FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Diplomarbeitspräsentation

ALGORITHMS AND COMPLEXITY GROUP

# Cross-Chain Traceability Analysis

## Analysis of privacy implications from currency hard-forks

Masterstudium:

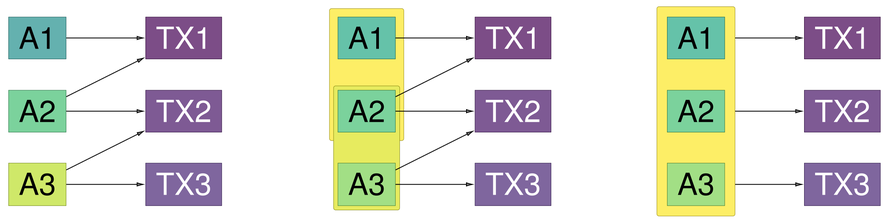
Computational Intelligence

Abraham Hinteregger

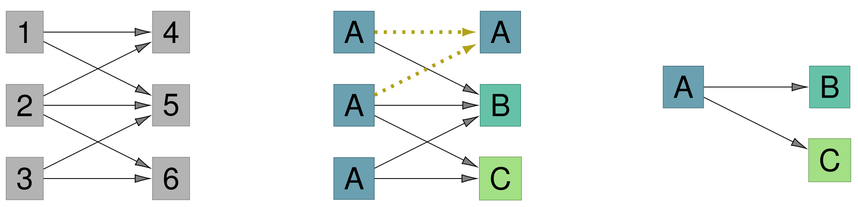
Technische Universität Wien
Institut für Informationssysteme
Arbeitsbereich: Algorithms and Complexity Group
Betreuer: Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Günther Raidl

## Motivation

- Several methods to analyze Bitcoin transactions history
- Multi-Input heuristic clusters addresses (A1-A3) of inputs occuring in single transaction (TX) as they likely belong to the same user



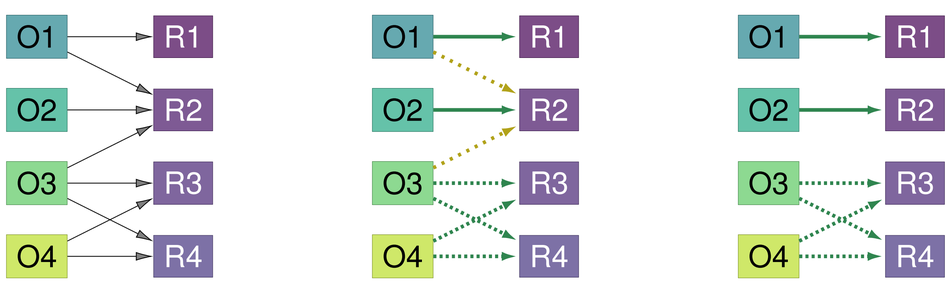

- Address-graph (left) labelled with address-clusters from multi-input heuristic (center) can be simplified to entity-graph (right)



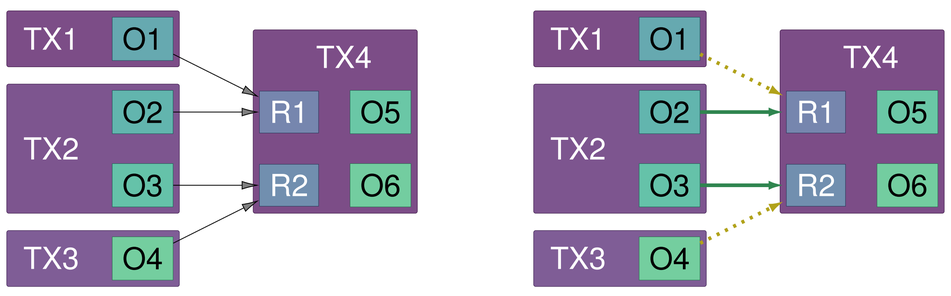

- Increased chance of users being identified via TX-history
- $\Rightarrow$ privacy-centric coins, e.g. Monero, based on CryptoNote [3]
- Features of Monero, privacy-coin with highest market-cap:
  - **Unlinkability:** *Stealth addresses* hide recipients of transactions
  - **Untraceability:** Each TX input is a ring instead of a TXO (TX output). A ring is a set of TXOs (with the same denomination), one of which is the real input and the others are decoys (*mixins*). These *ring signatures* obfuscates the path of a given coin.
  - **Fungibility:** Values of TXOs are hidden with RingCT (confidential TXs) since 2017, making denomination constraint of rings unnecessary.
- Analysis methods from other currencies do not work for Monero

## Traceability Analysis

- Two independent 2017 publications [1, 2] demonstrated that a majority of transactions are traceable. They used the following deductions techniques and heuristics:
  - Zero Mixin & Intersection Removal (ZMR & IR): Ring R1 has only one referenced TXO (O1), which is therefore the real input ( ) in that ring and all occurrences in other rings (R2) have to be decoys ( ) and can thus be removed. Intersection removal is a generalization of this technique that marks TXOs occoring in $n$ rings (R3,R4) with $n$ identical members (O3,O4) as spent ( ).



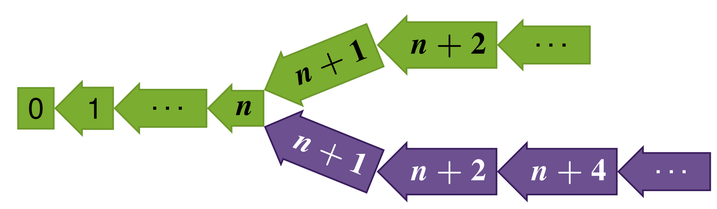

  - Guess Newest Heuristic (GNH): Exploits naive decoy sampling. As time distribution of decoys and real outputs differed, most recent TXO was real input in most cases.
  - Output Merging Heuristic (OMH): TX4 merges multiple TXOs (O2,O3) from TX2 in distinct rings (R1,R2). OMH assumes that those are the real inputs.



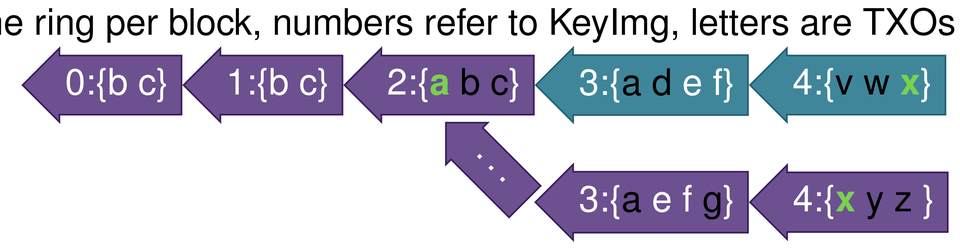

- Monero developers reacted by implementing countermeasures:
  - Higher mandatory minimum ringsize against ZMR (from 3 to 7)
  - Improved decoy sampling against GNH (sampling multiple $\leq$3 day old inputs and soon from a $\gamma$-distribution)
- This work contributes to the state of the art in two ways:
  - We propose a new tracing method, which exploits information leaked on currency-forks. We measure the privacy-impact from two recent forks (Monero Original & MoneroV)
  - We evaluate the accuracy of GNH & OMH based on results from our traceability analysis (using ZMR, IR and our new method).

## Forks & Cross Chain Analysis (CCA)

- Cryptocurrencies forks result in two coins with a common history

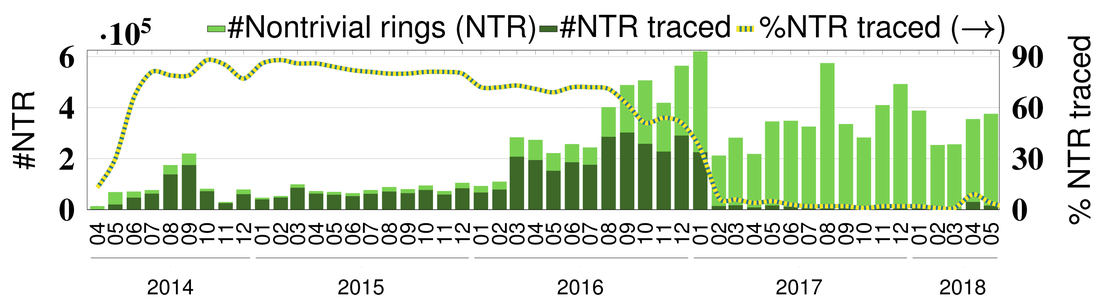



- Unspent pre-fork coins can be spent on both branches
- A *key image* (uniquely determined by real input) used to prevent double spending
- If multiple rings (one per branch) have the same KeyImg, the same pre-fork TXO is spent in them
- Real input is in intersection of the rings
- TXOs in the symmetric difference must be decoys
- Monero blockchain (XMR) two blocks before and after a fork (XMO)
- One ring per block, numbers refer to KeyImg, letters are TXOs




1. IR can be applied to ring 0 and 1, $b, c$ therefore decoys in ring 2.
2. ZMR sets $a$ as **real input** in ring 2 and decoy in both rings 3.
3. CCA sets $d, g$ as decoys because $\notin \{a,d,e,f\} \cap \{a,e,f,g\}$
4. CCA sets $x$ as real input because $|\{v,w,x\} \cap \{x,y,z\}| = 1$

## Results




Bar chart of monthly number of nontrivial rings (NTR, $> 1$ member). Shaded bars represent traced nontrivial rings. Until mandatory minimum ringsizes were introduced, most rings were traceable. With increasing mandatory minimum ringsizes (2016/09) the percentage of traceable NTR dropped continuously and since the introduction of Confidential Transactions (2017), only a tiny amount can be traced. The (small) peak in April and May 2018 is mostly due to our newly proposed method. Using the traced rings we looked at the accuracy of the GNH and found that its performance is no longer better than guessing. We would therefore advise against employing it for recent transactions. All things considered, the amount of traceable rings with the current transaction protocol is low enough to not jeopardize privacy of Monero's users.

## References

[1] Amrit Kumar et al. A Traceability Analysis of Monero's Blockchain. *IACR Cryptology ePrint Archive*, 2017:338, 2017.

[2] Malte Möser et al. An Empirical Analysis of Traceability in the Monero Blockchain. *Proceedings on Privacy Enhancing Technologies*, 2018(3):143–163, June 2018.

[3] Nicolas Van Saberhagen. *Cryptonote v 2. 0*. 2013.

Kontakt: a.hinteregger@outlook.at