A Traffic-Analysis Proof Solution to Allow K-Anonymous Payments in Pseudonymous Blockchains

Francesco Buccafurri, Vincenzo De Angelis, Sara Lazzaro

DIIES Dept, University Mediterranea of Reggio Calabria (Italy)

DLT2023 - 5th Distributed Ledger Technology Workshop

25–26 May 2023
1 Motivations

2 Our proposal

3 Conclusions
Motivations

**Pseudonymous blockchains** -> blockchain addresses make transactions **linkable** among them

**How to reach unlinkability?** -> make users change their blockchain address with every transaction (naive way)

**De-anonymization attacks** against **pseudonymous blockchains** based on:
- Data analysis on the transactions graph
- Network analysis

**Attacks based on network analysis**
- **Goal**: find a correlation between a blockchain nodes and IP addresses
- **Even anonymous blockchains are vulnerable to these attacks!**
Our proposal

Our goal

Allow users to make **anonymous payments** in **pseudonymous blockchains**

Borrowing notions from the Anonymous communication domain

- **Security property:** Sender anonymity (hide who makes a payment)
- **Threat model:** Global passive adversary (able to make traffic analysis attacks)

Key concepts

- organize users in anonymity sets
- information hiding mechanism enabled (cover transactions)
- No requirement for off-chain communication channels
Our Proposal

- **Ring**: anonymity set of \( k \) users.

**Ring Construction**

- Rings are built via a DHT based on blockchain addresses plus a **random salt**
- An attacker cannot precompute the ring in which it will fall

*the hash of a certain block in the blockchain*
Our Proposal

- **Ring**: anonymity set of $k$ users.
- **Cover Transactions**.
Our Proposal

- **Ring**: anonymity set of $k$ users.
- **Cover Transactions**.
- Smart contract as a shared deposit of cryptocurrency.
Our Proposal

- **Ring**: anonymity set of $k$ users.
- **Cover Transactions**.
- Smart contract as a shared deposit of cryptocurrency.
**Our Proposal**

- **Ring**: anonymity set of $k$ users.
- **Cover Transactions**.
- Smart contract as a shared deposit of cryptocurrency.
- $t$ over $k$ authorizations for a payment.
Conclusions

- Our proposal achieves $k$-anonymity guarantees in pseudonymous blockchains against a global passive adversary.
- Our anonymity guarantees resist traffic analysis attacks.
- The idea underlying our solution is to organize users in rings of cover transactions.
- No requirement for off-chain communication channels.
A Traffic-Analysis Proof Solution to Allow K-Anonymous Payments in Pseudonymous Blockchains

Francesco Buccafurri, Vincenzo De Angelis, Sara Lazzaro

DIIES Dept, University Mediterranea of Reggio Calabria (Italy)

DLT2023 - 5th Distributed Ledger Technology Workshop

25–26 May 2023