An Empirical Analysis of Anonymity in Zcash

George Kappos, Haaroon Yousaf, Mary Maller, Sarah Meiklejohn

University College London

What level of anonymity do users obtain by using Zcash?

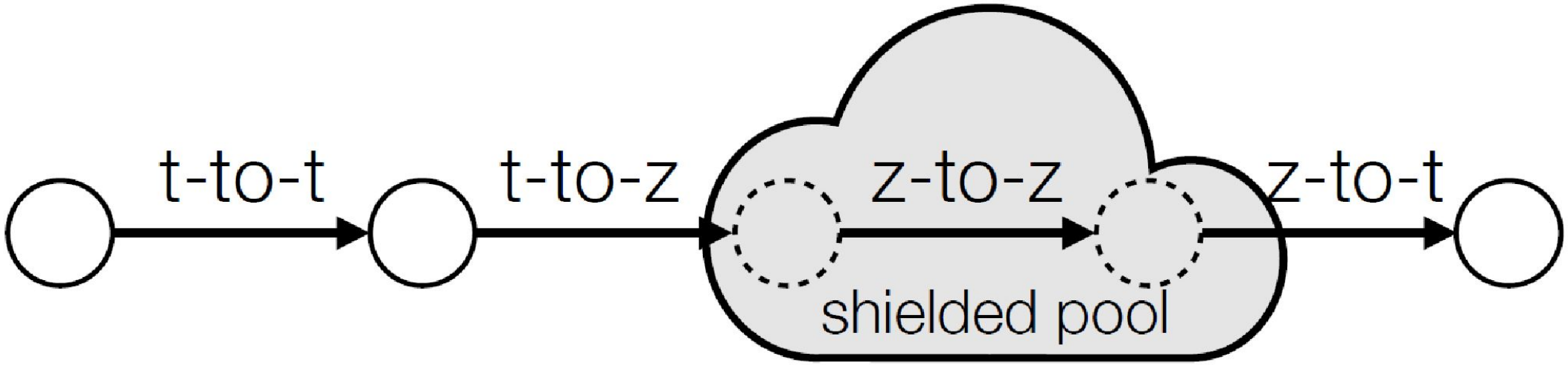
Our Contributions

- In many cases we identify the activity of founders and miners using private transactions.
- Implication is a significant shrink to the effective anonymity set for regular users.
- The developers of Zcash have already implemented some of our suggested fixes.

Ingredients:

1. Some simple heuristics for linking user activity.

Zcash uses a Shielded Pool



Transparent to Transparent

Transparent to Private

Private to Private

Private to Transparent

Zcash uses a Shielded Pool

Can often be deanonymised.

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†

ABSTRACT

Bitcoin is a purely online virtual currency, unbacked by either physical commodities or sovereign obligation; instead, it relies on a combination of cryptographic protection and a peer-to-peer protocol for witnessing settlements. Consequently, Bitcoin has the unintuitive property that while the ownership of money is implicitly anonymous, its flow is globally visible. In this paper we explore this unique characteristic further, using heuristic clustering to group Bitcoin wallets based on evidence of shared authority, and then using re-identification attacks (i.e., empirical purchasing of goods and services) to classify the operators of those clusters. From this analysis, we characterize longitudinal changes in the Bitcoin market, the stresses these changes are placing on the system, and the challenges for those seeking to use Bitcoin for criminal or fraudulent purposes at scale.

Categories and Subject Descriptors

K.4.4 [**Electronic Commerce**]: Payment schemes

Keywords

Bitcoin; Measurement; Anonymity

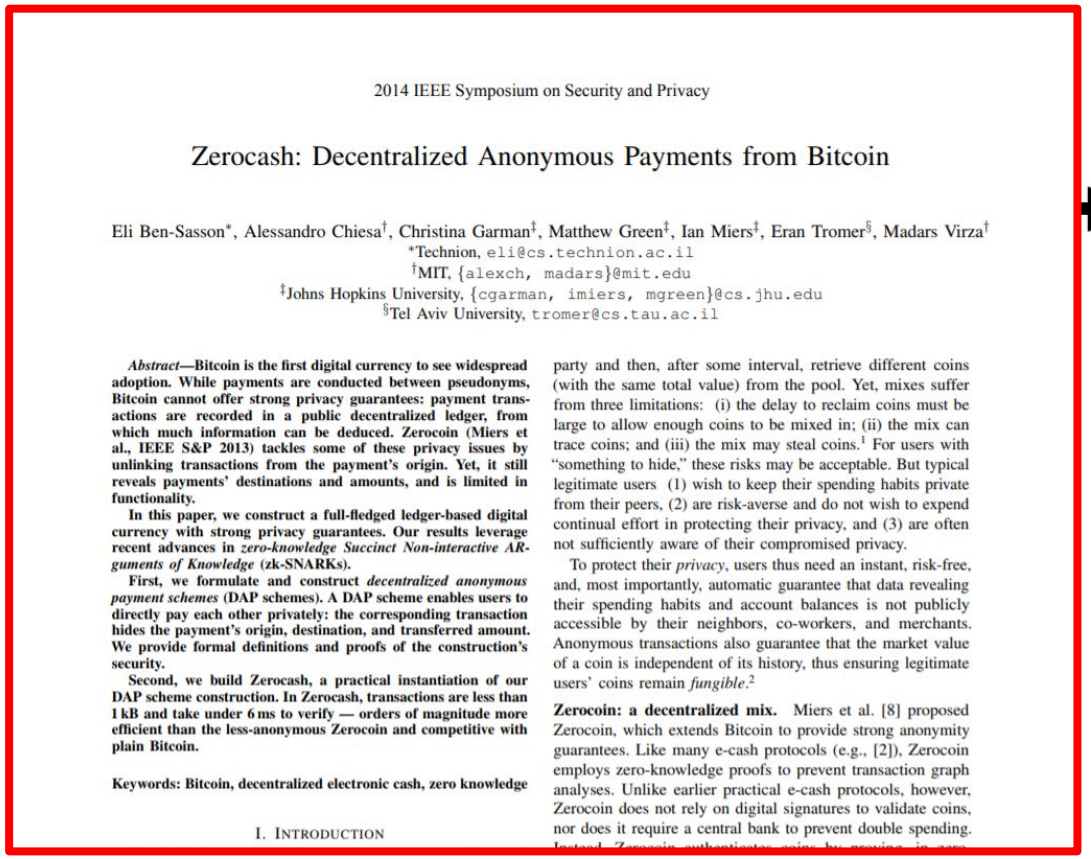
1. INTRODUCTION

Demand for low friction e-commerce of various kinds has driven

By far the most intriguing exception to this rule is Bitcoin. First deployed in 2009, Bitcoin is an independent online monetary system that combines some of the features of cash and existing online payment methods. Like cash, Bitcoin transactions do not explicitly identify the payer or the payee: a transaction is a cryptographically-signed transfer of funds from one public key to another. Moreover, like cash, Bitcoin transactions are irreversible (in particular, there is no *chargeback* risk as with credit cards). However, unlike cash, Bitcoin requires third party mediation: a global peer-to-peer network of participants validates and certifies all transactions; such decentralized accounting requires each network participant to maintain the entire transaction history of the system, currently amounting to over 3GB of compressed data. Bitcoin identities are thus *pseudo-anonymous*: while not explicitly tied to real-world individuals or organizations, all transactions are completely transparent.[2]

This unusual combination of features has given rise to considerable confusion about the nature and consequences of the anonymity that Bitcoin provides. In particular, there is concern that the combination of scalable, irrevocable, anonymous payments would prove highly attractive for criminals engaged in fraud or money laundering. In a widely leaked 2012 Intelligence Assessment, FBI analysts make just this case and conclude that a key "advantage" of Bitcoin for criminals is that "law enforcement faces difficulties detecting suspicious activity, identifying users and obtaining transaction records" [7]. Similarly, in a late 2012 report on Virtual Currency Schemes, the European Central Bank opines that the

Zcash uses a Shielded Pool



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

***Abstract*—Bitcoin is the first digital currency to see widespread adoption. While payments are conducted between pseudonyms, Bitcoin cannot offer strong privacy guarantees: payment transactions are recorded in a public decentralized ledger, from which much information can be deduced. Zerocoin (Miers et al., IEEE S&P 2013) tackles some of these privacy issues by unlinking transactions from the payment's origin. Yet, it still reveals payments' destinations and amounts, and is limited in functionality.**

In this paper, we construct a full-fledged ledger-based digital currency with strong privacy guarantees. Our results leverage recent advances in *zero-knowledge Succinct Non-interactive ARguments of Knowledge* (zk-SNARKs).

First, we formulate and construct *decentralized anonymous payment schemes* (DAP schemes). A DAP scheme enables users to directly pay each other privately: the corresponding transaction hides the payment's origin, destination, and transferred amount. We provide formal definitions and proofs of the construction's security.

Second, we build Zerocash, a practical instantiation of our DAP scheme construction. In Zerocash, transactions are less than 1 kB and take under 6 ms to verify — orders of magnitude more efficient than the less-anonymous Zerocoin and competitive with plain Bitcoin.

Keywords: Bitcoin, decentralized electronic cash, zero knowledge

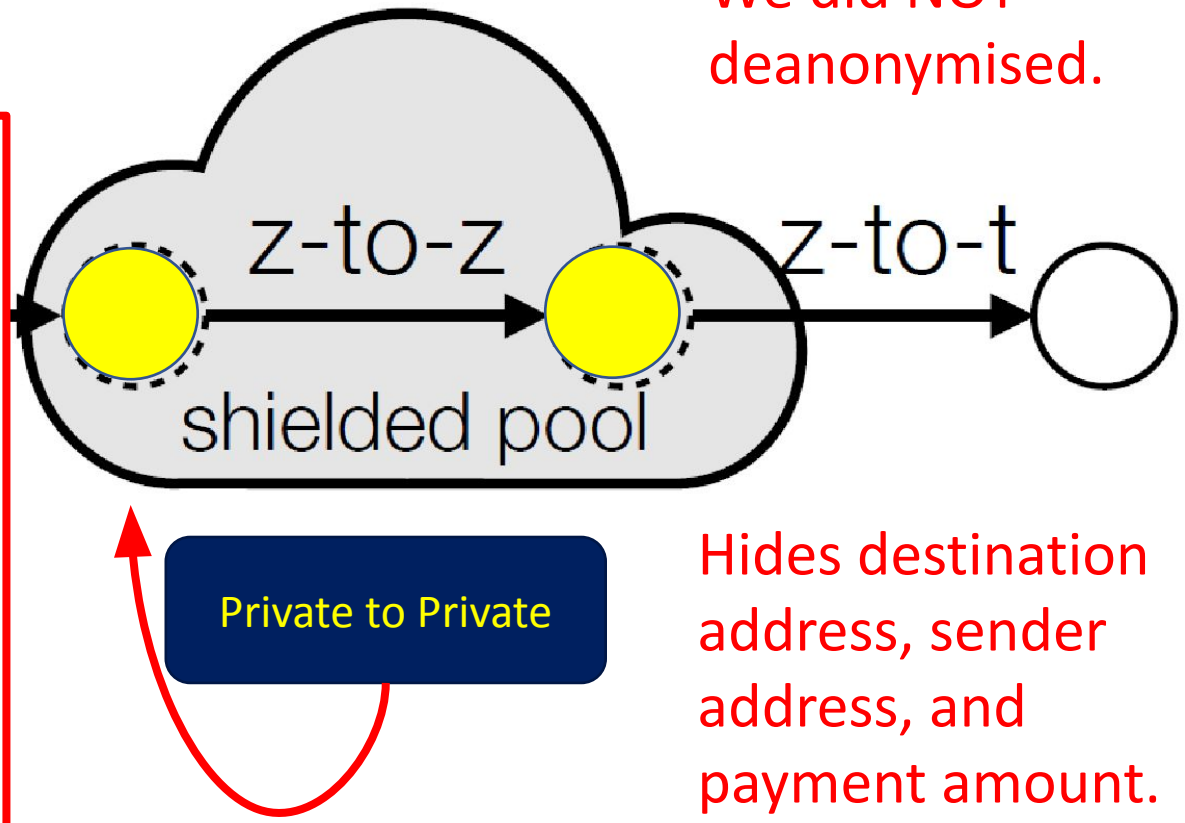
I. Introduction

party and then, after some interval, retrieve different coins (with the same total value) from the pool. Yet, mixes suffer from three limitations: (i) the delay to reclaim coins must be large to allow enough coins to be mixed in; (ii) the mix can trace coins; and (iii) the mix may steal coins.[1] For users with "something to hide," these risks may be acceptable. But typical legitimate users (1) wish to keep their spending habits private from their peers, (2) are risk-averse and do not wish to expend continual effort in protecting their privacy, and (3) are often not sufficiently aware of their compromised privacy.

To protect their *privacy*, users thus need an instant, risk-free, and, most importantly, automatic guarantee that data revealing their spending habits and account balances is not publicly accessible by their neighbors, co-workers, and merchants. Anonymous transactions also guarantee that the market value of a coin is independent of its history, thus ensuring legitimate users' coins remain *fungible*.[2]

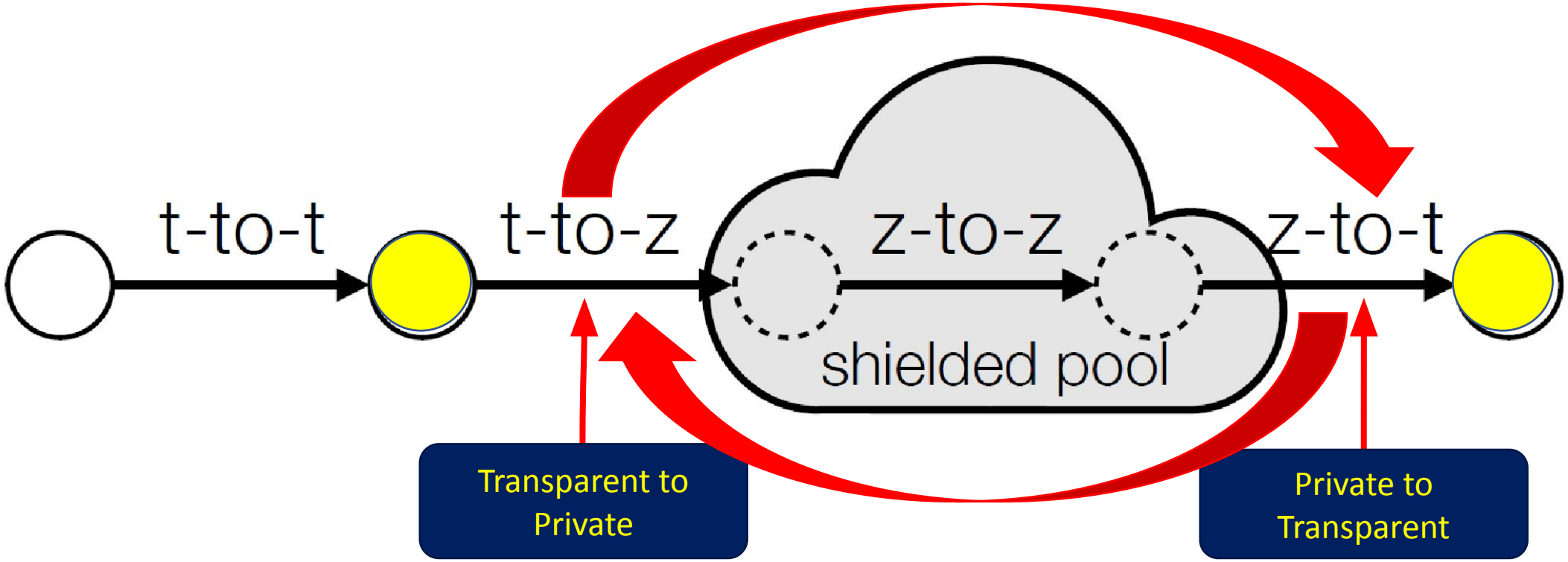
Zerocoin: a decentralized mix. Miers et al. [8] proposed Zerocoin, which extends Bitcoin to provide strong anonymity guarantees. Like many e-cash protocols (e.g., [2]), Zerocoin employs zero-knowledge proofs to prevent transaction graph analyses. Unlike earlier practical e-cash protocols, however, Zerocoin does not rely on digital signatures to validate coins, nor does it require a central bank to prevent double spending. Instead, Zerocoin authenticates coins by proving, in zero

We did NOT deanonymised.



Hides destination address, sender address, and payment amount.

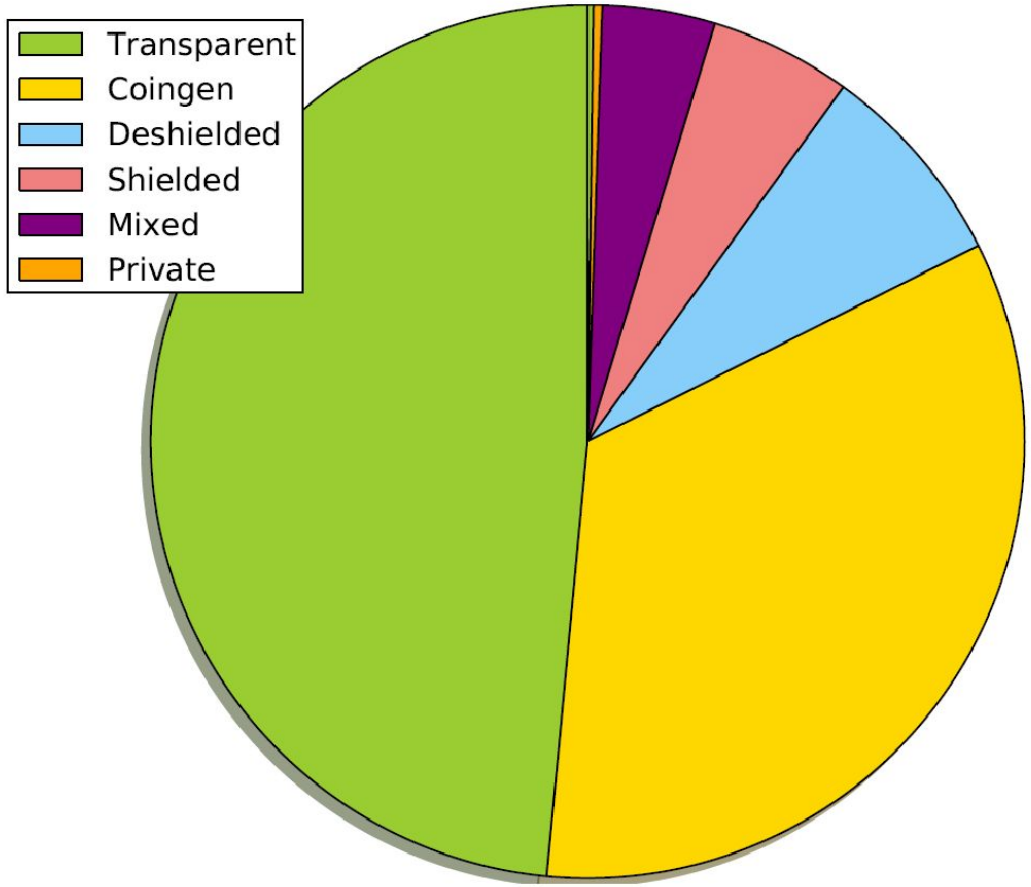
Zcash uses a Shielded Pool



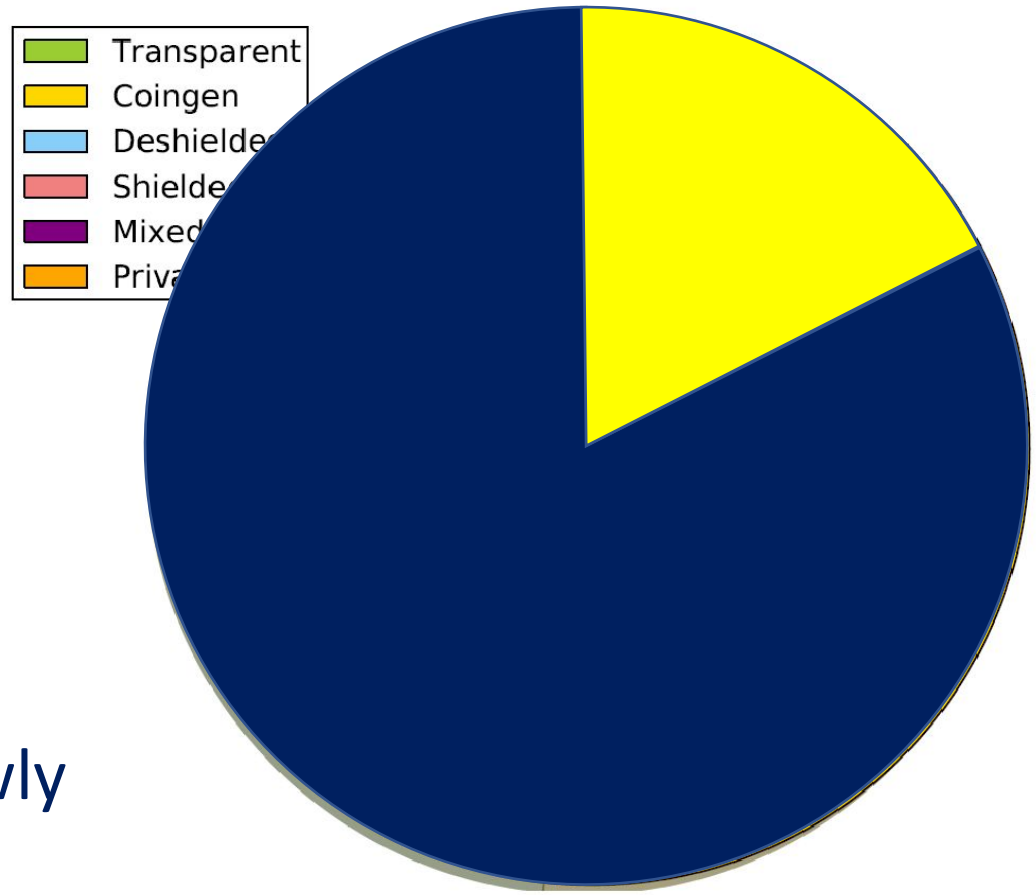
Hides destination address.

Hides sender address.

Blockchain statistics

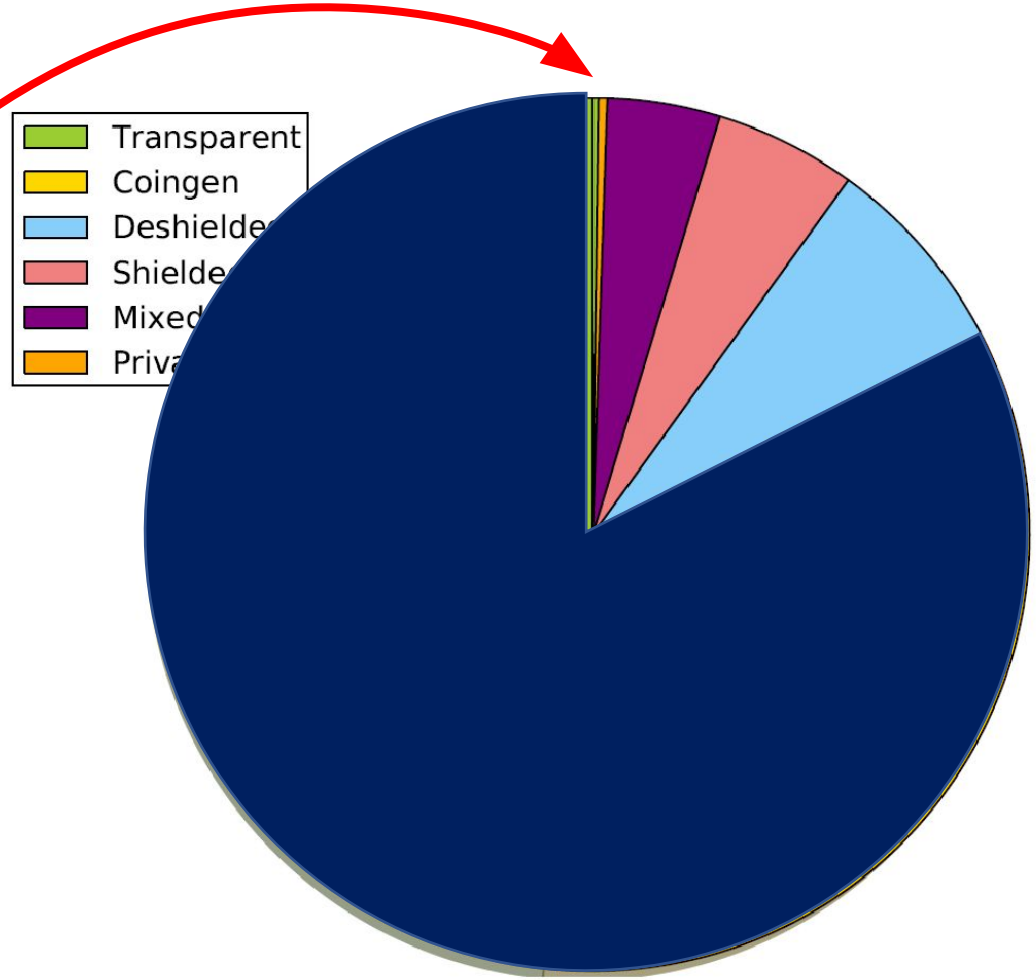


Blockchain statistics



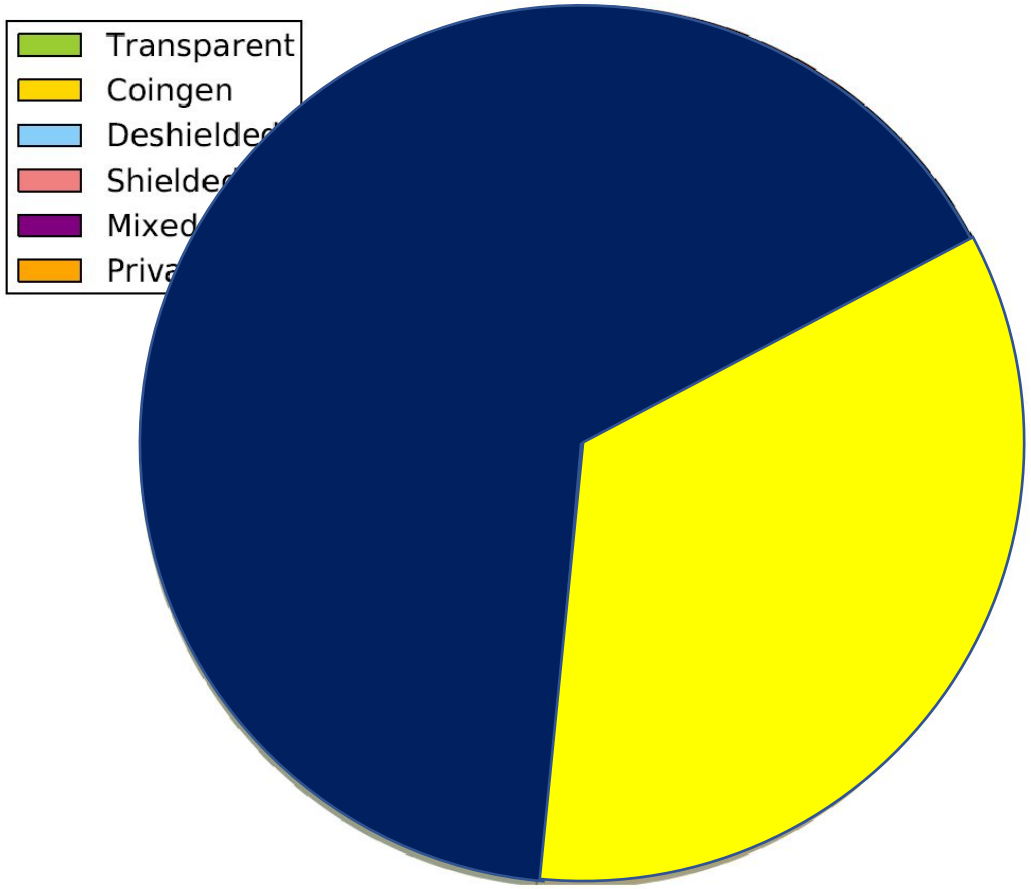
- About 85% of transactions are public i.e. transparent or newly generated coins.

Blockchain statistics



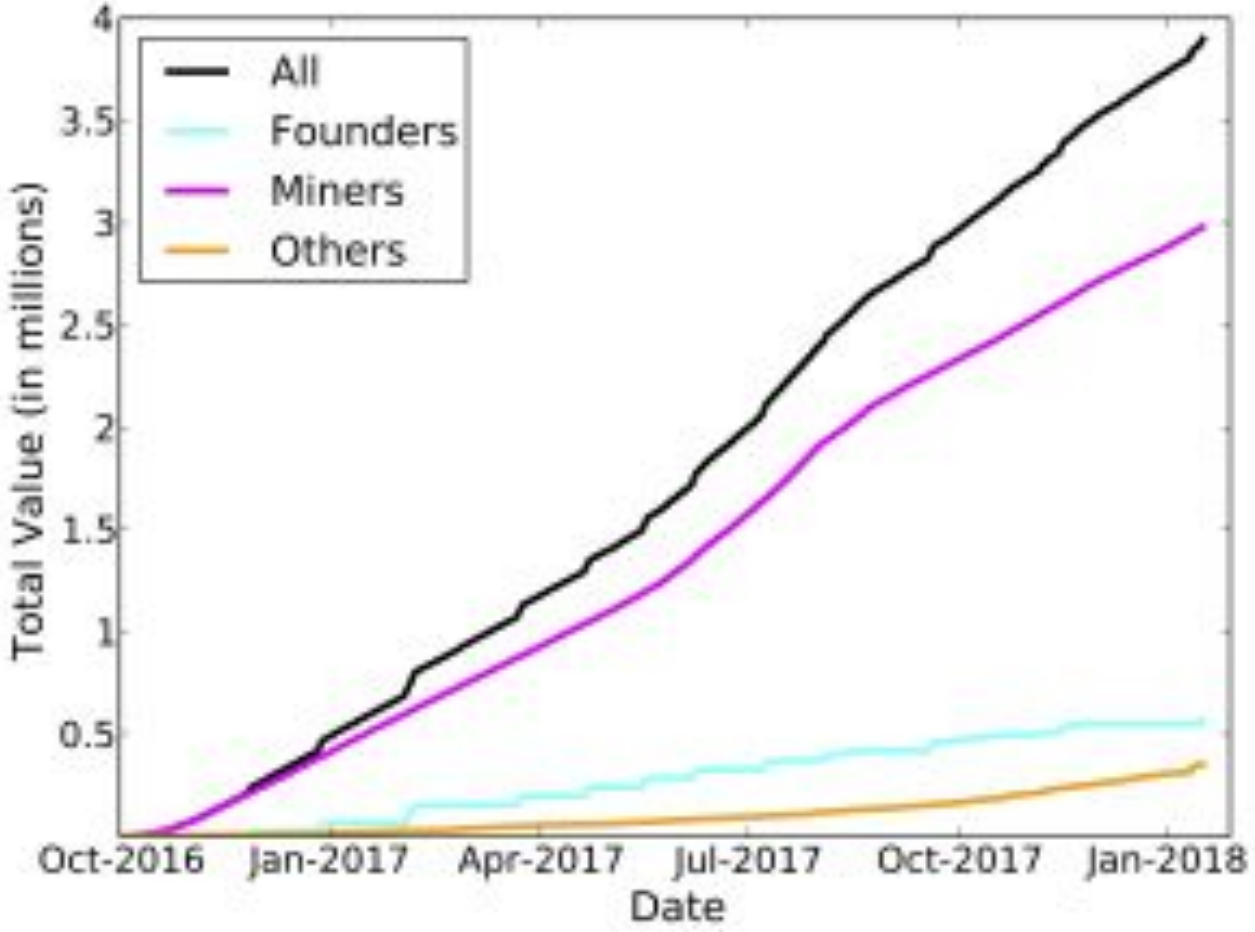
- Very few transactions are private to private

Miners and Founders



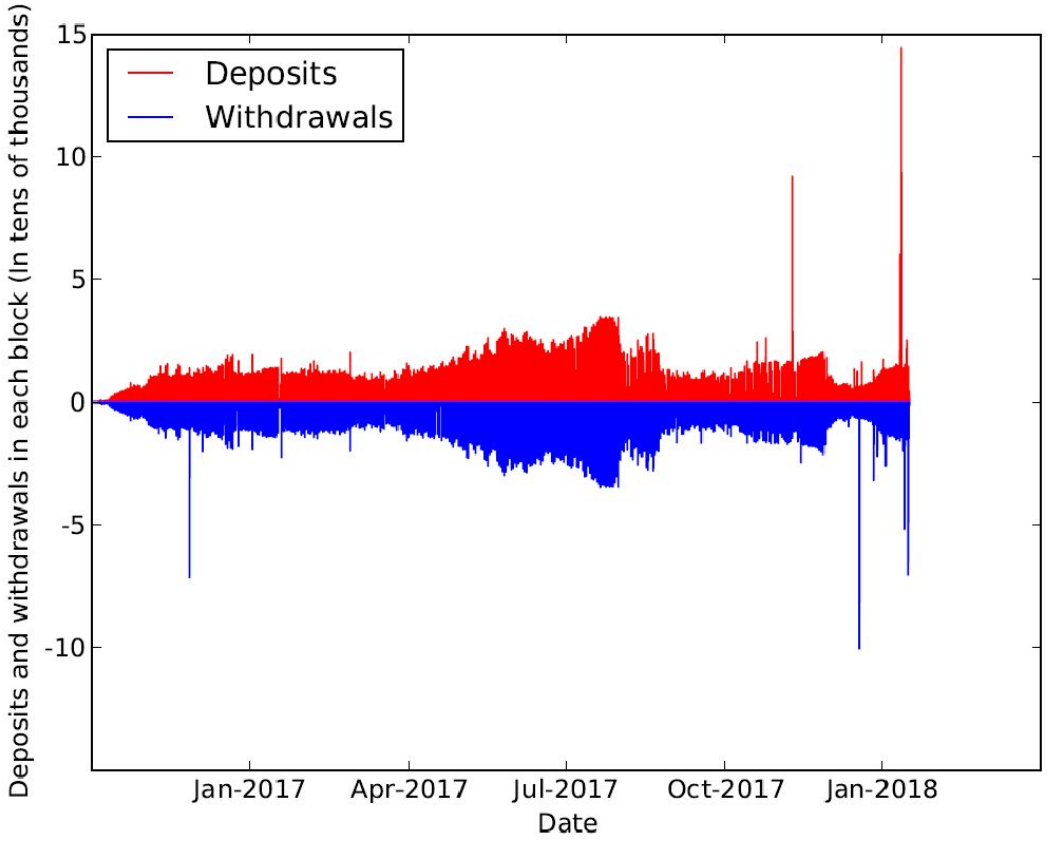
- All new coins go to either the miners or the founders.
- New coins are required to be sent to the shielded pool before they can be spent.

Miners and Founders



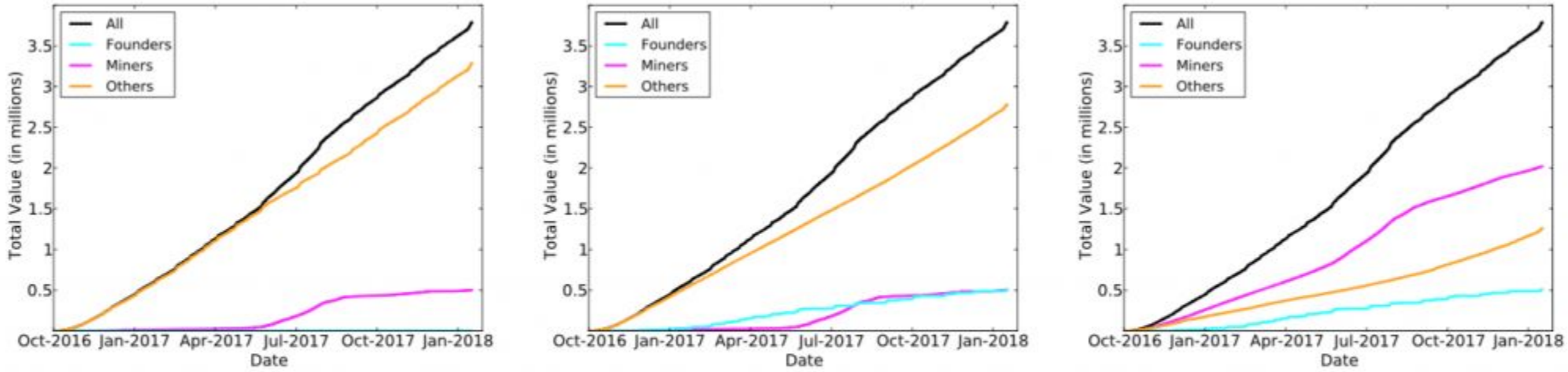
- Tracked coins being put into the pool.
- Founders addresses are public so can be identified.
- Miners addresses can be identified from coin generation transactions.

Blockchain statistics



- Most of the coins put into the pool are immediately removed again.

Miners and Founders



(a) No heuristics (b) Founder heuristic (c) Founder and miner heuristics

Figure 8: The z-to-t transactions we associated with miners, founders, and 'other', after running some combination of our heuristics.

We could associate 69% of the activity surrounding the shielded pool with miners and founders, leaving 31% left as the anonymity set for regular users.

Identifying Founders

- 75% of founder transactions into the pool were of the value 249.9999 ZEC.
- Found 1,953 withdrawals of exactly 250.0001 ZEC.
- Found correlation in block interval between deposits and withdrawals.

Identifying Miners

- Most mining activity comes from mining pools.
- Some pools engaged with the shielded pool in a predictable fashion.
- We identified withdrawals as belonging to a miner if it had over 100 recipients, with one of them belonging to a known mining pool.

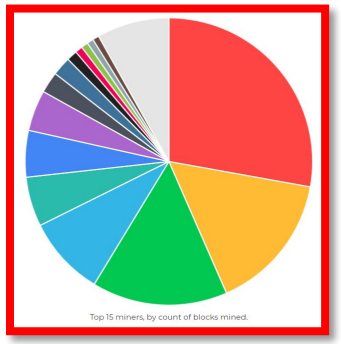
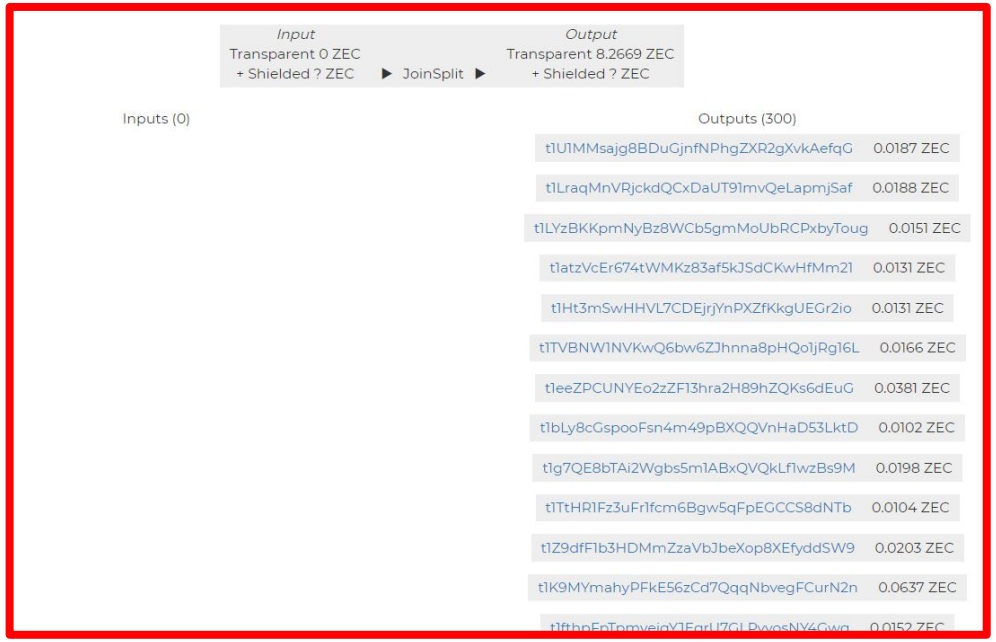


Image of mining pool distribution from *explorer.zcha.in*



Transaction from *explorer.zcha.in*

Consequences

What does this mean for other users?

Identifying Users

- Used Jeffrey Quesnelle heuristic which links deposit and withdrawal transactions if they had exactly the same value and this particular value was unique in the whole blockchain.
- Correlated 28.5% of all coins ever deposited in the pool.
- Most (87%) of the linked coins were in transactions already attributed to the founders and miners.

Case Study: The Shadow Brokers

- The Shadow Brokers (TSB) are a hacker collective that sell and distribute tools supposedly created by the NSA.
- One cluster sent transactions to the shielded pool with amounts and timings that corresponded to TSB's sale activity.
- The cluster belonged to a new user.
- Most of their coins from Bitfinex.

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

Price of monthly dump in ZEC.

Recommendations to Users

- Do not mint and spend coins in the same block. Ideally keep part of your wallet shielded to use at a later date.
- Do not deposit and withdraw the exact same amount.
- When taking change from a shielded transaction, store the change in a shielded address rather than a transparent address.
- Try to ensure that withdrawal addresses cannot be linked to deposit addresses using standard bitcoin clustering techniques.

Recommendations to Developers

Recommendation	Solutions in progress
Do not rely on user or miner behaviour for security.	
Have a less recognisable pattern when withdrawing founders rewards.	
Try to help more people use the shielded functionality of Zcash.	
Ultimately, none of our heuristics would work on a fully anonymous system.	

Recommendations to Developers

Recommendation	Solutions in progress
Do not rely on user or miner behaviour for security.	Wallet upgrades.
Have a less recognisable pattern when withdrawing founders rewards.	Developers have already done this.
Try to help more people use the shielded functionality of Zcash.	One of the aims of the Sapling upgrade.
Ultimately, none of our heuristics would work on a fully anonymous system.	Weigh up the technical and legal consequences of a fully anonymous system.

Recommendations to Developers

Ultimately, none of our heuristics would work on a fully anonymous system.	Weigh up the technical and legal consequences of a fully anonymous system.

Shameless plug: follow our work on updatable and universal common reference strings for zk-SNARKs.

Thank-you for listening