An Empirical Analysis of Anonymity in Zcash

George Kappos, Haaroon Yousaf, Mary Maller, Sarah Meiklejohn

University College London

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.

But that didn't work out very well

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

By Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, Stefan Savage
Communications of the ACM, April 2016, Vol. 59 No. 4, Pages 86-93

But that didn't work out very well

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

By Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, Stefan Savage
Communications of the ACM, April 2016, Vol. 59 No. 4, Pages 86-93

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

But that didn't work out very well

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

By Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, Stefan Savage
Communications of the ACM, April 2016, Vol. 59 No. 4, Pages 86-93

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

Evaluating User Privacy in Bitcoin

Elli Androulaki[1], Ghassan O. Karame[2], Marc Roeschlin[1], Tobias Scherer[1], and Srdjan Capkun[1]

[1] ETH Zurich, 8092 Zuerich, Switzerland
elli.androulaki@inf.ethz.ch, romarc@student.ethz.ch, schereto@student.ethz.ch, capkuns@inf.ethz.ch
[2] NEC Laboratories Europe, 69115 Heidelberg, Germany
ghassan.karame@neclab.eu

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.*

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

Some better approaches - Monero

CryptoNote v 2.0

Nicolas van Saberhagen

October 17, 2013

1 Introduction

"Bitcoin" [1] has been a successful implementation of the concept of p2p electronic cash. Both professionals and the general public have come to appreciate the convenient combination of public transactions and proof-of-work as a trust model. Today, the user base of electronic cash is growing at a steady pace; customers are attracted to low fees and the anonymity provided by electronic cash and merchants value its predicted and decentralized emission. Bitcoin has effectively proved that electronic cash can be as simple as paper money and as convenient as credit cards.

Some better approaches - Monero

CryptoNote v 2.0

Nicolas van Saberhagen

October 17, 2013

1 Introduction

"Bitcoin" [1] has been a successful implementation of the concept of p2p electronic cash. Both professionals and the general public have come to appreciate the convenient combination of public transactions and proof-of-work as a trust model. Today, the user base of electronic cash is growing at a steady pace; customers are attracted to low fees and the anonymity provided by electronic cash and merchants value its predicted and decentralized emission. Bitcoin has effectively proved that electronic cash can be as simple as paper money and as convenient as credit cards.

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

What about 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*

What about 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

18	Tezos	$797,042,506	$1.31	$3,405,918	607,489,041 XTZ *	1.80%	
19	Zcash	$609,149,278	$133.09	$110,780,290	4,576,819 ZEC	-5.63%	
20	OmiseGO	$522,286,338	$3.72	$35,702,678	140,245,398 OMG *	6.36%	

What about 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

18	Tezos	$797,042,506	$1.31	$3,405,918	607,489,041 XTZ *	1.80%	
19	Zcash	$609,149,278	$133.09	$110,780,290	4,576,819 ZEC	-5.63%	
20	OmiseGO	$522,286,338	$3.72	$35,702,678	140,245,398 OMG *	6.36%	

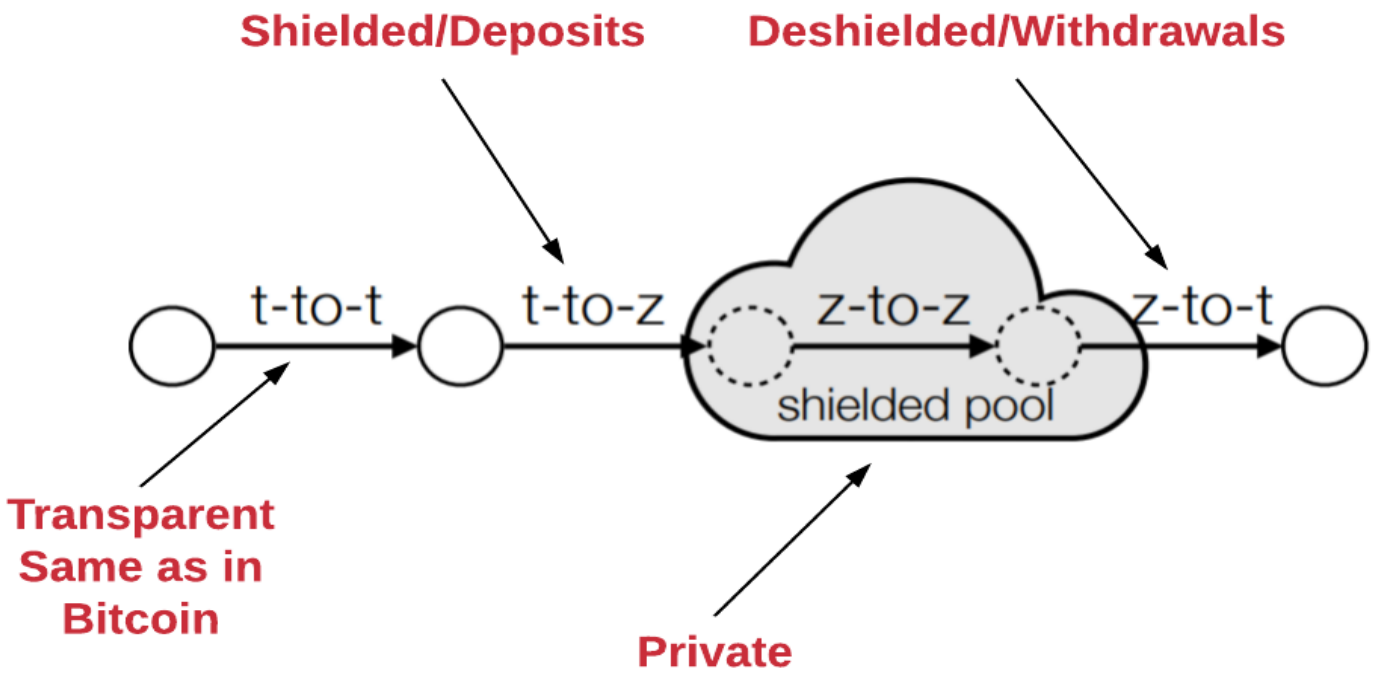
Edward Snowden @Snowden · 15h

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...

286 1.2K 2.5K

Zcash in a nutshell



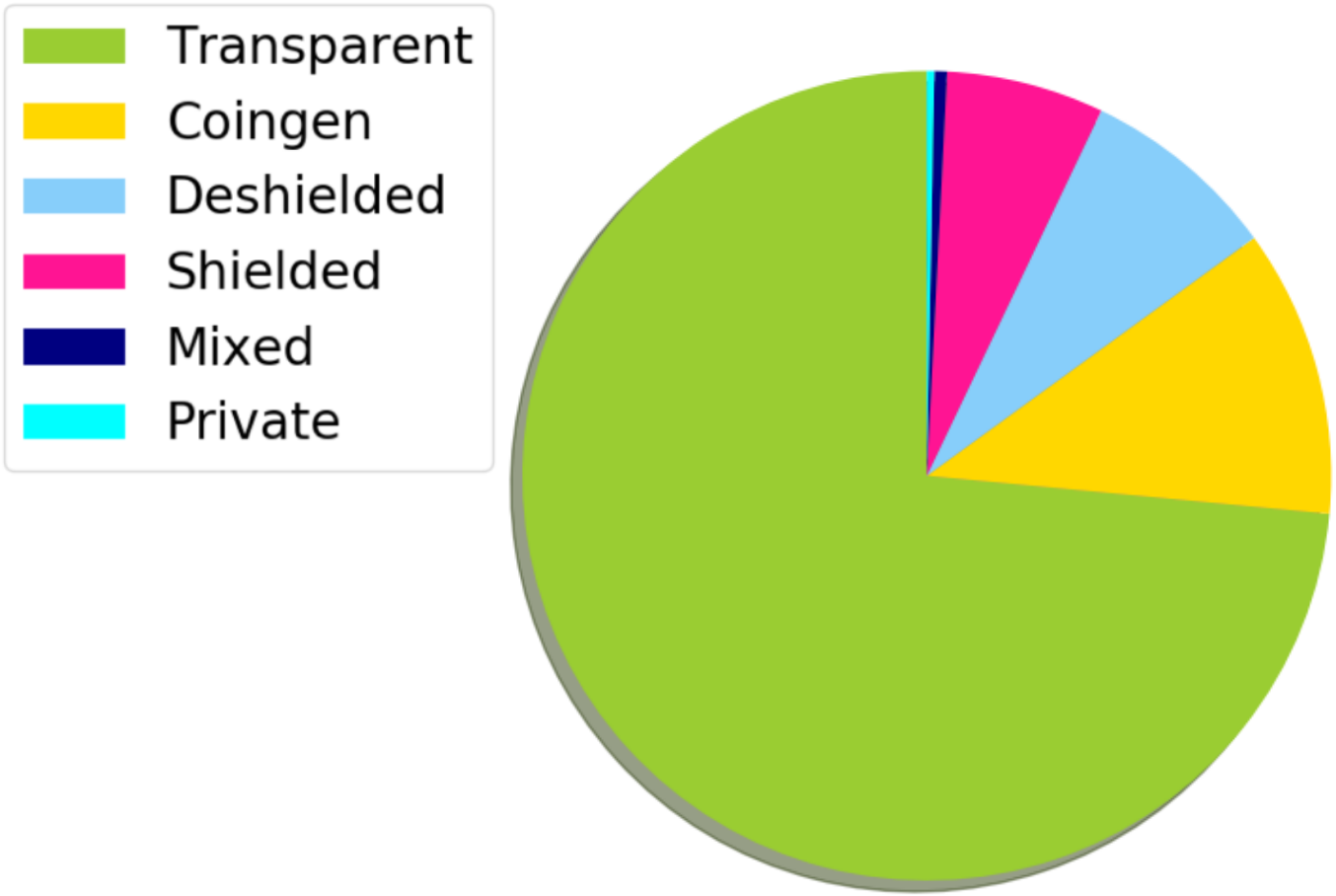
- 2 types of addresses:
  1. Transparent t-address
  2. Private z-address

- The set of z-addresses is a “shielded pool”

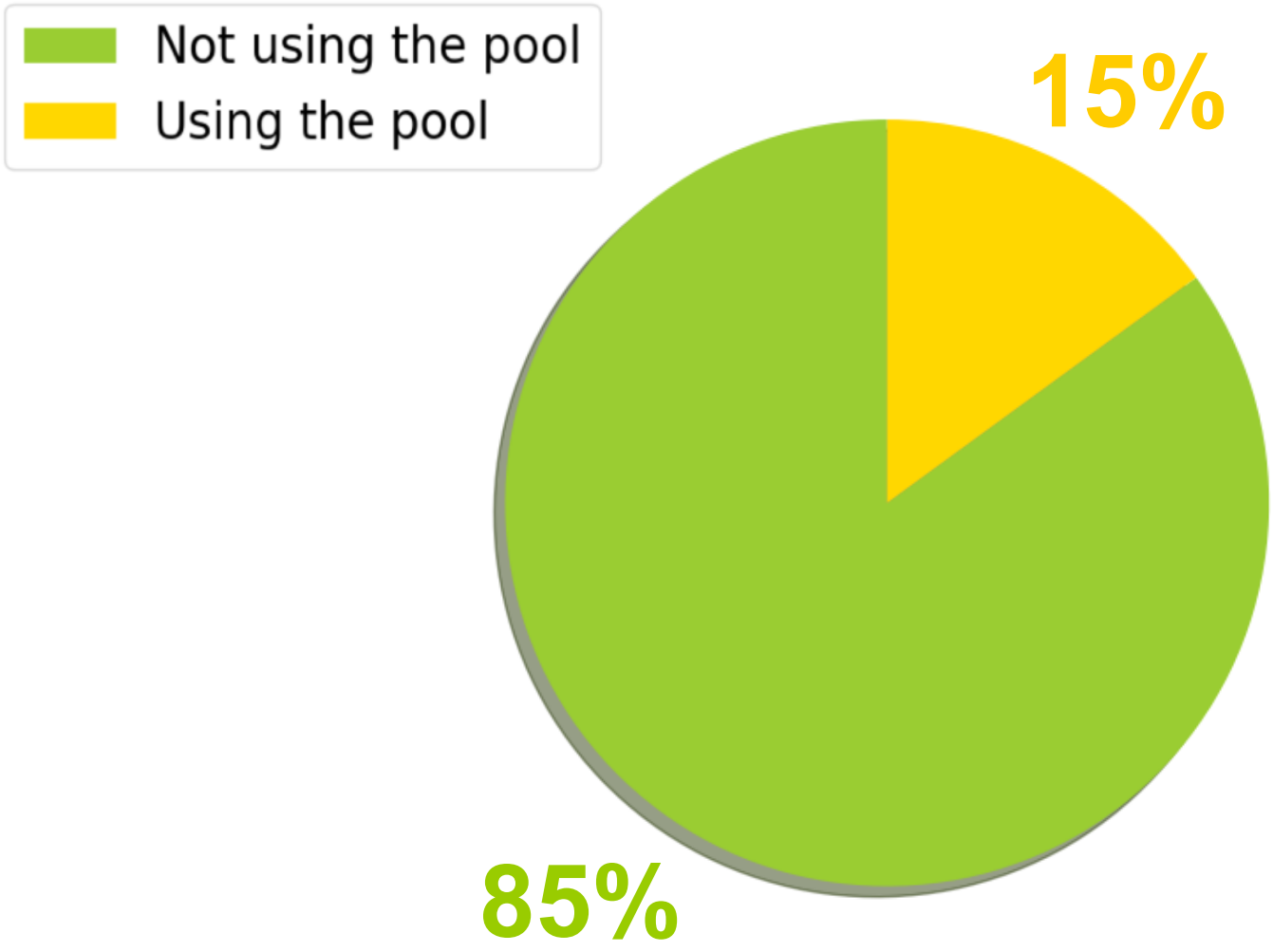
Our Contributions

- Performed a blockchain analysis on Zcash
- Created clusters of users based on t-to-t transactions
- Defined and implemented new heuristics that deanonymized 69.1% of transactions interacting with the shielded pool
- Used our heuristics to investigate the activity of a hacker collective in Zcash (the Shadow Brokers, see paper…)

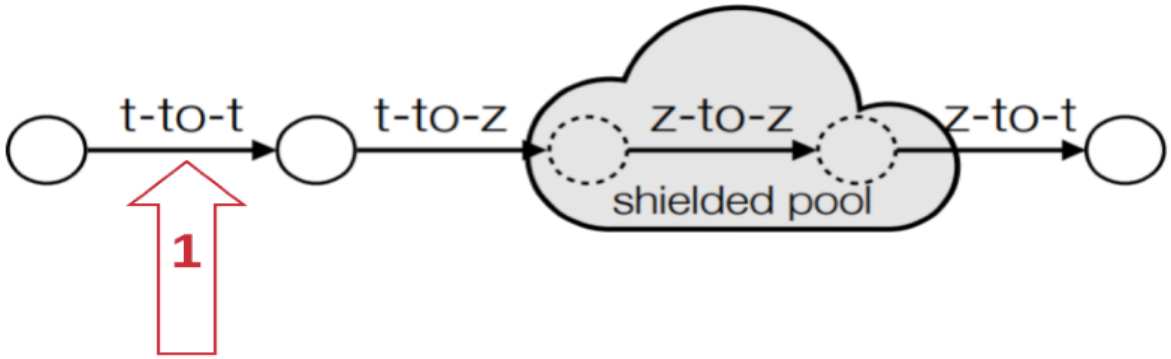
Interactions in Zcash



Interactions in Zcash



Transparent transactions (t-to-t)



Transparent transactions (t-to-t)

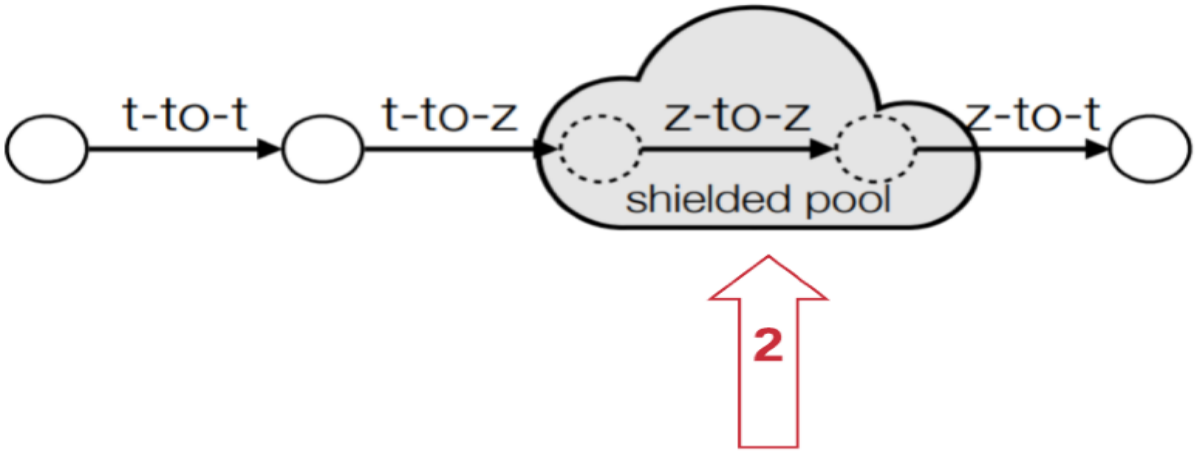
- 85% of the total transactions
- We clustered addresses belonging to the same logical entity and tagged them
- Exploited the techniques used for Bitcoin

Transparent transactions (t-to-t)

Smaller numbers - bigger cluster

Service	Cluster	# deposits	# withdrawals	
Binance	7	1	1	Exchanges
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	

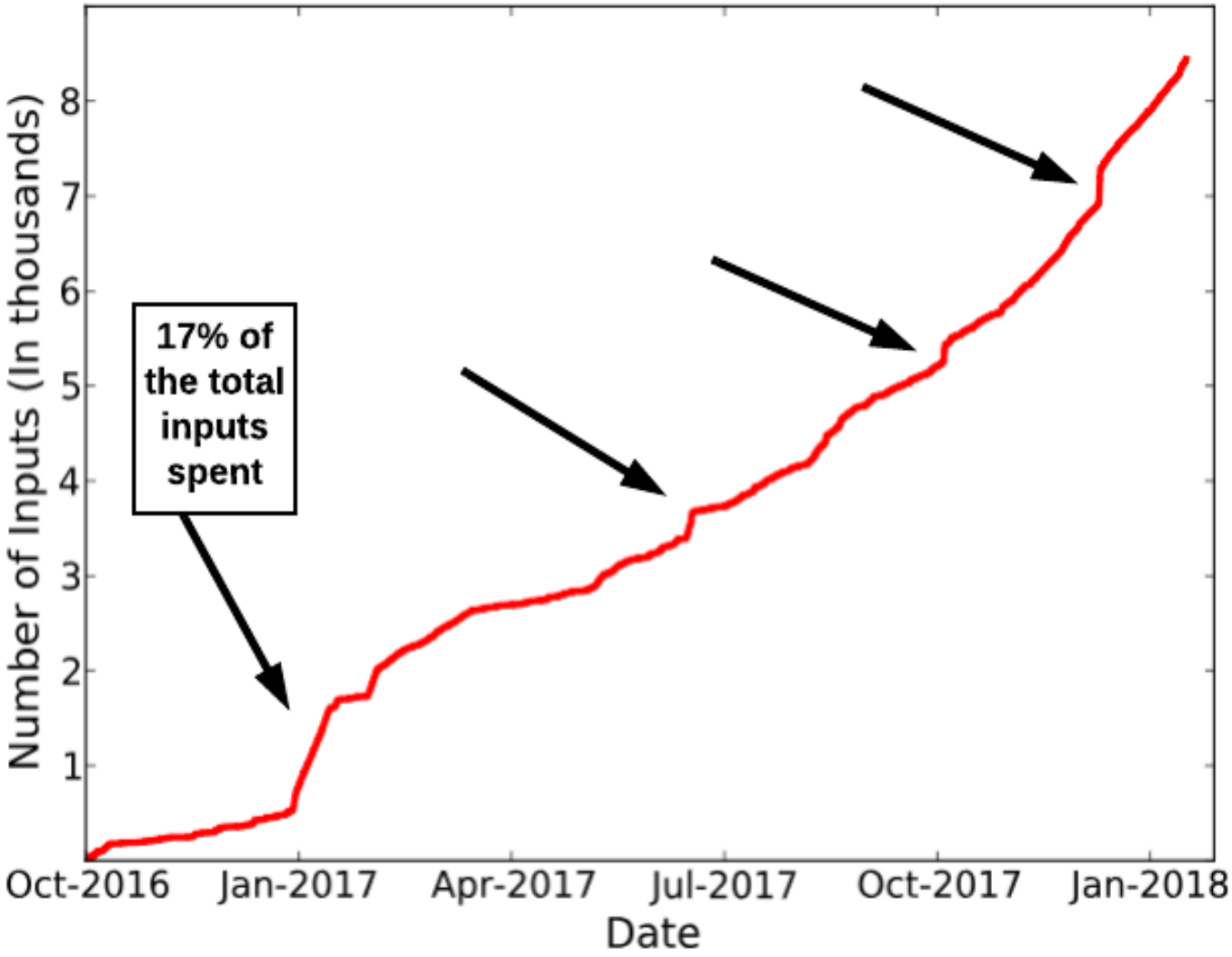
Private transactions (z-to-z)



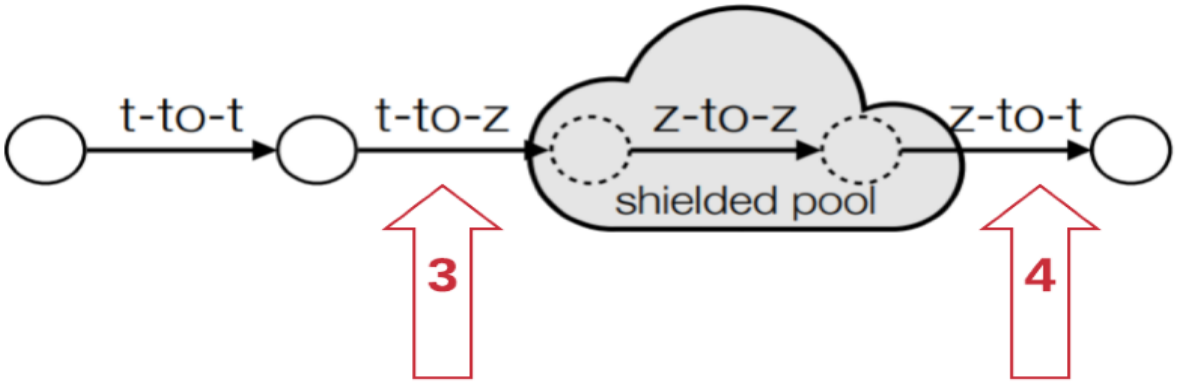
Private transactions (z-to-z)

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

Private transactions (z-to-z)



Shielded and deshielded transactions (t-to-z & z-to-t)



Who is using the pool?

- **Miners**

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

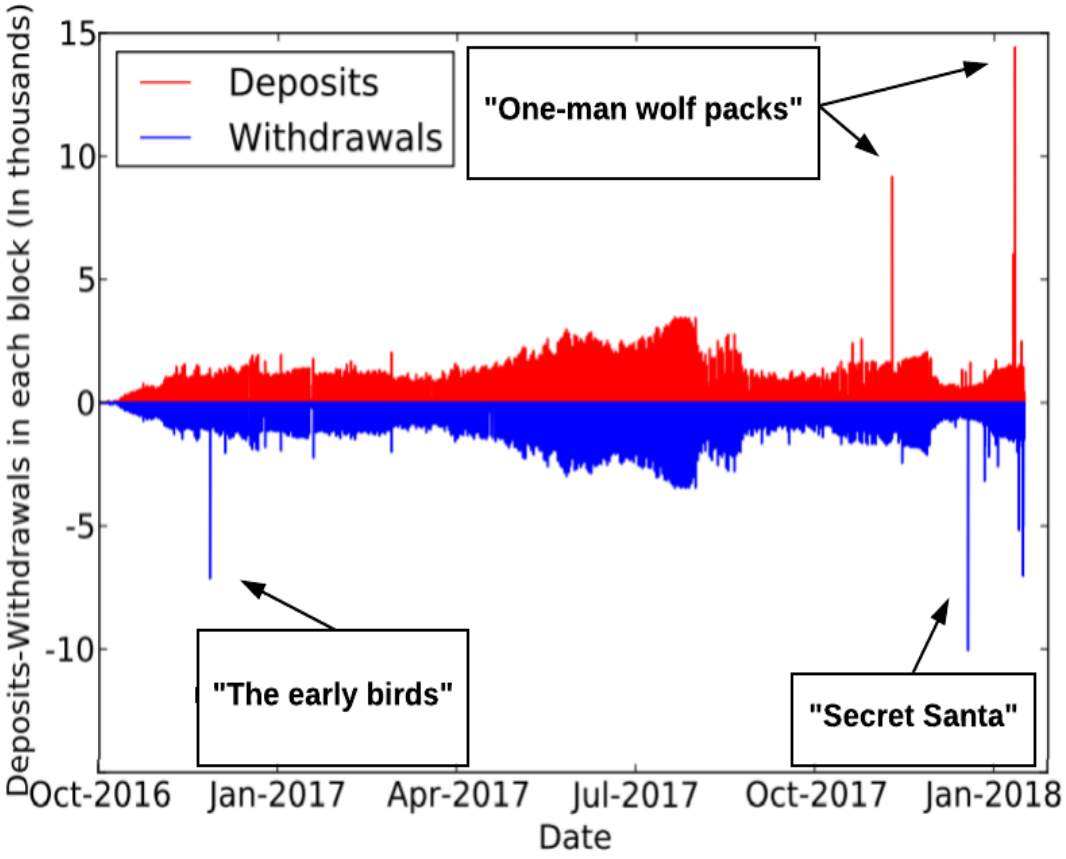
- **Founders**

1. They get 2.5 ZEC from each block mined
2. Their addresses are publicly known

- **Others**

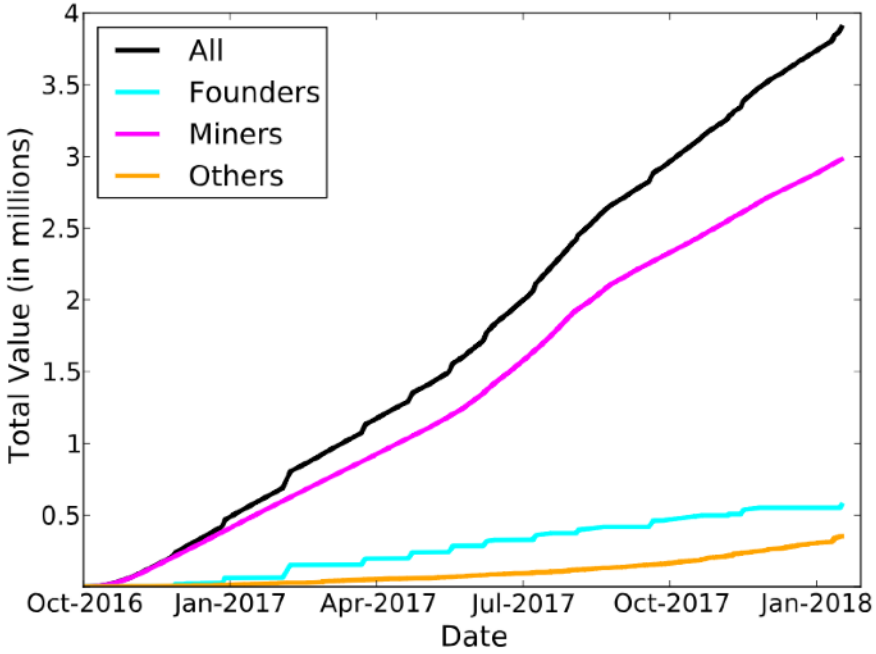
Individual users, exchanges, wallets, etc.

Deposits and Withdrawals



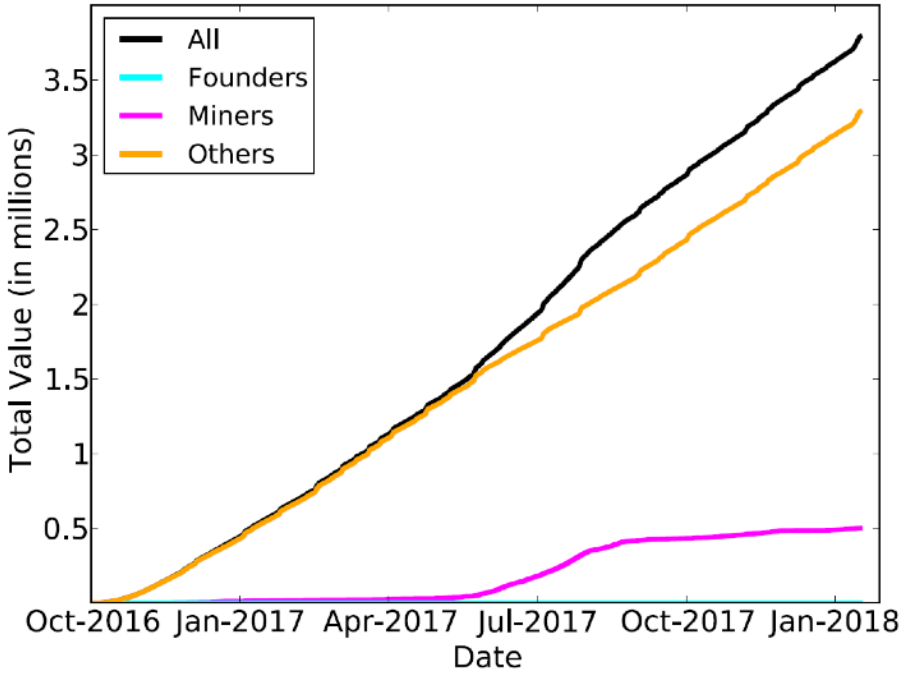
- Almost perfect symmetry
- Pool as a “pass-through” mechanism
- Interesting spikes

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

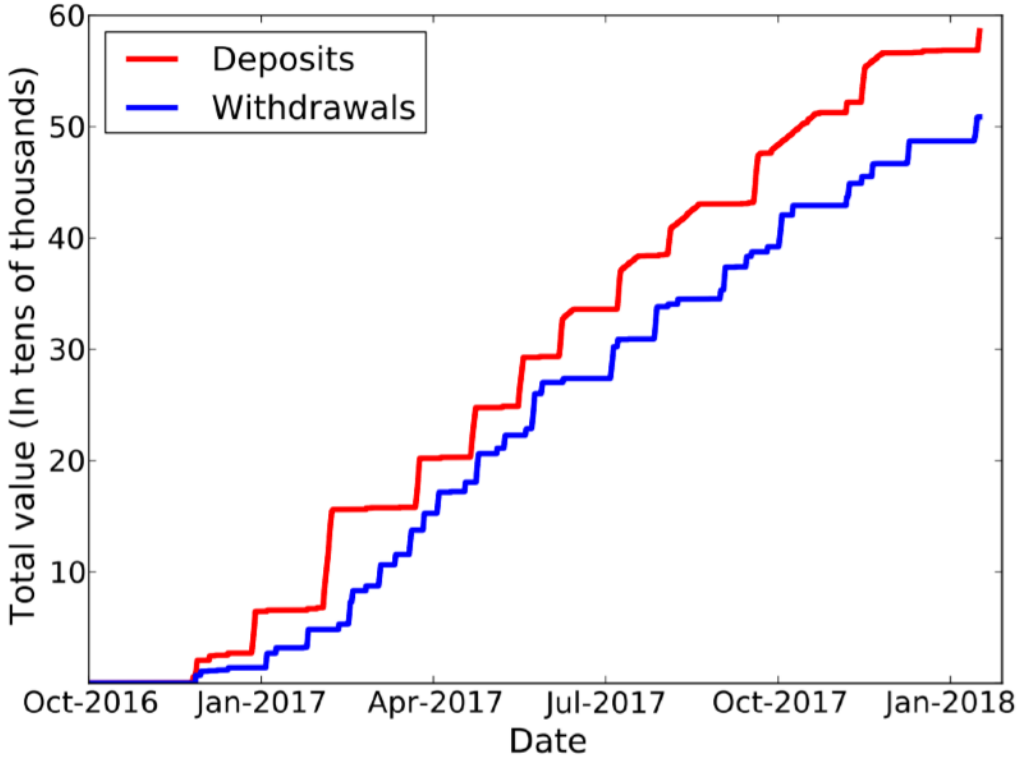
- Need for heuristics for tagging addresses and transactions

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

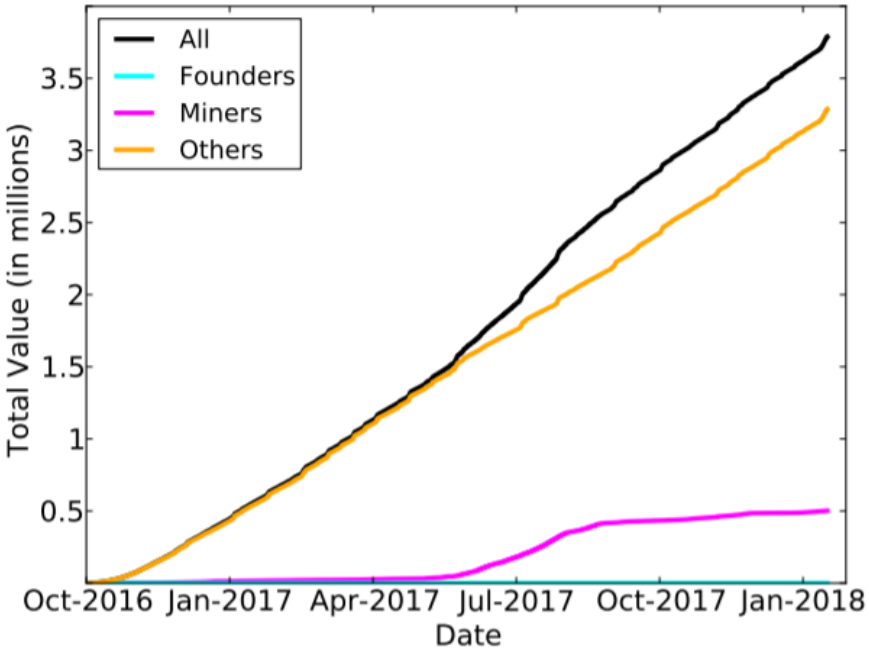
Any z-to-t transaction carrying 250.001 ZEC in value is done by the founders

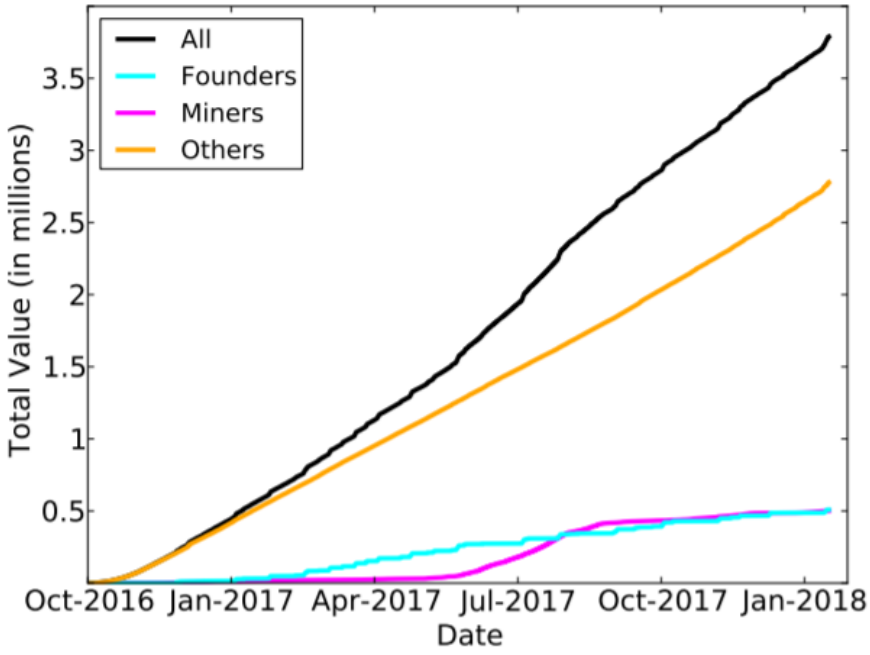
False Positives

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

Heuristic – Identifying Founders – Results

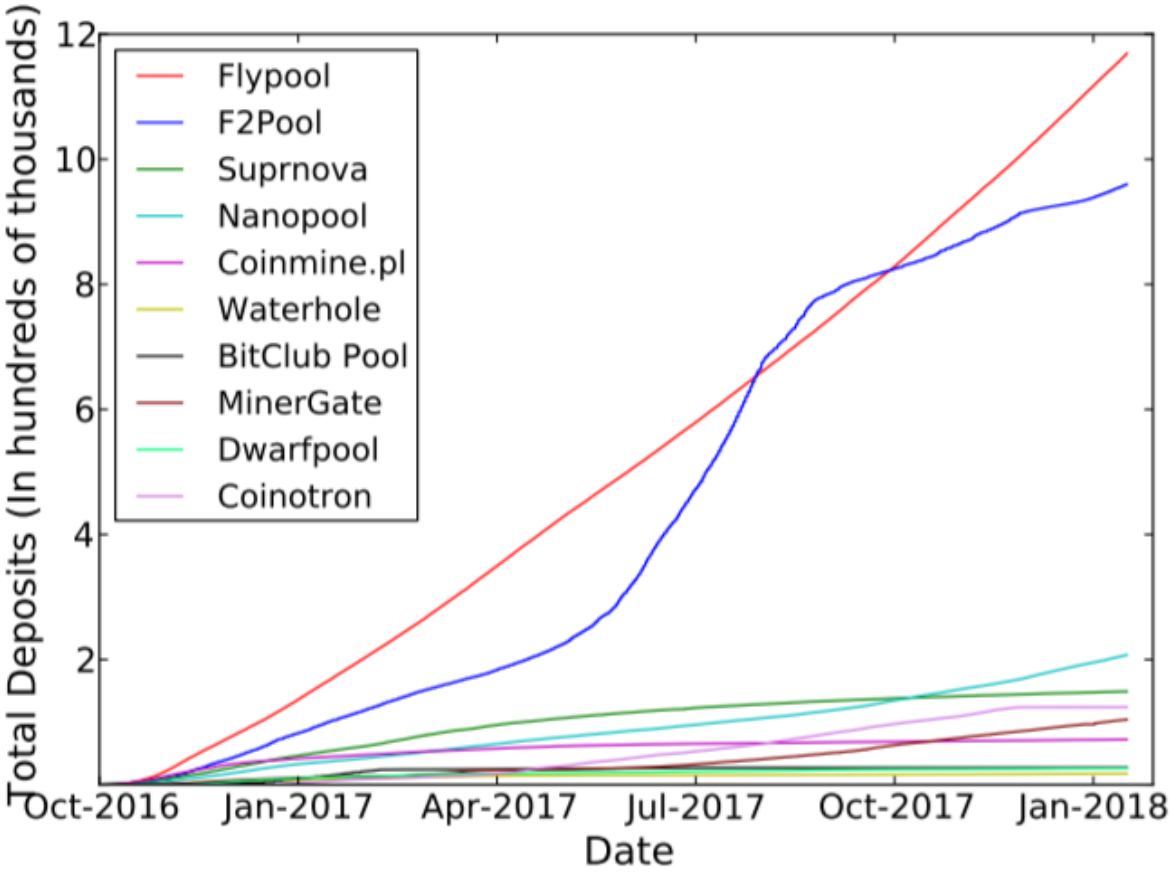
- We flagged 1,953 transactions as founders withdrawals
- Identified a big percentage of the shielded pool's activity as founder activity



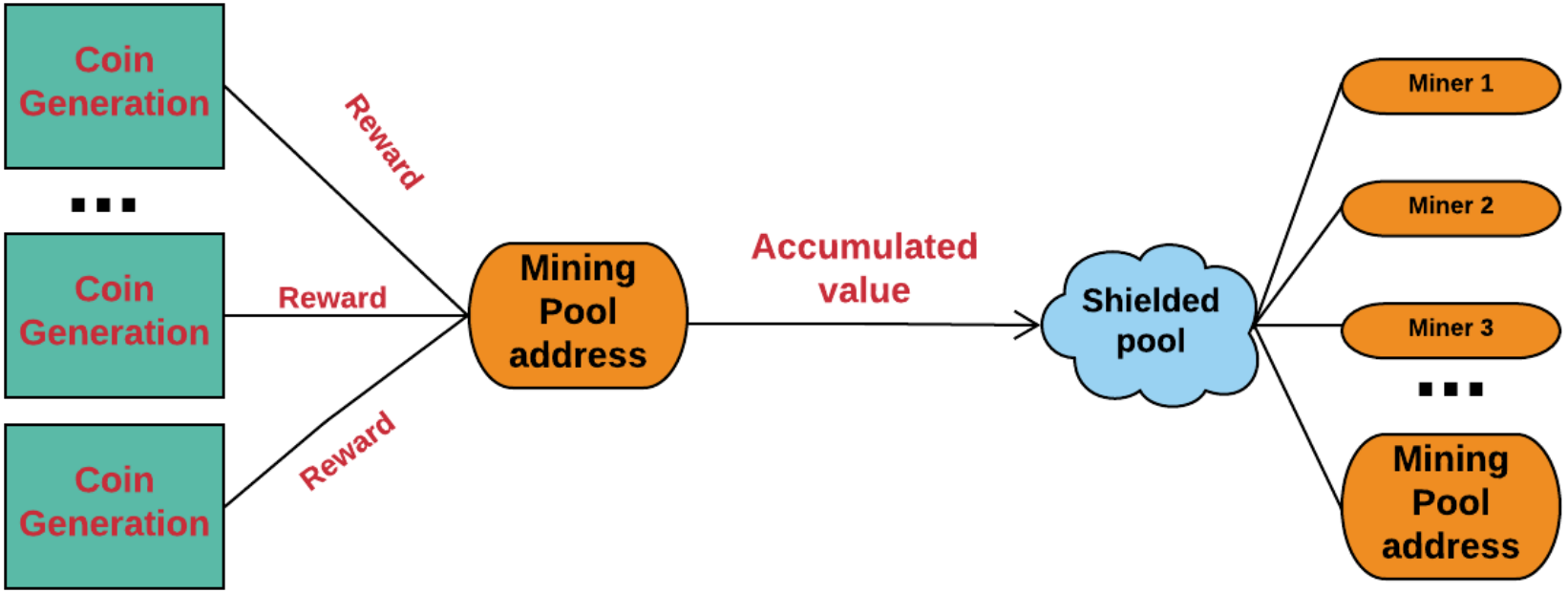


Mining pools behaviour

- 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

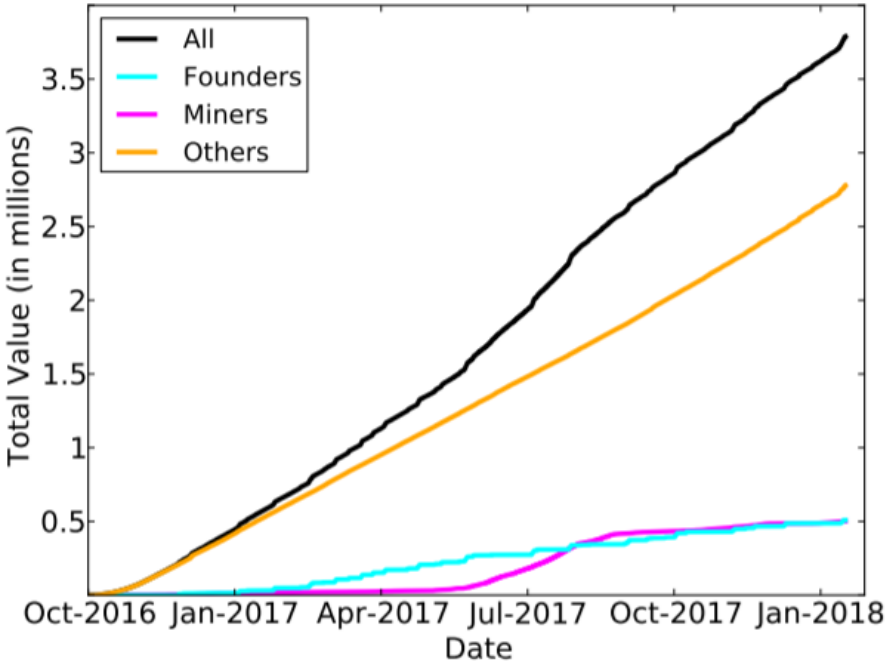
False Positives

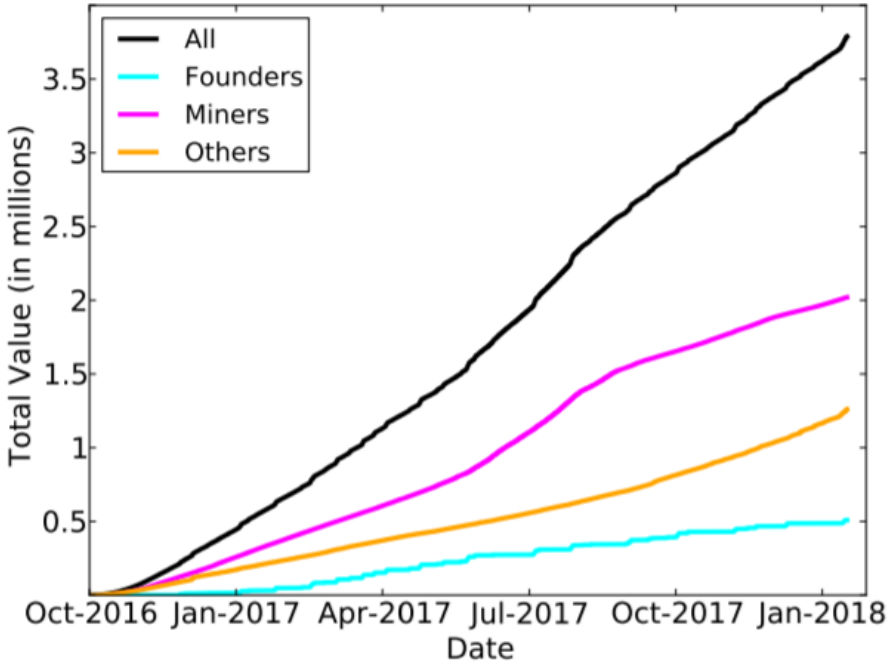
- The inclusion of a mining pool address makes it unlikely to be a transaction not related to miners

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…)





Capturing everyone
Unique deposits-withdrawals

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

Keypoints

- **Usage of the pool is very limited**
  -Incentives for people to use it?

- **Those who do, mostly do it badly**
  -We deanonymized 69.1% of transactions

- The underlying crypto is still secure so Zcash has the potential to provide better anonymity

THANK YOU

QUESTIONS?