# Deanonymisation in Ethereum Using Existing Methods for Bitcoin

Robin Klusman
Tim Dijkhuizen

Supervisor: Arno Bakker

RP1 #61

06-02-2018

# Introduction

- Blockchain
  - Decentralised
  - Peer-to-peer
  - Miners
  - Anonymous reputation
- Forensics
  - Track malicious actors

*Image source - thenounproject.com*

# Introduction

## The integrity of the block*chain*

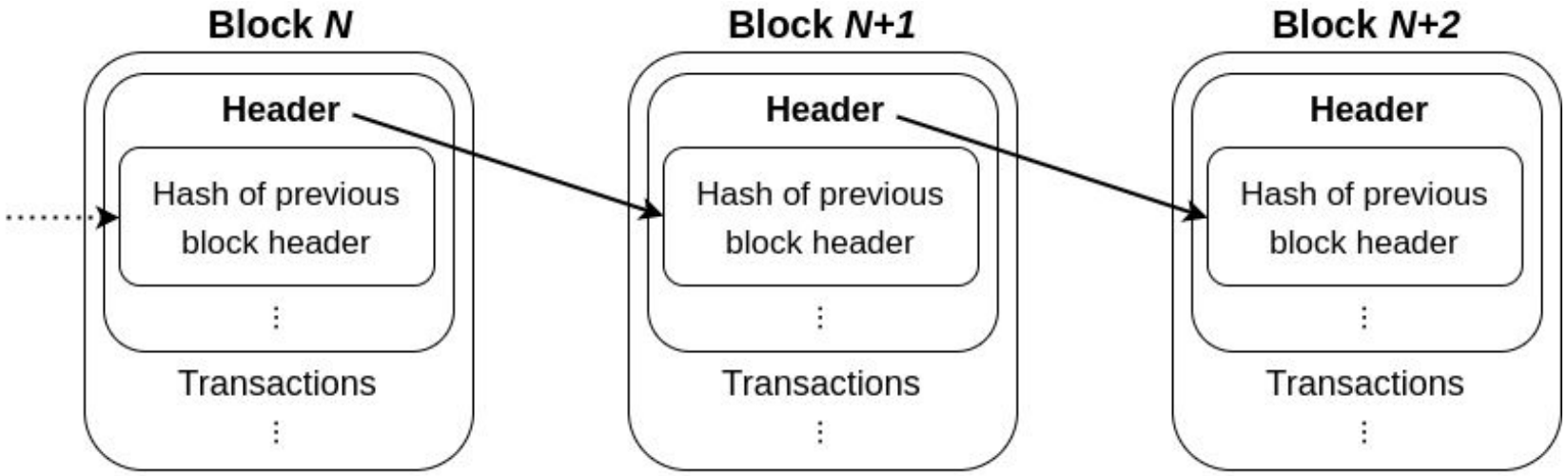



Figure 1: Overview of how blocks in a blockchain are linked to each other

# Introduction

## Blockchain popularity

- Bitcoin
  - 2009
  - ‘Satoshi Nakamoto’

- Ethereum
  - 2015
  - Vitalik Buterin

# Research Question

"Is deanonymisation of clients feasible for the Ethereum network?"

*Image source - thenounproject.com*

# Related Work

- Survey on Bitcoin security and privacy issues
  - Essential background knowledge
  - Attacks on Bitcoin
    - BitIodine
- Survey on Ethereum smart contracts
  - Aimed at illegitimately obtaining funds
  - DAO attack

# Bitcoin

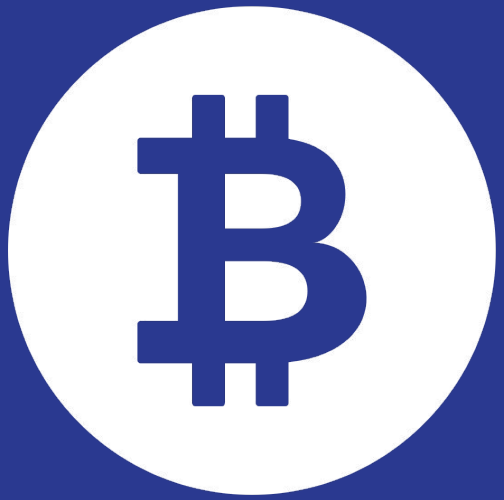
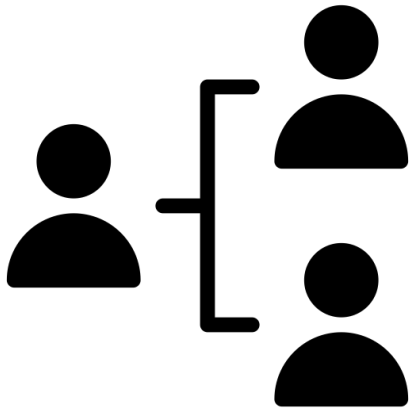


*Image source - thenounproject.com*

# Bitcoin P2P Network

Discovering clients:

- Hardcoded seed servers
- Clients maintain 8 entry-nodes
- `getaddr` message



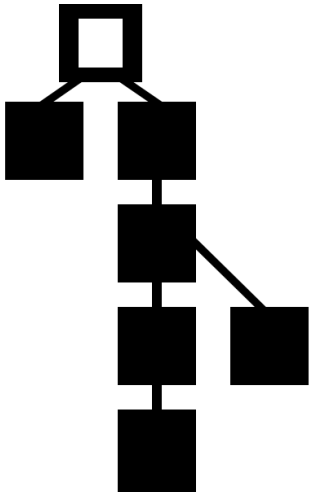
Transaction propagation:

- Trickling
  - Queueing `inv` messages
  - 100ms

# Bitcoin Blockchain

Transactions

- Based on UTXO
- Use up all inputs
- Change



Blocks:

- Merkle tree
- Header hash
- Forks

*Image source - thenounproject.com*

# Bitcoin (& Ethereum) Consensus Model

PoW (Proof of Work):

- Based on computational power
- Against Sybil attack

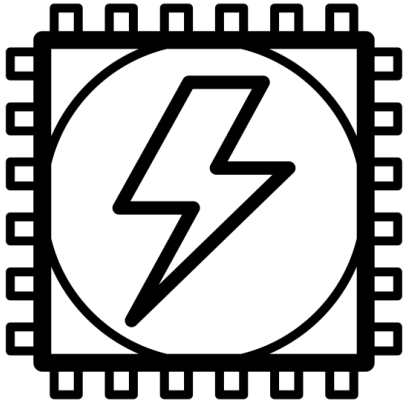


*Image source - thenounproject.com*

# Ethereum

*Image source - thenounproject.com*

# Ethereum Smart Contracts

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

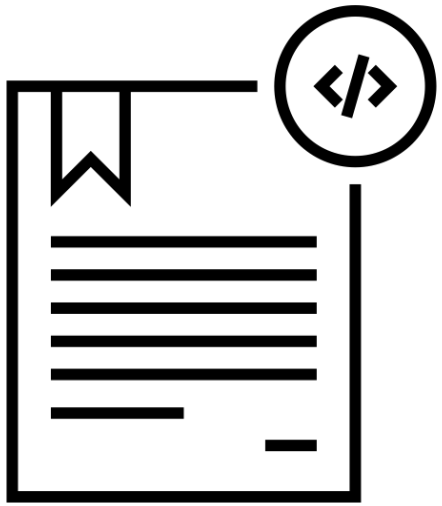
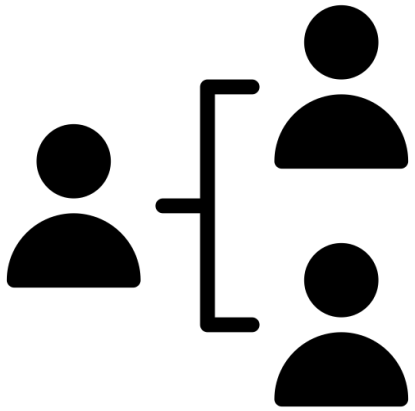


*Image source - thenounproject.com*

# Ethereum P2P Network

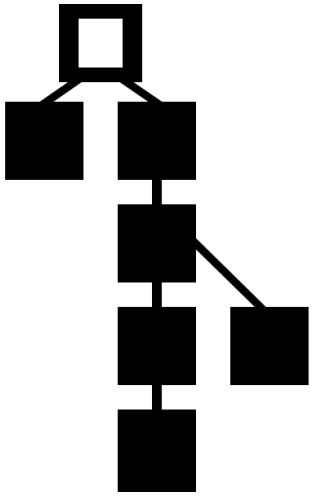
- Kademlia based
- Bootnodes
- Find nodes
  - `nodeID` from public key
  - Closeness
  - XOR of SHA-3 hash



# Ethereum Blockchain

Transactions:

- No UTXO
- Account balance



Blocks:

- Global state
- Transaction *trie*
- Ommers

*Image source - thenounproject.com*

# Attacks

*Image source - thenounproject.com*

# Existing Attacks - Finding IP Addresses

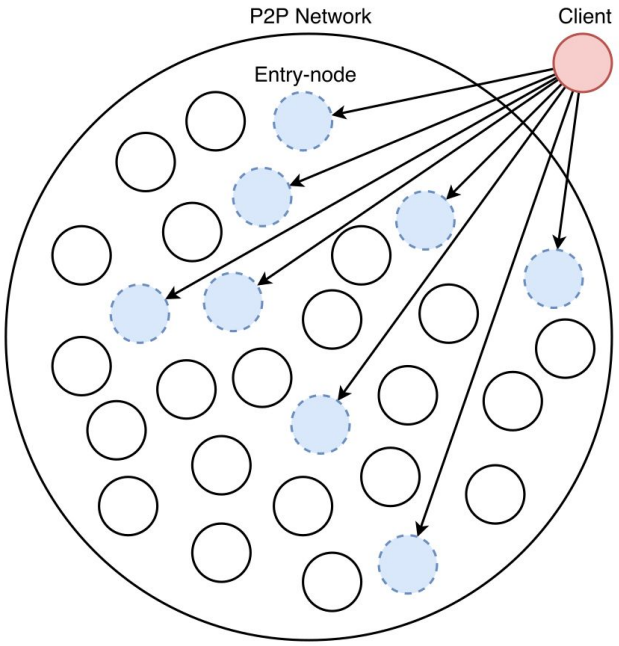



Figure 2: Entry-nodes in Bitcoin

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

# Effectiveness - Finding IP Addresses

- Peers of a node more volatile
- No set number of peers

# Existing Attacks - Clustering

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

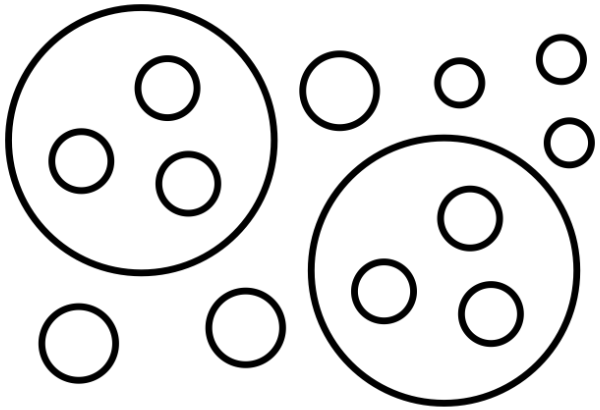
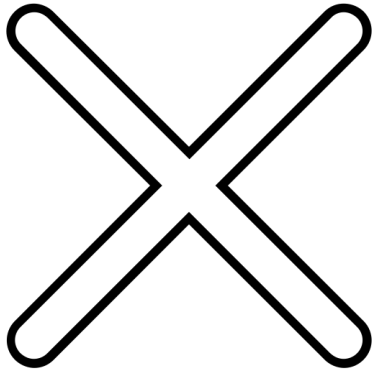


*Image source - thenounproject.com*

# Effectiveness - Clustering

- No multi input
- No change
- No shadow addresses



# Discussion & Conclusion

"*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


- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
- Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 151, 1-32.
- Conti, M., Lal, C., & Ruj, S. (2017). A survey on security and privacy issues of bitcoin. arXiv preprint arXiv:1706.00916.
- Atzei, N., Bartoletti, M., & Cimoli, T. (2017, April). A survey of attacks on Ethereum smart contracts (SoK). In International Conference on Principles of Security and Trust (pp. 164-186). Springer, Berlin, Heidelberg.
- Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014, November). Deanonymisation of clients in Bitcoin P2P network. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 15-29). ACM.
- Spagnuolo, M., Maggi, F., & Zanero, S. (2014, March). Bitiodine: Extracting intelligence from the bitcoin network. In International Conference on Financial Cryptography and Data Security (pp. 457-468). Springer, Berlin, Heidelberg.

# Questions

*Image source - thenounproject.com*