Data Analytics and Consensus Mechanisms in Blockchains

Daniel Feher

University of Luxembourg

24 September 2020

PhD Defense

UNIVERSITÉ DU
LUXEMBOURG

Outline

Introduction

Linkability of Mining in Zcash

Further Transaction Linking in Zcash

ASIC Mining Zcash

Introduction to Blockchains

- Started by Bitcoin
- First decentralized P2P currency
- Key new features popularized and introduced (PoW, UTXO)
- Digital Signature based transaction authentication
- Transactions in Blocks, Blocks in an immutable Hash Chain

Unspent Transaction Outputs

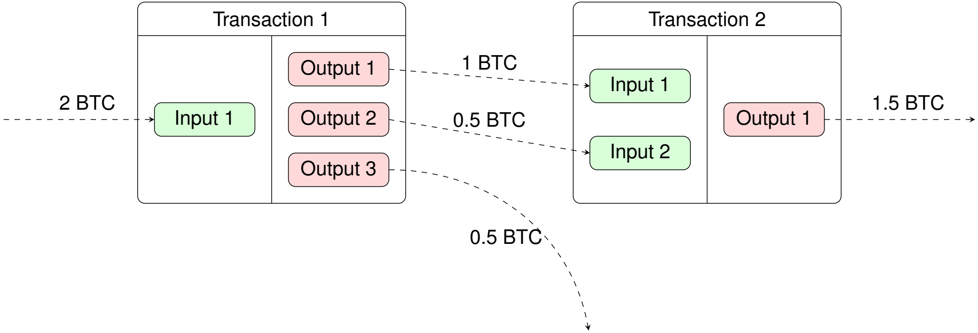


Figure: An example for the transaction structure of Bitcoin. See that the output of a transaction is then the input of a later transaction, chaining all transactions together.

Proof-of-Work

- The next solver of a difficult hash puzzle (PoW) generates the new blocks
- The generator receives reward in coins
- Only way of minting new coins
- Performed in pools of miners to reduce the variance of payouts

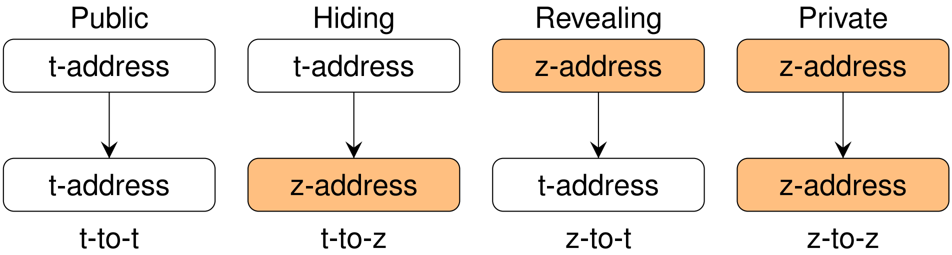
Introduction to Zcash

- Bitcoin has a few privacy issues
- Zcash is a privacy oriented digital currency.
- Built on a variety of cryptographic primitives:
  - zkSNARKs, commitment schemes, Merkle trees, encryption, etc.
- Zcash coins are called ZECs. 1 ZEC corresponds to 10^8 Zatoshis.

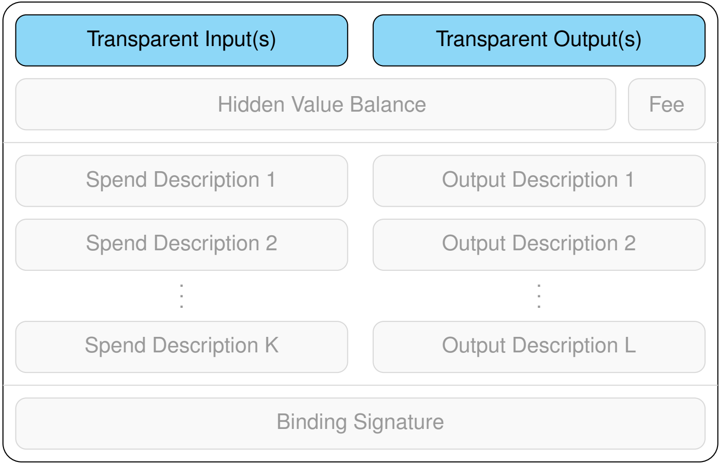
Zcash: Addresses

- Zcash offers two types of addresses:
  - *transparent* or *public*, commonly referred to as *t-addresses*.
  - *shielded* or *private*, commonly referred to as *z-addresses*.

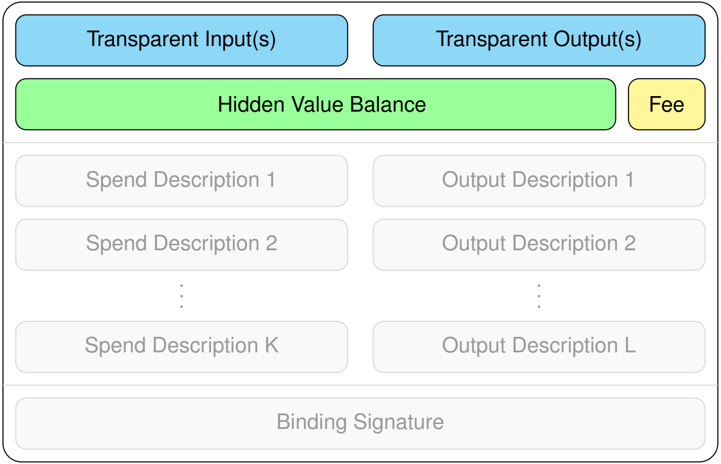
Zcash Transaction Types



Zcash Transaction Layout



Zcash Transaction Layout



Transparent Input(s)

Transparent Output(s)

Hidden Value Balance

Fee

Spend Description 1

Output Description 1

Spend Description 2

Output Description 2

⋮

⋮

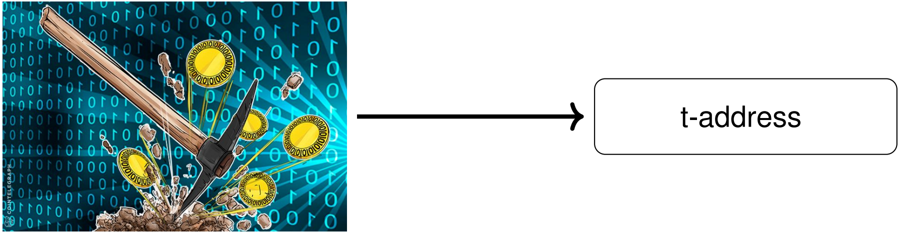
Spend Description K

Output Description L

Binding Signature

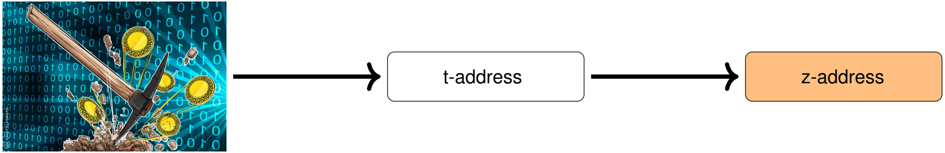
Picture credit: Cointelegraph

Zcash Mining



t-address

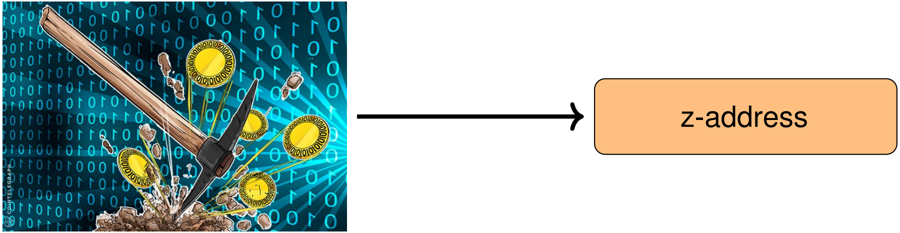
Zcash Mining



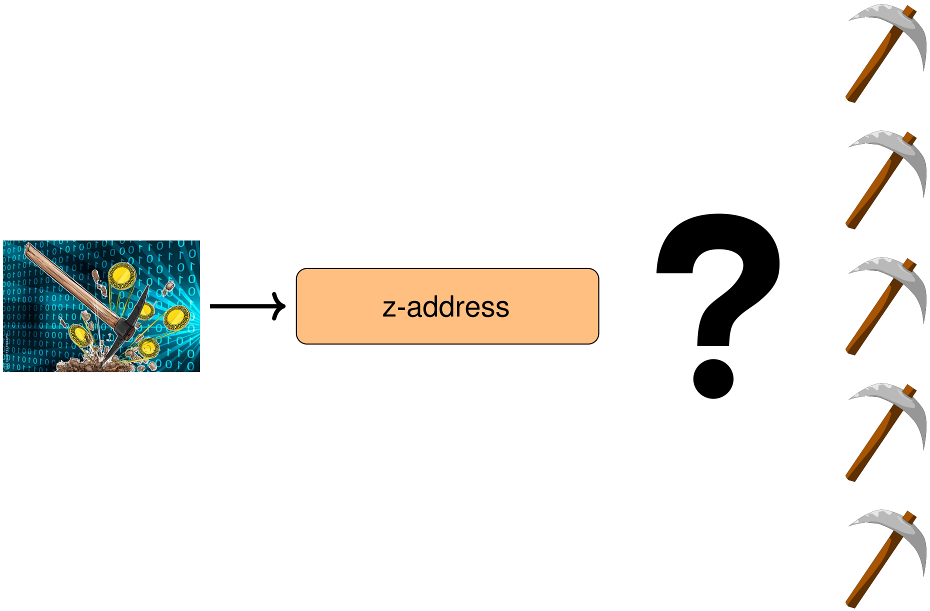
t-address

z-address

Zcash Mining

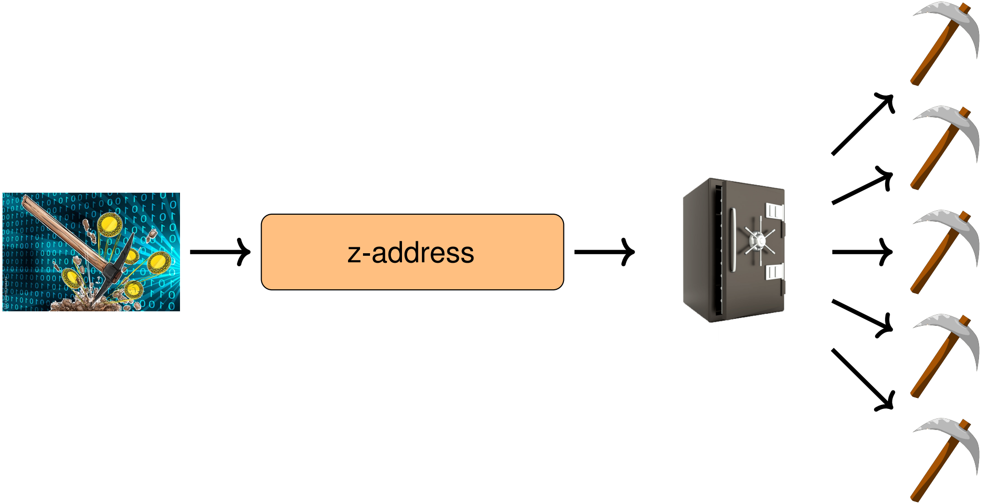


z-address



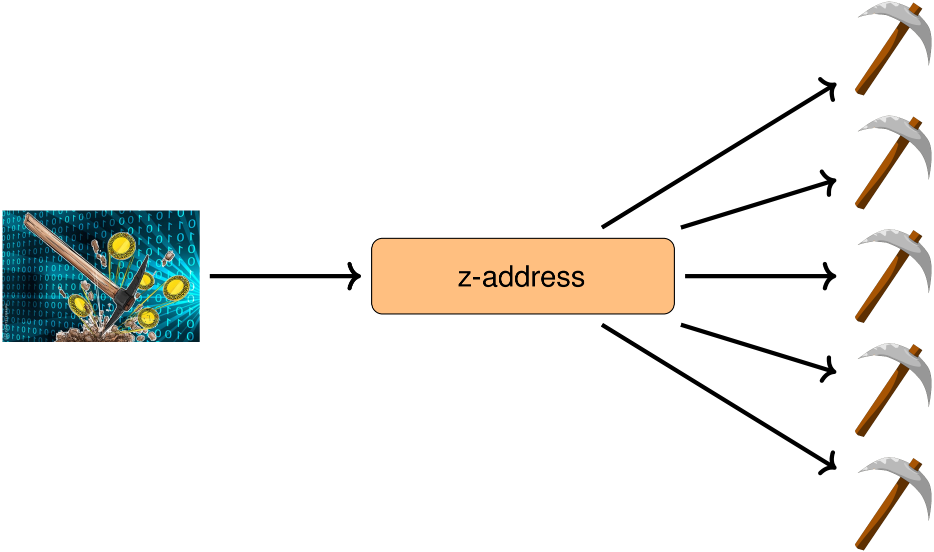
z-address

Pattern T



z-address

Pattern Z



z-address

Introduction

Linkability of Mining in Zcash

Further Transaction Linking in Zcash

ASIC Mining Zcash

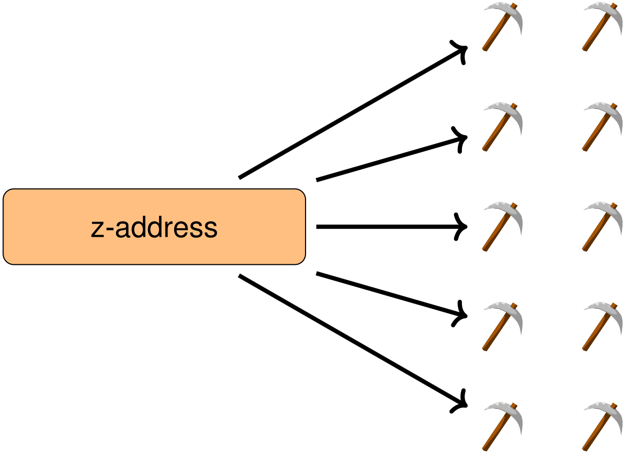
Core Idea

- We know how much is hidden per mining pool
- Link it to the same revealed amount
- Verify by examining different block periods

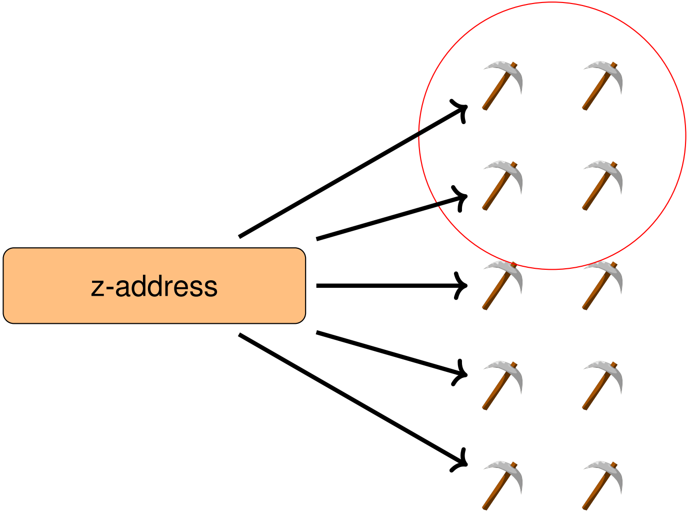
Pattern T Payouts

- Calculate received amount for every address
- Compare with amounts mined and hidden
- Verify by investigating different connecting block periods

Pattern Z Payouts



Pattern Z Payouts



Results

- 88.4% of mining rewards linked
- 84% of all z-t revealing volume has been linked
- 68.4% of all revealing transactions in terms of number of transactions have been linked
- 95.5% of all Zcash transactions are linkable, close to privacy level of Bitcoin

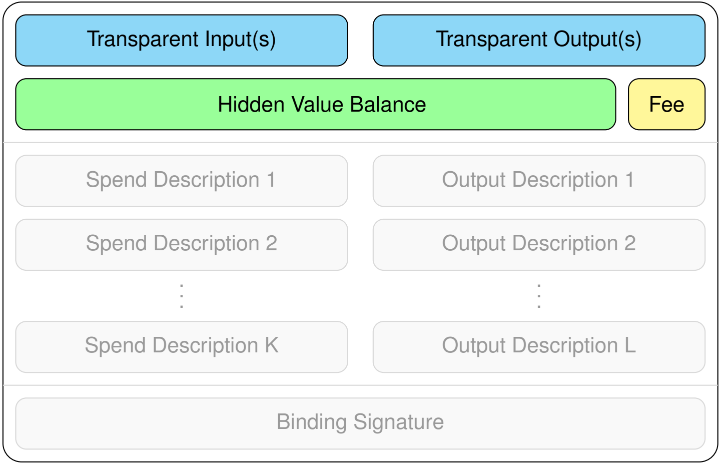
Introduction

Linkability of Mining in Zcash

Further Transaction Linking in Zcash

ASIC Mining Zcash

Zcash Transaction Layout



Transparent Input(s)

Transparent Output(s)

Hidden Value Balance

Fee

Spend Description 1

Output Description 1

Spend Description 2

Output Description 2

⋮

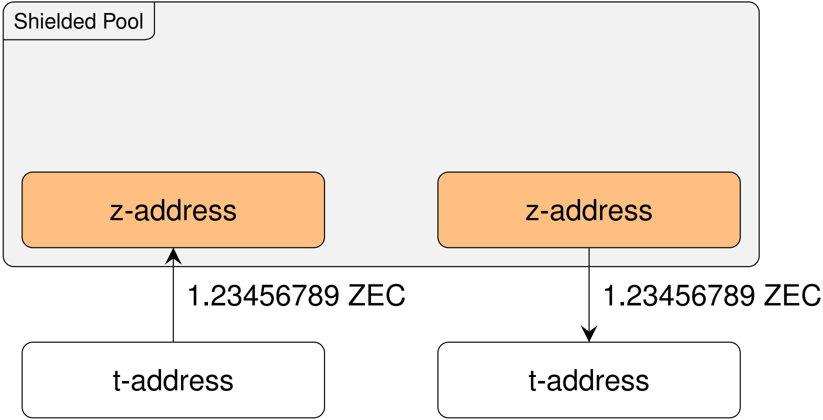
⋮

Spend Description K

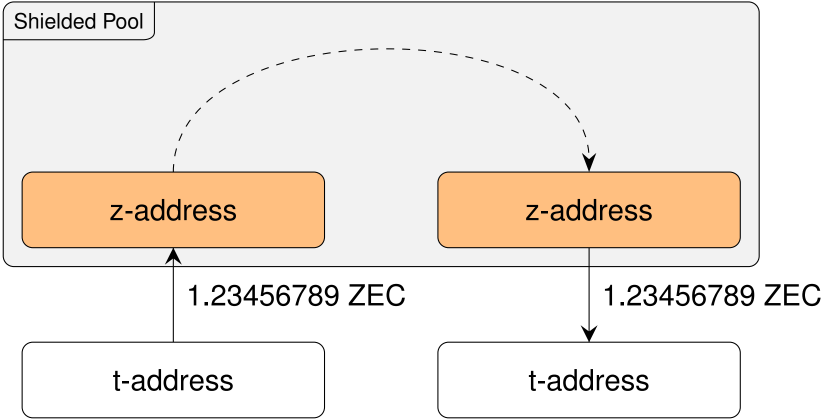
Output Description L

Binding Signature

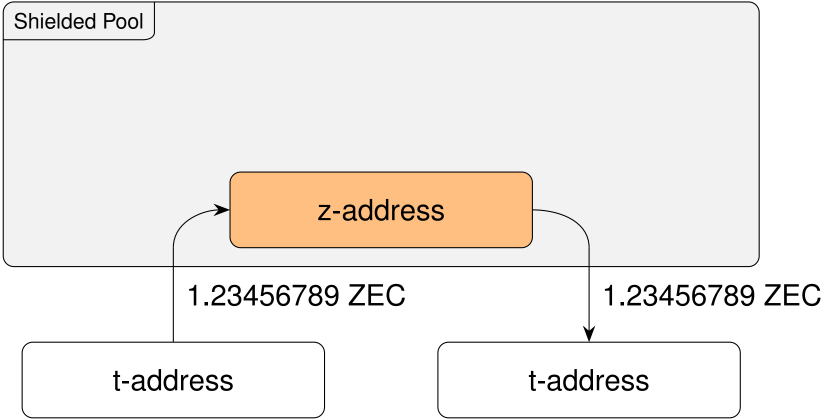
Transaction Linking v1



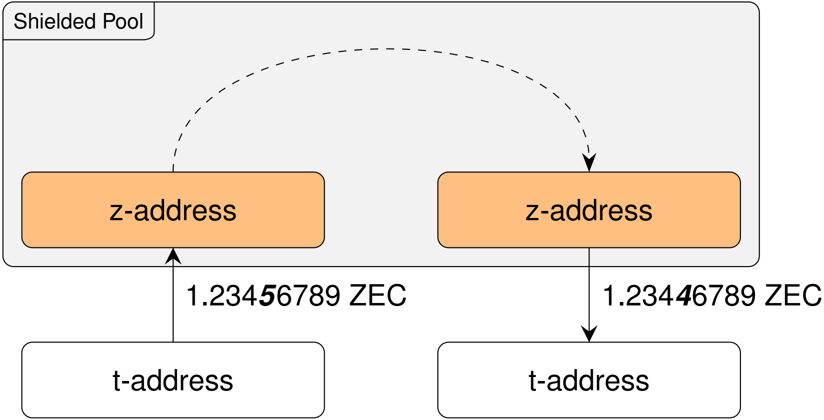
Transaction Linking v1



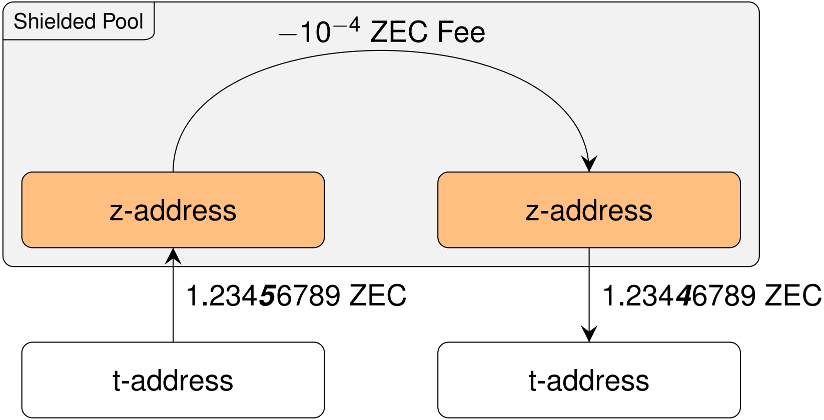
Transaction Linking v1



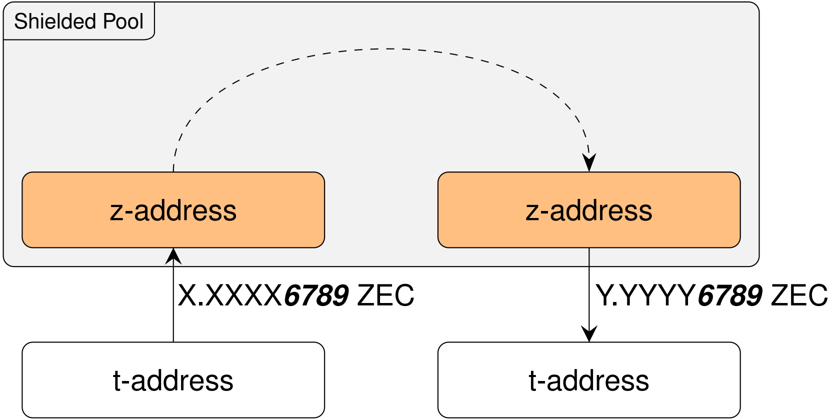
Transaction Linking v2



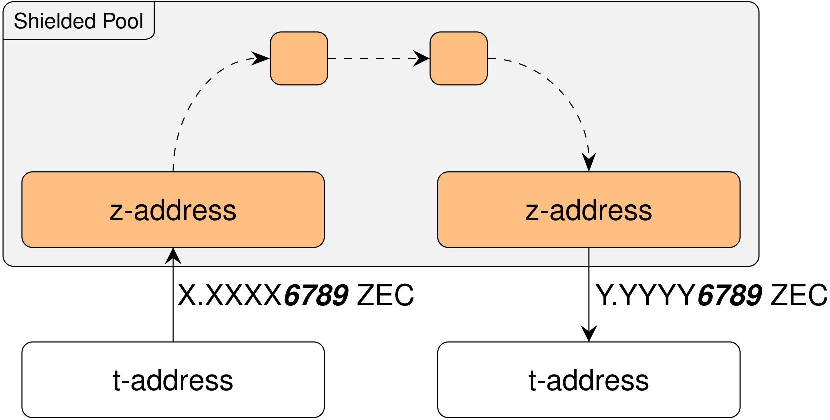
Transaction Linking v2



Transaction Linking v3



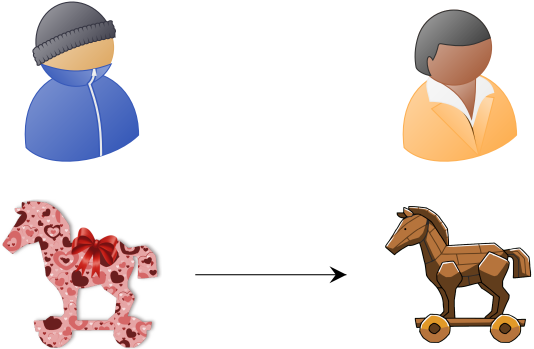
Transaction Linking v3



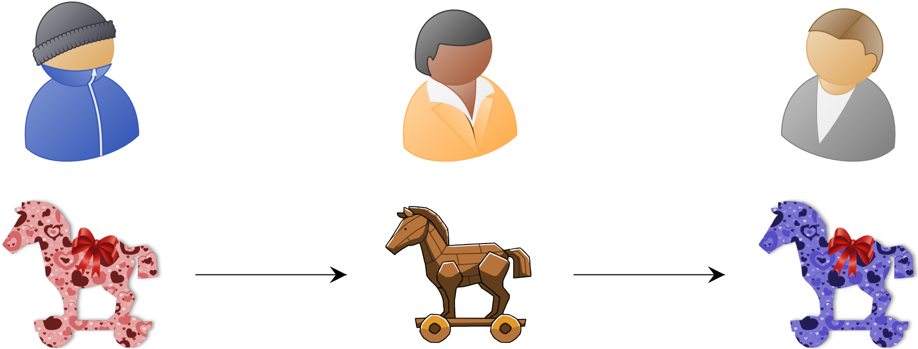
Value Fingerprints

- $\sim$ 97% of shielded transactions use 10^4 Zatoshis as fee.
- Last 4 digits are not changed by the fee.
- Can be used maliciously

Danaan-Gift Attack



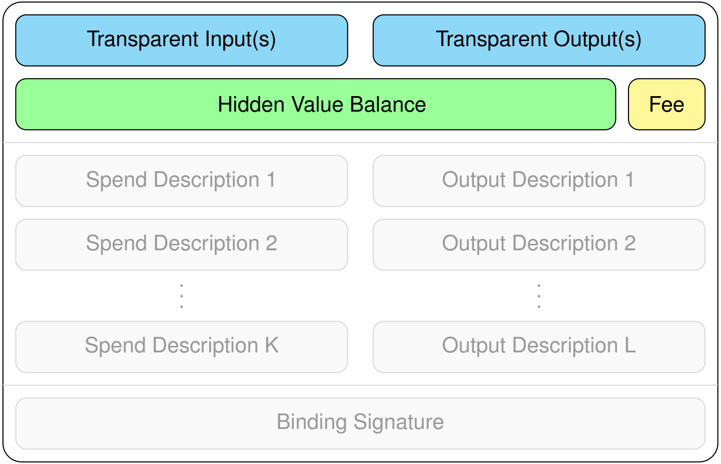
Danaan-Gift Attack



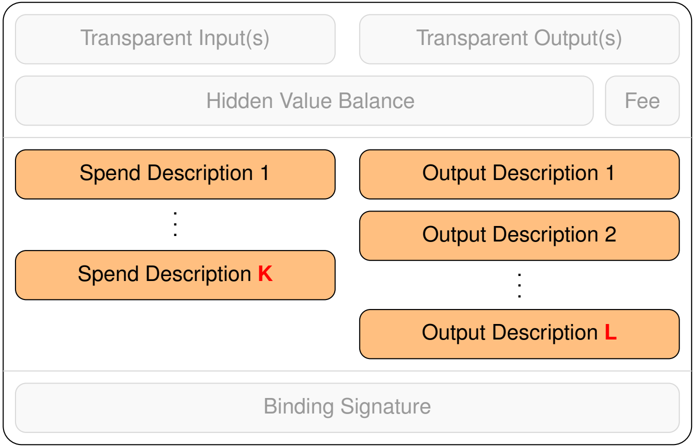
Danaan-Gift Attack

- What is the success ratio of the attack?
- What is the likelihood of a fingerprint surviving?

Zcash Transaction Layout



Zcash Transaction Layout



Transparent Input(s)

Transparent Output(s)

Hidden Value Balance

Fee

Spend Description 1

⋮

Spend Description **K**

Output Description 1

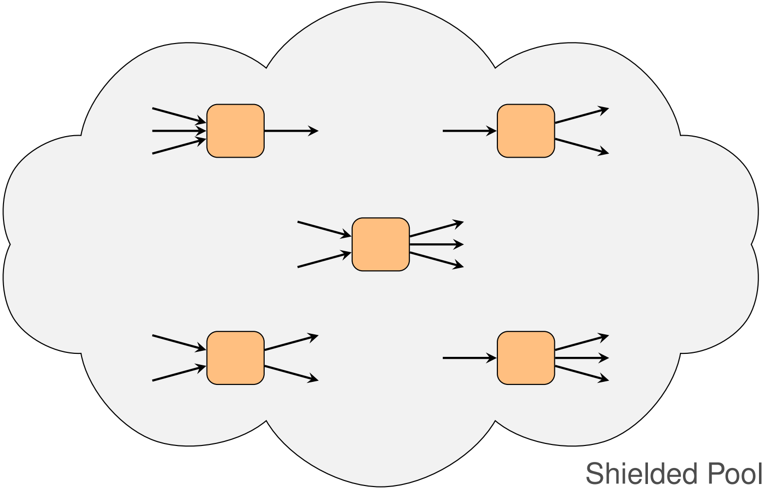
Output Description 2

⋮

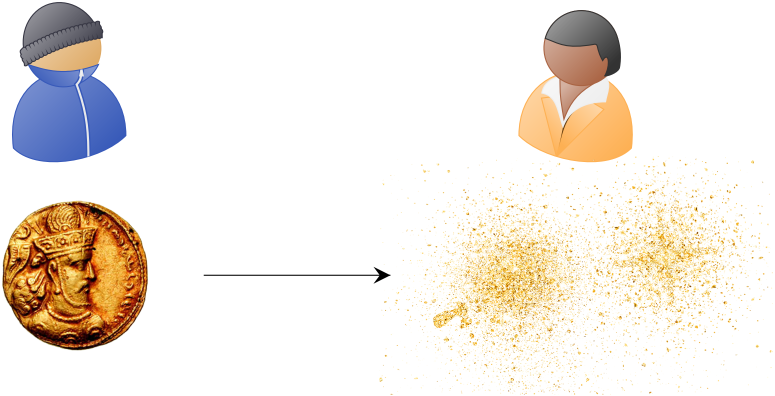
Output Description **L**

Binding Signature

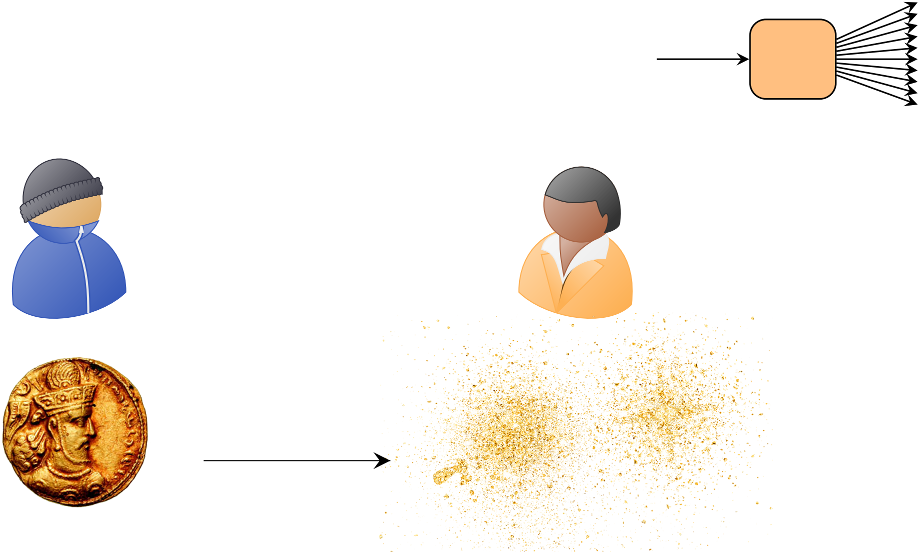
Zcash Transaction Layout



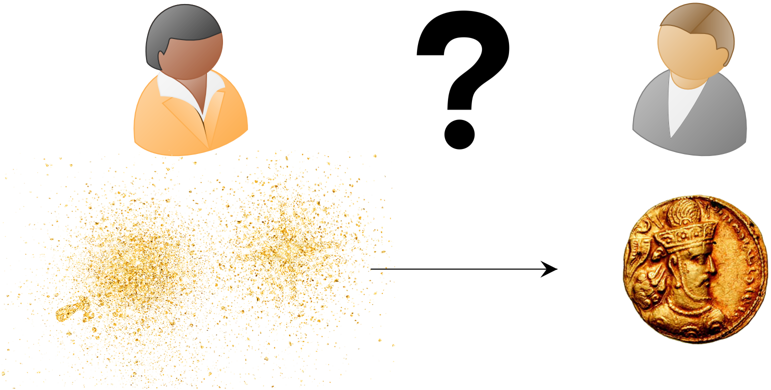
Dust Attack



Dust Attack

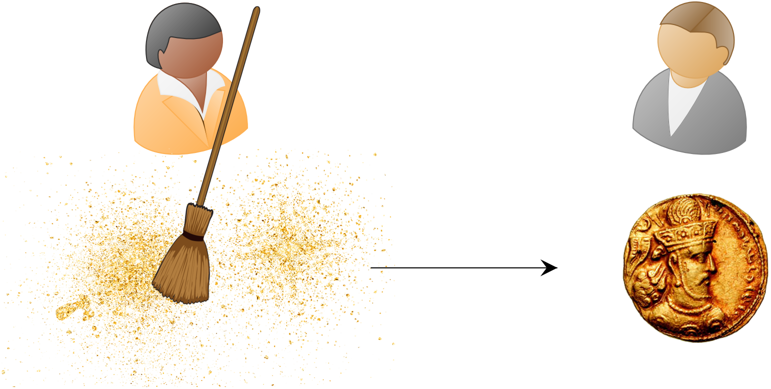


Dust Attack

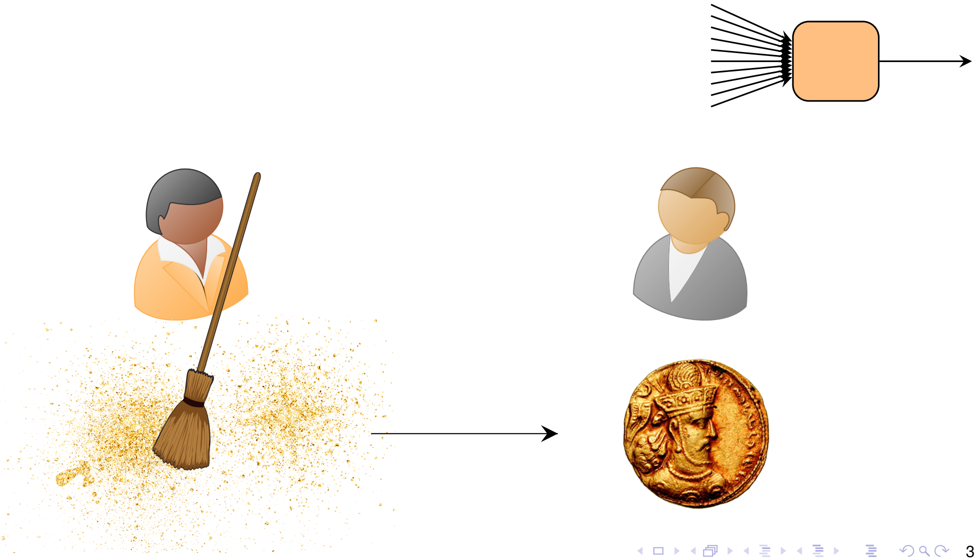


Dust Attack

Dust Attack



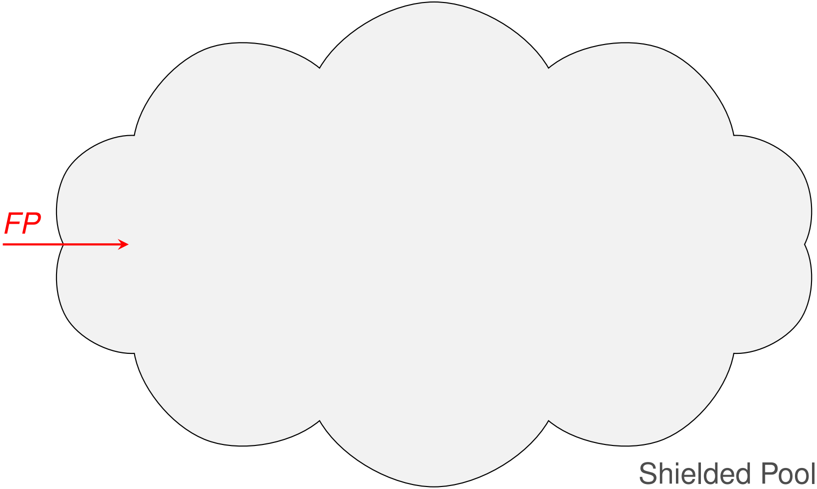
Dust Attack



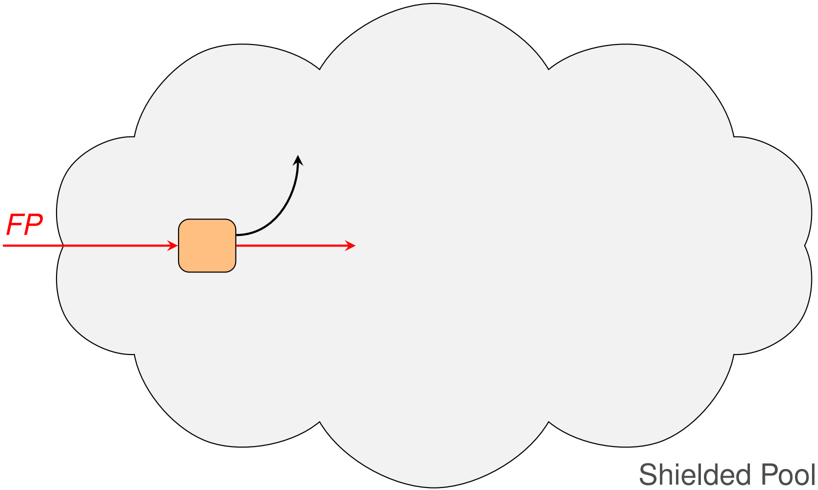
The Survival Probability of Fingerprints

- We have developed a statistical model for the shielded pool.
- Based on the number of inputs and outputs in a shielded transaction.
- Markov-chain of all possible scenarios.
- Sample data based on characteristically the same public transactions.

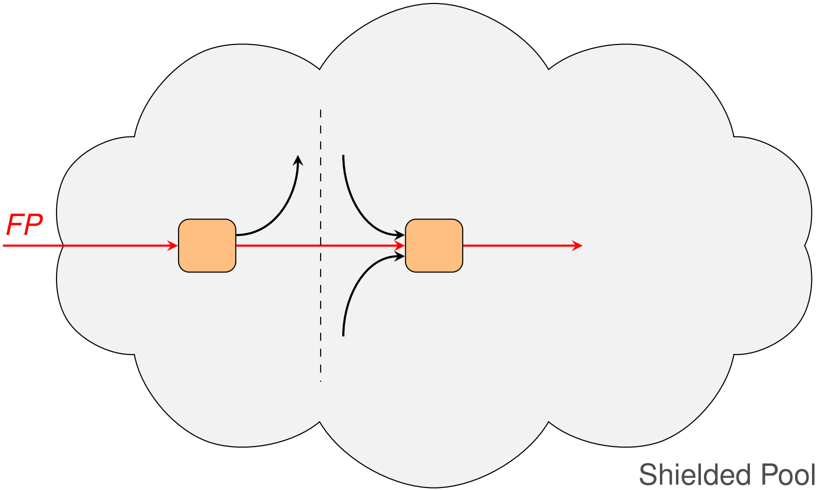
The Survival Probability of Fingerprints



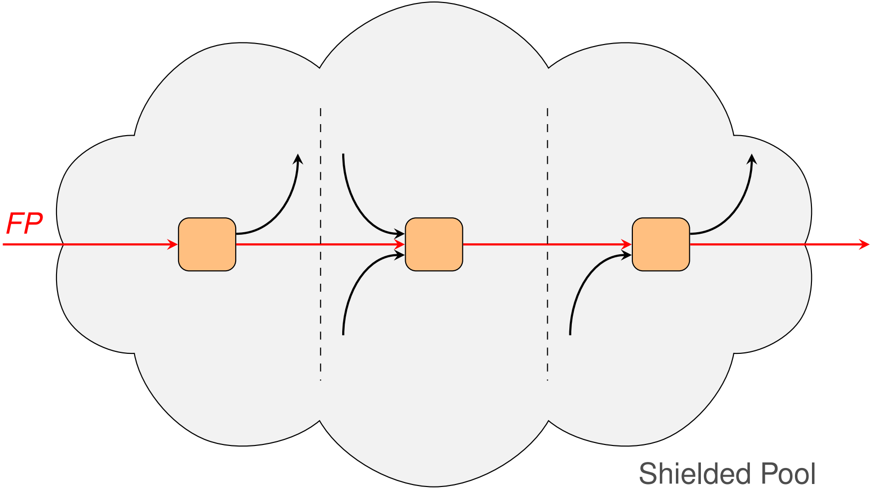
The Survival Probability of Fingerprints



The Survival Probability of Fingerprints



The Survival Probability of Fingerprints



The Survival Probability of Fingerprints

- The average number of hops a path goes through inside the shielded pool is only 1.42.

- The survival probability of *good* fingerprints is $\sim 16.6\%$.

- The survival probability of fingerprints corresponds, in turn, to the success probability of Danaan-gift Attack.

Countermeasures

- Dust Attack is recognizable: move funds once.
- Danaan-gift Attack *manual defense*: do not use default fees.
- Danaan-gift Attack *built-in defense*: default fee is a random value between 0.00009500 ZEC and 0.00010500 ZEC.

Introduction

Linkability of Mining in Zcash

Further Transaction Linking in Zcash

ASIC Mining Zcash

GPU and ASIC mining

- Evolution of mining hardware
- GPUs are more accessible
- More decentralization
- ASICs have higher entry cost but higher efficiency

Introduction of ASICs

- Zcash uses Equihash-200,9 hashing algorithm
- Designed to be ASIC resistant, mining only with GPUs
- Late May, 2018 multiple ASIC (application-specific integrated circuit) miners were announced for the version implemented in Zcash
- Was there hidden ASIC mining in Zcash?
- Similar circumstances in Monero, where the likelihood of hidden mining was high

Developer Fees

- Most used mining software have built-in developer fees (not to confuse with the founder's fee in Zcash)
- Developer fee is paid by mining 2% of the time to the developer's address
- Find the addresses of developers
- Approximate their mining power, extrapolate for entire mining power (function of time, received payouts and global hashing rate)
- Remaining mining power might be ASICs

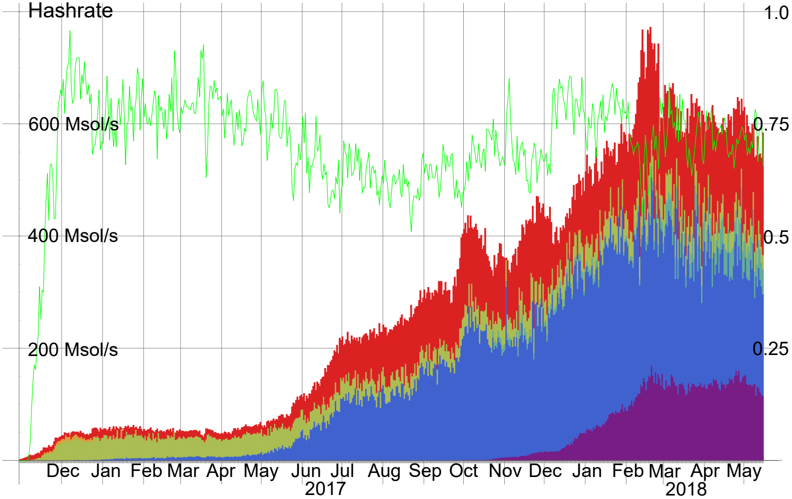


Figure: Lower bound of GPU mining power based on the developer fees (Green: Claymore, Blue: EWBF, Purple: dstm, Light Blue: Bminer, Orange: Optiminer, Red: Remaining Hash rate)

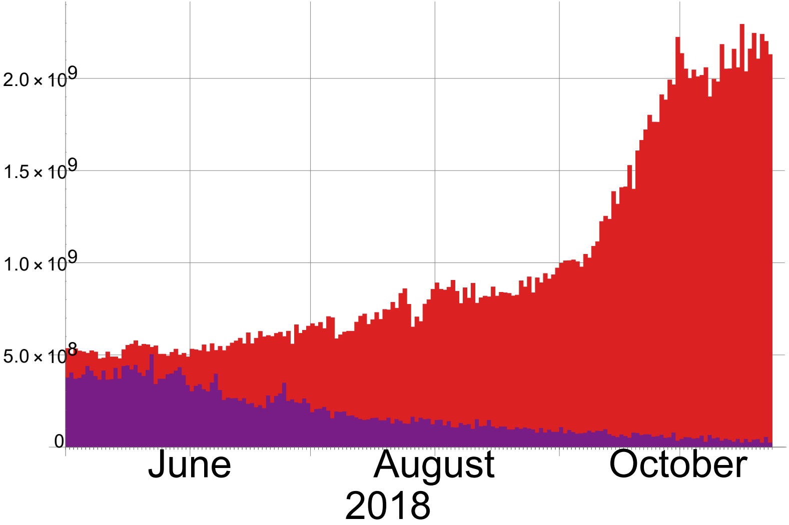
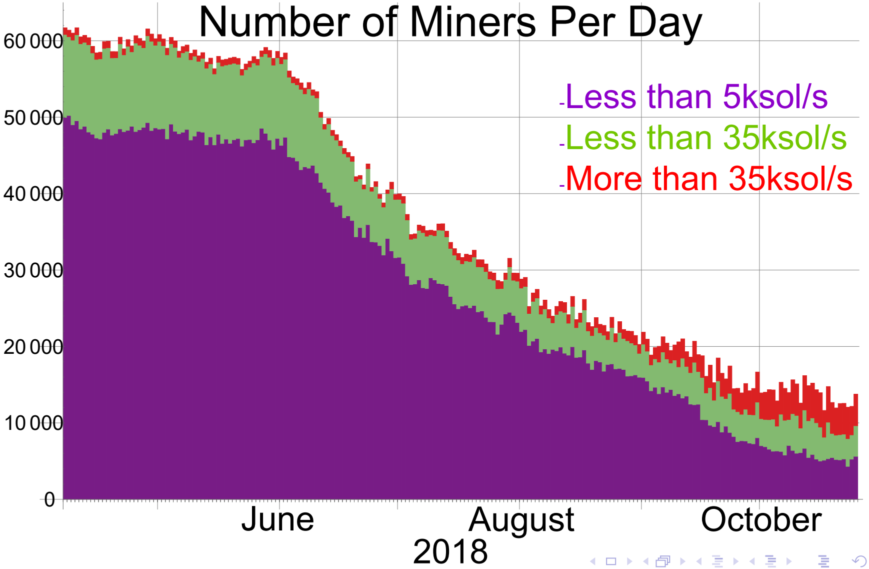


Figure: The recent change in the projected mining power from dev-fees for the overall Equihash hash rate

Mining Centralization



Summary

- Linkability of mining payouts in Zcash
- Further privacy issues
- Two novel attacks against Zcash user privacy
- Explored the effect of ASICs in Zcash mining

List of Publications

- Biryukov, Feher, *Portrait of a Miner in a Landscape*. CrybBlock 2020
- Biryukov, Feher, *Privacy and Linkability of Mining in Zcash*. IEEE CNS 2019
- Biryukov, Feher, Vitto, *Privacy Aspects and Subliminal Channels in Zcash*. ACM CCS 2019
- Biryukov, Feher, *ReCon: Sybil-Resistant Consensus from Reputation*. Pervasive and Mobile Computing 2020