Deanonymisation in Ethereum Using Existing Methods for Bitcoin

Robin Klusman
Tim Dijkuizen

Supervisor: Arno Bakker
Introduction

- **Blockchain**
  - Decentralised
  - Peer-to-peer
  - Miners
  - Anonymous reputation

- **Forensics**
  - Track malicious actors
Introduction

The integrity of the blockchain

Figure 1: Overview of how blocks in a blockchain are linked to each other
Introduction

Blockchain popularity

- Bitcoin
  - 2009
  - ‘Satoshi Nakamoto’

- Ethereum
  - 2015
  - Vitalik Buterin
"Is deanonymisation of clients feasible for the Ethereum network?"
Related Work

- Survey on Bitcoin security and privacy issues
  - Essential background knowledge
  - Attacks on Bitcoin
    - Bitlodge
- Survey on Ethereum smart contracts
  - Aimed at illegitimately obtaining funds
  - DAO attack
Bitcoin
Discovering clients:
- Hardcoded seed servers
- Clients maintain 8 entry-nodes
- `getaddr` message

Transaction propagation:
- Trickling
  - Queueing `inv` messages
  - 100ms
Bitcoin Blockchain

Transactions

- Based on UTXO
- Use up all inputs
- Change

Blocks:

- Merkle tree
- Header hash
- Forks
Bitcoin (& Ethereum) Consensus Model

PoW (Proof of Work):

- Based on computational power
- Against Sybil attack
Ethereum
Ethereum Smart Contracts

- Code written for EVM
  - Turing complete
  - Solidity
- Immutable once deployed
- Miners paid in gas - prevent DoS
- Crowd funding
Ethereum P2P Network

- Kademlia based
- Bootnodes
- Find nodes
  - nodeID from public key
  - Closeness
  - XOR of SHA-3 hash
Ethereum Blockchain

Transactions:

- No UTXO
- Account balance

Blocks:

- Global state
- Transaction trie
- Ommers
Attacks
Existing Attacks - Finding IP Addresses

- Identifying entry-nodes
  - Monitor ‘server’ nodes
  - Listen for `addr` messages
- Monitor network
- Transaction broadcasts
- Very resource intensive

Figure 2: Entry-nodes in Bitcoin
Effectiveness - Finding IP Addresses

- Peers of a node more volatile
- No set number of peers
Existing Attacks - Clustering

- Crawler
- Multi-input transactions
- Transaction ‘change’
Effectiveness - Clustering

- No multi input
- No change
- No shadow addresses
"Is deanonymisation of clients feasible for the Ethereum network?"

Deanonymisation attacks difficult to apply:

- Finding IP
  - Nodes not static
- Clustering
  - No multiple addresses

But, possibilities for similar attacks
Future Work

- **Bootnodes**
  - Shadow network
  - Government

- **Peer selection protocol**
  - Create nodes
  - Identify nodes

- **Attack wallet software**
  - Less resource intensive
References

Questions