An Empirical Analysis of Monero Cross-Chain Traceability

Abraham Hinteregger[1,2] Bernhard Haslhofer[1]

[1]Austrian Institute of Technology

[2]Vienna University of Technology

February 18, 2019

Monero

- Public nature of Bitcoin TX history prevents meaningful level of anonymity
- Monero (based on CryptoNote, [Van Saberhagen, 2013]) addresses this with the following methods:
    - Stealth Addresses (hide recipient addr.) → unlinkability

Monero

- Public nature of Bitcoin TX history prevents meaningful level of anonymity
- Monero (based on CryptoNote, [Van Saberhagen, 2013]) addresses this with the following methods:
  - Stealth Addresses (hide recipient addr.) → unlinkability
  - Ring Signatures (obfuscate spent TXO) → untraceability

Monero

- Public nature of Bitcoin TX history prevents meaningful level of anonymity
- Monero (based on CryptoNote, [Van Saberhagen, 2013]) addresses this with the following methods:
  - Stealth Addresses (hide recipient addr.) → unlinkability
  - Ring Signatures (obfuscate spent TXO) → untraceability
  - Confidential Transactions (hide amounts) → fungibility

Monero

- Public nature of Bitcoin TX history prevents meaningful level of anonymity
- Monero (based on CryptoNote, [Van Saberhagen, 2013]) addresses this with the following methods:
    - Stealth Addresses (hide recipient addr.) → unlinkability
    - Ring Signatures (obfuscate spent TXO) → untraceability
    - Confidential Transactions (hide amounts) → fungibility

Ring Signatures & Traceability

- Each TX input references:

Ring Signatures & Traceability

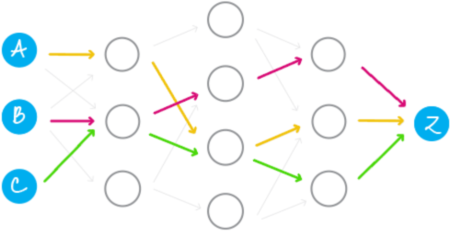
- Each TX input references:
  - Bitcoin: Output from older TX (TXO)

Ring Signatures & Traceability

- Each TX input references:
  - Bitcoin: Output from older TX (TXO)
  - Monero: Non-empty set of TXOs (a ring)

Ring Signatures & Traceability

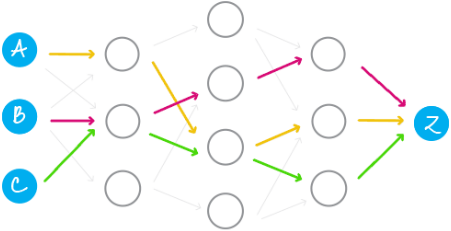
- Each TX input references:
  - Bitcoin: Output from older TX (TXO)
  - Monero: Non-empty set of TXOs (a ring)
- One ringmember is real, the others are decoys (mixins)



Source: `https://cryptonote.org/inside/`

Ring Signatures & Traceability

- Each TX input references:
  - Bitcoin: Output from older TX (TXO)
  - Monero: Non-empty set of TXOs (a ring)
- One ringmember is real, the others are decoys (mixins)



Source: `https://cryptonote.org/inside/`

- Decoys are sampled from set of eligible outputs

Known Traceability Methods

- Zero Mixin Removal (ZMR)

Known Traceability Methods

- Zero Mixin Removal (ZMR)
  - remove known spent outputs from rings

Known Traceability Methods

- Zero Mixin Removal (ZMR)
  - remove known spent outputs from rings
- Intersection removal (IR)

Known Traceability Methods

- Zero Mixin Removal (ZMR)
  - remove known spent outputs from rings
- Intersection removal (IR)
  - generalized ZMR; “closed set attack”

Known Traceability Methods

- Zero Mixin Removal (ZMR)
  - remove known spent outputs from rings
- Intersection removal (IR)
  - generalized ZMR; “closed set attack”
- Output Merging Heuristic (OMH)

Known Traceability Methods

- Zero Mixin Removal (ZMR)
    - remove known spent outputs from rings
- Intersection removal (IR)
    - generalized ZMR; “closed set attack”
- Output Merging Heuristic (OMH)
    - outputs were split up into denominations; if two outputs from a single TX are redeemed in another TX, assume that those inputs are real

Known Traceability Methods

- Zero Mixin Removal (ZMR)
  - remove known spent outputs from rings
- Intersection removal (IR)
  - generalized ZMR; “closed set attack”
- Output Merging Heuristic (OMH)
  - outputs were split up into denominations; if two outputs from a single TX are redeemed in another TX, assume that those inputs are real
- Guess Newest Heuristic (GNH)

Known Traceability Methods

- Zero Mixin Removal (ZMR)
    - remove known spent outputs from rings
- Intersection removal (IR)
    - generalized ZMR; “closed set attack”
- Output Merging Heuristic (OMH)
    - outputs were split up into denominations; if two outputs from a single TX are redeemed in another TX, assume that those inputs are real
- Guess Newest Heuristic (GNH)
    - temporal distribution of mixins and real spending behavior didn’t match - most recent input often the real one

Improvements to the protocol

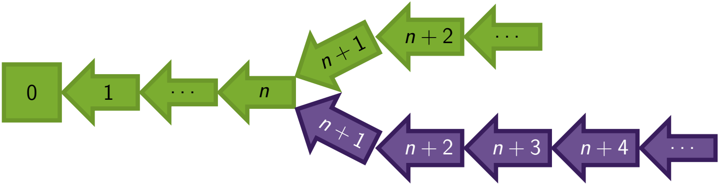
- ZMR works like a chain reaction from an initial set of inputs without decoys.
  - Since 2016, the mandatory minimum ringsize has been increased
  - Minimum ringsizes + RingCT TX were effective
  - Ringsize $\equiv 11$ since last update
- Mixin sampling has been improved with different approaches
  - Triangular distribution
  - Recent zone: Force 25-50% recent outputs
  - Gamma distribution: Distribution based on empirical analysis

Contribution of this work

- Reevaluation of existing methods
  - Previous studies published shortly after introduction of RingCT
  - Changes to mixin sampling and ringsize in 09/2017 and 04/2018.
- Quantification of impact due to recent (Spring 2018) Monero hardforks
  - Monero Original: Continuation of Monero v6 (ASIC compatible)
  - MoneroV: Fork with some changes to emission curve

Currency hardforks

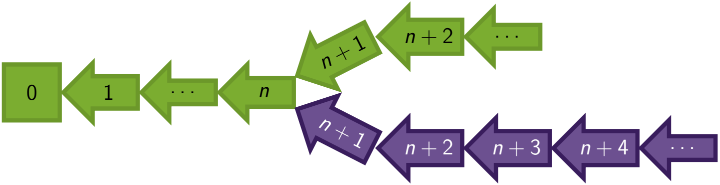
- A cryptocurrency can be forked, resulting in two currencies with a shared TX history



- Pre-fork funds can be spent on both chains
- Monero prevents double spends with *key images* (unique identifier derived from spent output)

Currency hardforks

- A cryptocurrency can be forked, resulting in two currencies with a shared TX history

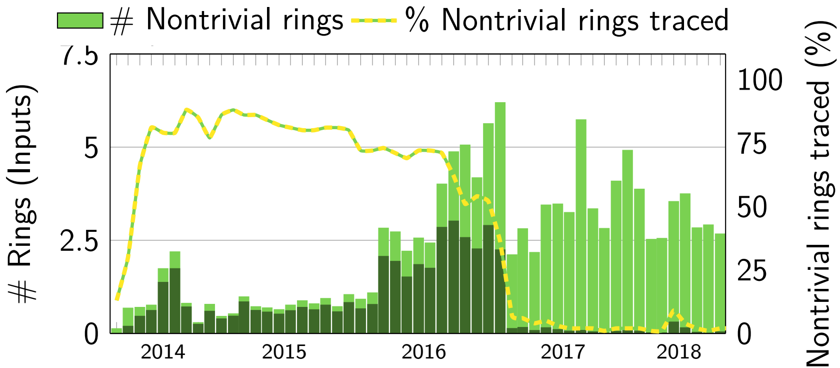


- Pre-fork funds can be spent on both chains
- Monero prevents double spends with *key images* (unique identifier derived from spent output)
- If two rings on separate branches share a key image, they spend the same output.

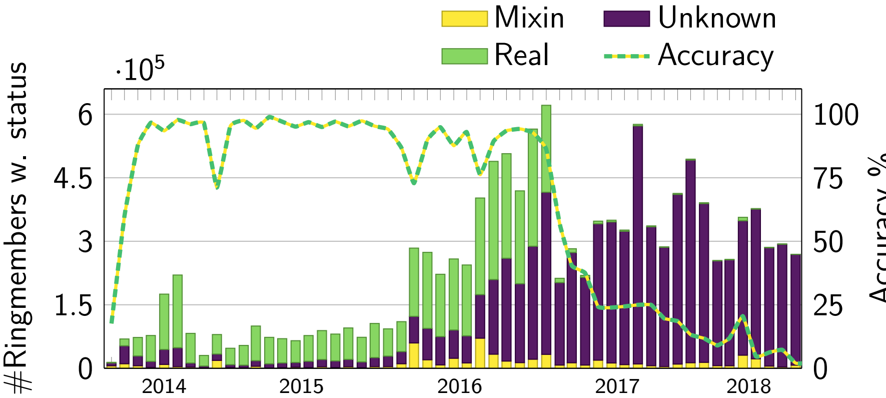
Dataset & Method

1. Exported Monero (XMR), MoneroV (XMV) and Monero Original (XMO) blockchain up to Aug. 31$^{\text{th}}$, 2018.
2. Employed Zero Mixin Removal & Intersection Removal
3. Added fork data and applied cross chain analysis (+ZMR/IR)
4. Applied heuristics from [Kumar et al., 2017] and [Möser et al., 2018]:
   - Guess Newest Heuristic
   - Output Merging Heuristic
5. Evaluated accuracy with ground truth (where possible) with results from steps 3 (OMH see paper).

Traced Inputs



Guess Newest Heuristic



Summary

- Nowadays, most Monero TXs are untraceable with known passive attack vectors

Summary

- Nowadays, most Monero TXs are untraceable with known passive attack vectors
- Guess Newest Heuristic does not work with current mixin sampling technique

Summary

- Nowadays, most Monero TXs are untraceable with known passive attack vectors
- Guess Newest Heuristic does not work with current mixin sampling technique
- Impact from Cross Chain Analysis not very large

Summary

- Nowadays, most Monero TXs are untraceable with known passive attack vectors
- Guess Newest Heuristic does not work with current mixin sampling technique
- Impact from Cross Chain Analysis not very large
    1. Forks so far didn't have a lot of traction (maybe disputes over ASICs change that)

Summary

- Nowadays, most Monero TXs are untraceable with known passive attack vectors
- Guess Newest Heuristic does not work with current mixin sampling technique
- Impact from Cross Chain Analysis not very large
  1. Forks so far didn't have a lot of traction (maybe disputes over ASICs change that)
  2. Mandatory ringsize of 7 enough to prevent chain reactions (11 is even better)

Data & source available:

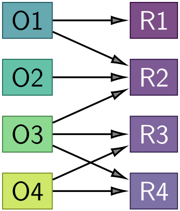
References

- Kumar, A. et al. (2017).
  A traceability analysis of Monero's blockchain.
  In *European Symposium on Research in Comp. Sec.*

- Möser, M. et al. (2018).
  An Empirical Analysis of Traceability in the Monero Blockchain.
  PoPET, 2018(3):143–163, DOI: 10.1515/popets-2018-0025.

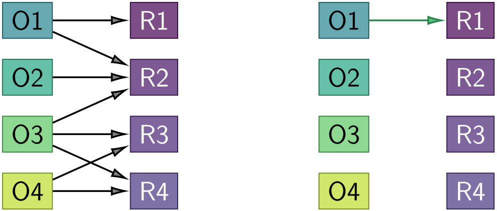
- Van Saberhagen, N. (2013).
  Cryptonote v 2. 0.
  https://cryptonote.org/whitepaper.pdf.

Zero Mixin Removal & Intersection Removal



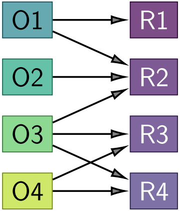
- Outputs O1-O4 are referenced in rings R1-R4

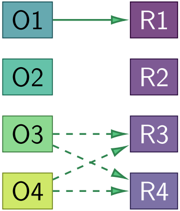
Zero Mixin Removal & Intersection Removal



- Outputs O1-O4 are referenced in rings R1-R4
- R1 only references O1 $\implies$ must be the real input

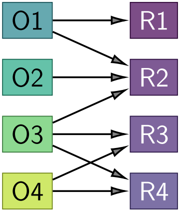
Zero Mixin Removal & Intersection Removal

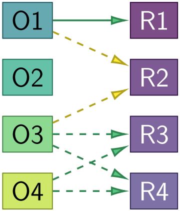




- Outputs O1-O4 are referenced in rings R1-R4
- R1 only references O1 $\implies$ must be the real input
- $I = \{R3, R4\}$ reference $O = \{O3, O4\}$
  $|I| = |O| \implies$ O3 & O4 spent in R3 & R4

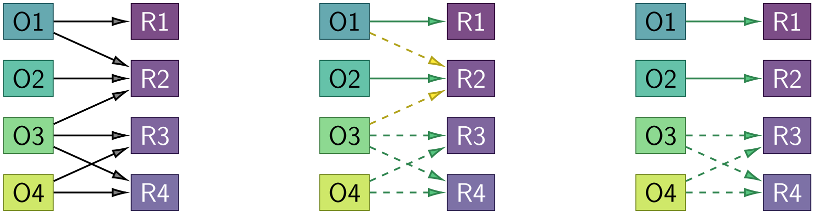
Zero Mixin Removal & Intersection Removal





- Outputs O1-O4 are referenced in rings R1-R4
- R1 only references O1 $\implies$ must be the real input
- $I = \{R3, R4\}$ reference $O = \{O3, O4\}$
  $|I| = |O| \implies$ O3 & O4 spent in R3 & R4
- $R2$ only has one non-mixin reference remaining.

Zero Mixin Removal & Intersection Removal



- Outputs O1-O4 are referenced in rings R1-R4
- R1 only references O1 $\implies$ must be the real input
- $I = \{R3, R4\}$ reference $O = \{O3, O4\}$

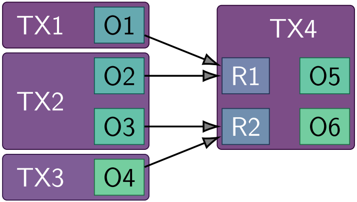
  $|I| = |O| \implies$ O3 & O4 spent in R3 & R4
- $R2$ only has one non-mixin reference remaining.

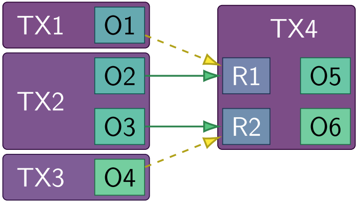
Output Merging Heuristic (OMH)

- Output merging mostly due to denomination splitting:
  - Initially, amounts were disclosed on blockchain
  - Ring signatures required multiple outputs with identical amounts
  - Outputs were partitioned to facilitate this ($7 \rightarrow 5 + 2$)

Output Merging Heuristic (OMH)

- Output merging mostly due to denomination splitting:
  - Initially, amounts were disclosed on blockchain
  - Ring signatures required multiple outputs with identical amounts
  - Outputs were partitioned to facilitate this (7 → 5 + 2)

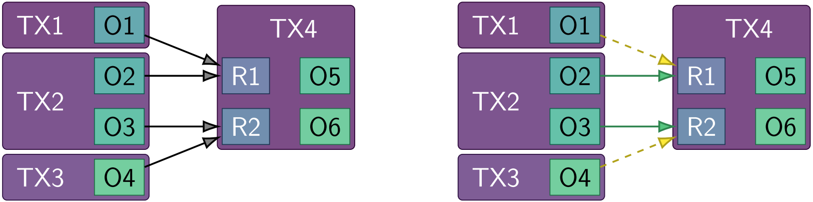




- TX4 has two inputs which reference a TXO from TX2

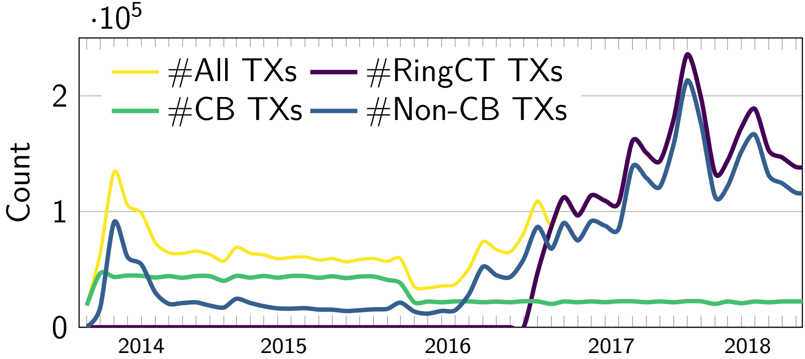
Output Merging Heuristic (OMH)

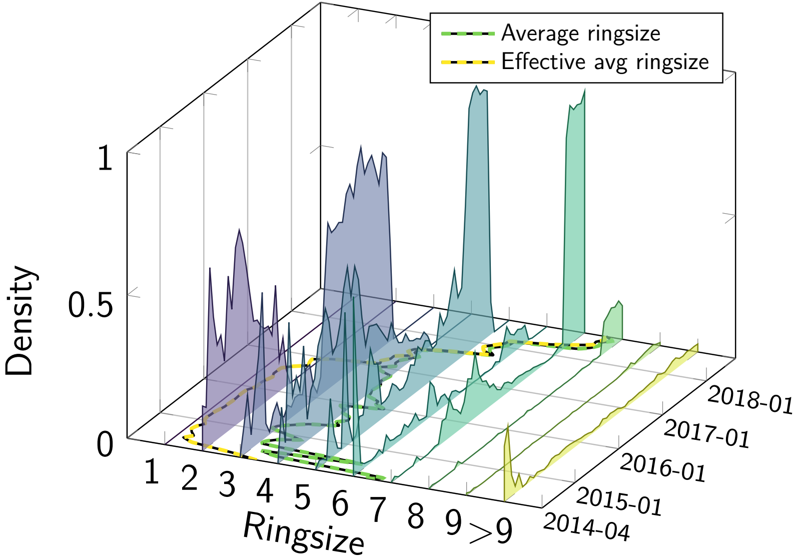
- Output merging mostly due to denomination splitting:
  - Initially, amounts were disclosed on blockchain
  - Ring signatures required multiple outputs with identical amounts
  - Outputs were partitioned to facilitate this (7 → 5 + 2)

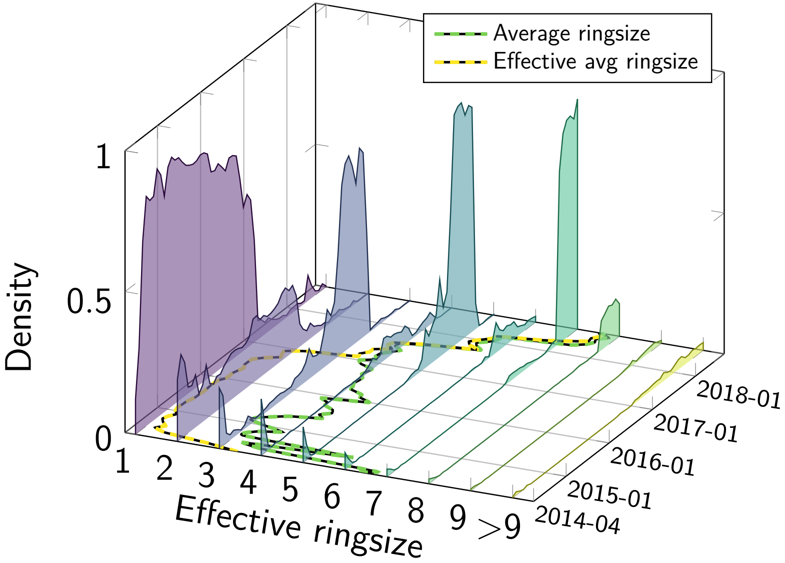


- TX4 has two inputs which reference a TXO from TX2
- OMH assumes that these outputs are real

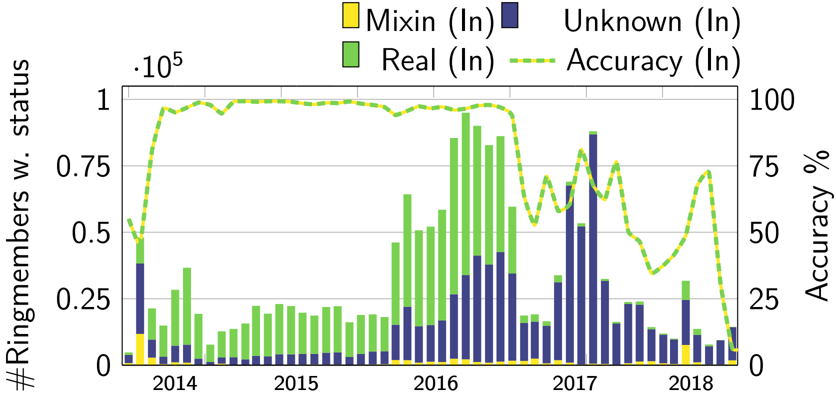
Monero Activity



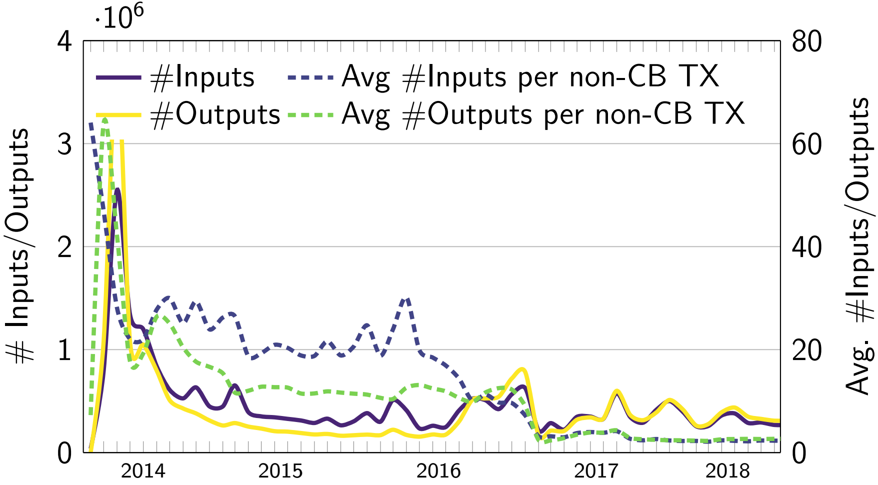

Average ringsize
Effective avg ringsize
Density
1
0.5
0
Ringsize
1
2
3
4
5
6
7
8
9
>9
2018-01
2017-01
2016-01
2015-01
2014-04


Average ringsize
Effective avg ringsize
Density
1
0.5
0
1
2
3
4
5
6
7
8
9
>9
Effective ringsize
2014-04
2015-01
2016-01
2017-01
2018-01

Output Merging Heuristic



Inputs/Outputs (per TX)


·10^6
# Inputs/Outputs
Avg. #Inputs/Outputs
#Inputs
#Outputs
Avg #Inputs per non-CB TX
Avg #Outputs per non-CB TX