



---

# DE-ANONYMIZATION IN BITCOIN AND BEYOND

SARAH MEIKLEJOHN (UCL)

# RISKS OF ANONYMOUS PAYMENTS

## ONLINE DRUG SALES



**LAB TESTED USA DOMESTIC FENTANYL HCL 98% pure -1400mg - Thanks Giving Special 1400mg per order til holiday/ 2500mg per order only on black friday(normally the 1000mg listing)**

From now until ThanksGiving, I am running a special on all my Fentanyl listings and discounting them drastically. The 1000mg listing will now get you 1400mg until the holiday passes. On black friday and only black friday, this amount will be 2500mg. There is no limit to the amount you can order so get your bitcoins ready This is HCL Fentanyl, the strongest you can get. this is as pure FENTANYL ...

Sold by [redacted] - 41 sold since Mar 4, 2016  
Vendor Level 7 Trust Level 5



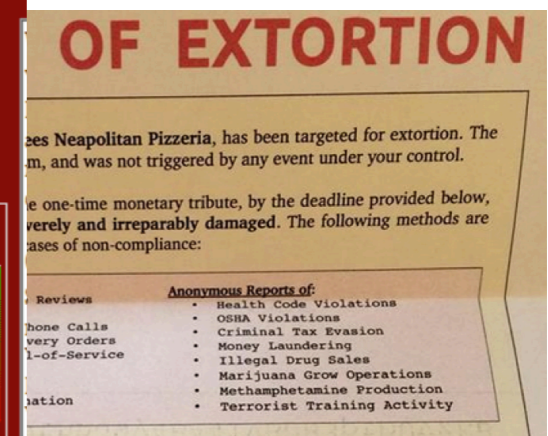
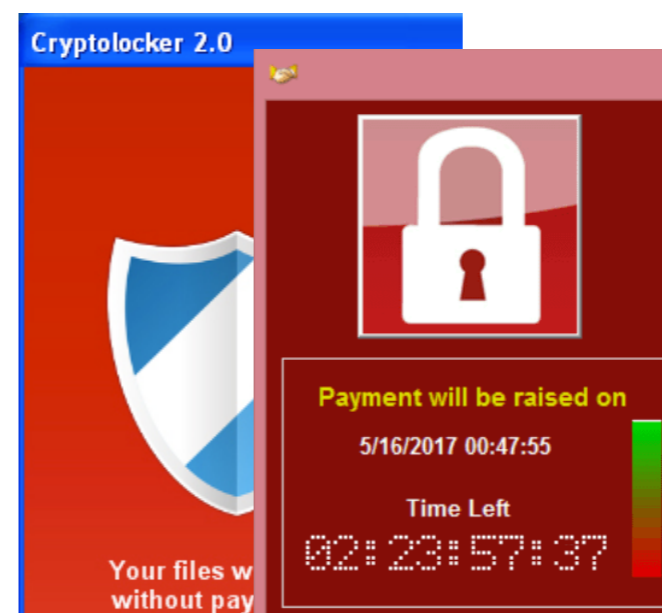
## “CYCLE THEFT”



## THEFTS

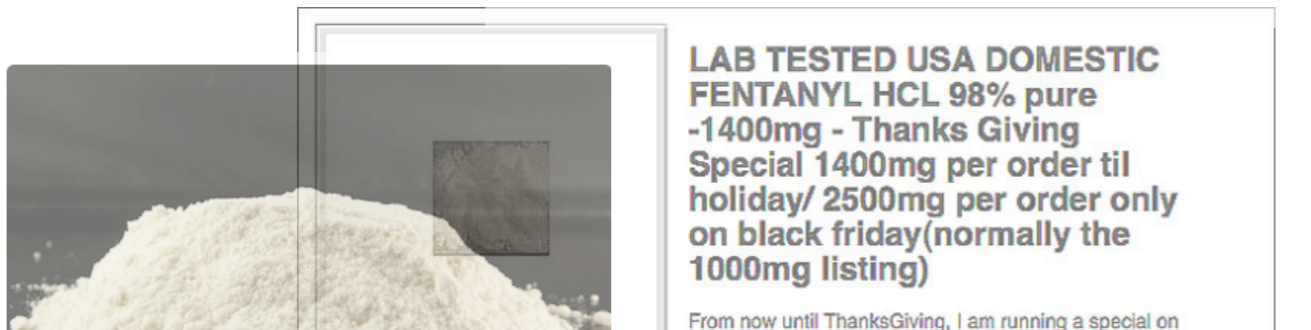


## EXTORTION



# RISKS OF ANONYMOUS PAYMENTS

## ONLINE DRUG SALES



## “CYCLE THEFT”

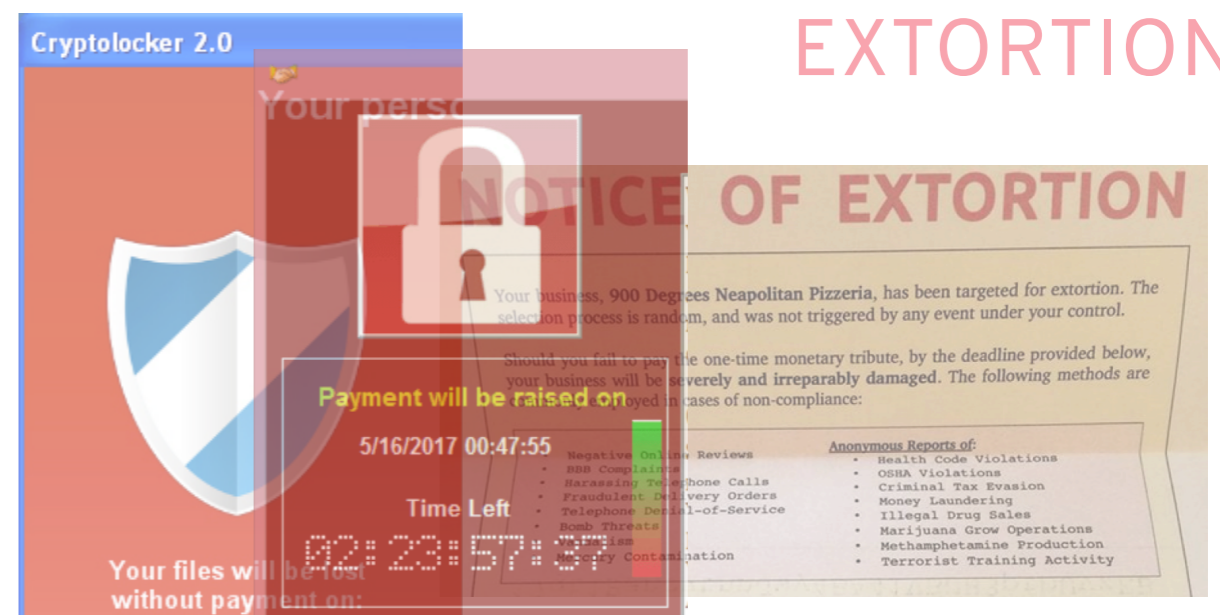


## WHAT ANONYMITY DO CRYPTOCURRENCIES PROVIDE?

## THEFTS



## EXTORTION



# ANONYMITY IN BITCOIN

---

## Quantitative Analysis of the Full Bitcoin Transaction Graph

Dorit Ron and Adi Shamir

Department of Computer Science and Applied Mathematics,  
The Weizmann Institute of Science, Israel  
{dorit.ron, adi.shamir}@weizmann.ac.il

## An Analysis of Anonymity in the Bitcoin System

Fergal Reid and Martin Harrigan

## BitIodine: Extracting Intelligence from the Bitcoin Network

Michele Spagnuolo, Federico Maggi, and Stefano Zanero

Politecnico di Milano, Italy  
michele.spagnuolo@mail.polimi.it, federico.maggi@polimi.it,  
stefano.zanero@polimi.it

## Evaluating User Privacy in Bitcoin

Elli Androulaki<sup>1</sup>, Ghassan O. Karame<sup>2</sup>, Marc Roeschlin<sup>1</sup>,  
Tobias Scherer<sup>1</sup>, and Srdjan Capkun<sup>1</sup>

<sup>1</sup> ETH Zurich, 8092 Zuerich, Switzerland  
elli.androulaki@inf.ethz.ch, romarc@student.ethz.ch,  
schereto@student.ethz.ch, capkuns@inf.ethz.ch

<sup>2</sup> NEC Laboratories Europe, 69115 Heidelberg, Germany  
ghassan.karame@neclab.eu

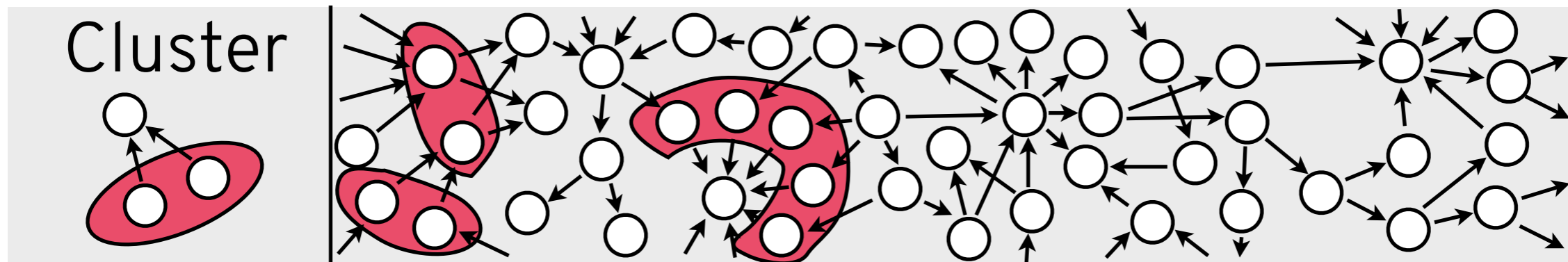
## A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn   Marjori Pomarole   Grant Jordan  
Kirill Levchenko   Damon McCoy<sup>†</sup>   Geoffrey M. Voelker   Stefan Savage



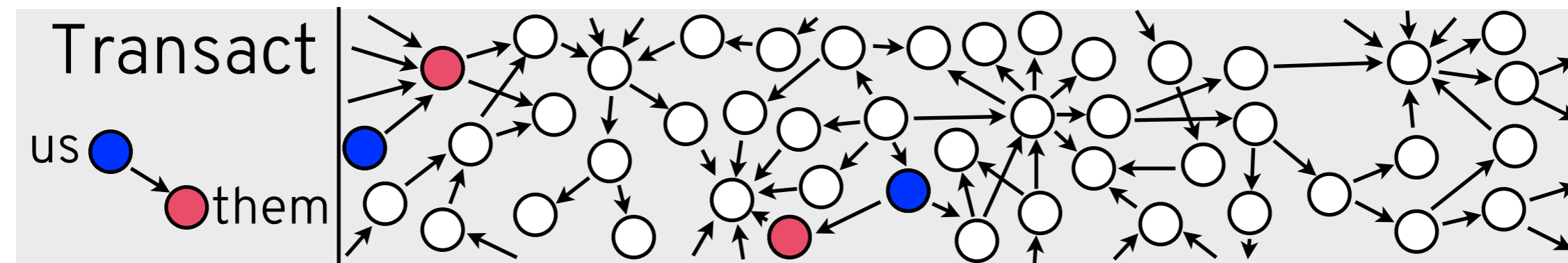
# FISTFUL OF BITCOINS [MPJLMVS'13]

**Problem:** Users or services can use **many addresses**



**Solution:** Develop heuristics to form **address clusters** that represent distinct entities

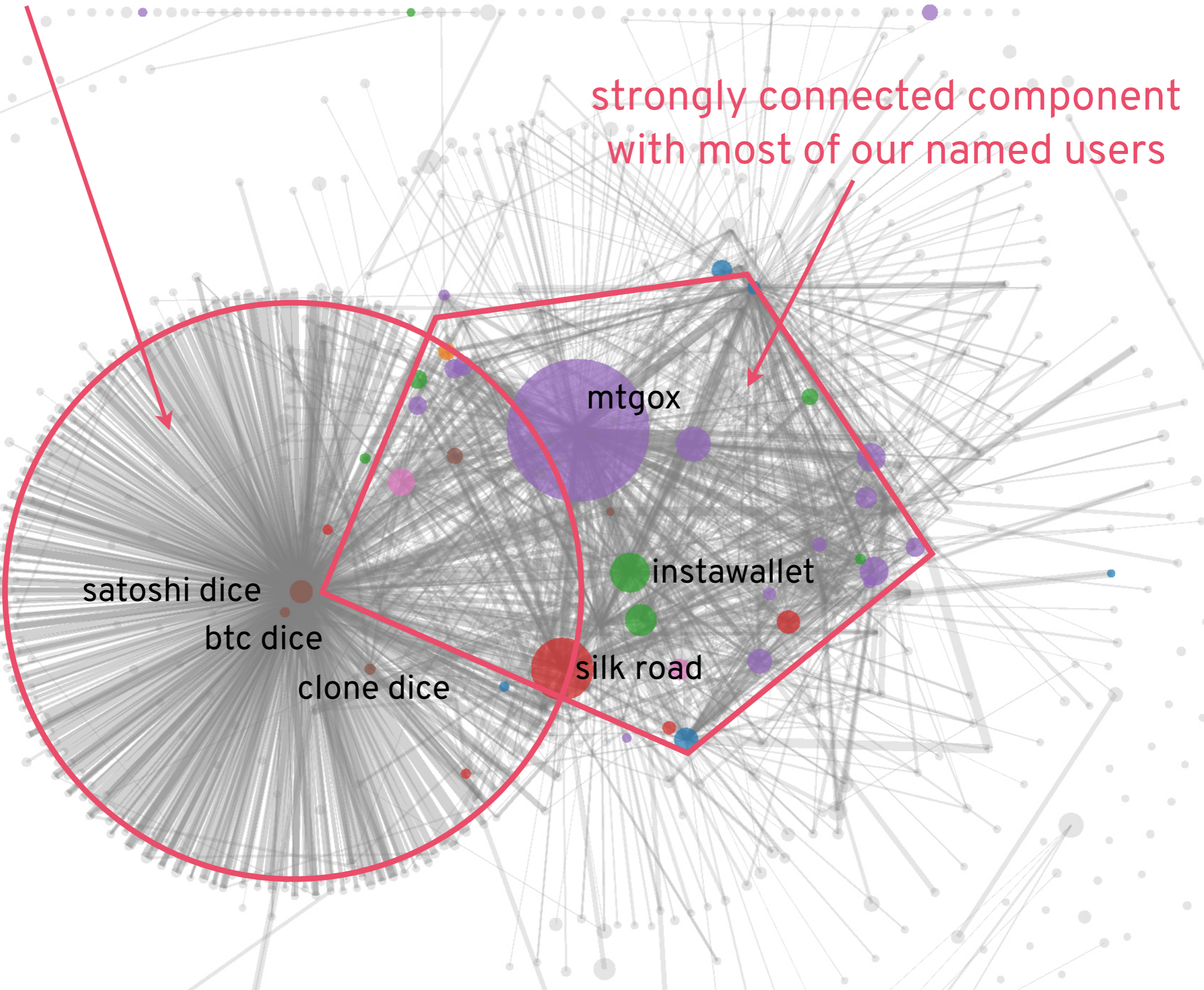
**Problem:** Still don't know **who is who**



**Solution:** Collect **ground truth data** by participating in transactions

“bicycle wheel” with gambling at center

strongly connected component with most of our named users



# RISKS OF ANONYMOUS PAYMENTS

## ONLINE DRUG SALES

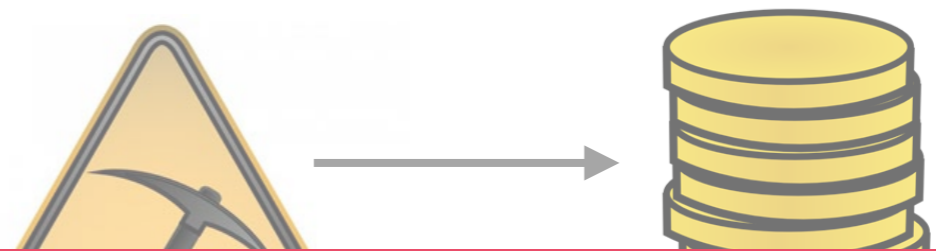


**Andy Greenberg**, Forbes Staff  
Covering the worlds of data security, privacy and hacker culture.  
[+ Follow](#) (1,142)

SECURITY | 9/05/2013 @ 10:36AM | 131,694 views

### Follow The Bitcoins: How We

## “CYCLE THEFT” [HDM+’14]

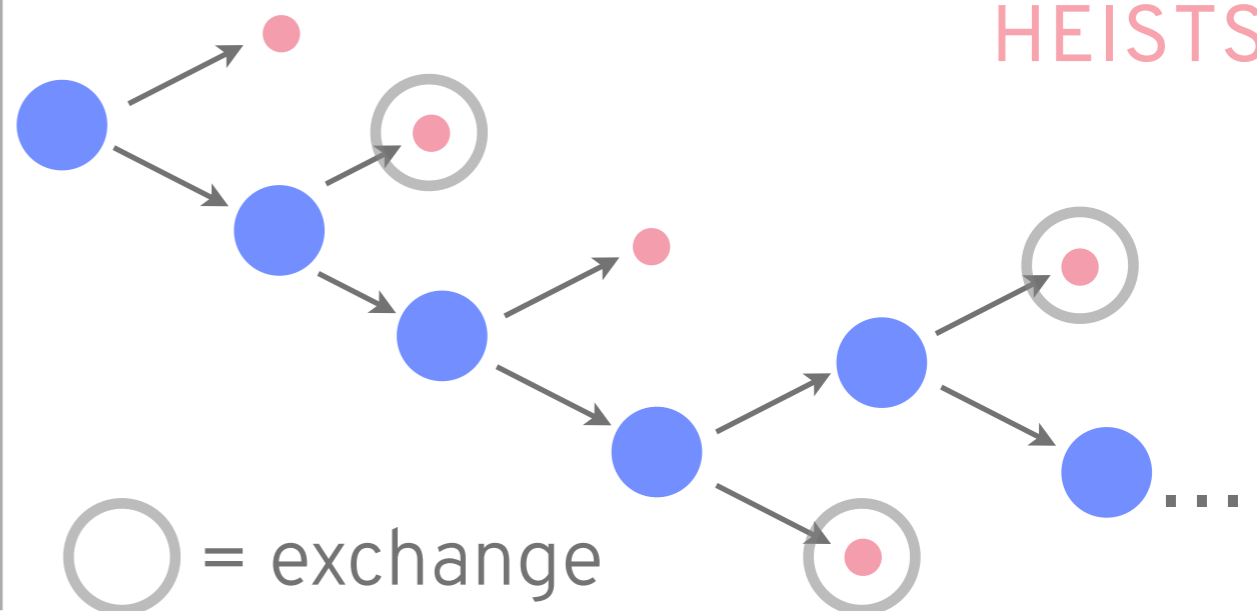


WE TRACED OVER \$3M BACK TO ILLICIT ACTIVITIES!

## THEFTS



## HEISTS





# REAL-WORLD BITCOIN TRACKING

---

**Prosecutors Trace \$13.4M in Bitcoins From the Silk Road to Ulbricht's Laptop**

**The Imperfect Crime: How the WannaCry Hackers Could Get Nabbed**



Quanta**Bytes**























ELLIPTIC



**CHAINALYSIS**



1	 <b>Bitcoin</b>	BTC	11	 <b>TRON</b>	TRX
2	 <b>Ethereum</b>	ETH	12	 <b>IOTA</b>	MIOTA
3	 <b>XRP</b>	XRP	13	 <b>Dash</b>	DASH
4	 <b>Bitcoin Cash</b>	BCH	14	 <b>Binance Coin</b>	BNB
5	 <b>EOS</b>	EOS	15	 <b>NEO</b>	NEO
6	 <b>Stellar</b>	XLM	16	 <b>Ethereum Classic</b>	ETC
7	 <b>Litecoin</b>	LTC	17	 <b>NEM</b>	XEM
8	 <b>Tether</b>	USDT	18	 <b>Tezos</b>	XTZ
9	 <b>Cardano</b>	ADA	19	 <b>VeChain</b>	VET
10	 <b>Monero</b>	XMR	20	 <b>Zcash</b>	ZEC

1

 Bitcoin

BTC

3

 XRP

Pedro Moreno-Sanchez\*, Muhammad Bilal Zafar, and Aniket Kate\*

**Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network**

 Dash

DASH

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**

**A Traceability Analysis of Monero's Blockchain**

Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena

**Privacy-Enhancing Overlays in Bitcoin**

Sarah Meiklejohn<sup>1</sup> and Claudio Orlandi<sup>2</sup>

10

 Monero

XMR

1

 Bitcoin

BTC

3

 XRP

Pedro Moreno-Sanchez\*, Muhammad Bilal Zafar, and Aniket Kate\*

**Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network**

 Dash

DASH

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**

**A Traceability Analysis of Monero’s Blockchain**

Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena

**Privacy-Enhancing Overlays in Bitcoin**

Sarah Meiklejohn<sup>1</sup> and Claudio Orlandi<sup>2</sup>

**An Empirical Analysis of Anonymity in Zcash**

*George Kappos, Haaron Yousaf, Mary Maller, and Sarah Meiklejohn*

10

 Monero

XMR

20

 Zcash

ZEC

# ANONYMITY IN ZCASH [KYMM'18]

## 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



Replying to @JBTheCryptoKing @ANON\_WeAreANON

> Do you comment on coins besides ETH? I was curious 🤔🤔

I do sometimes. @zcashco is cool.

1:58 PM - 10 Aug 2018

9 Retweets 61 Likes



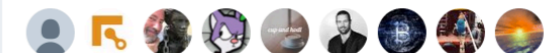
Agree. Zcash's privacy tech makes it the most interesting Bitcoin alternative. Bitcoin is great, but "if it's not private, it's not safe."

Mason & Co. @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...

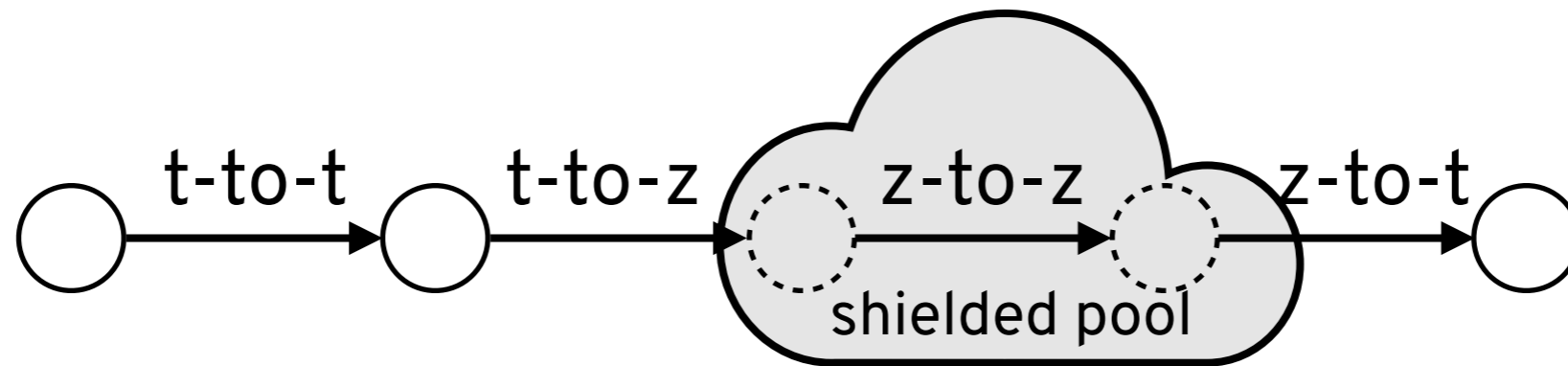
4:23 PM - 28 Sep 2017

1,764 Retweets 3,717 Likes

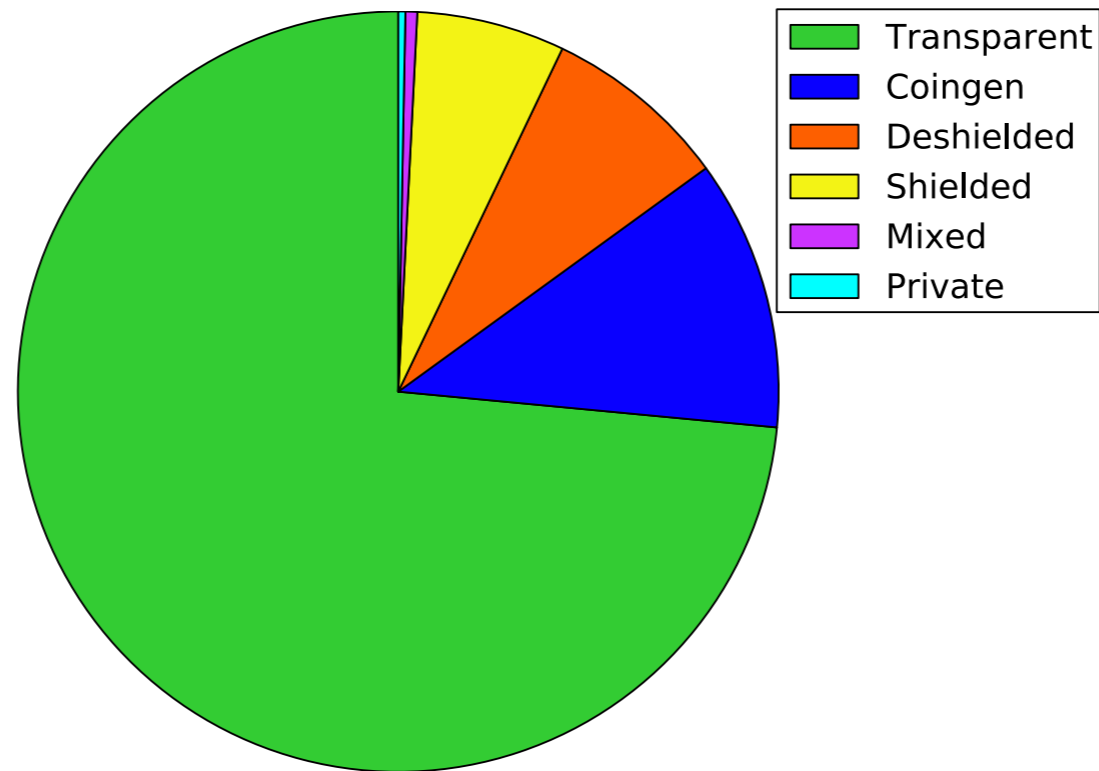
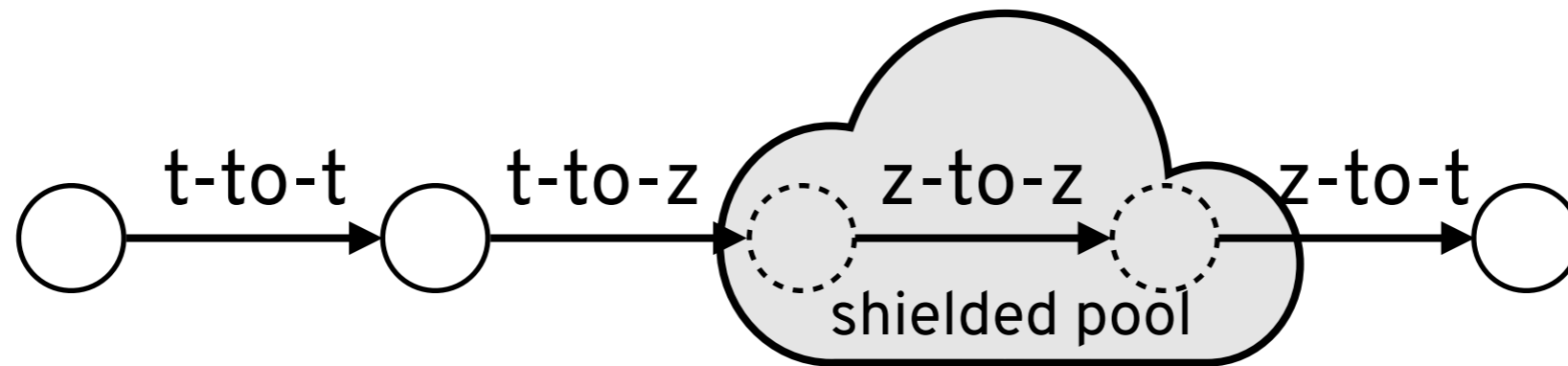




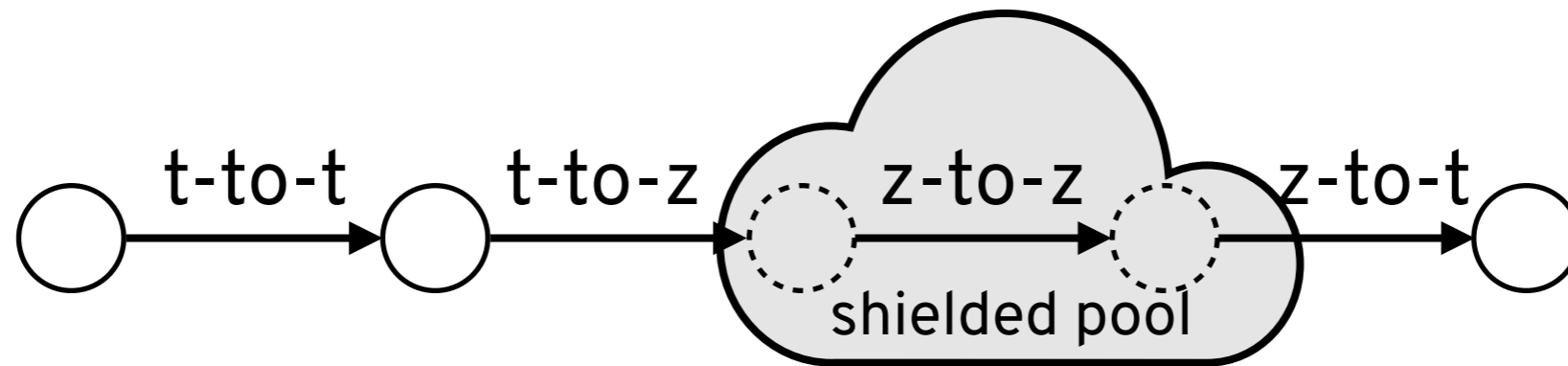
# HOW DOES ZCASH WORK?



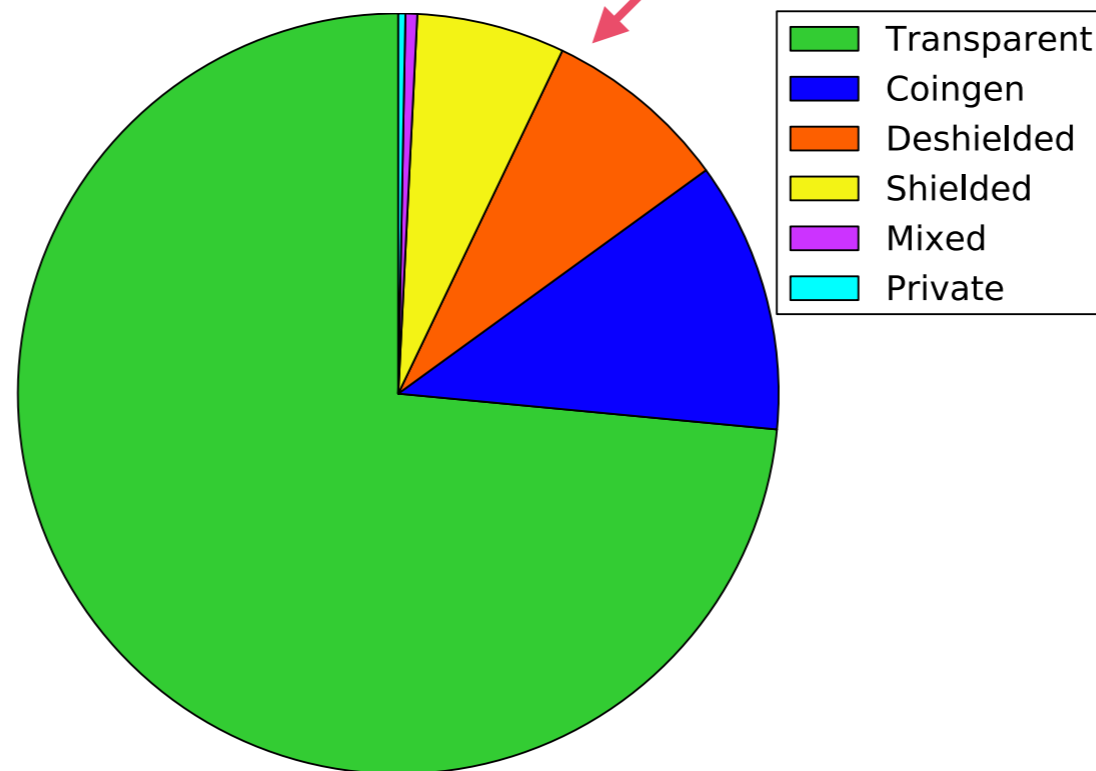
# HOW DOES ZCASH WORK?



# HOW DOES ZCASH WORK?

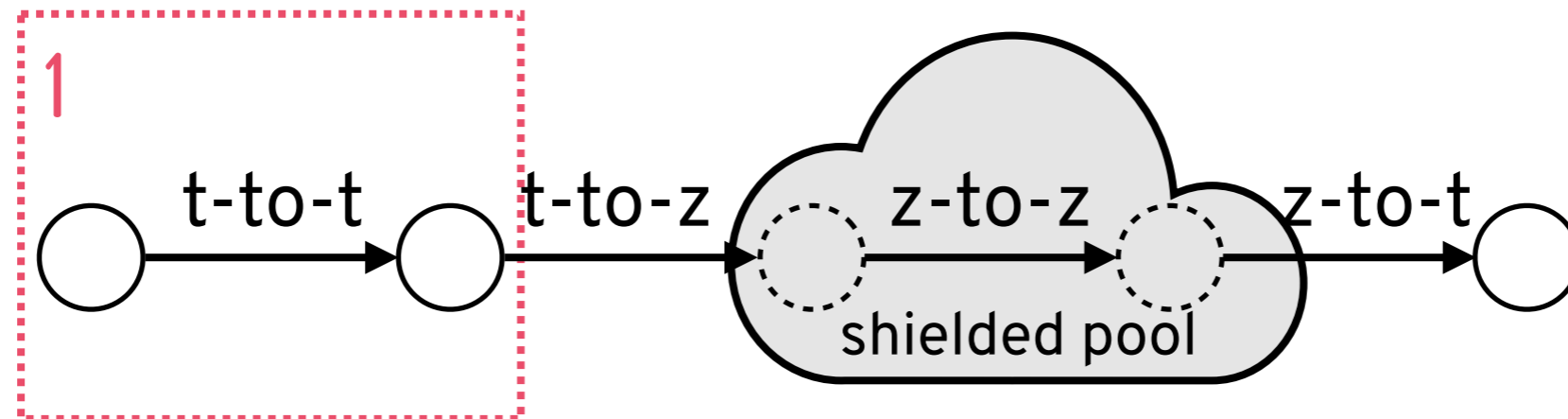


only 15% of txs use the pool at all!



# INTERACTIONS IN ZCASH

---





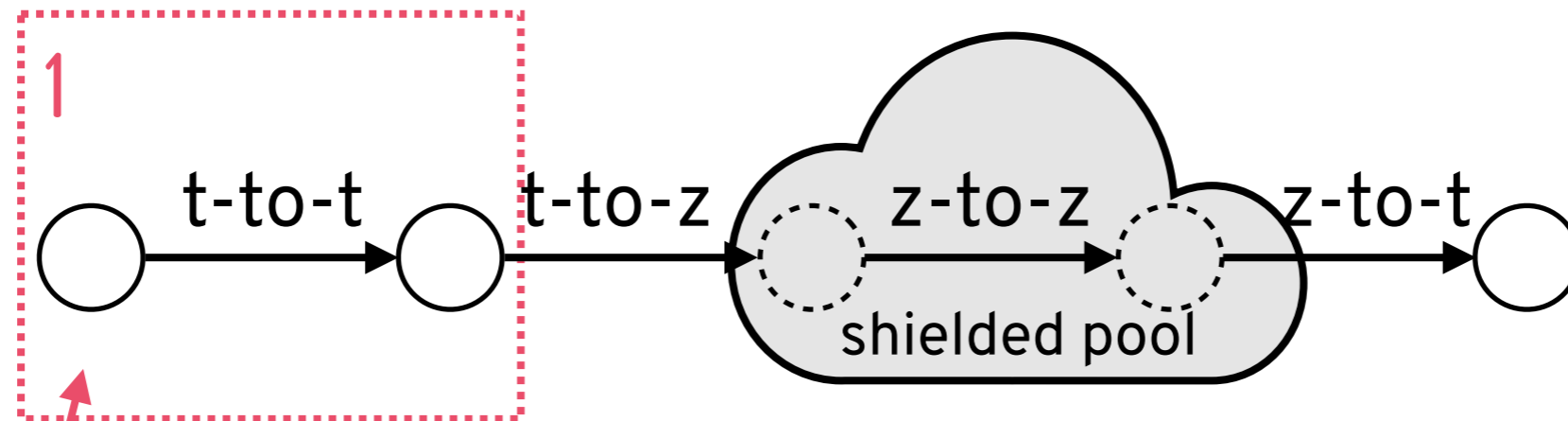
# T-TO-T ADDRESS CLUSTERING

Same structure as Bitcoin, so can just repeat Bitcoin analysis (clustering + tagging)

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

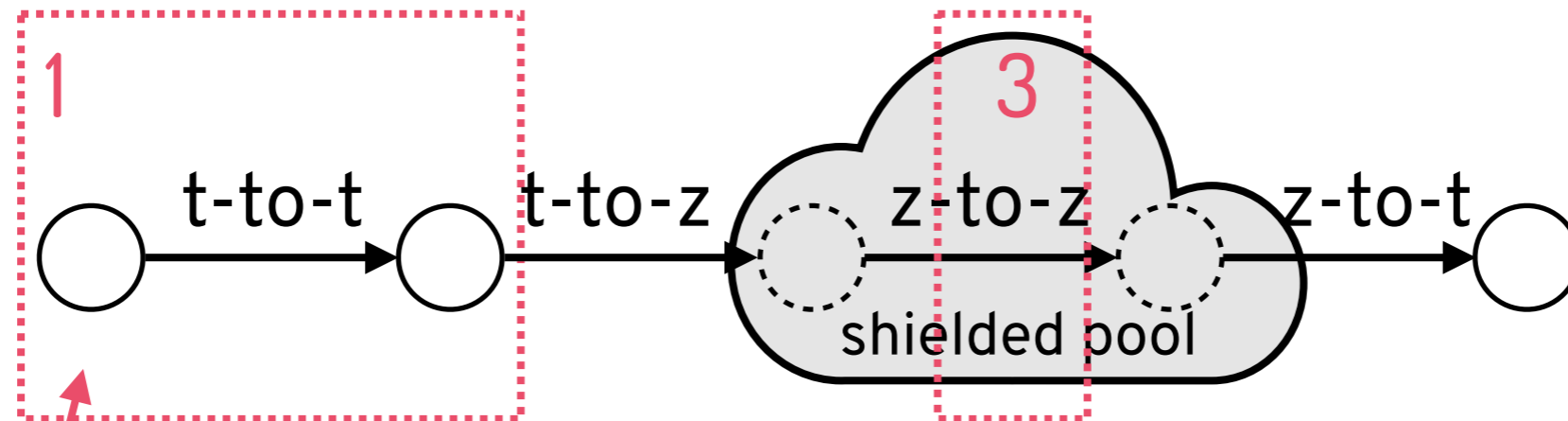
smaller number means bigger cluster

# INTERACTIONS IN ZCASH



just like in Bitcoin,  
dominated by exchanges  
(by far most heavily used)

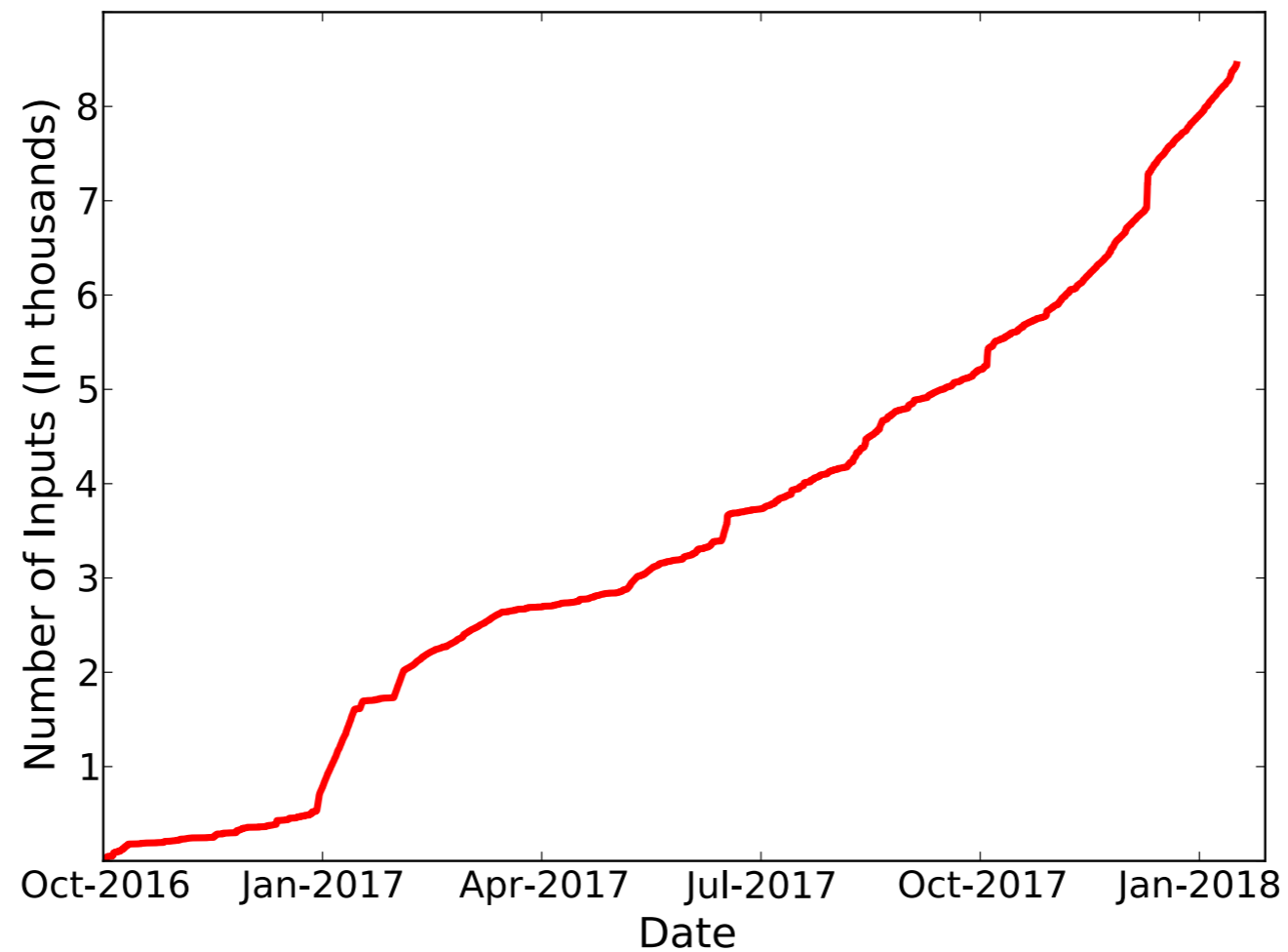
# INTERACTIONS IN ZCASH



just like in Bitcoin,  
dominated by exchanges  
(by far most heavily used)

# Z-TO-Z TRANSACTIONS

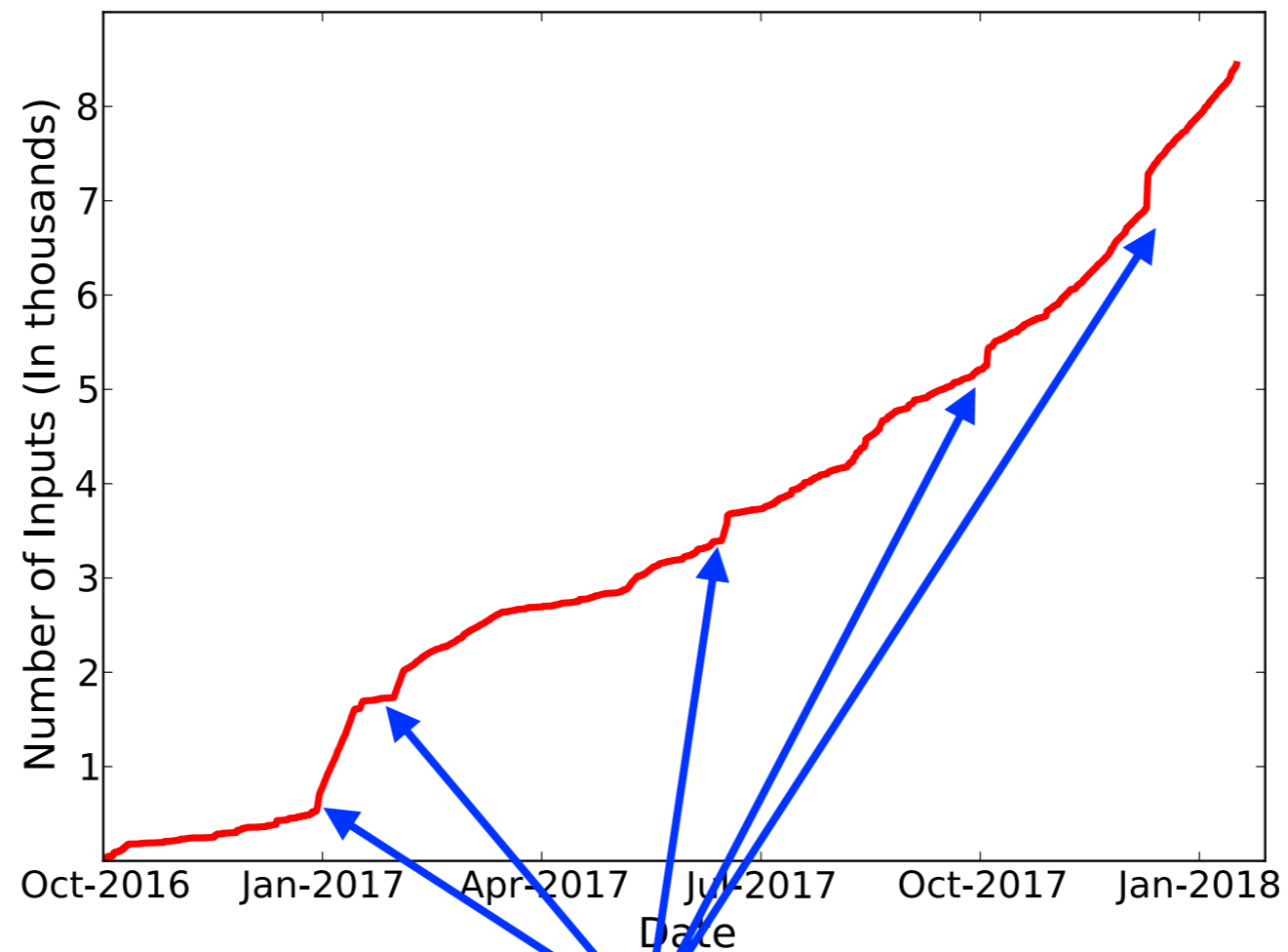
—  
possible that only a small number of users make transactions  
(based on irregular patterns)





# Z-TO-Z TRANSACTIONS

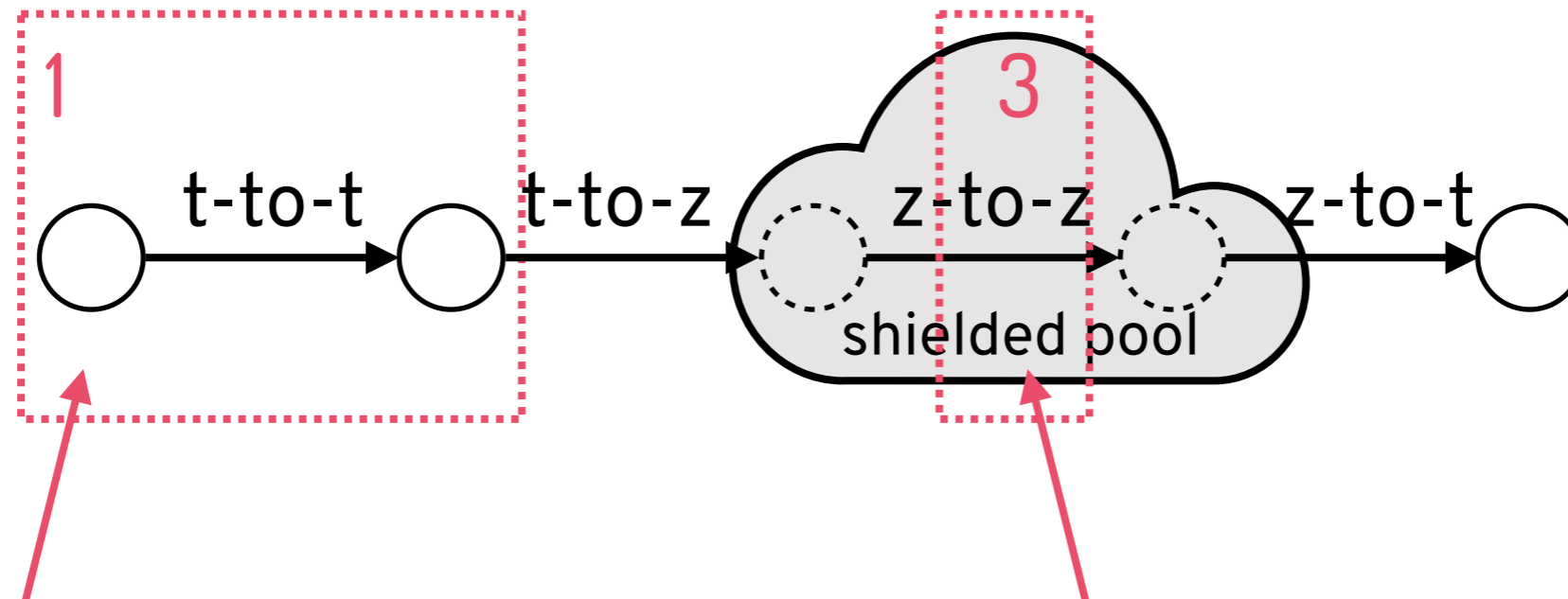
possible that only a small number of users make transactions  
(based on irregular patterns)



first spike is 17% of all transactions

# INTERACTIONS IN ZCASH

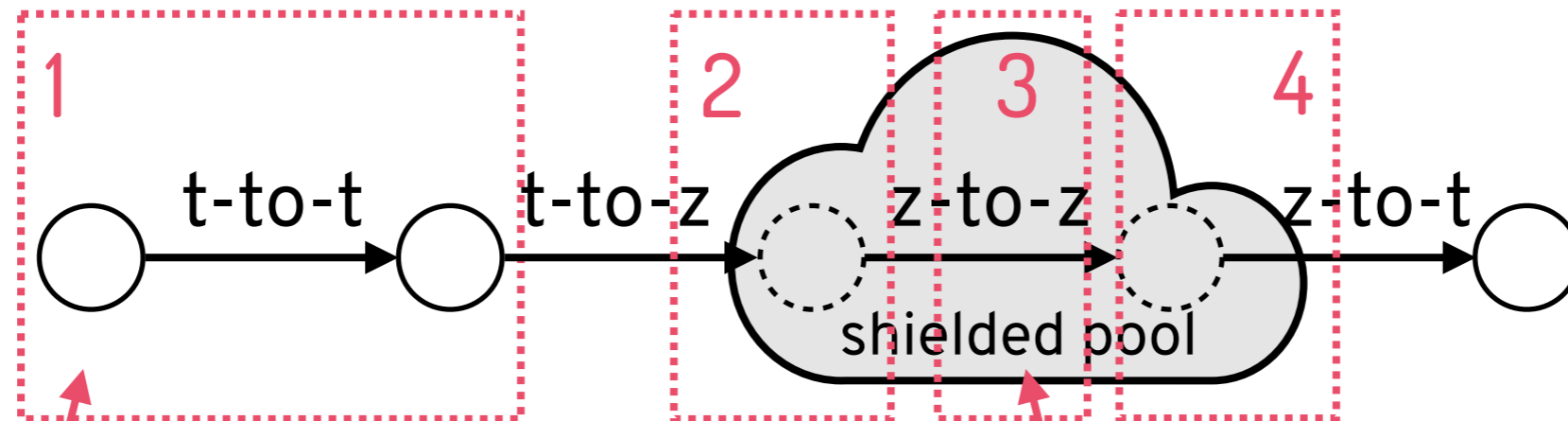
---



just like in Bitcoin,  
dominated by exchanges  
(by far most heavily used)

no obvious methods of  
de-anonymization  
(but almost never used)

# INTERACTIONS IN ZCASH

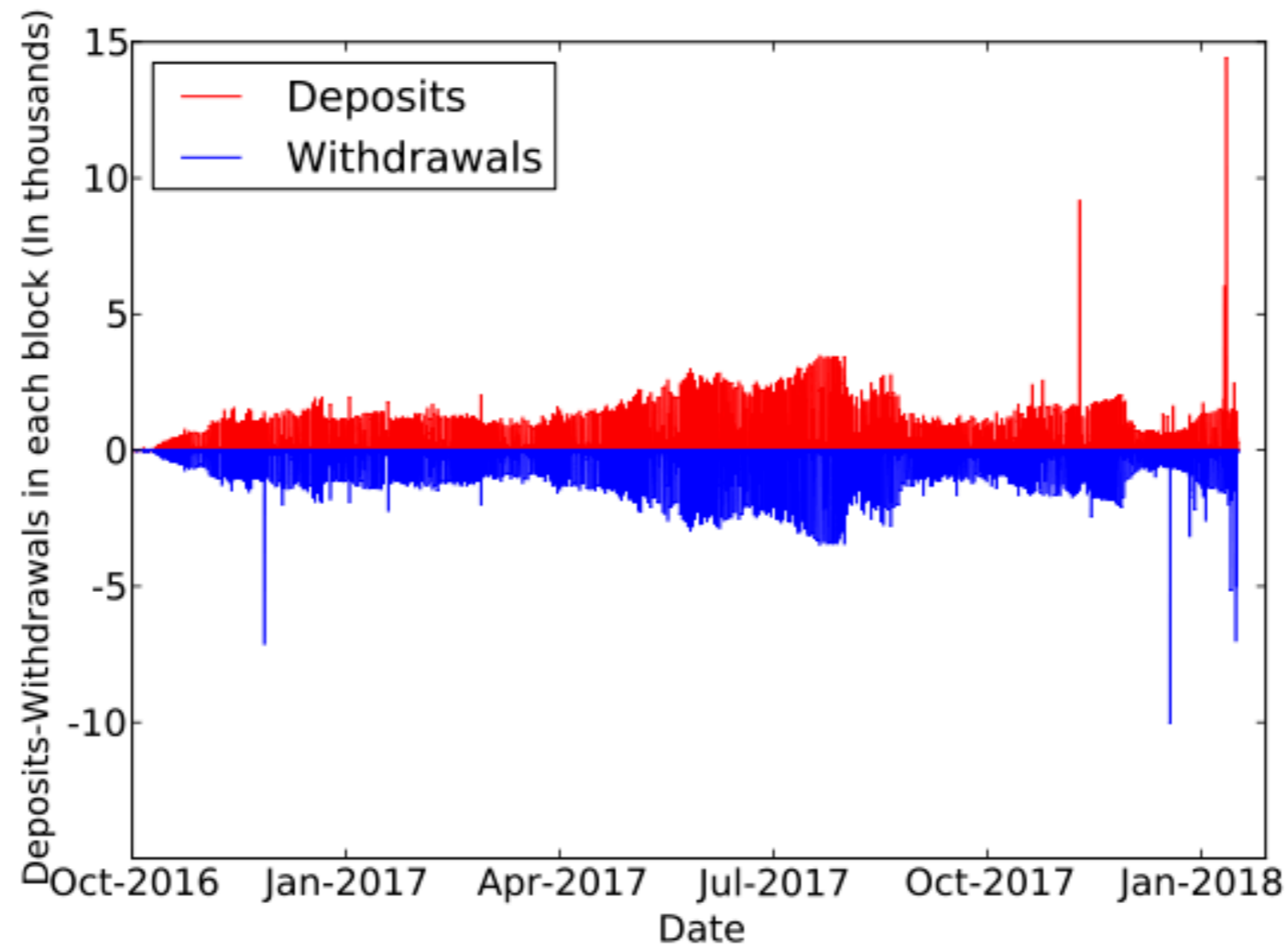


just like in Bitcoin,  
dominated by exchanges  
(by far most heavily used)

no obvious methods of  
de-anonymization  
(but almost never used)

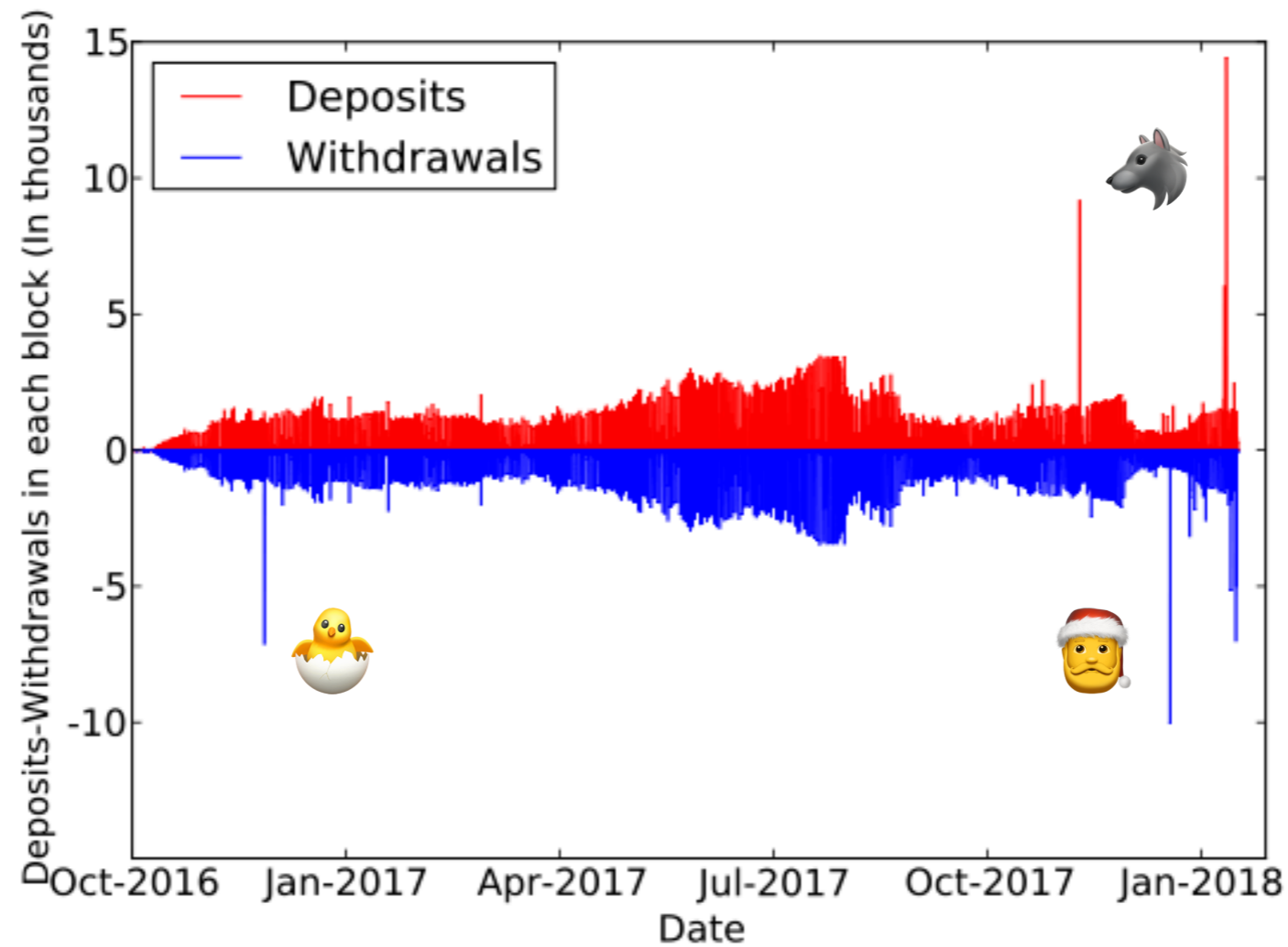
# DEPOSITS AND WITHDRAWALS

pool seems used largely as a “pass-through” mechanism



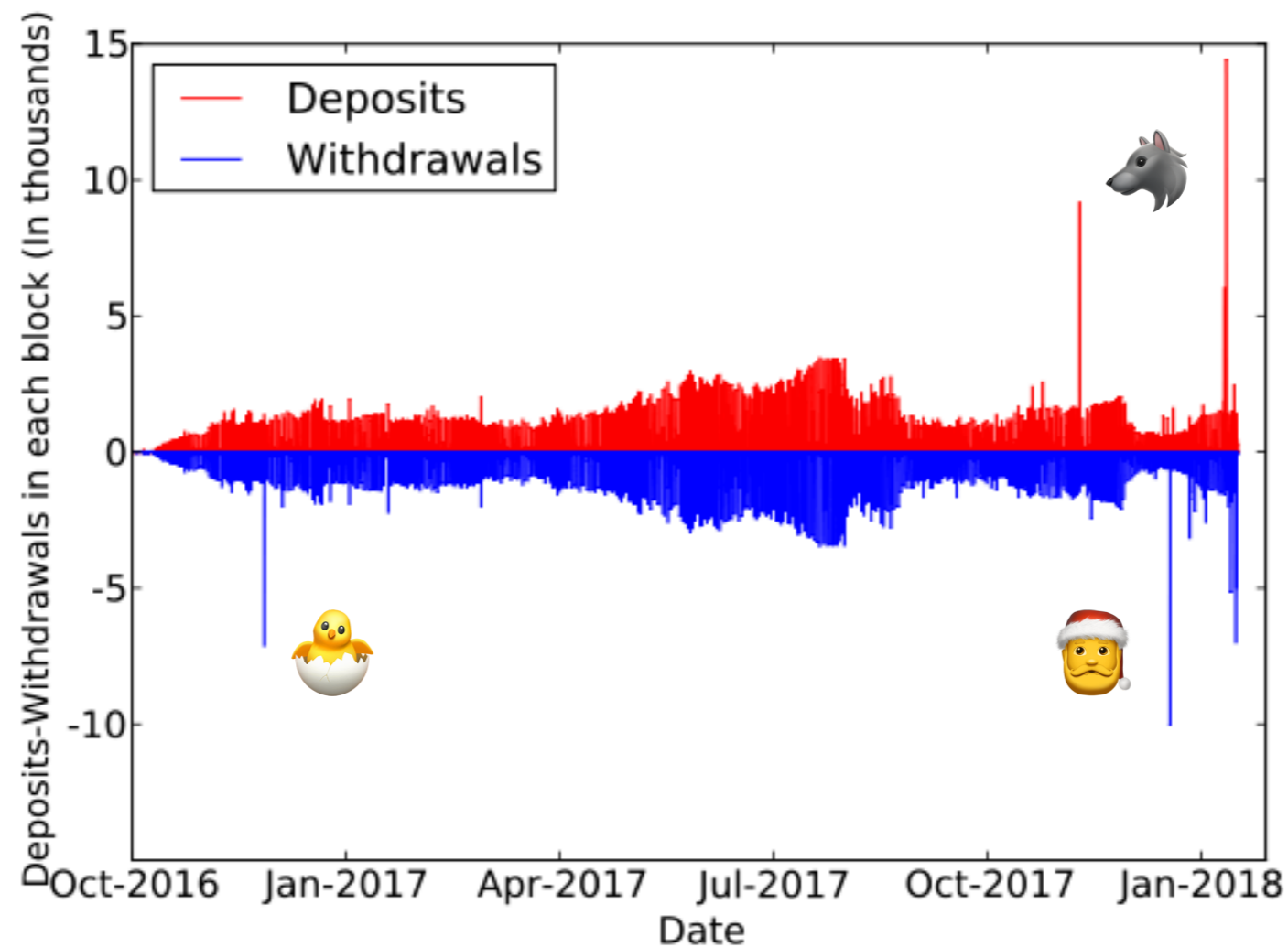
# DEPOSITS AND WITHDRAWALS

pool seems used largely as a “pass-through” mechanism



# DEPOSITS AND WITHDRAWALS

pool seems used largely as a “pass-through” mechanism



but who are the people making these transactions?



# TYPES OF ZCASH USERS

---

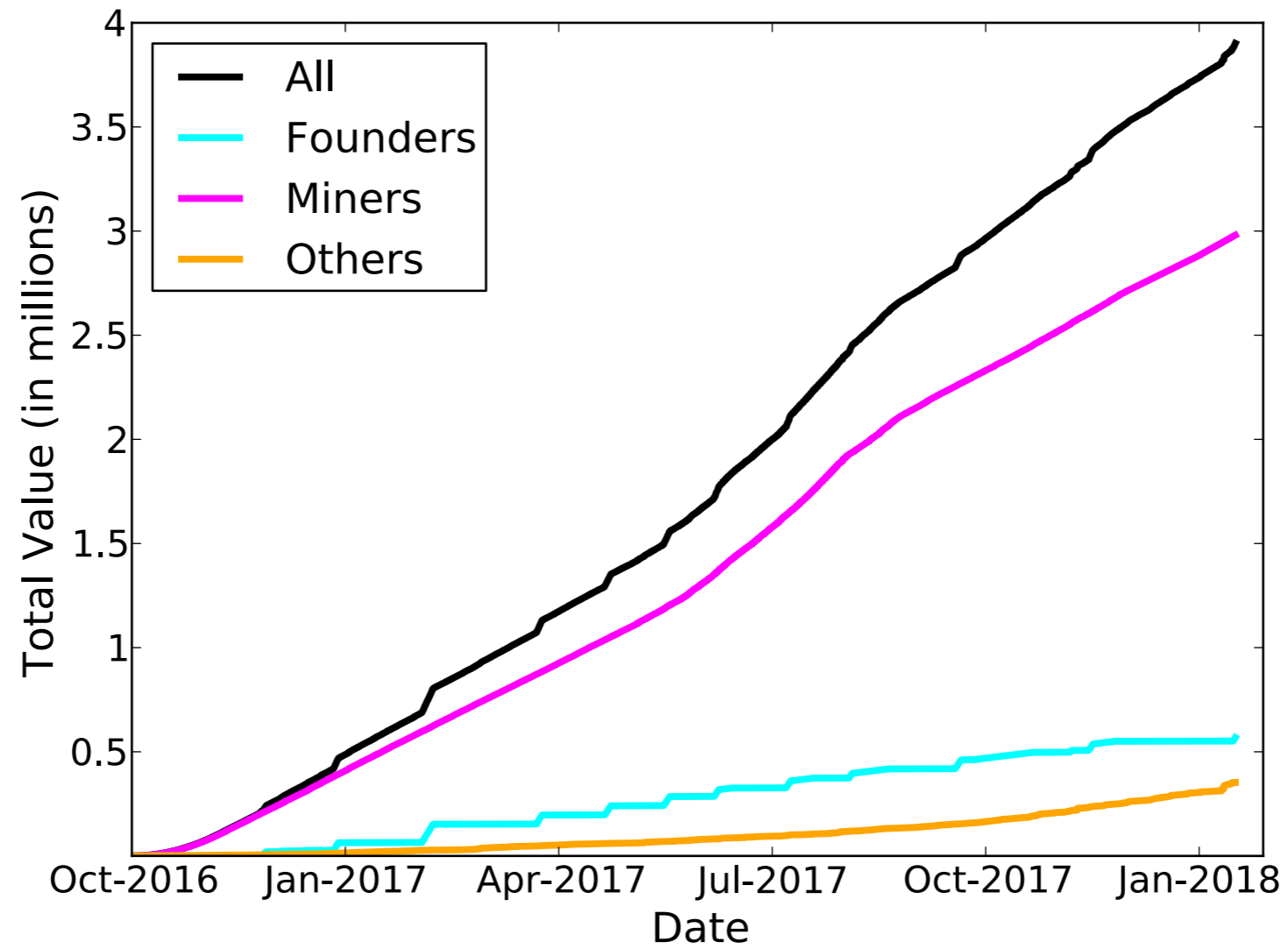
**Miners** get 12.5 ZEC per block mined

**Founders** get 2.5 ZEC per block mined (“founder’s reward”)

All newly mined coins must go into shielded pool immediately

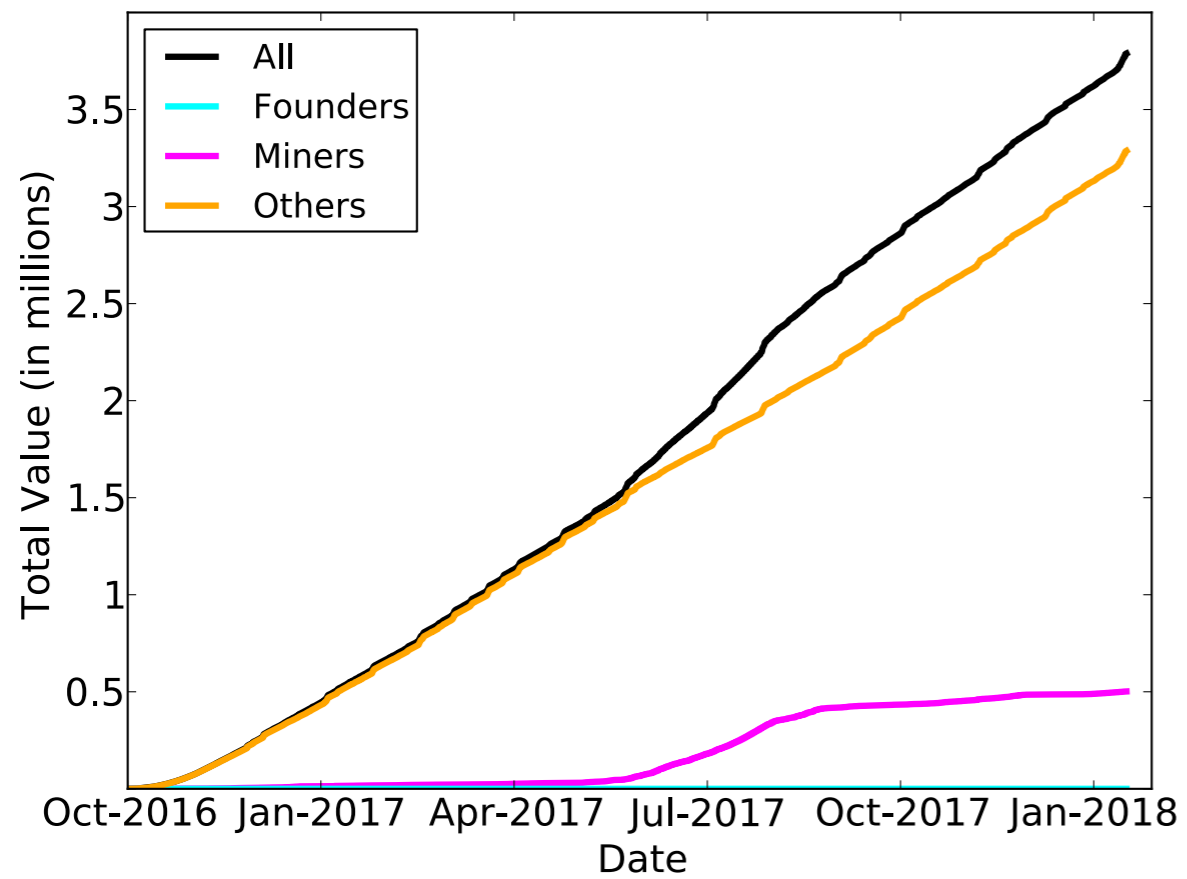
**Others** are individual users and services

# DEPOSITS



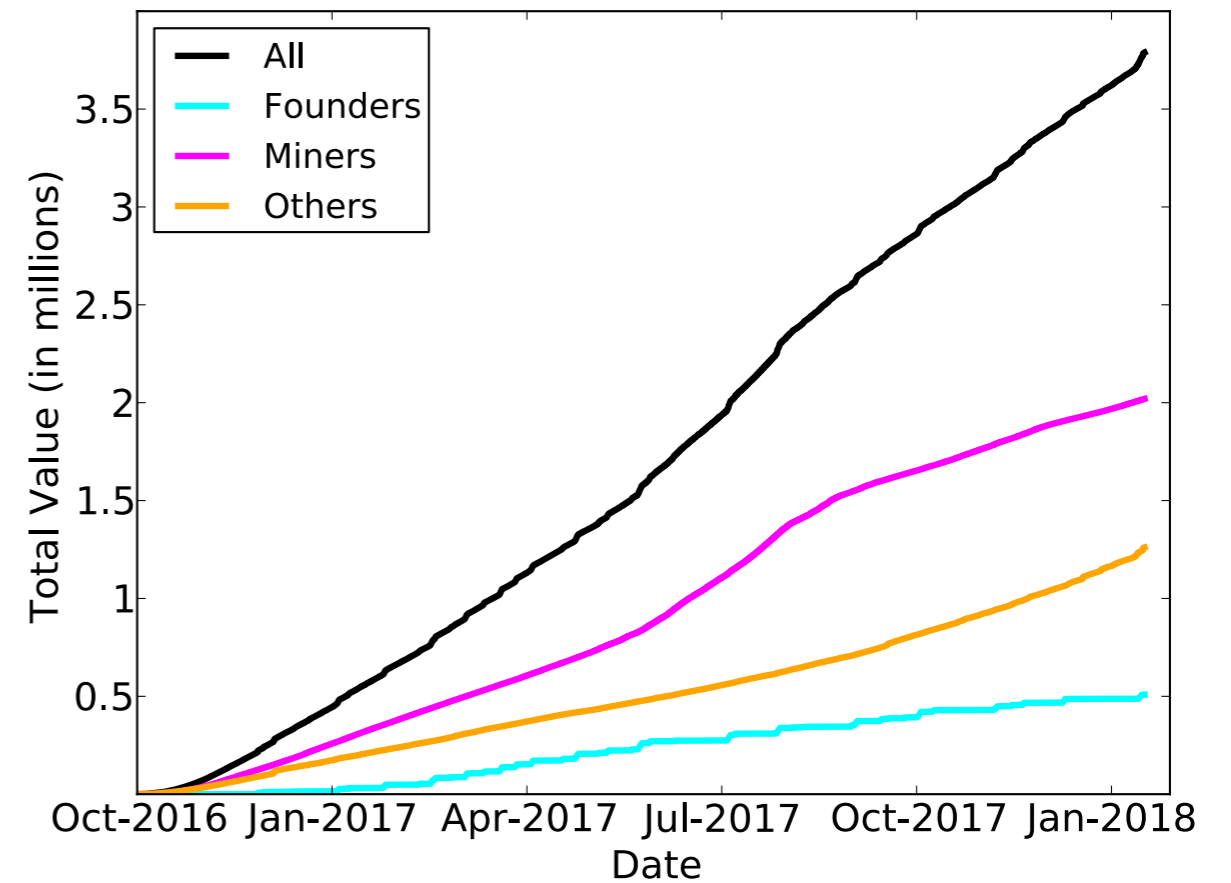
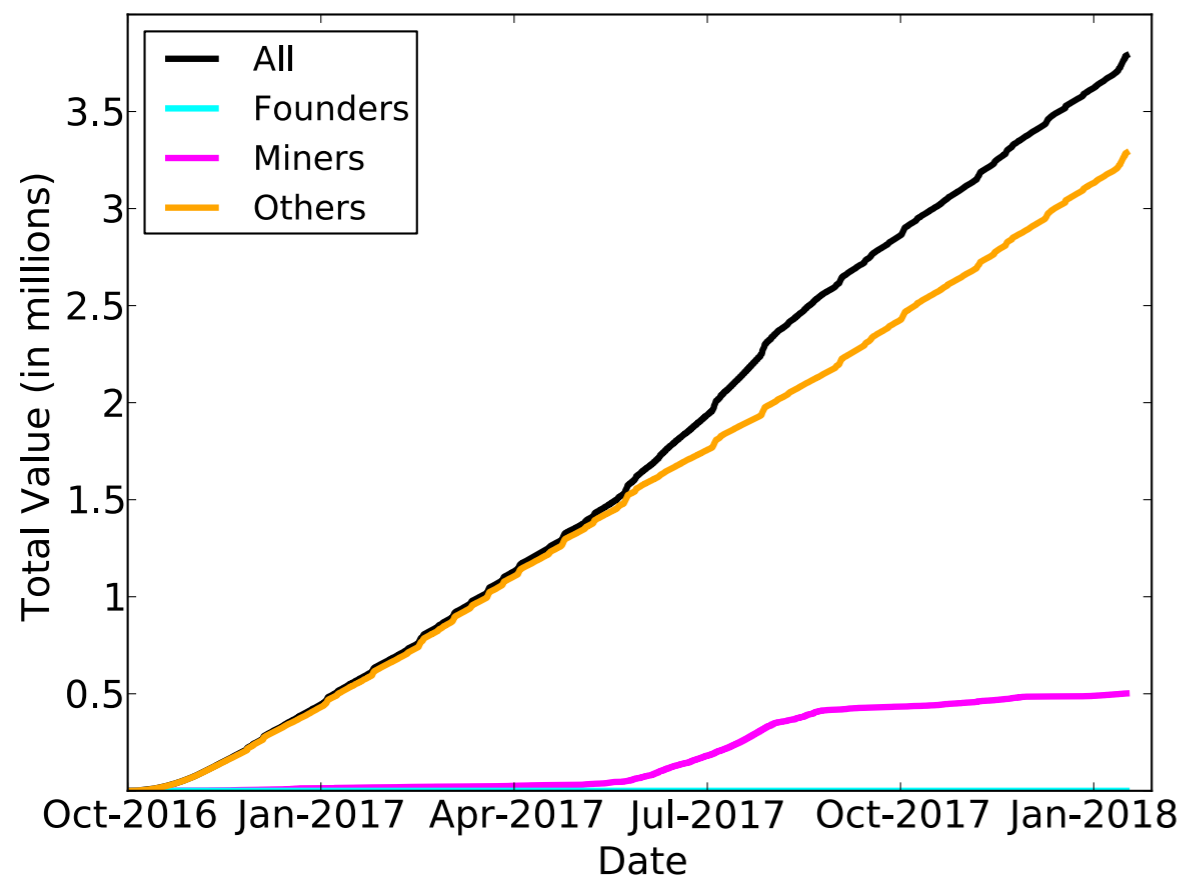
proportions correspond with rewards given to miners/founders

# WITHDRAWALS



no obvious reuse of the same addresses...

# WITHDRAWALS: BEFORE AND AFTER

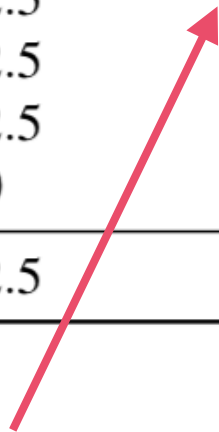


...but via custom heuristics we can shrink the anonymity set by 69.1%

# BEHAVIOR OF FOUNDERS

---

	# 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



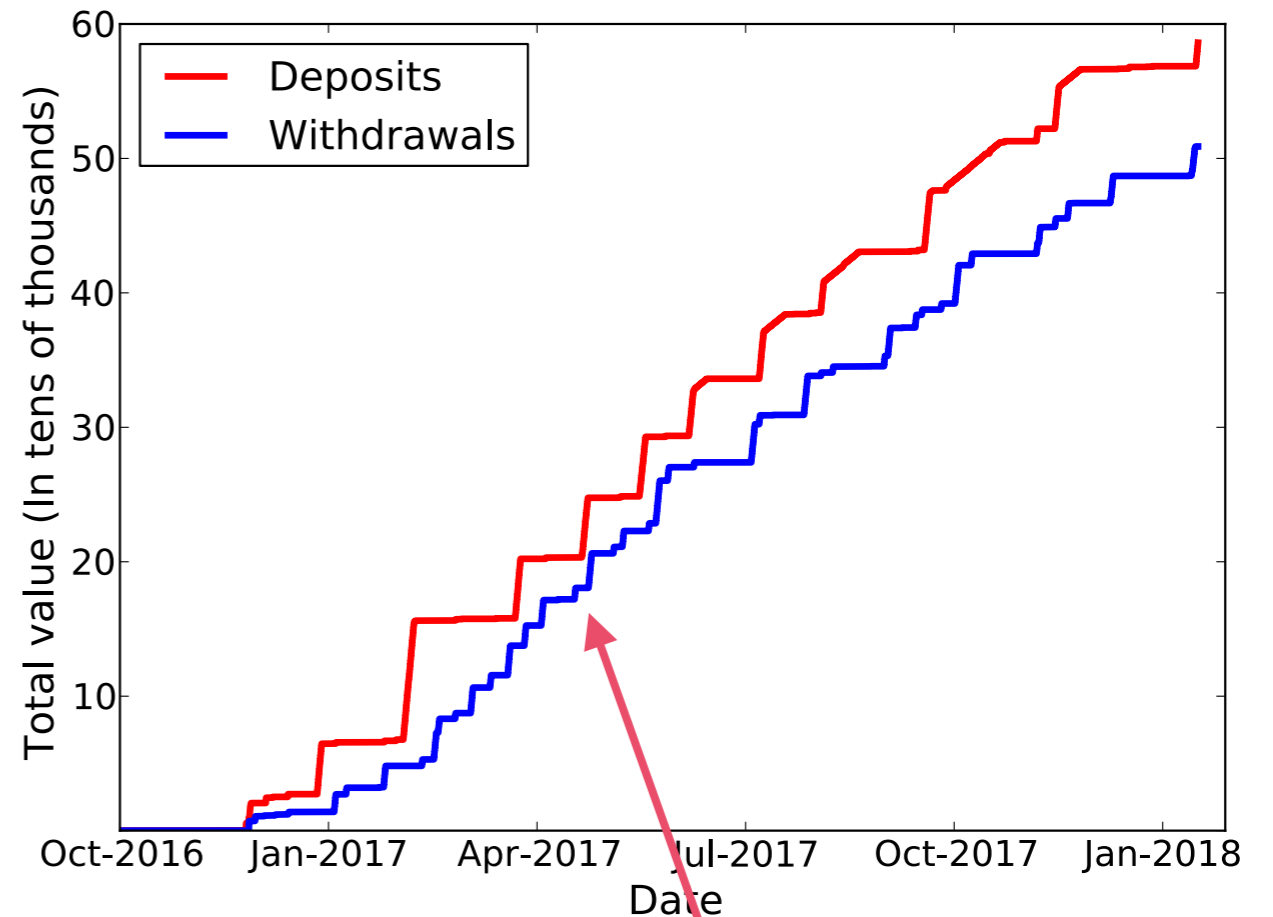
also regular in terms of value (249.999 ZEC)

# BEHAVIOR OF FOUNDERS

---

	# 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

---



also regular in terms of value (249.999 ZEC)

withdrawals of amount 250.001 ZEC



# HEURISTIC FOR FOUNDERS

---

## Heuristic

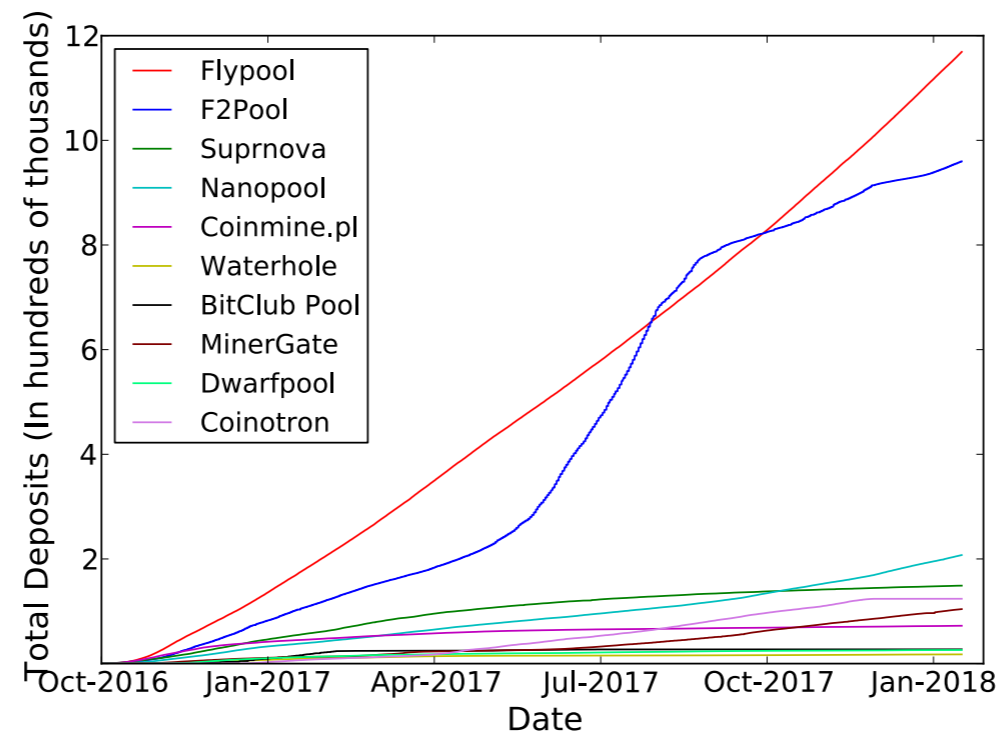
Any z-to-t transaction carrying 250.001 ZEC in value is done by the founders

## False positive risk?

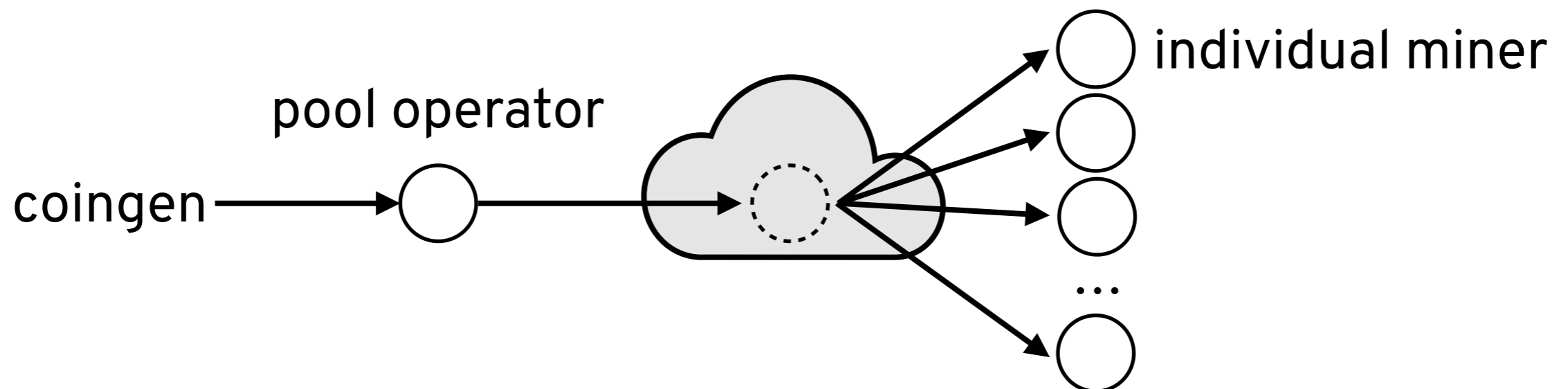
Only five deposits ever of approximately 250 ZEC that didn't come from the founders

# BEHAVIOR OF MINERS

miners naturally form mining pools



mining pools often pay individuals by “shattering” the reward



# HEURISTIC FOR MINERS

---

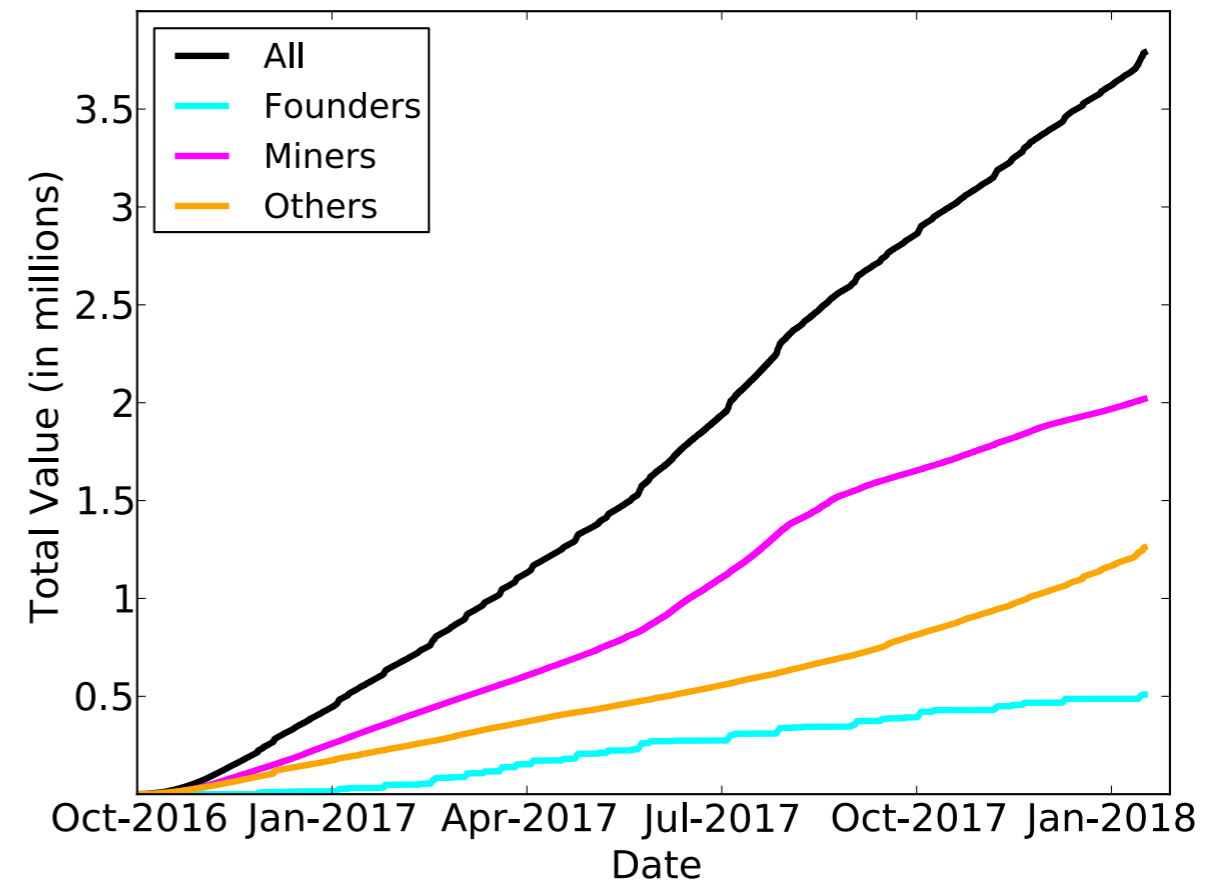
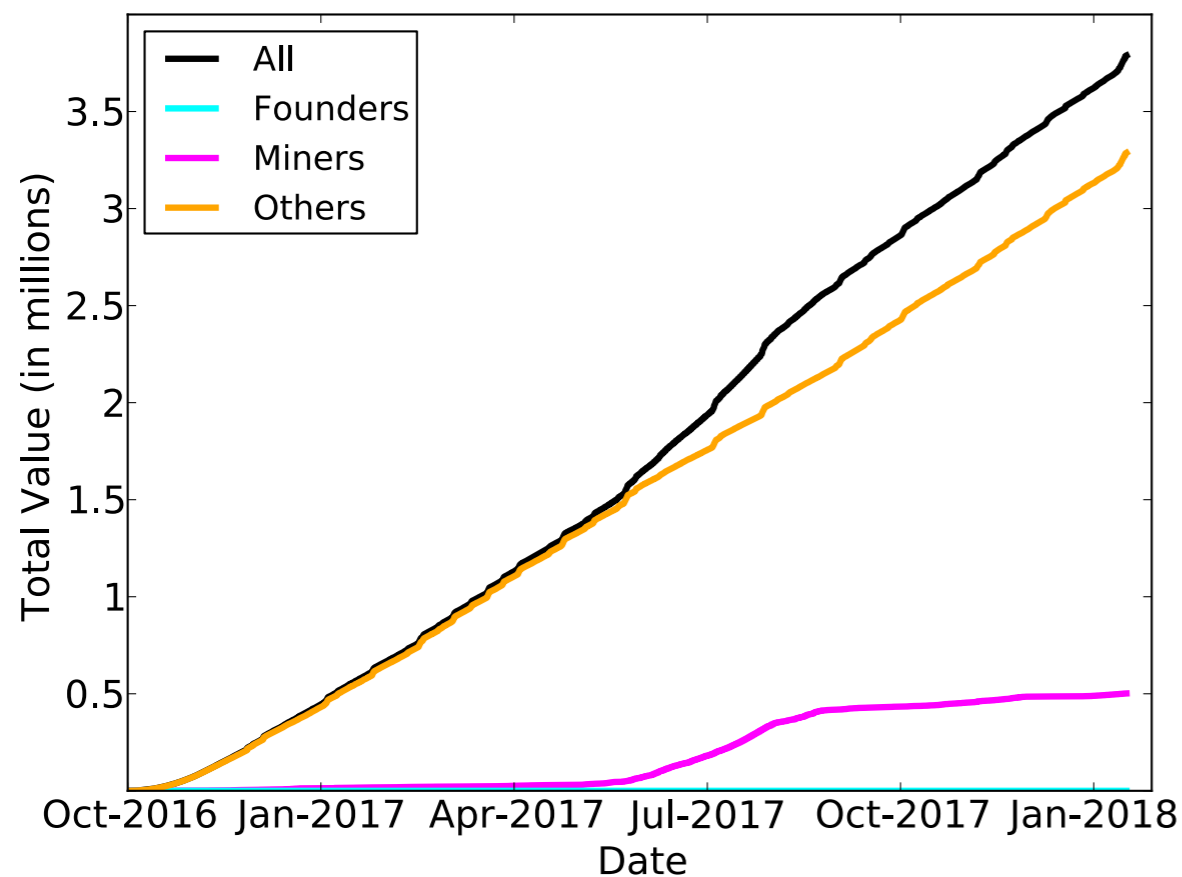
## **Heuristic**

If (1) a z-to-t transaction has over 100 output t-addresses and (2) one of them belongs to a known mining pool, then all non-pool output t-addresses belong to miners

## **False positive risk?**

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

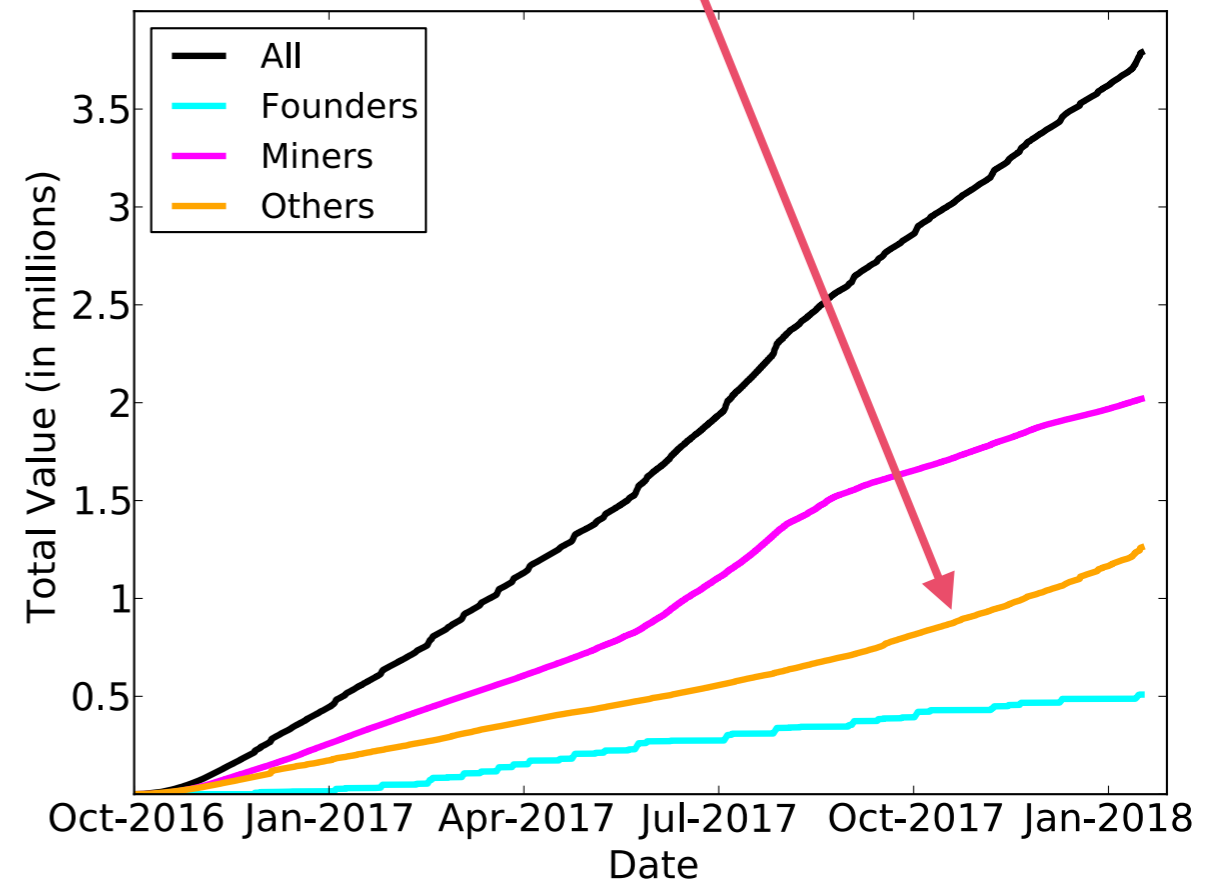
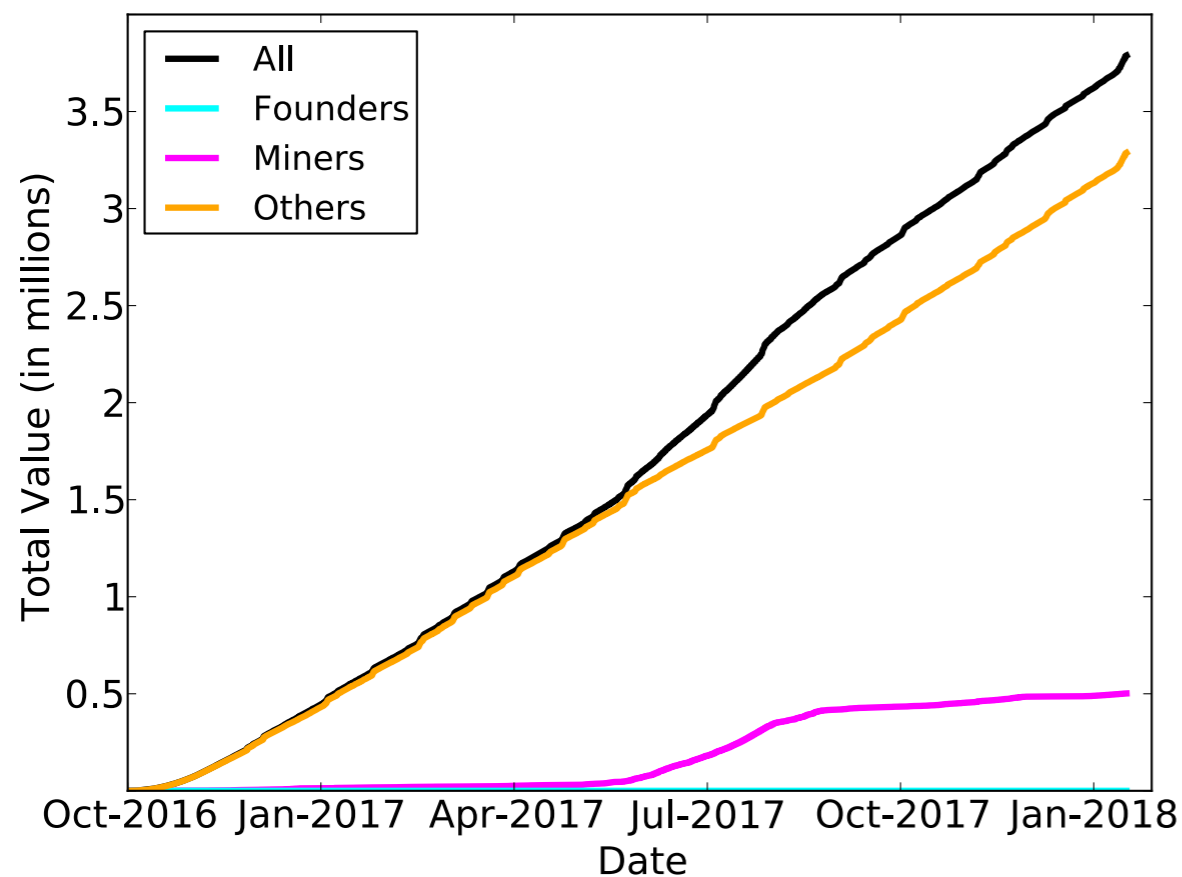
# WITHDRAWALS: BEFORE AND AFTER



...but via custom heuristics for founders and miners  
we can shrink the anonymity set by 65.6%

# WITHDRAWALS: BEFORE AND AFTER

— even for ‘others’ we can link transactions based on value, capture 28.5% this way (an additional 3.5%)

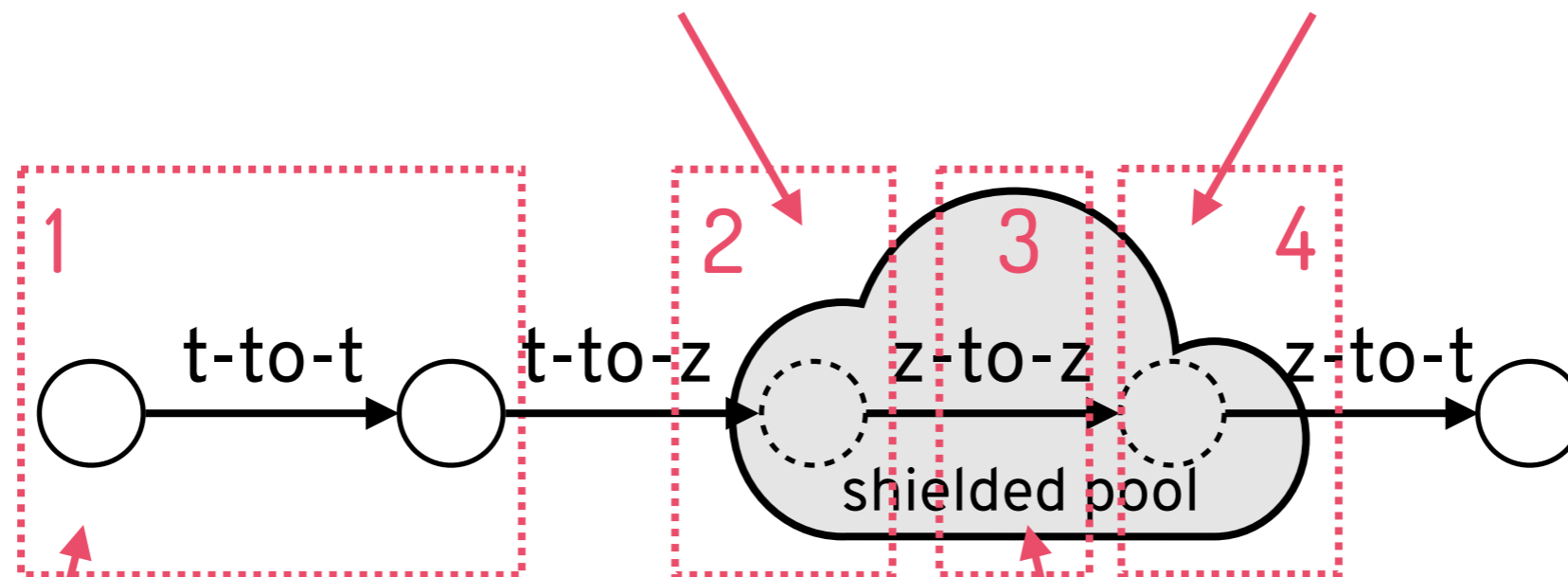


...but via custom heuristics for founders and miners we can shrink the anonymity set by 65.6%

# INTERACTIONS IN ZCASH

trivial to identify  
founders and miners

can often (69.1%) link back  
to deposits via heuristics



just like in Bitcoin,  
dominated by exchanges  
(by far most heavily used)

no obvious methods of  
de-anonymization  
(but almost never used)



# CONCLUSIONS

**Anonymity is a subtle issue:** bad actors should not be able to get away with misbehavior and good actors should be able to avoid surveillance

Need to explore it from both sides





---

THANKS!  
ANY QUESTIONS?