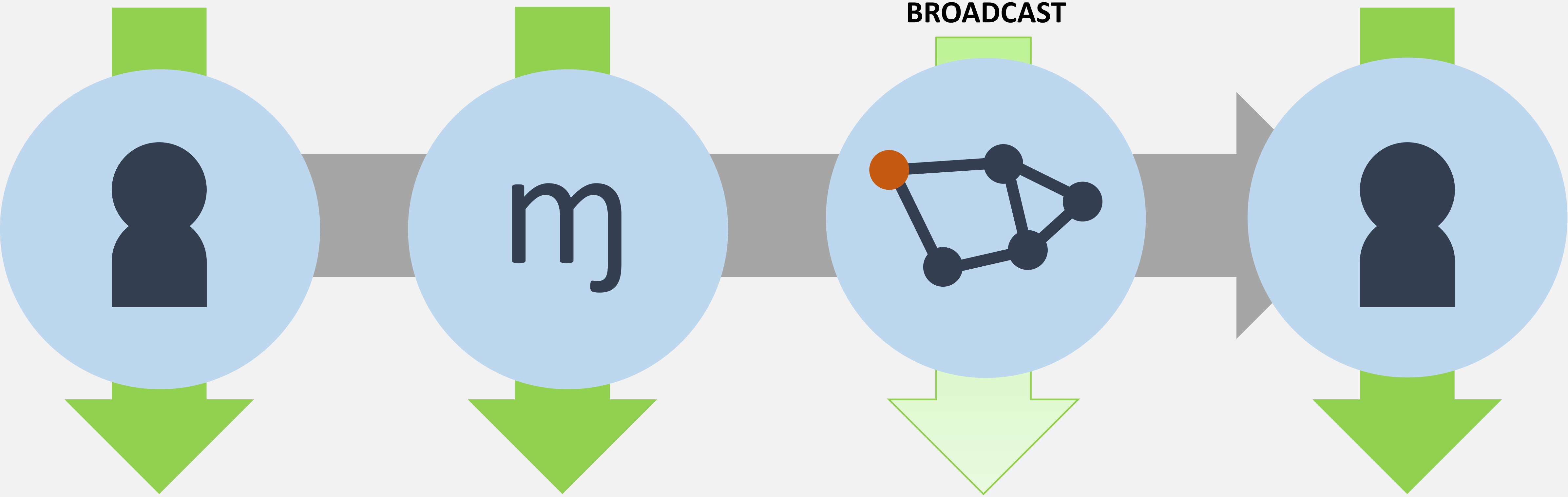
RING SIGNATURES

MONERO

Monero Privacy Components



SENDER

RING SIGNATURES

AMOUNT

RING CONFIDENTIAL TRANSACTIONS (RINGCT)

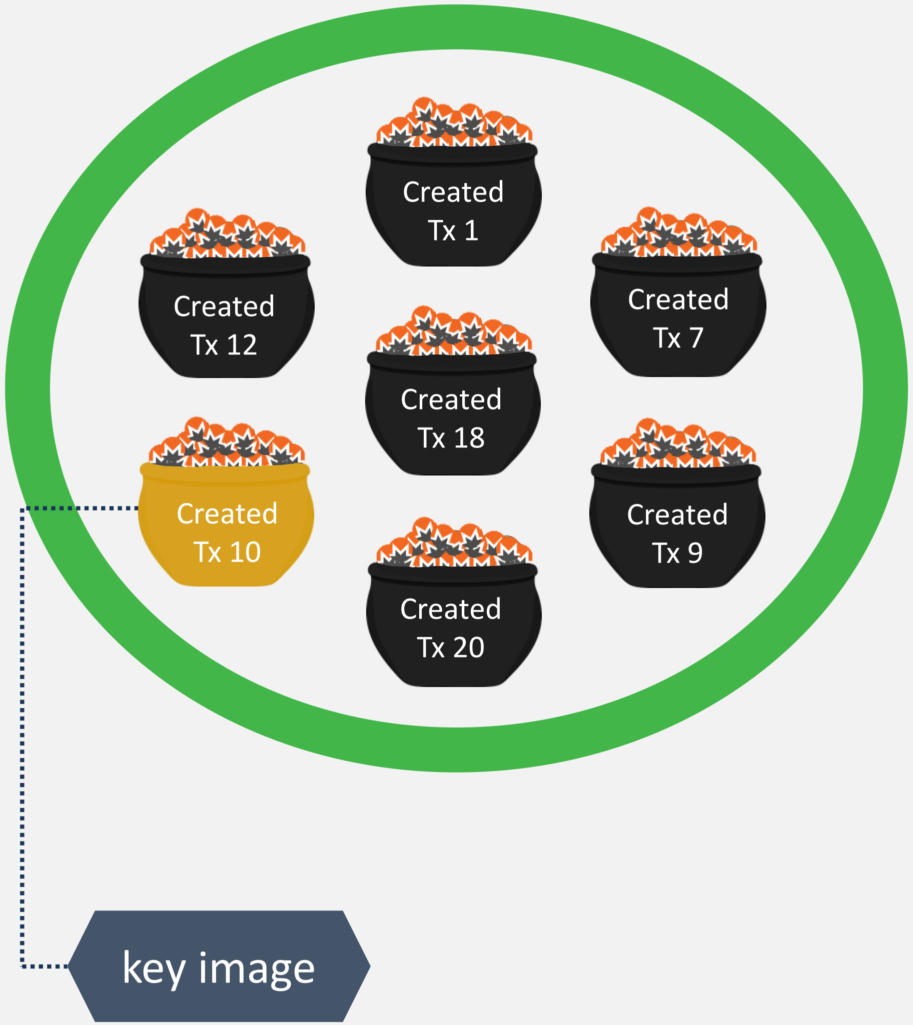
TRANSACTION BROADCAST

KOVRI (I2P ROUTER)

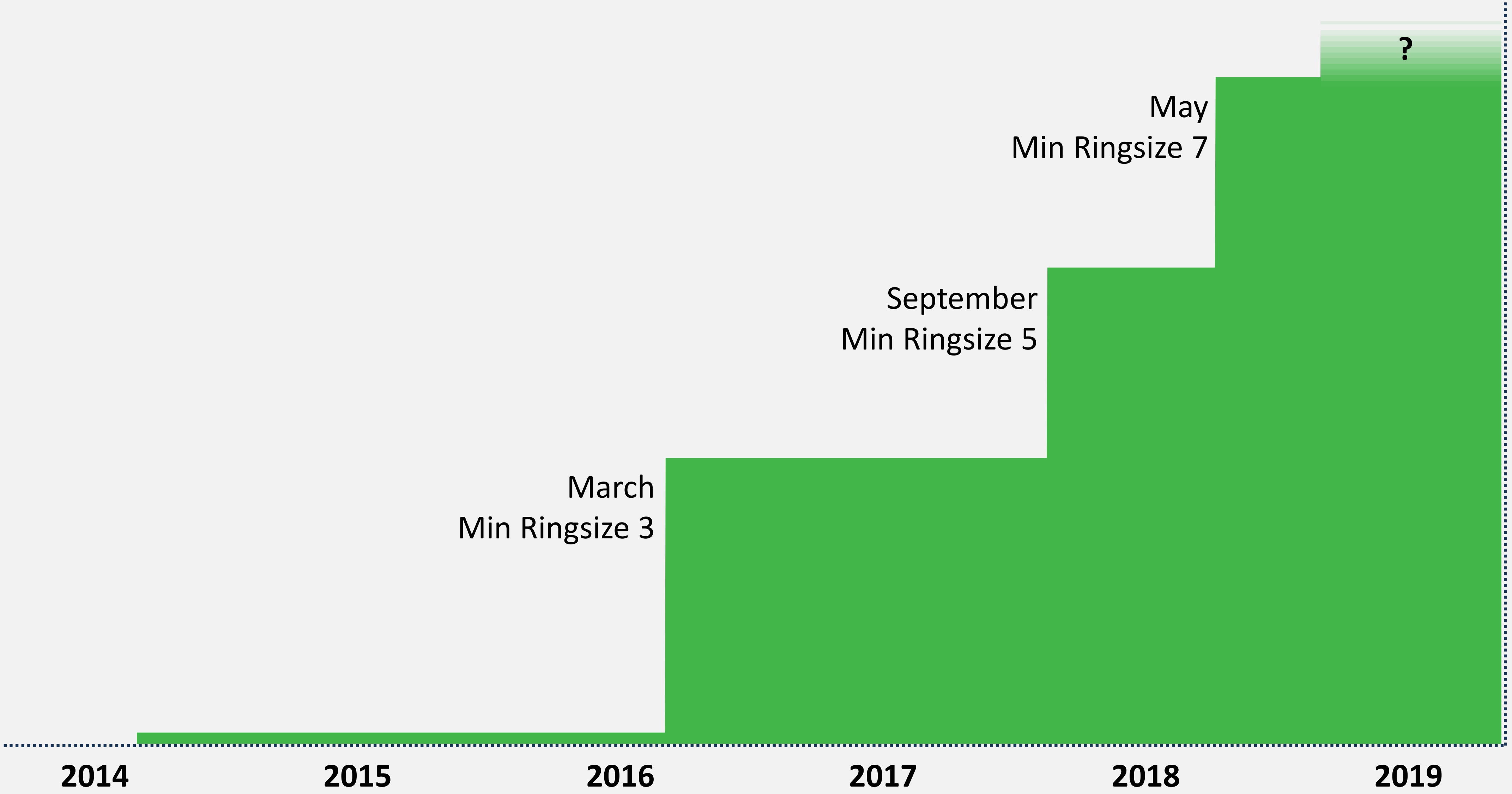
RECEIVER

STEALTH ADDRESSES

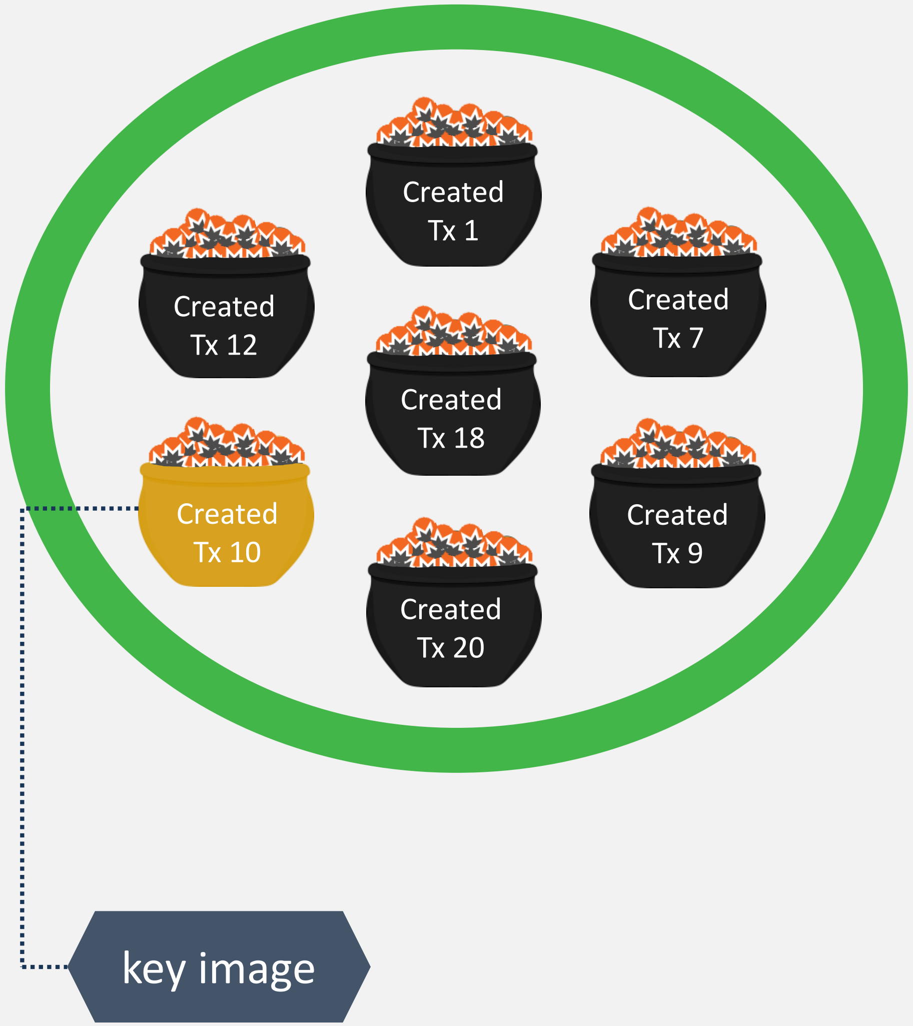
Ring Signatures and Plausible Deniability



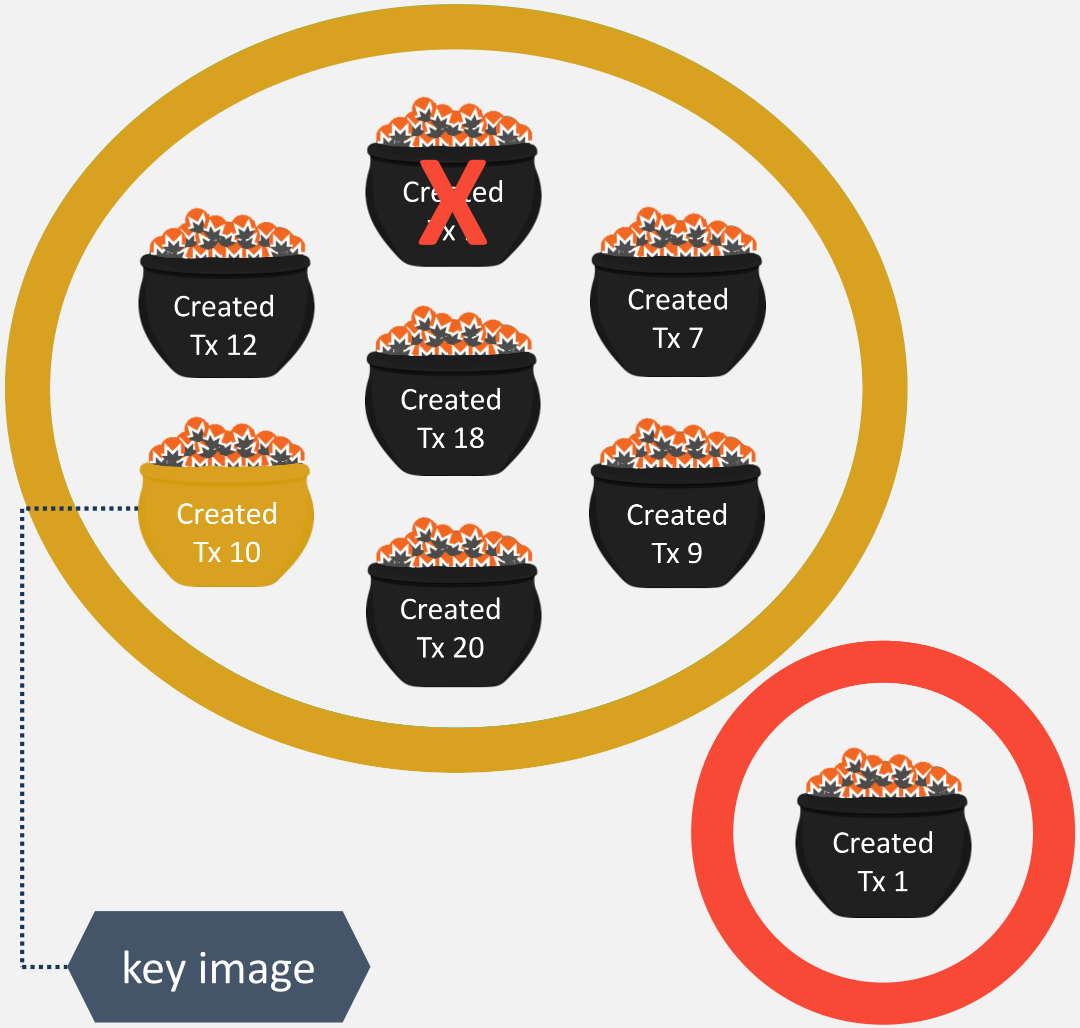
History of Ringsizes in Monero



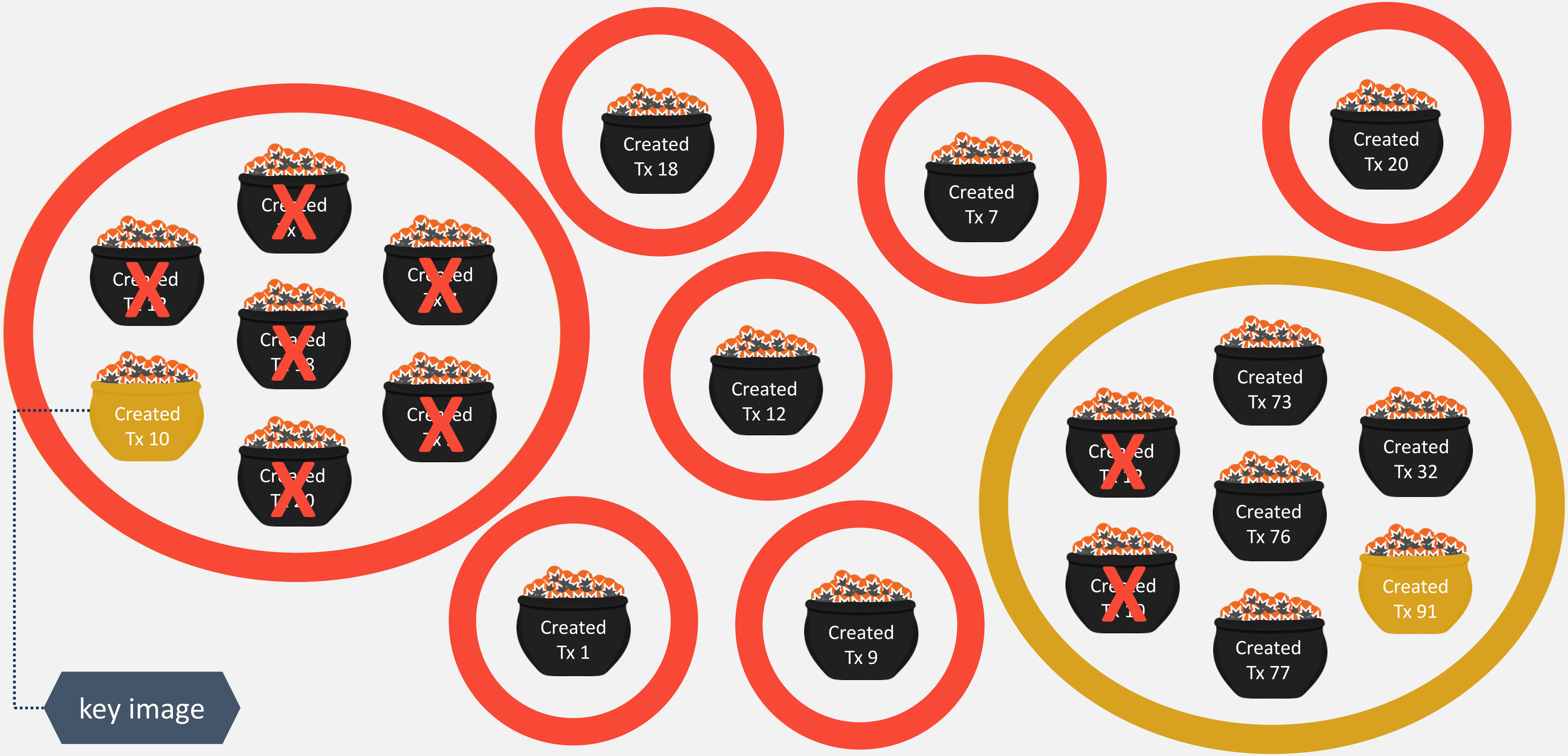
0-Decoy Attack and Chain Reaction



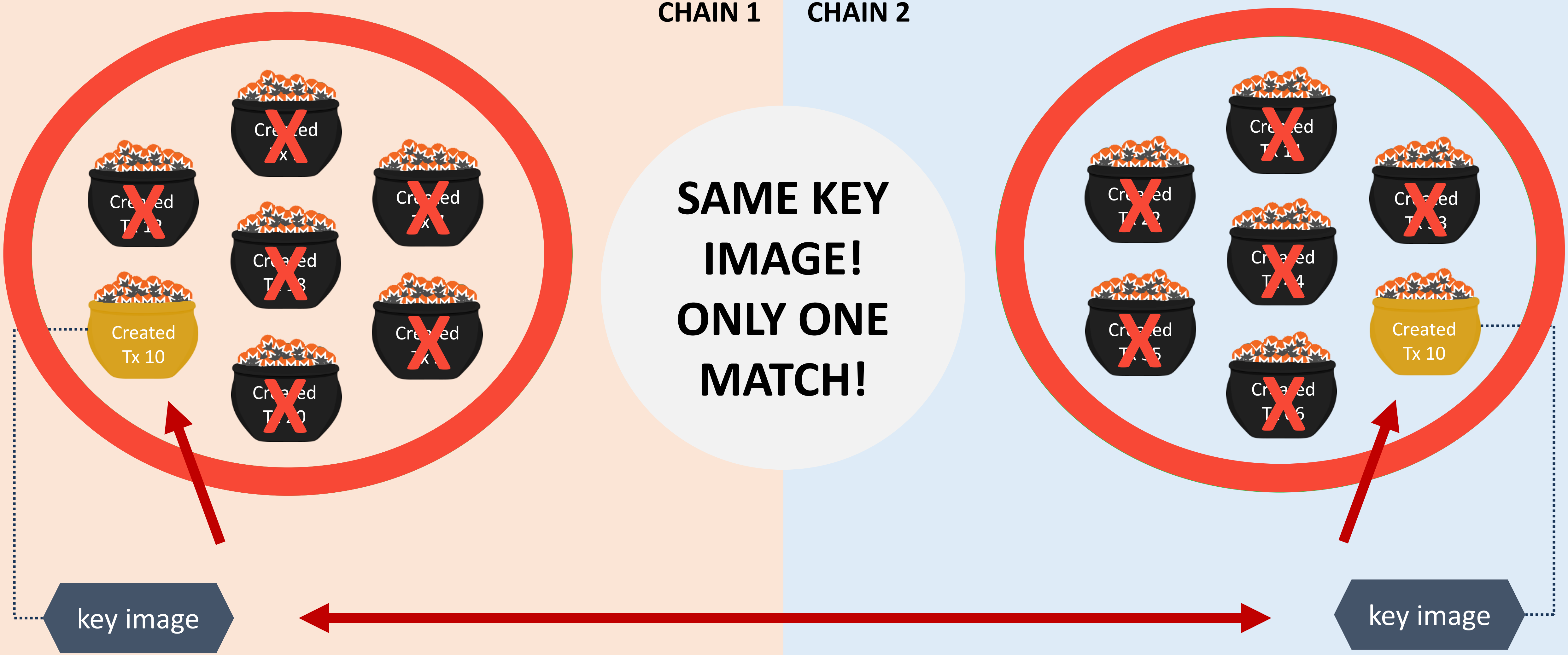
0-Decoy Attack and Chain Reaction



0-Decoy Attack and Chain Reaction



Chain Split and Key Image Reuse

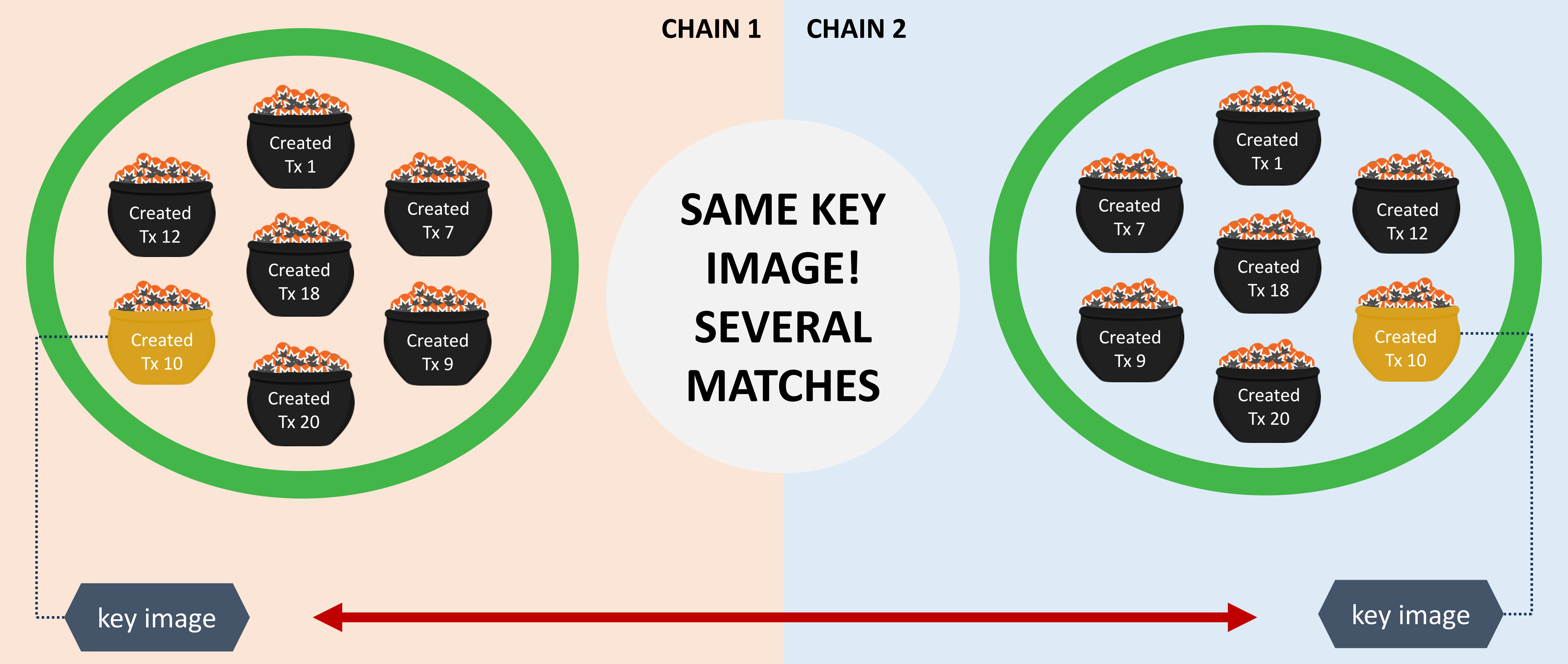


CHAIN 1

CHAIN 2

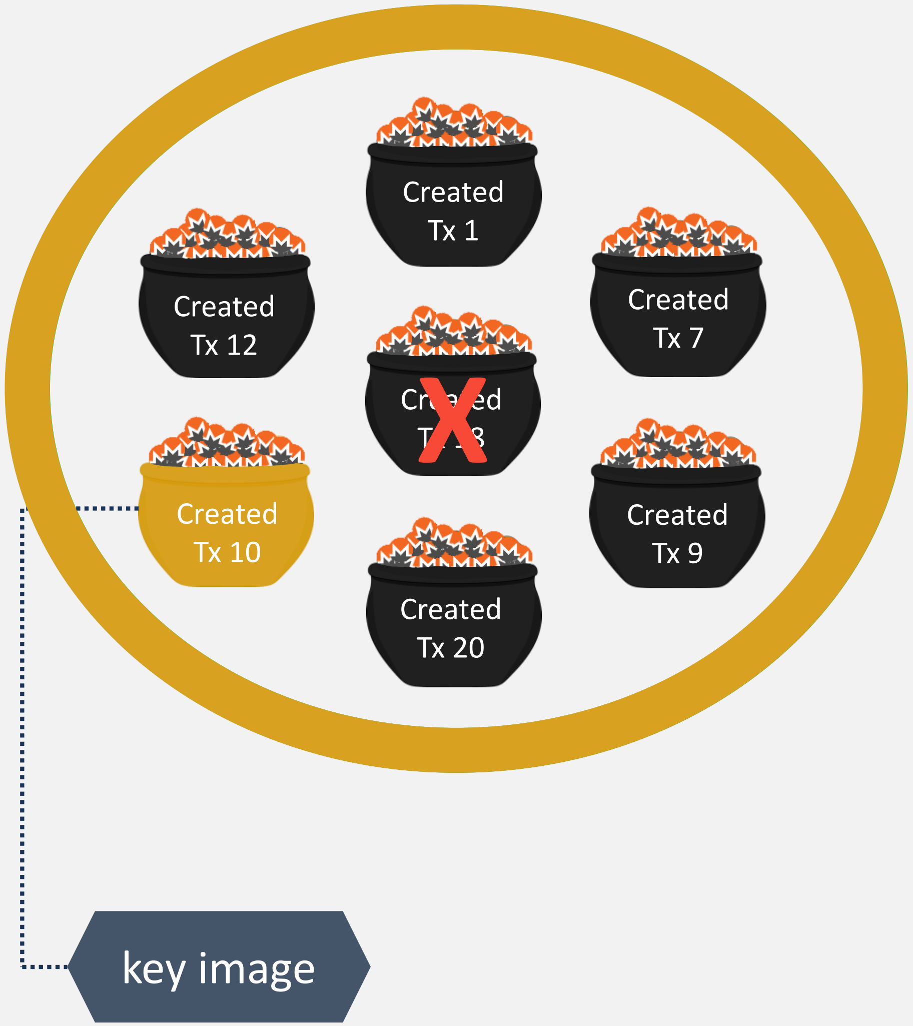
SAME KEY IMAGE! ONLY ONE MATCH!

Chain Split and Key Image Reuse

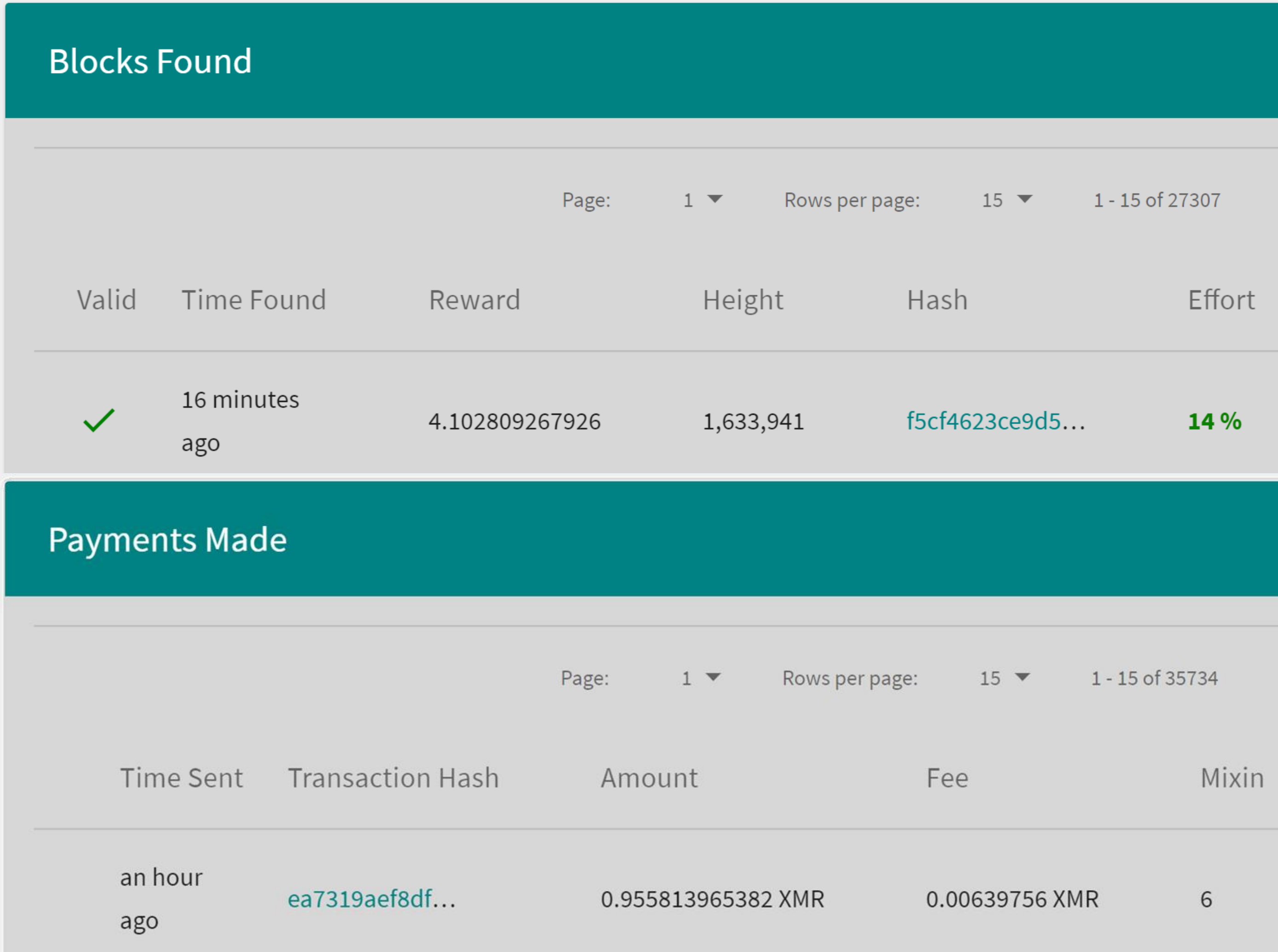


SAME KEY IMAGE! SEVERAL MATCHES

Mining Pool Public Data



Data: supportxmr.com



Blocks Found

Page: 1 ▾ Rows per page: 15 ▾ 1 - 15 of 27307

Valid	Time Found	Reward	Height	Hash	Effort
✓	16 minutes ago	4.102809267926	1,633,941	f5cf4623ce9d5…	14 %

Payments Made

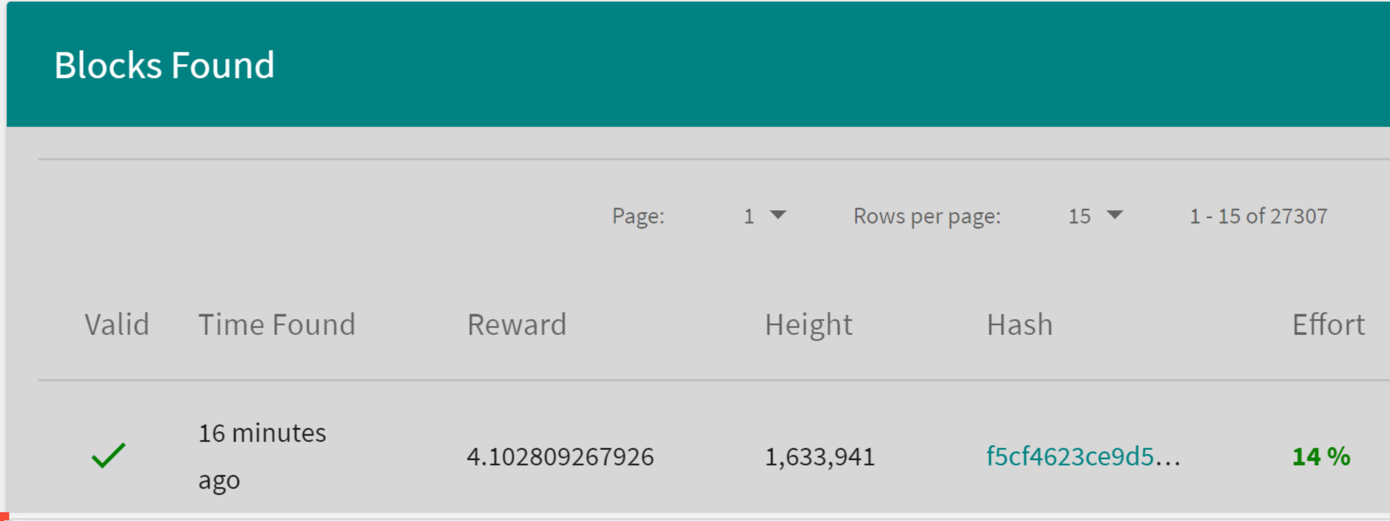
Page: 1 ▾ Rows per page: 15 ▾ 1 - 15 of 35734

Time Sent	Transaction Hash	Amount	Fee	Mixin
an hour ago	ea7319aef8df…	0.955813965382 XMR	0.00639756 XMR	6

Mining Pool Public Data

Data: supportxmr.com

Secret churning
Blackball coinbase outputs

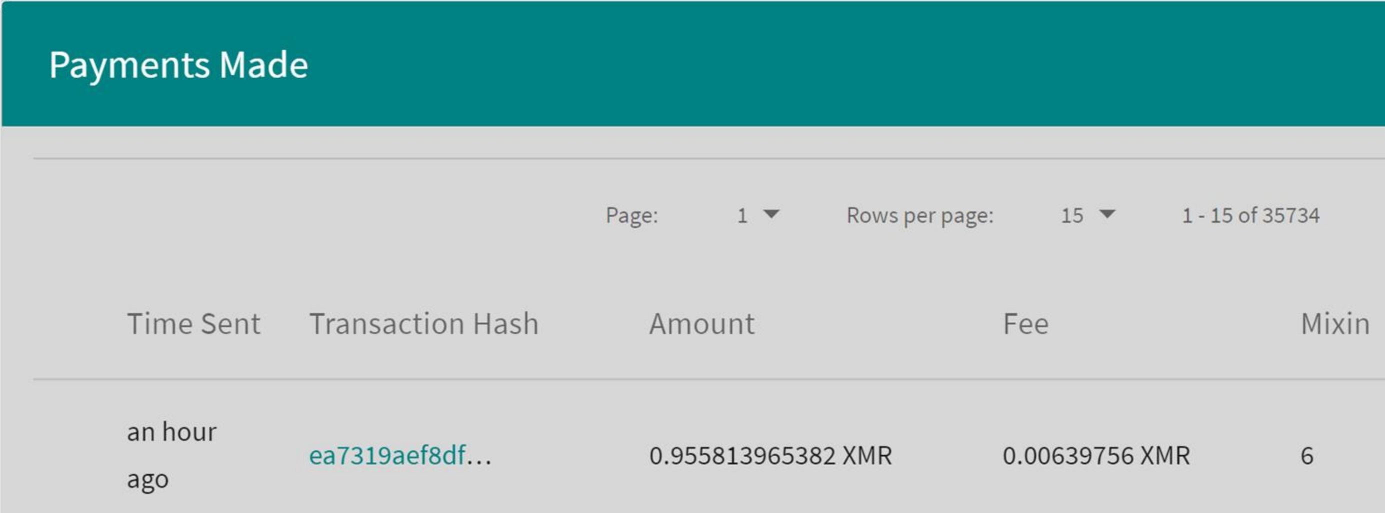


Blocks Found

Page: 1 ▾ Rows per page: 15 ▾ 1 - 15 of 27307

Valid	Time Found	Reward	Height	Hash	Effort
✓	16 minutes ago	4.102809267926	1,633,941	f5cf4623ce9d5...	14 %

Modified input selection algorithm

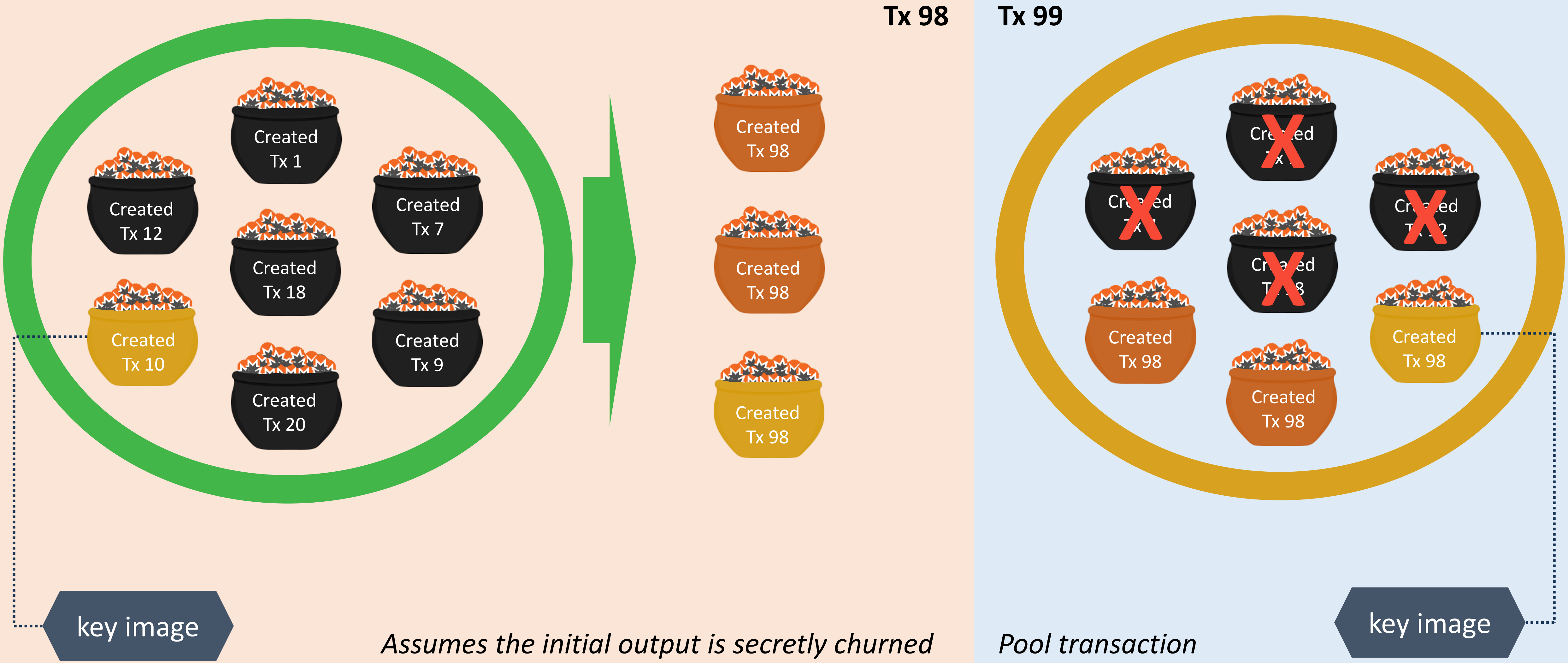


Payments Made

Page: 1 ▾ Rows per page: 15 ▾ 1 - 15 of 35734

Time Sent	Transaction Hash	Amount	Fee	Mixin
an hour ago	ea7319aef8df...	0.955813965382 XMR	0.00639756 XMR	6

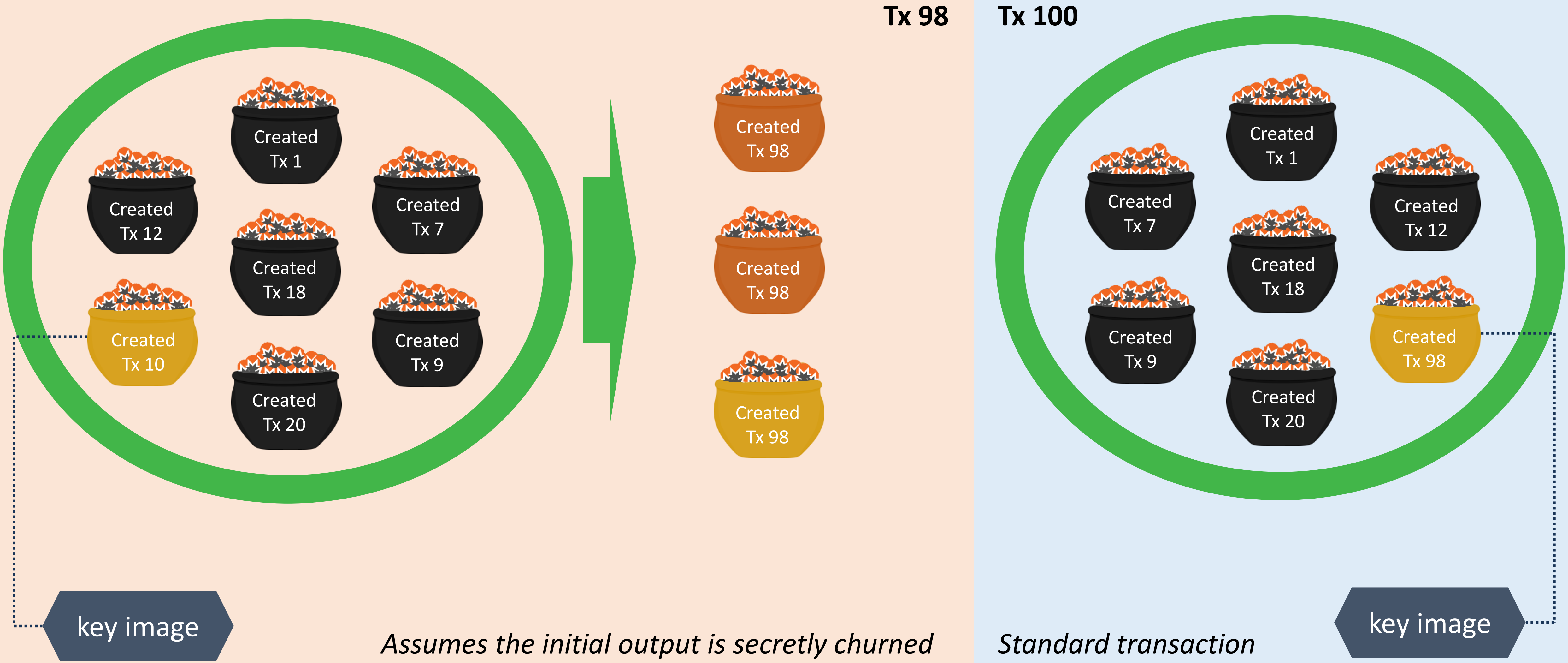
Mining Pool Public Data



Assumes the initial output is secretly churned

Pool transaction

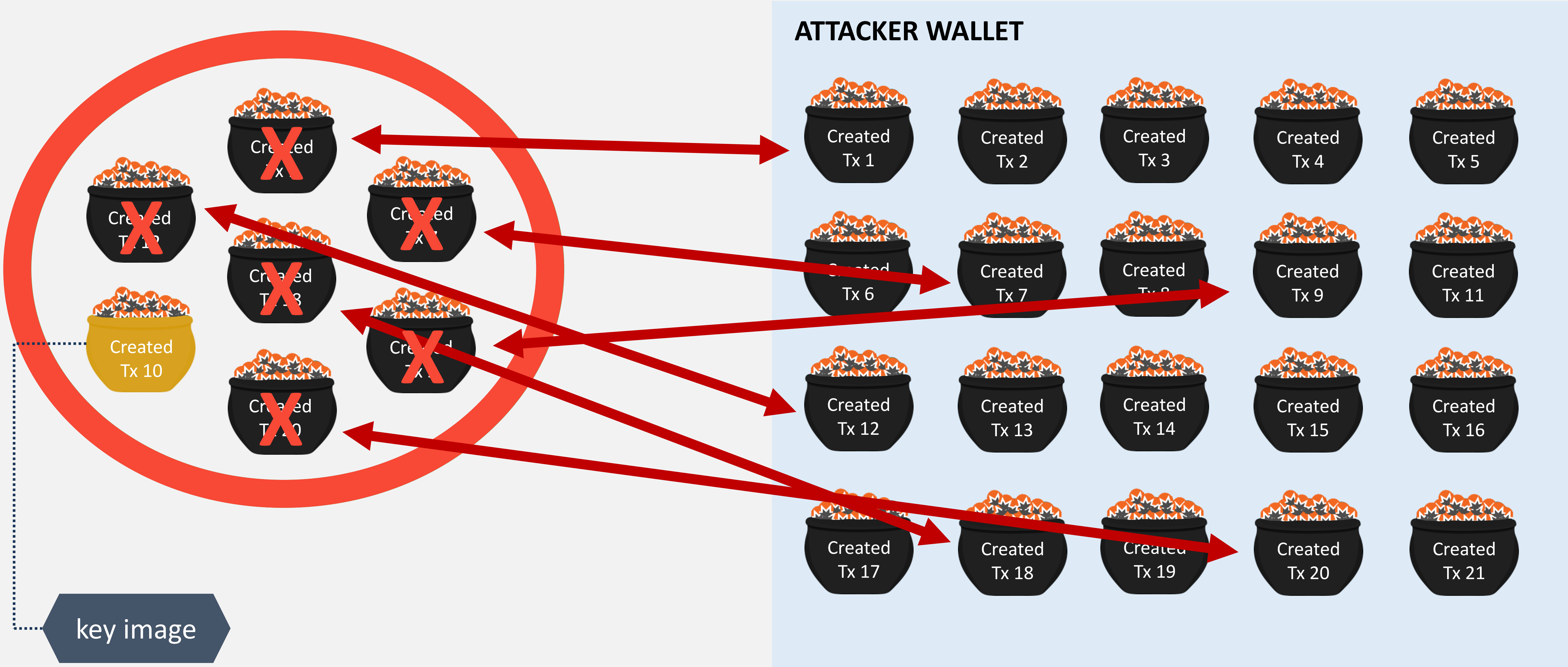
Mining Pool Public Data



Assumes the initial output is secretly churned

Standard transaction

High Output Control (Exchanges & Wallets)

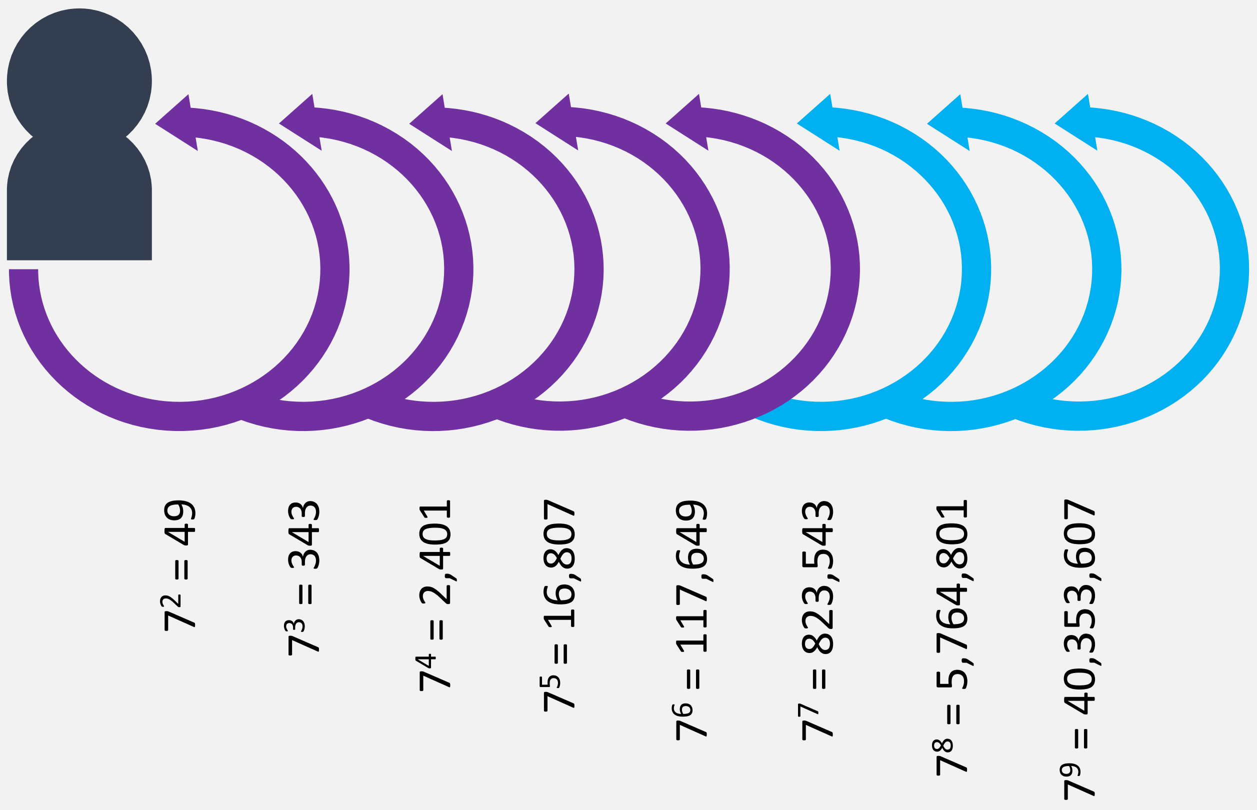


What Can You Do?

Blackball Known Compromised Outputs

- Exclude them from your ring signature
- Items to exclude:
  - 0-decoy transaction inputs (low priority)
  - Unique inputs used on several chains with identical key images
  - Public pool data
  - Outputs known to be controlled by large wallets and exchange (difficult to obtain)

Churn



$7^2 = 49$

$7^3 = 343$

$7^4 = 2,401$

$7^5 = 16,807$

$7^6 = 117,649$

$7^7 = 823,543$

$7^8 = 5,764,801$

$7^9 = 40,353,607$

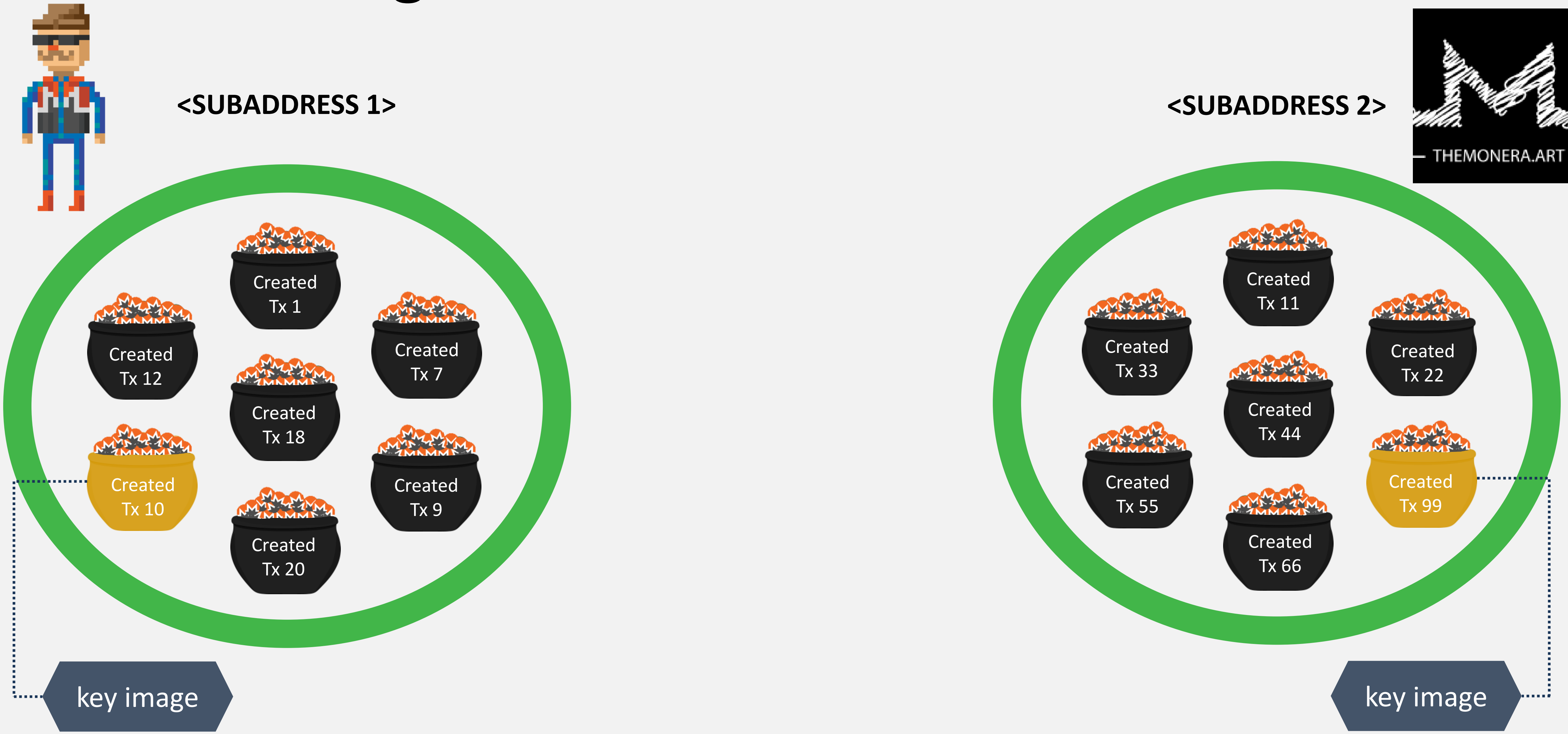
ANONYMITY SET

Spend During Good Times

- Avoid spending shortly before or after times when the network has a high proportion of poisoned outputs
- Impossible to avoid all of these since not all information is public, but can work around announced chain splits, etc. if possible
- Avoid spending if the Monero network is being spammed with transactions

Different Types of Linkability

Linking Subaddresses and Transactions



<SUBADDRESS 1>

Created Tx 1

Created Tx 12

Created Tx 7

Created Tx 18

Created Tx 10

Created Tx 9

Created Tx 20

key image

<SUBADDRESS 2>

Created Tx 11

Created Tx 33

Created Tx 22

Created Tx 44

Created Tx 55

Created Tx 99

Created Tx 66

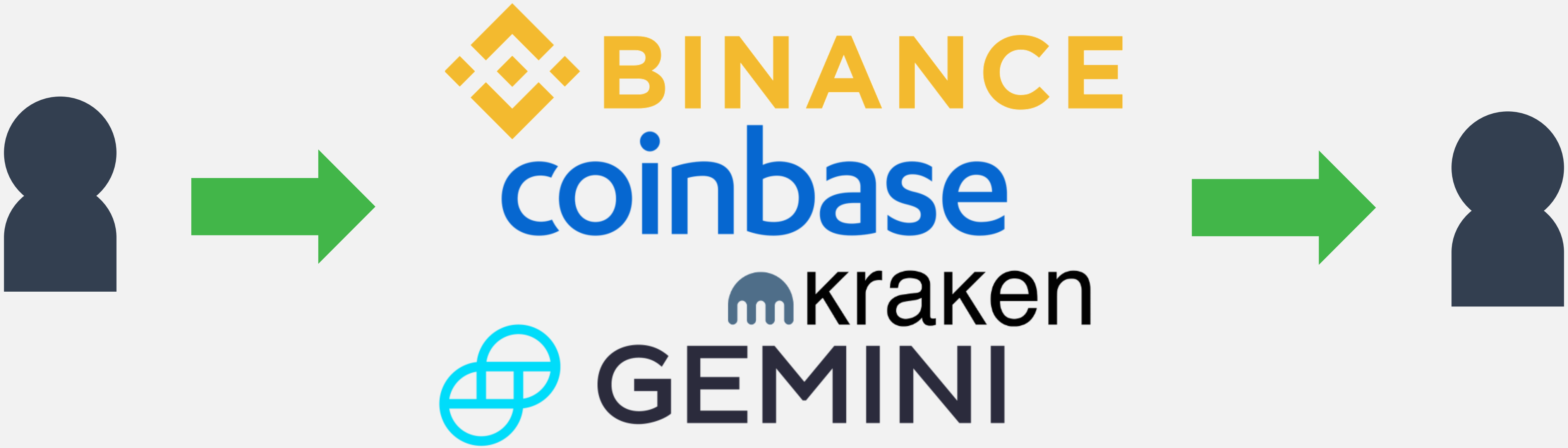
key image

THEMONERA.ART

Linking (Sub)Addresses to Real-World Identity

Adding additional entropy before and after sending funds to someone who knows your identity, including friends, family, merchants, and KYC/AML exchanges

Churn before making these transactions



Linking Outputs

You want every output you touch to have no association with any other outputs you have

Ideally a trait in a completely fungible system, but Monero is not completely fungible against all heuristics, only plausible deniability

Always churn every output separately, and churn every time you receive funds, including non-churn change from your transactions

Challenges for Increasing the Ringsize

Ringsize Challenges

Summary

- Covered 4 different ways for ring signatures to lose plausible deniability
- Covered several considerations for heuristic tests
- Covered best-practices for using Monero’s ring signatures correctly in a variety of use-cases
- Covered the challenges of increasing Monero’s ringsize

Thank You!

getmonero.org

/r/Monero

monero.stackexchange.com

justin@ehrenhofer.org