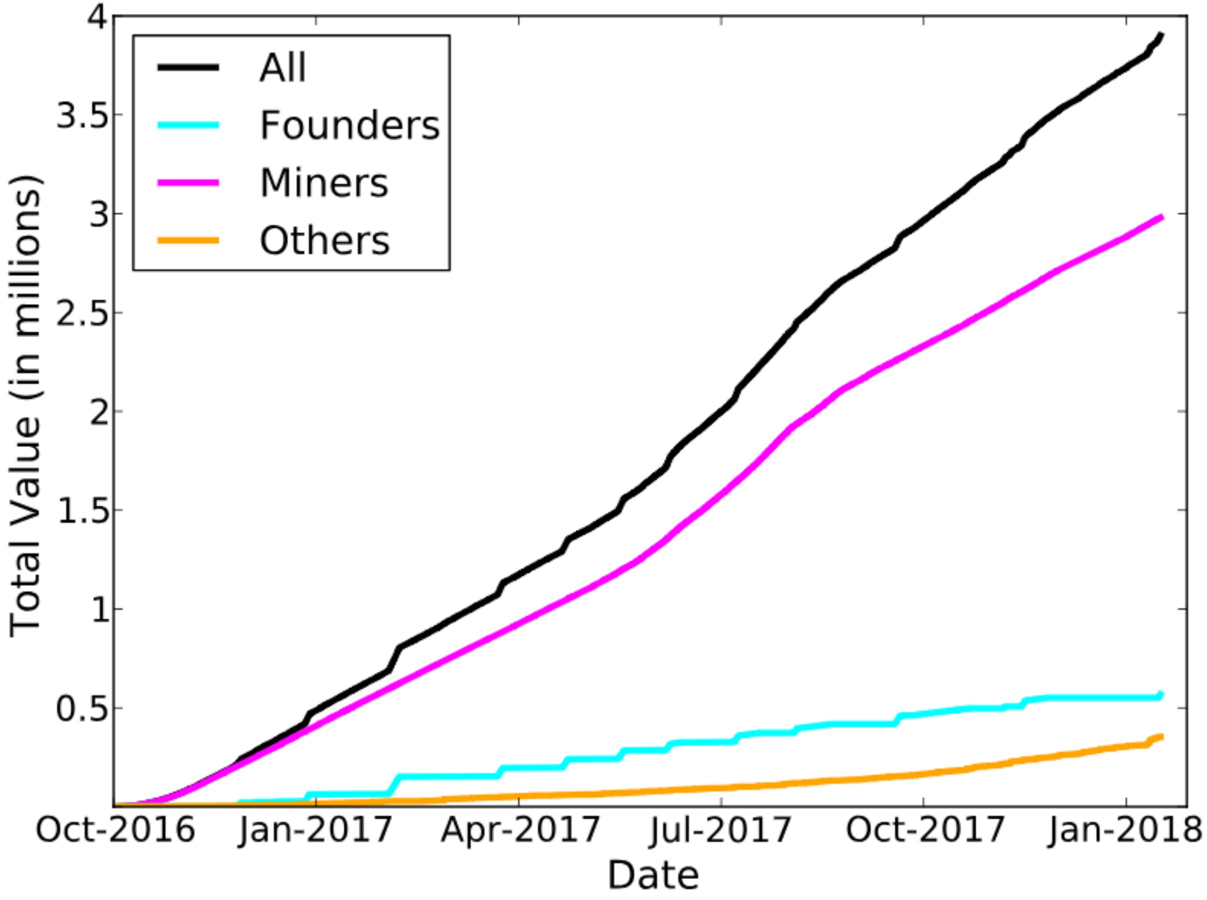


Deposits and Withdrawals in the pool



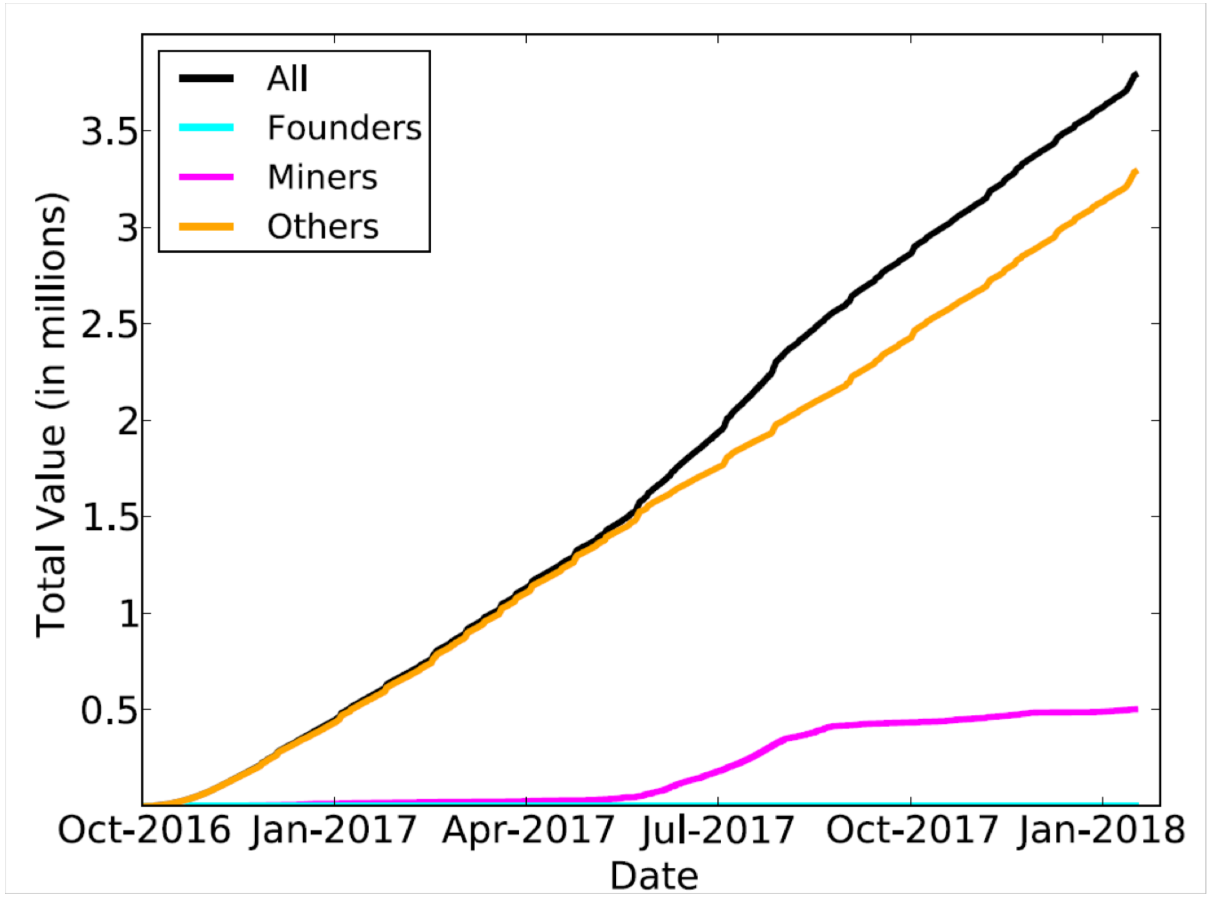
- Almost perfect symmetry
- Pool as a ”pass-through” mechanism
- Interesting spikes

Deposits in the shielded pool using trivially identifiable addresses



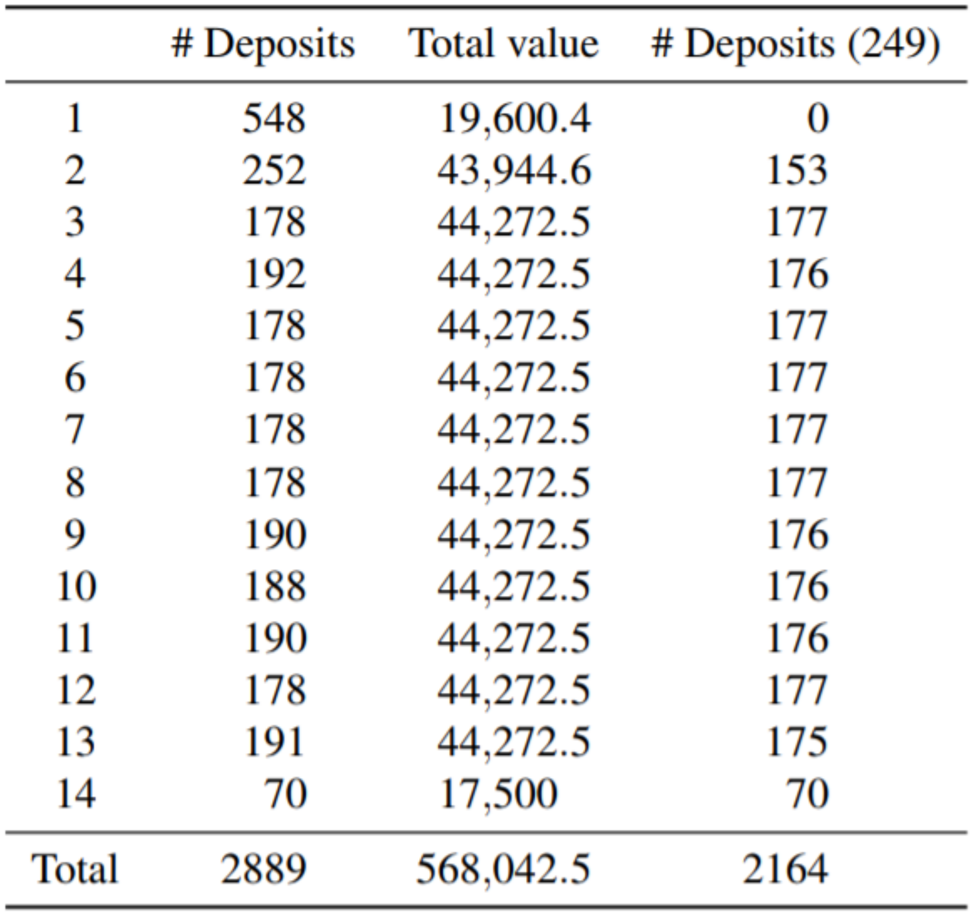
- Almost 80% of the total deposits come from miners
- Founders however create all the visible steps since they deposit bigger values

Withdrawals from the shielded pool using trivially identifiable addresses



- Almost 90% of the total withdrawals were unidentifiable using the trivial addresses
- Need for heuristics for tagging addresses and transactions

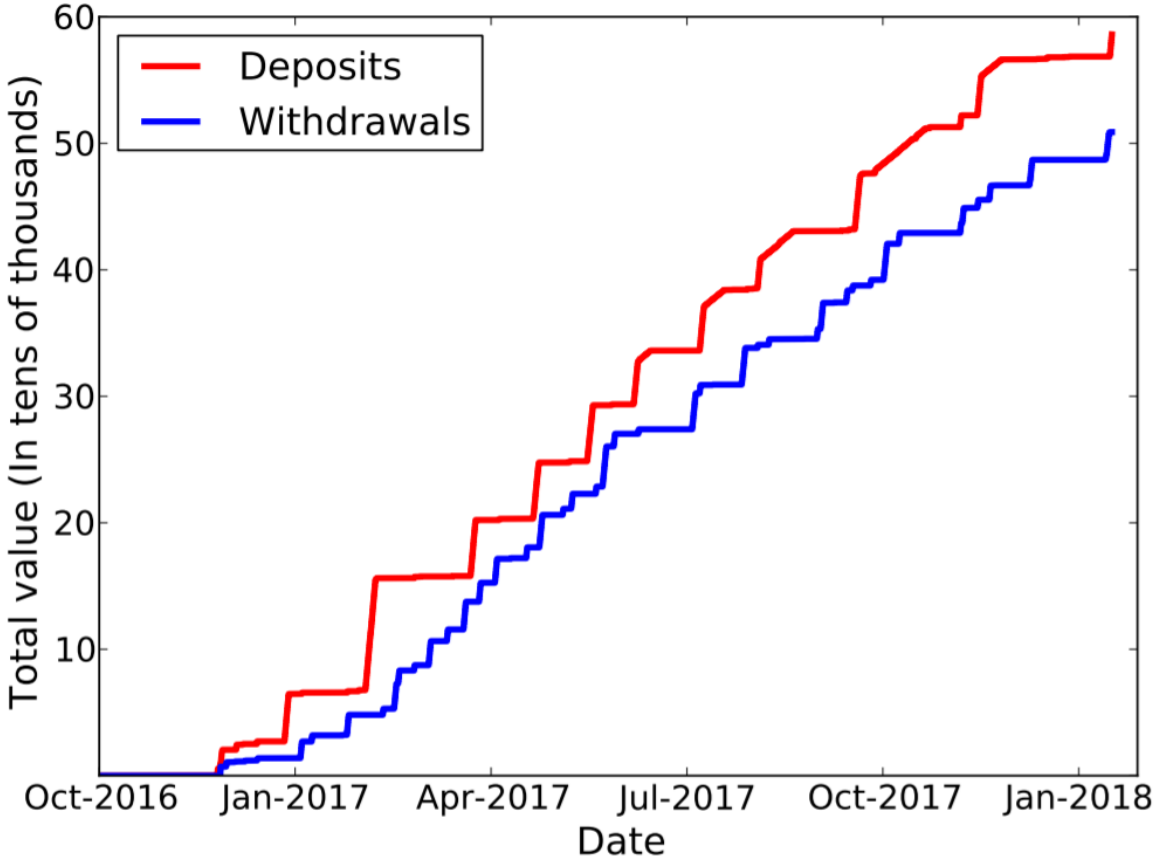
Founders Behaviour



	# Deposits	Total value	# Deposits (249)
1	548	19,600.4	0
2	252	43,944.6	153
3	178	44,272.5	177
4	192	44,272.5	176
5	178	44,272.5	177
6	178	44,272.5	177
7	178	44,272.5	177
8	178	44,272.5	177
9	190	44,272.5	176
10	188	44,272.5	176
11	190	44,272.5	176
12	178	44,272.5	177
13	191	44,272.5	175
14	70	17,500	70
Total	2889	568,042.5	2164

- Founders almost always deposited 249.999 ZEC into the pool
- But there were 0 withdrawals of this value
- And they never withdrew with their known addresses

Founder deposits and withdrawals of 250.001 ZEC



- We did however find a lot of withdrawals of value 250.001 ZEC!

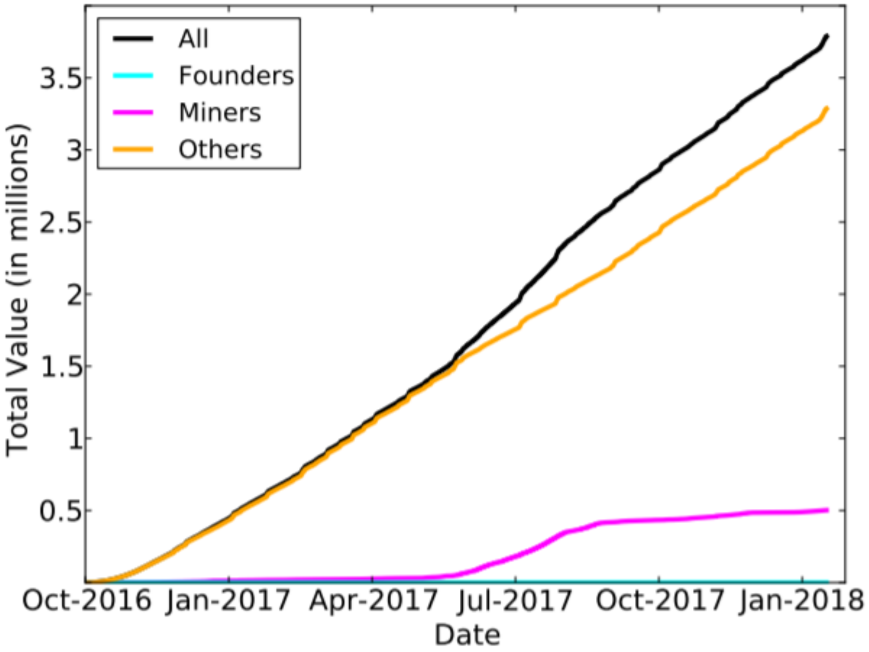
Heuristic – Identifying Founders

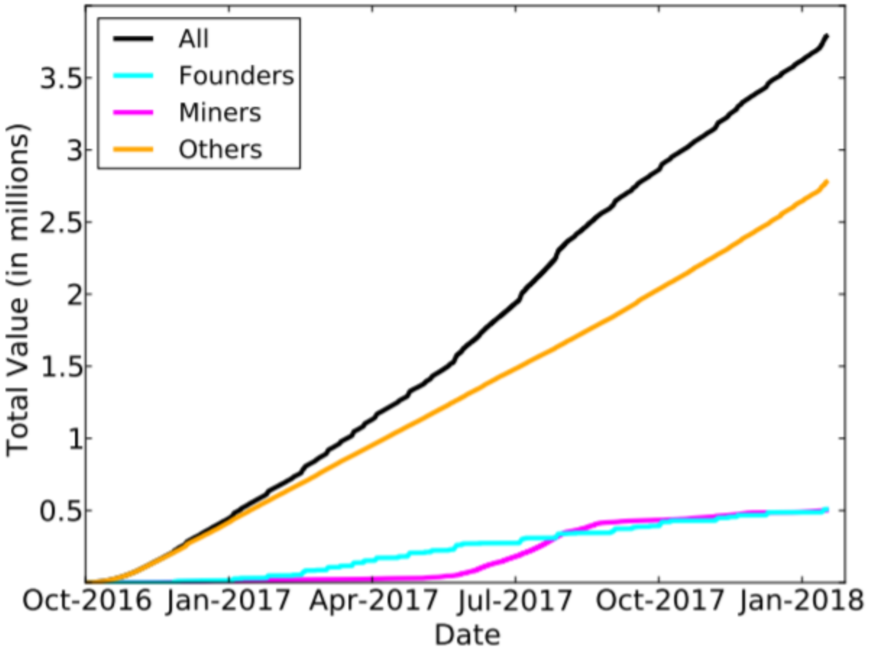
Any z-to-t transaction carrying 250.001 ZEC in value is done by the founders

False Positives

- There were only ever 5 deposits into the pool of approximately 250 ZEC that did not come from the founders

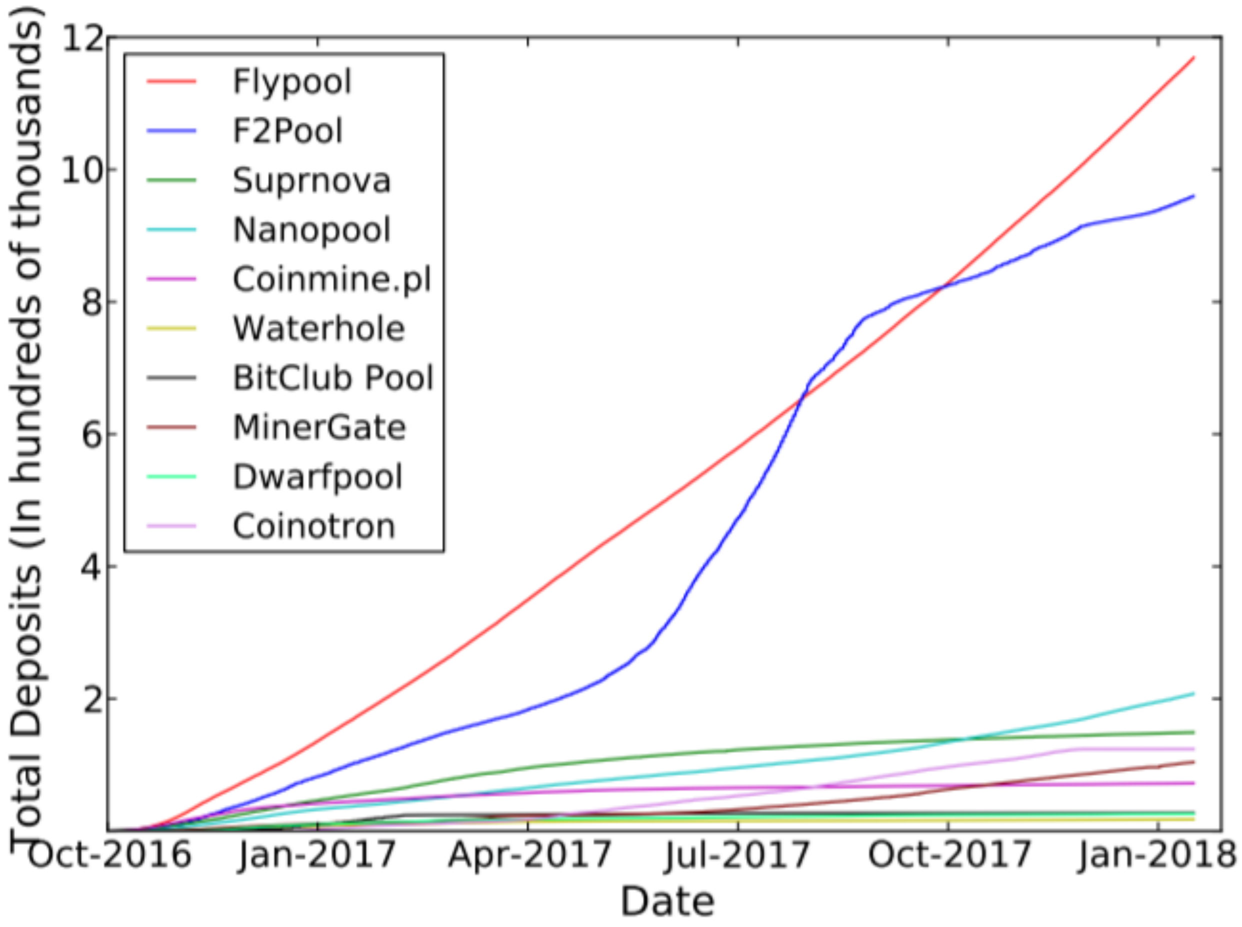
Heuristic – Identifying Founders – Results





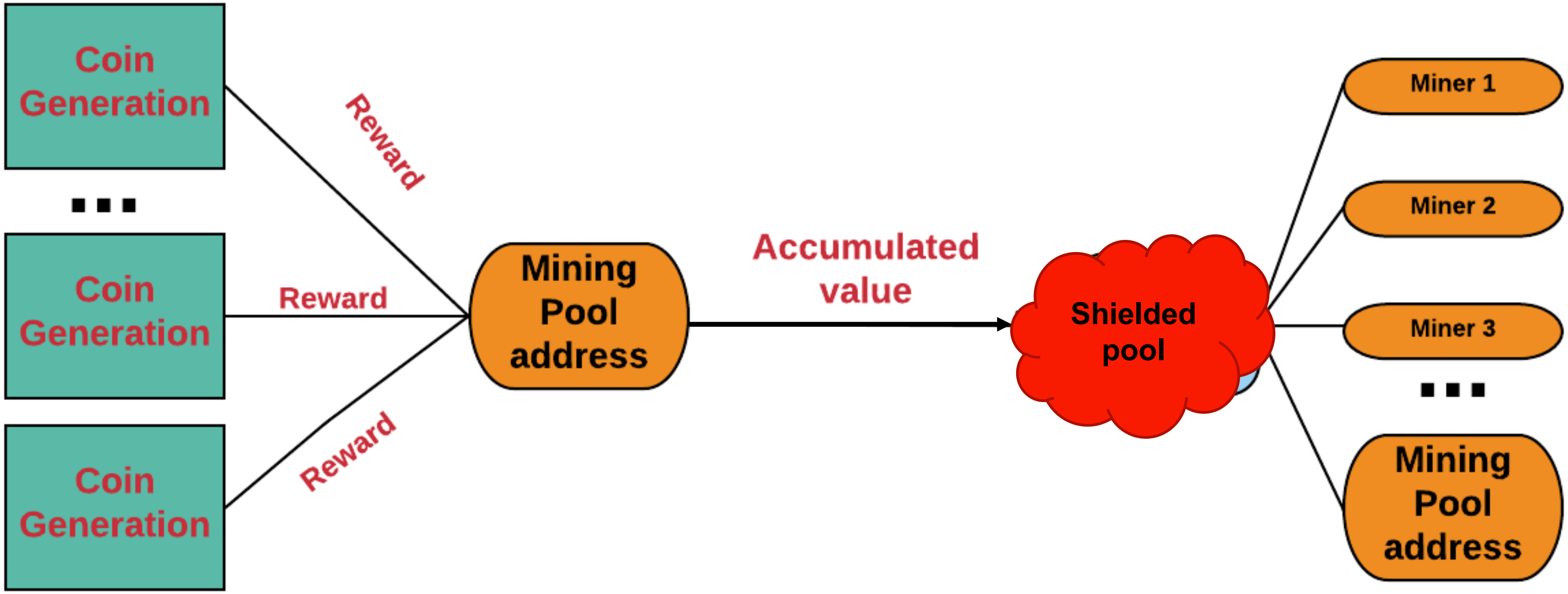
- We flagged 1,953 transactions as founders withdrawals
- Identified a big percentage of the shielded pool’s activity as founder activity

Mining pools behaviour



- We investigated more than 15 different pools but 2 were by far the most dominant ones, Flypool and F2Pool

Mining pools behaviour



There are usually hundreds of recipient addresses!

Heuristic – Identifying Miners

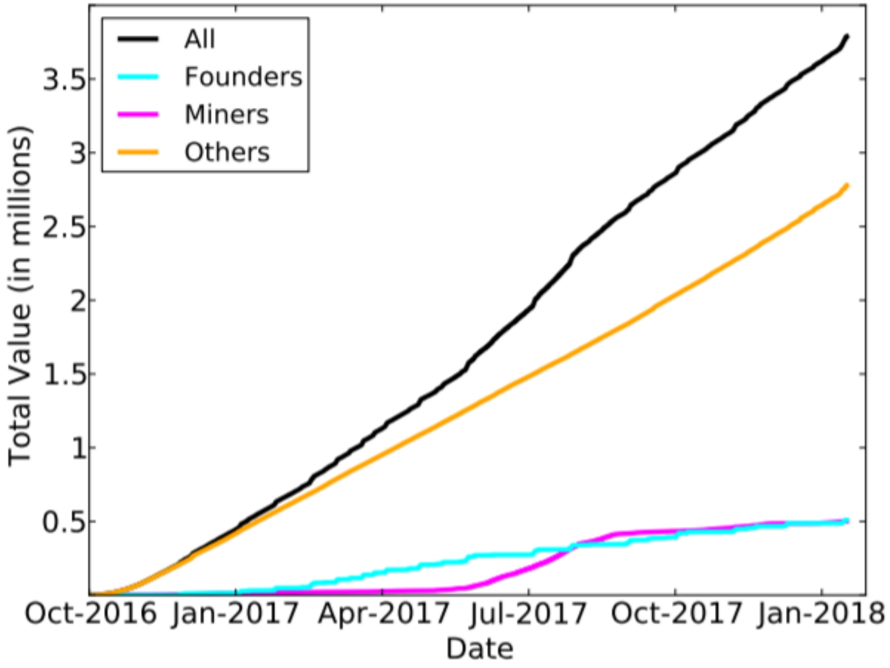
If a z-to-t transaction has over 100 output t-addresses, one of which belongs to a known mining pool, then we label the transaction as a mining withdrawal (associated with that pool), and label all non-pool output t-addresses as belonging to miners

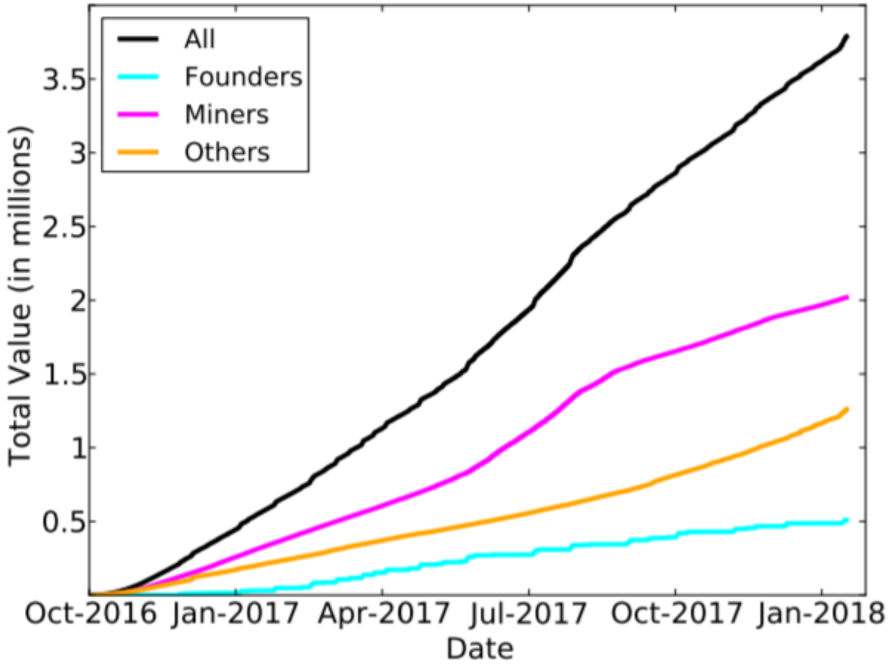
False Positives

The inclusion of a mining pool address makes it unlikely to be a transaction not related to miners

Heuristic – Identifying Miners – Results

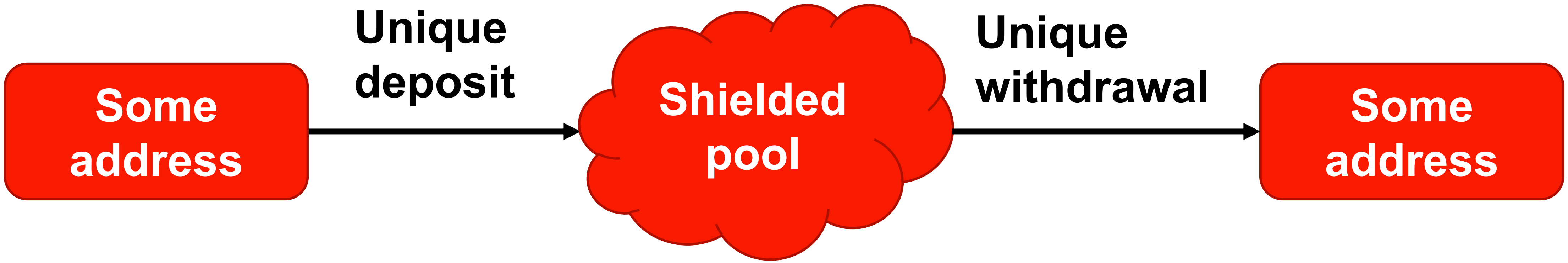
- We flagged 110,918 new addresses as miners
- We associated a large part of the shielded pool's activity as miner activity
  - And we didn't even capture Flypool! (Other people did*…)





*Deanonymization of Hidden Transactions in Zcash, Alex Biryukov, Daniel Feher, University of Luxembourg

Capturing everyone
Unique deposits-withdrawals



Heuristic – Identifying Others

Heuristic – Identifying Others

For a value v, if there exists exactly one t-to-z transaction carrying value v and one z-to-t transaction carrying value v, where the z-to-t transaction happened after the t-to-z one and within some small number of blocks, then these transactions are linked.

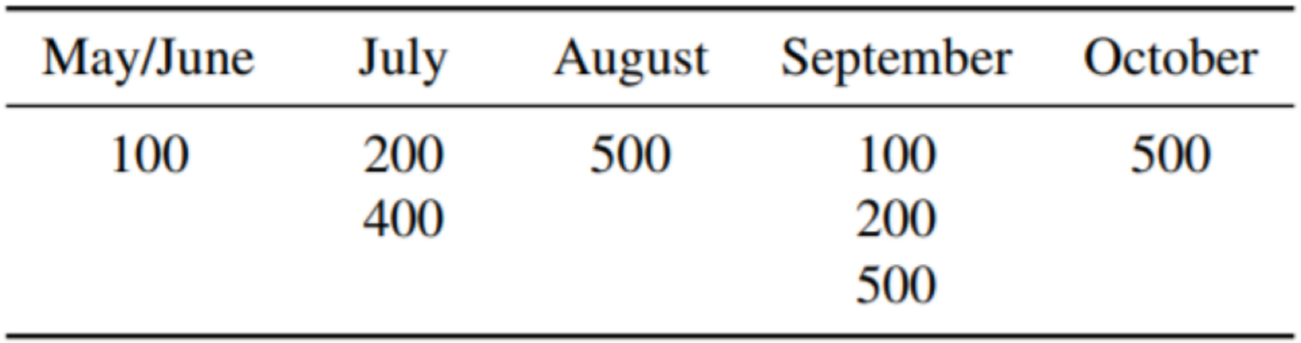
False Positives

- 98.9% of the unique values had at least 3 decimal points
- The heuristic was implemented prior to our work*

*J. Quesnelle. On the linkability of Zcash transactions

Case study: The Shadow Brokers

- Hacker collective that sell and distribute tools supposedly created by the NSA
- One cluster sent transactions to the shielded pool with the amounts and timings that corresponding to TSBs sale activity
- The cluster was a new user
- Most of their coins from Bitfinex!



May/June	July	August	September	October
100	200	500	100	500
	400		200	
			500	

Price of monthly dump in ZEC.

Potential solutions to incentivise private transactions*

- Increase transaction fees for non-private
- Reduce fees for private
- Increase mining reward proportionally to number of private transactions within new blocks
  - May cause an increase in inflation or reduction in existing rewards
- Improve usability
  - Create a user interface
  - Simplify command line interface

*Incentivising Privacy in Cryptocurrencies, Sarah Azouvi, Alexander Hicks, Haaroon Yousaf, OPERANDI 2018

Potential solutions to incentivise private transactions*

- Enforce use of the private pool
  - Difficult to move coins into the pool
  - Potential lock-down of public coins
  - Reduces fungiblity and ownership
    - Increases difficulty for exchanges, law enforcement and services to identify tainted coins
    - Full privacy may cause regulatory issues
- Prevent users in private transactions from not splitting their coins

*Incentivising Privacy in Cryptocurrencies, Sarah Azouvi, Alexander Hicks, Haaroon Yousaf, OPERANDI 2018

THANK YOU

Questions?