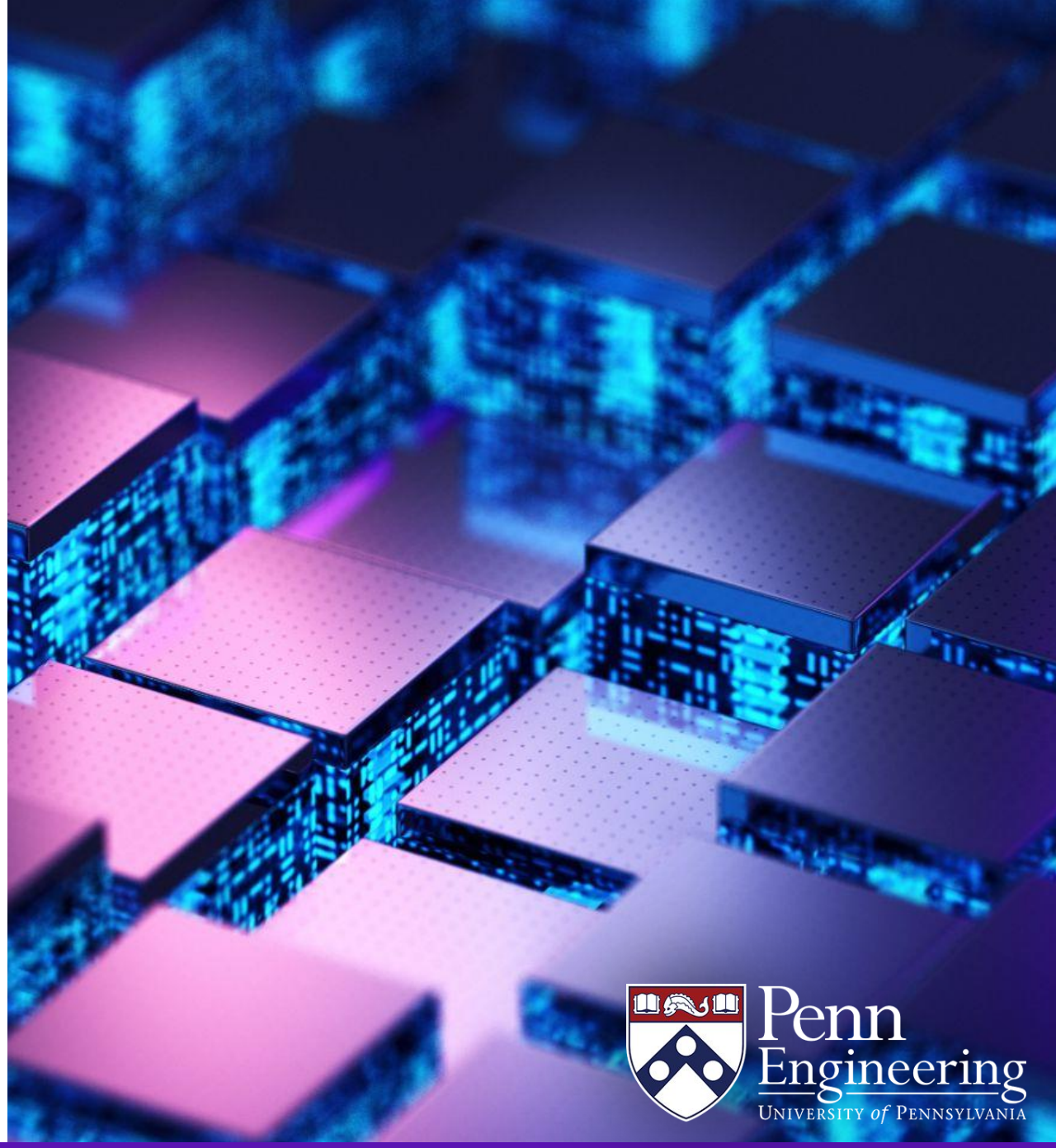
EAS 5830: BLOCKCHAINS

# De-anonymizing ZCash

Professor Brett Hemenway Falk



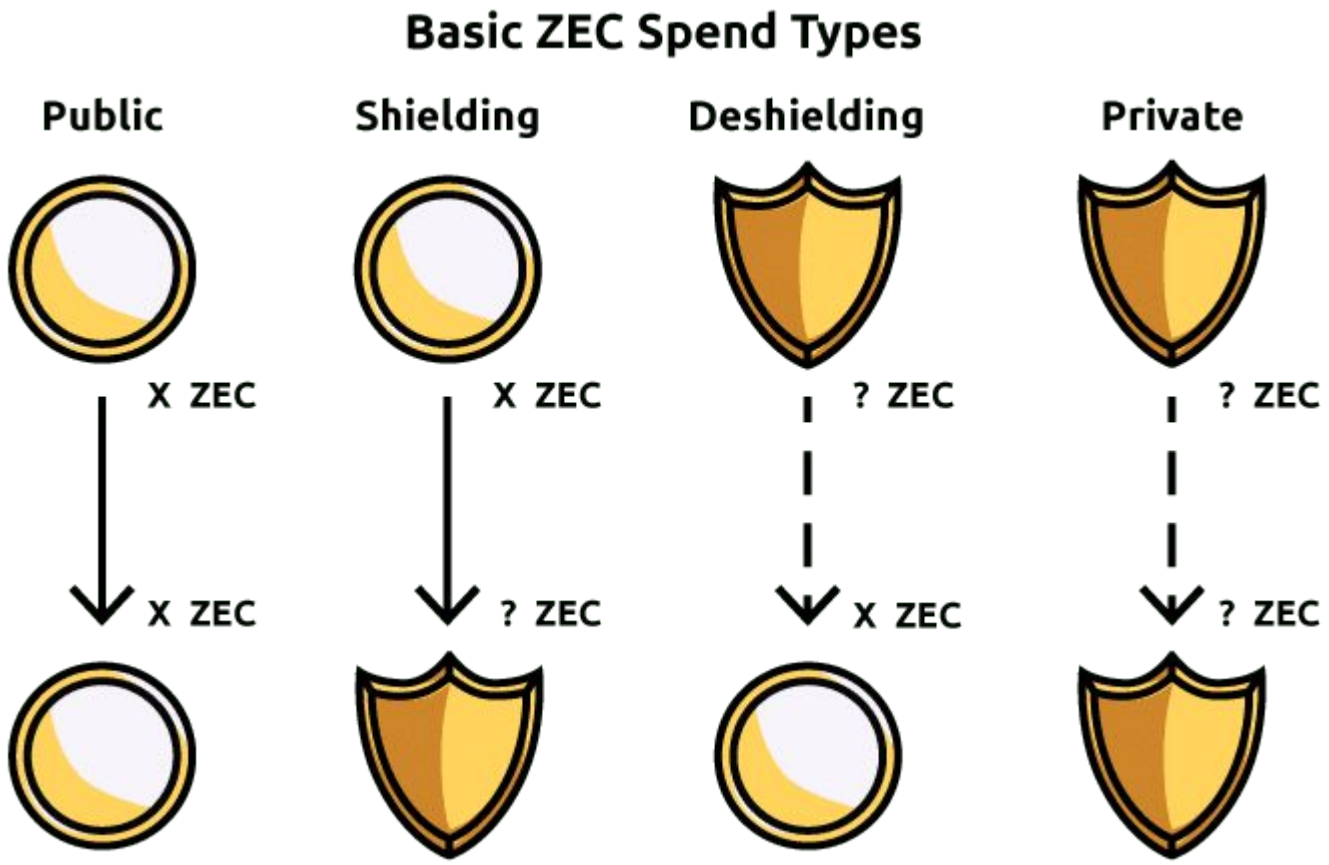
Penn Engineering
University of Pennsylvania

# Account types

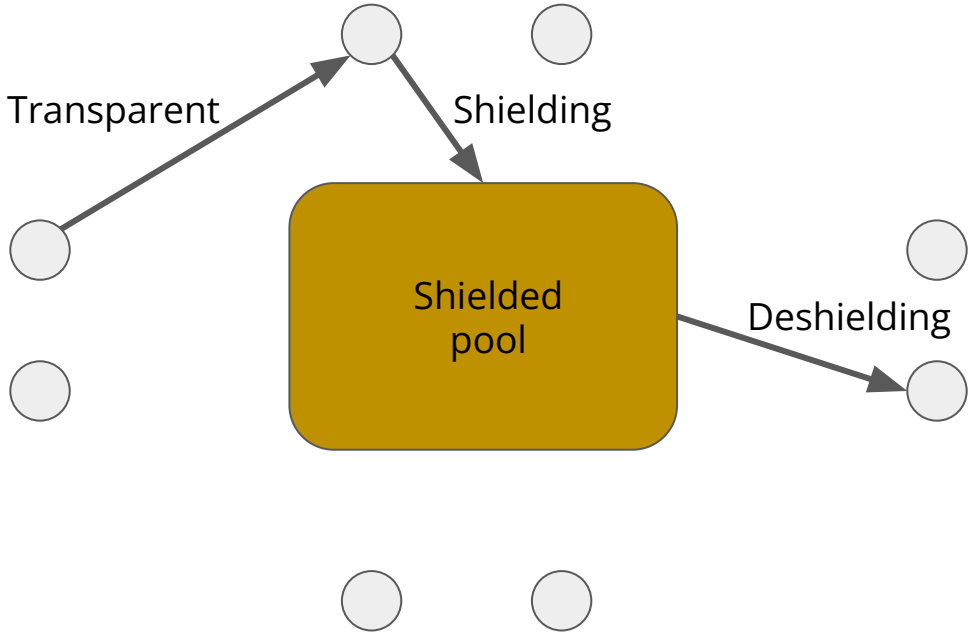
- Transparent
  - t-addresses have the same privacy as Bitcoin (none)

- Shielded
  - z-addresses are private

# Zcash

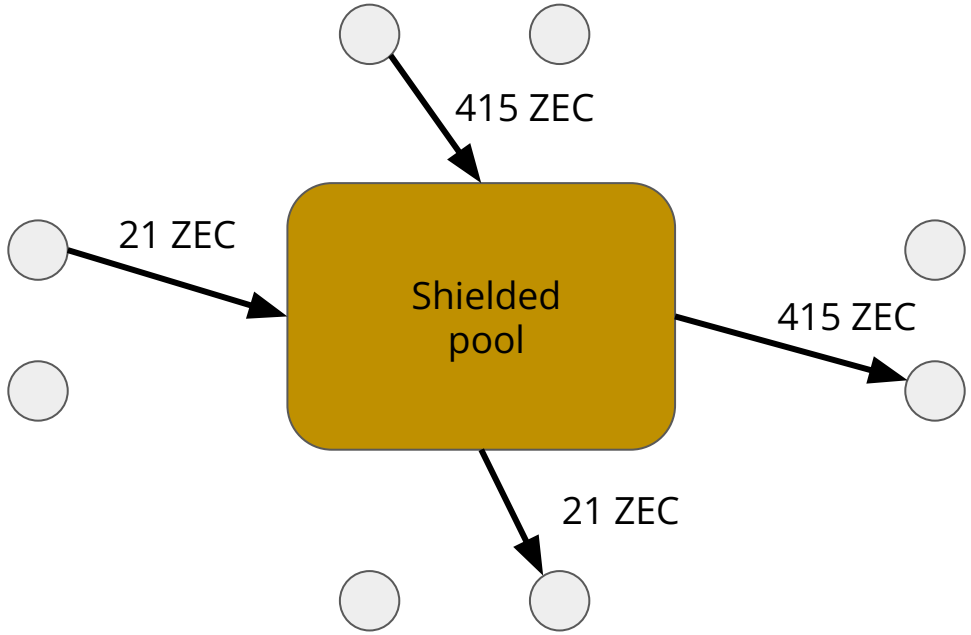

Basic ZEC Spend Types
Public
Shielding
Deshielding
Private
X ZEC
X ZEC
? ZEC
? ZEC
X ZEC
? ZEC
X ZEC
? ZEC

# Zcash transactions




- Transactions within the shielded pool (Z-to-Z) hide
  - sender
  - receiver
  - amount
- Shielding and deshielding leak information

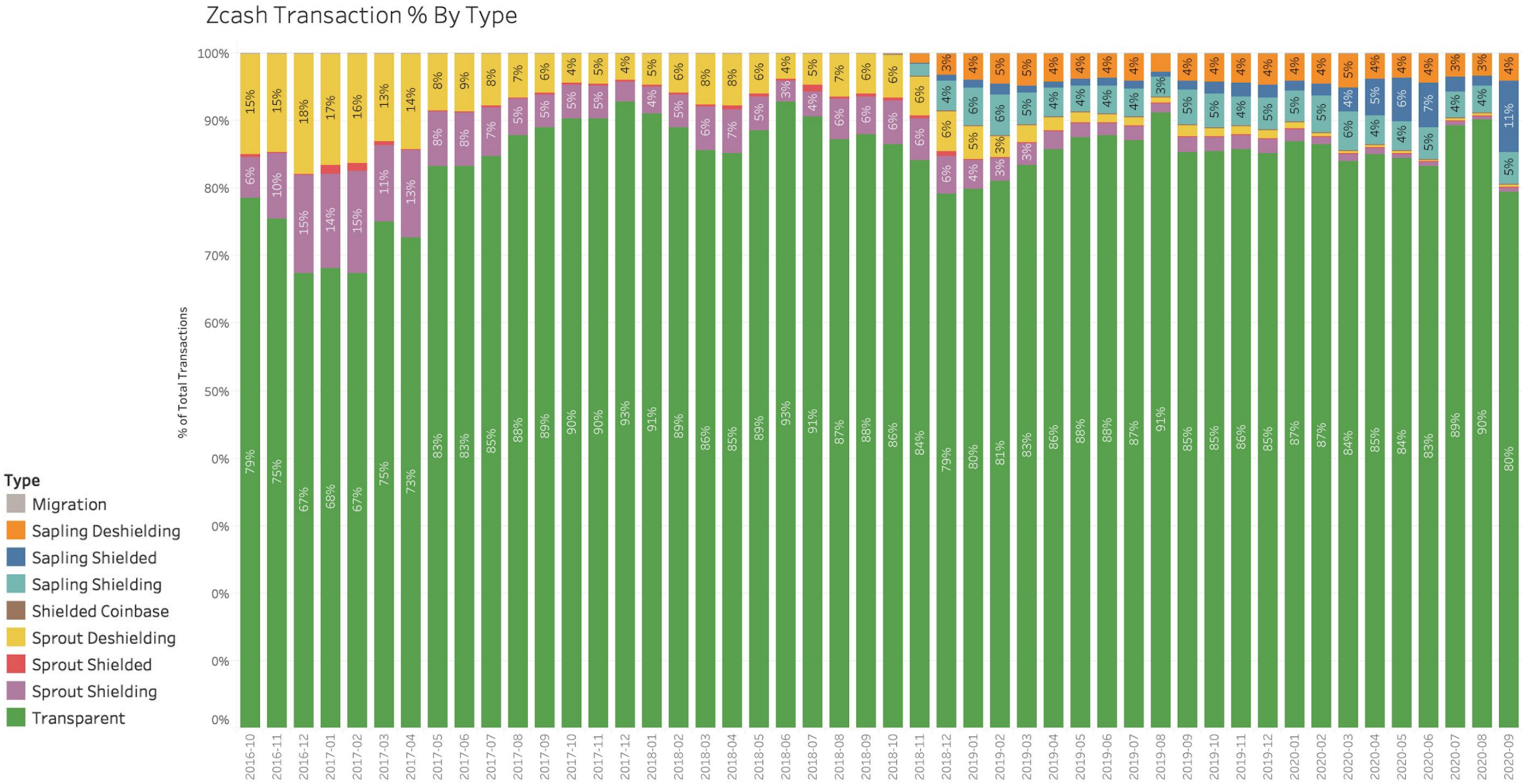
# Zcash transactions



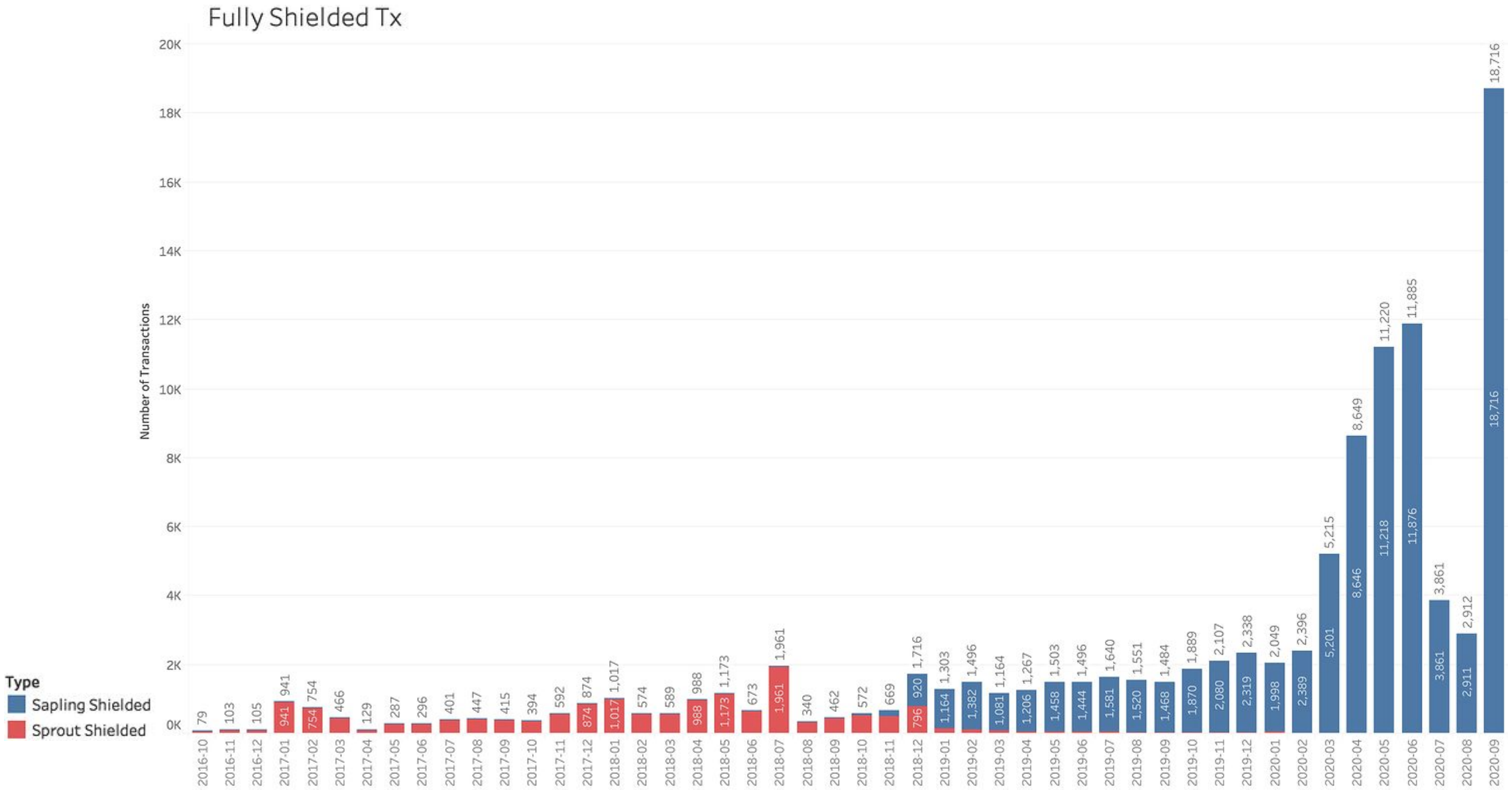

If you shield and then deshield the same amount, this reveals information

31% of transactions can be linked in this way (2017)

# Majority of ZCash transactions remain unshielded



# Majority of ZCash transactions remain unshielded



# Clustering transparent addresses

- Multi-input addresses
  - If two different accounts are used as input on the same transaction, they belong to the same individual
- Change addresses
  - If a transaction has multiple output addresses, and exactly one of them has never been seen before, then it is a ‘change’ address and belongs to the same individual as the input

# An Empirical Analysis of Anonymity in Zcash

USENIX 2018

# Heuristics

- **Timing:** 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.
- **Founders:** Any z-to-t transaction carrying 250.0001 ZEC in value is done by the founders.
- **Mining pools:** 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.

# Privacy

- No known attacks on the underlying cryptography
  - Devastating bug found (and fixed) by Zcash itself in 2018
- Lack of privacy stems from user behavior
  - Failure to use shielded addresses
  - Shielded and de-shielding in rapid succession