

# Not so Anonymous - Deanononymization of Blockchain Users

Johannes Ahlmann

CorkSec Meetup

2019-03-12

# Agenda

- Is Bitcoin anonymous?
- What is Deanonimization?
- Why should I care?
- What can I do about it?
- Where to get cryptos?
- Alternatives



# About Me

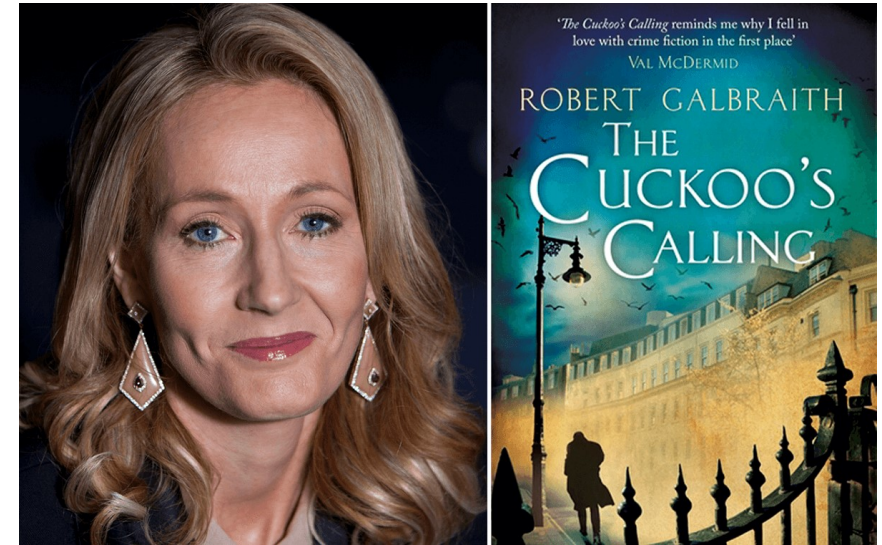
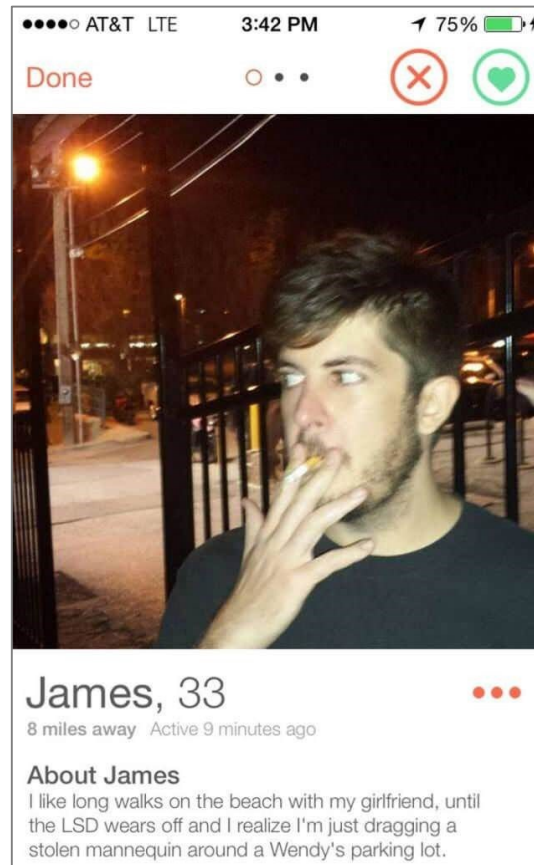
- Johannes Ahlmann
- [sensatus.io](https://sensatus.io)
  - On-Prem AI Models
  - Gathering and Enriching Web Data
  - Sales & Client Intelligence
- [webdata.org](https://webdata.org)
  - Share Libraries and Best Practices
  - Bring Data Scientists and SME Companies together
  - [ForDevelopers](#)
  - [AwesomeAvailableDatasets](#)
- Contact:  
[johannes@sensatus.io](mailto:johannes@sensatus.io)





# Pseudonyms

- 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX
- secret@protonmail.com
- @johannes\_cork
- reddit\_user
- slashdot\_user
- ahljoh
- 083 1762676
- Dread Pirate Roberts



# Anonymity & Privacy

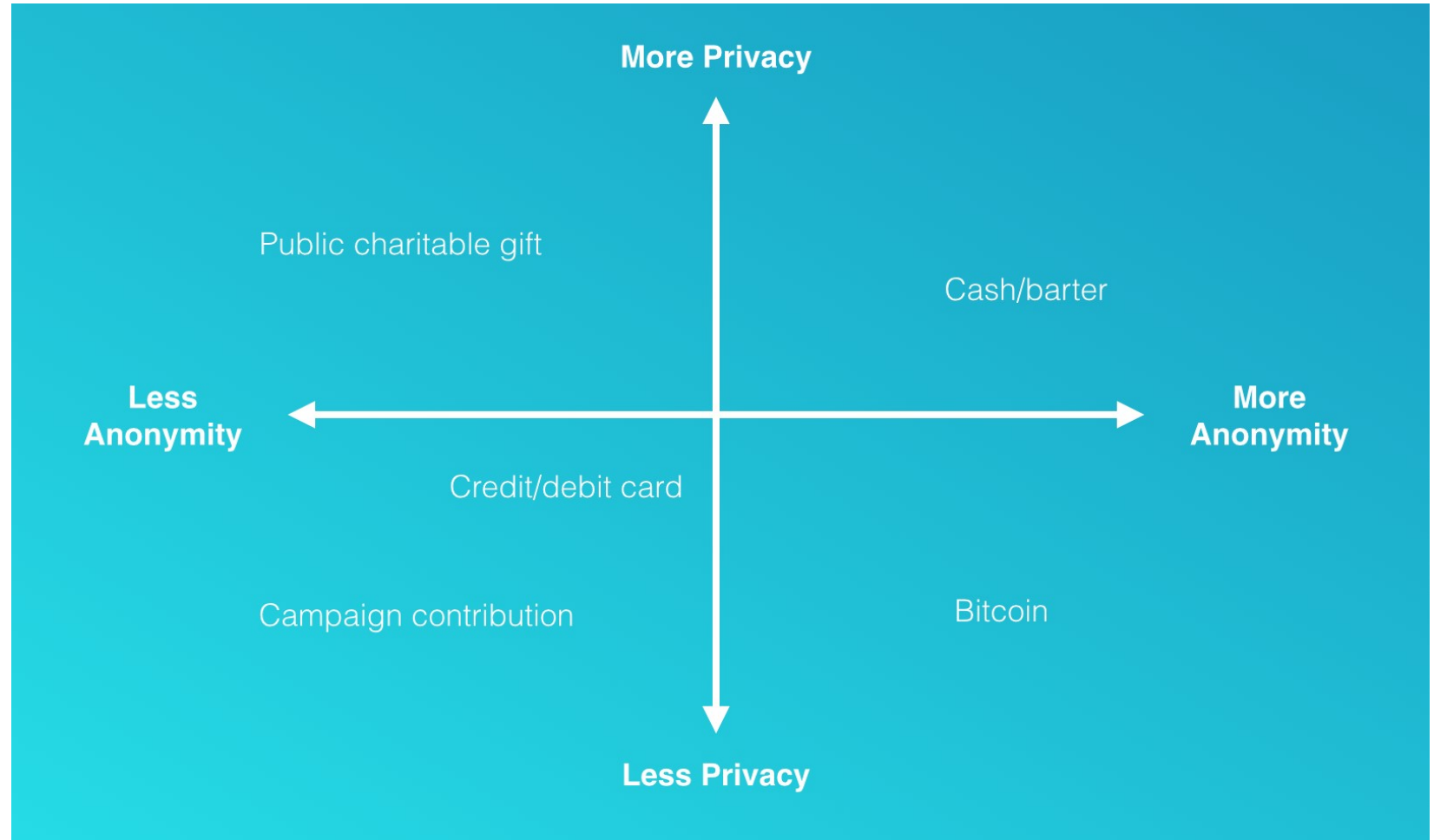
## Anonymity

"without a name"

Noone knows **who you are**

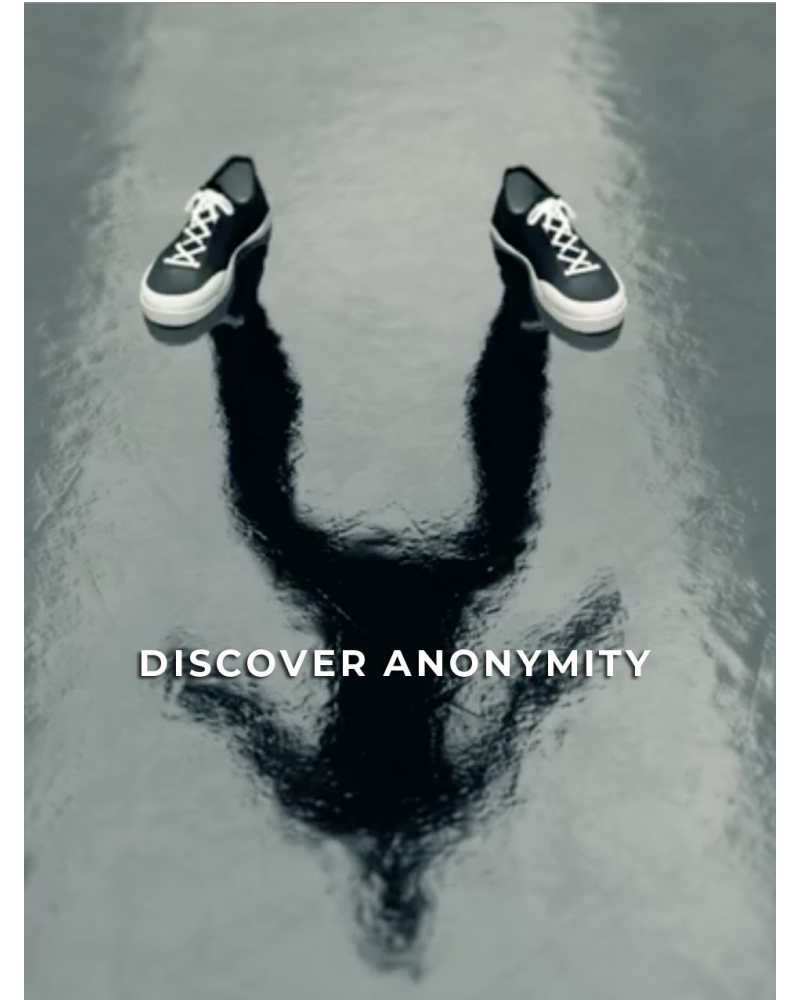
## Privacy

Noone knows **what you purchased and for what amount**



# Anonymity 1/2

- Pseudonymity - People are aware of one or multiple pseudonyms of yours, but not your true identity
- **Anonymity = Pseudonymity + Unlinkability**
- Unlinkability
  - Different actions of the same user should not be linkable to each other
  - Linking of addresses to users
  - Linking of transactions to users
  - Linking of senders to recipients



# Anonymity 2/2

- Privacy vs. Decentralization
  - Public Ledger is core component in consensus and sharing state of the world
- Bitcoin is pseudonymous, not anonymous
  - public addresses = pseudonyms
  - much less privacy than cash
- Many Bitcoins are acquired through Exchanges or Mining Pools
- Relatively few merchants/ market participants to trade with (retroactive geolocation)
- Deanonymizing TOR using Bitcoin ;)
- Fungibility





# What is Deanonymization

- Linking you to your addresses
- Linking you to your transactions
- Tagging, clustering of totality of addresses, transactions
- Approaches
  - Transaction Graph Analysis
  - Realtime Network Analysis of P2P network







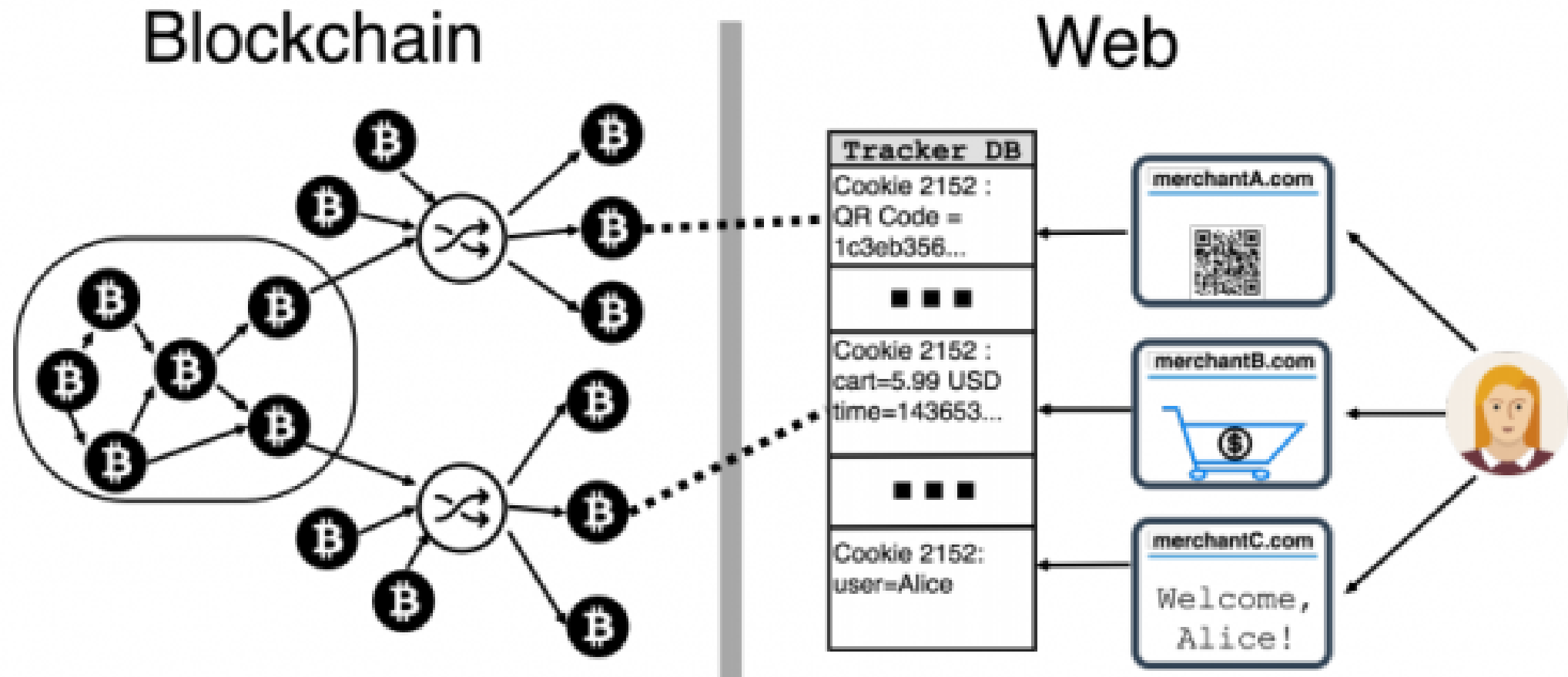
# Case: 1 - Harvard Bomb Threat

- Eldo Kim was connected to Tor network around that time.
- Suspected Eldo Kim wanted to get out of a final and admitted he made the bomb threat when interviewed.
- Kim took several steps to hide his identity, but in the end, it was the WiFi that got him.



## Lessons Learned:

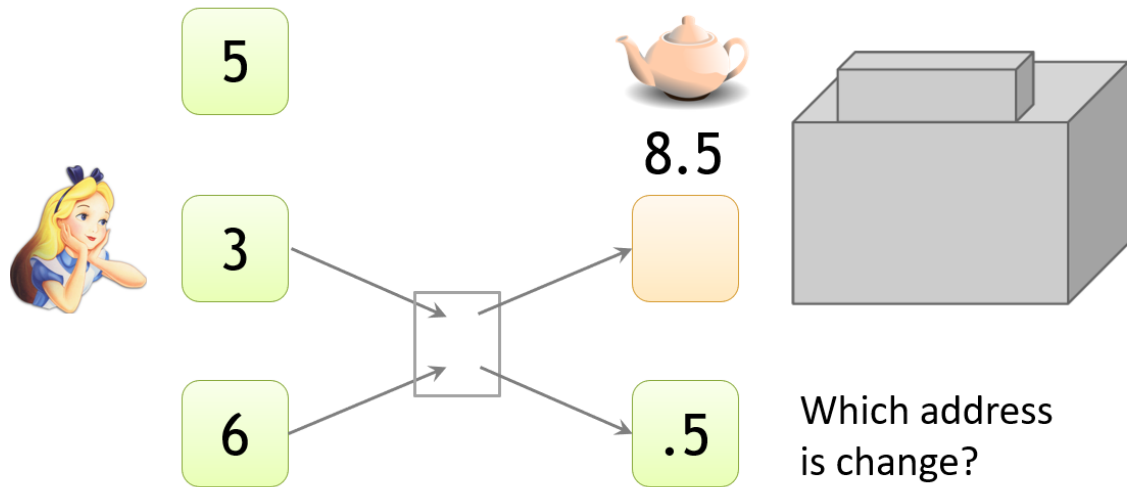
- ❑ Don't be the only person using Tor on a monitored network at a given time.
- ❑ Never access Tor from your college WiFi.
- ❑ Don't admit anything.



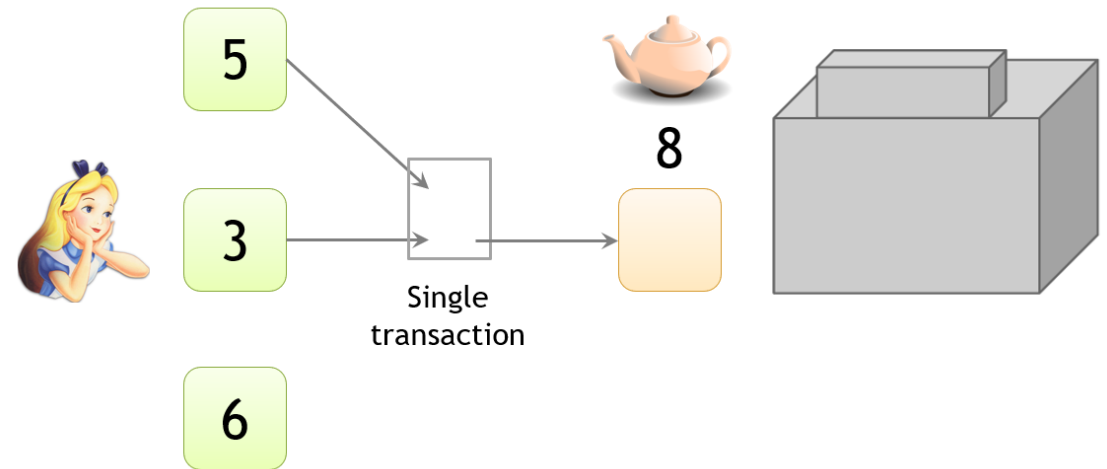
- 130 major merchants accepting Bitcoin
- 53/ 130 leak payment information with > 40 total parties
- Known fiat amount, timestamp
- Unique linkage possible for 60% of (these specific) cases

# Transaction Graph Analysis 1/2

Change Address



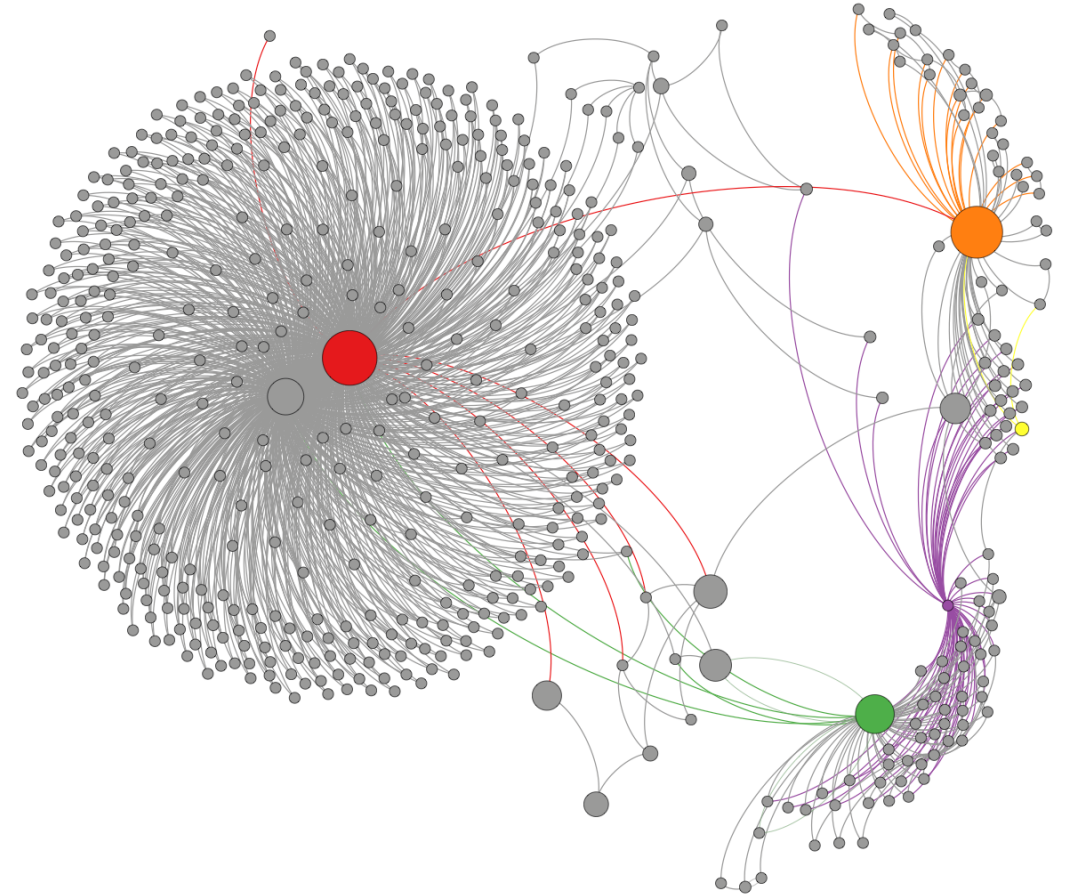
Combined Addresses





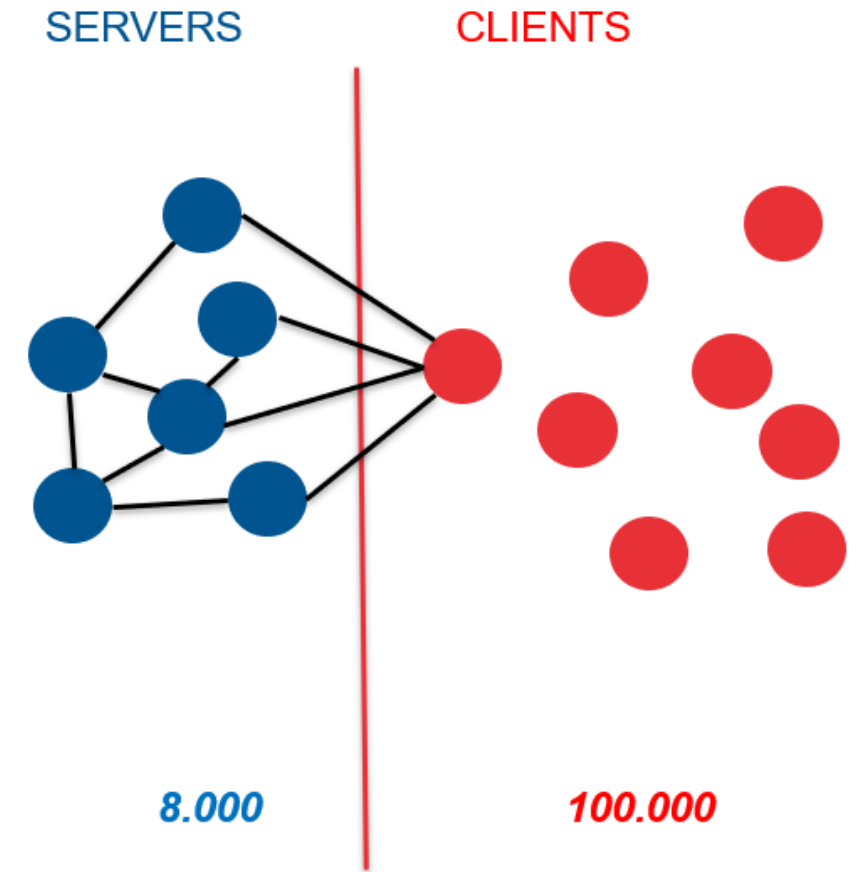
# Transaction Graph Analysis 2/2

- Bitcoin transactions are public
- Active collection
  - Mining pools
  - Online wallets
  - Exchanges
  - Merchants
  - Gambling
- Tagging clusters
  - One tagged address in cluster tags all cluster
- Bitcoin address should only be used once

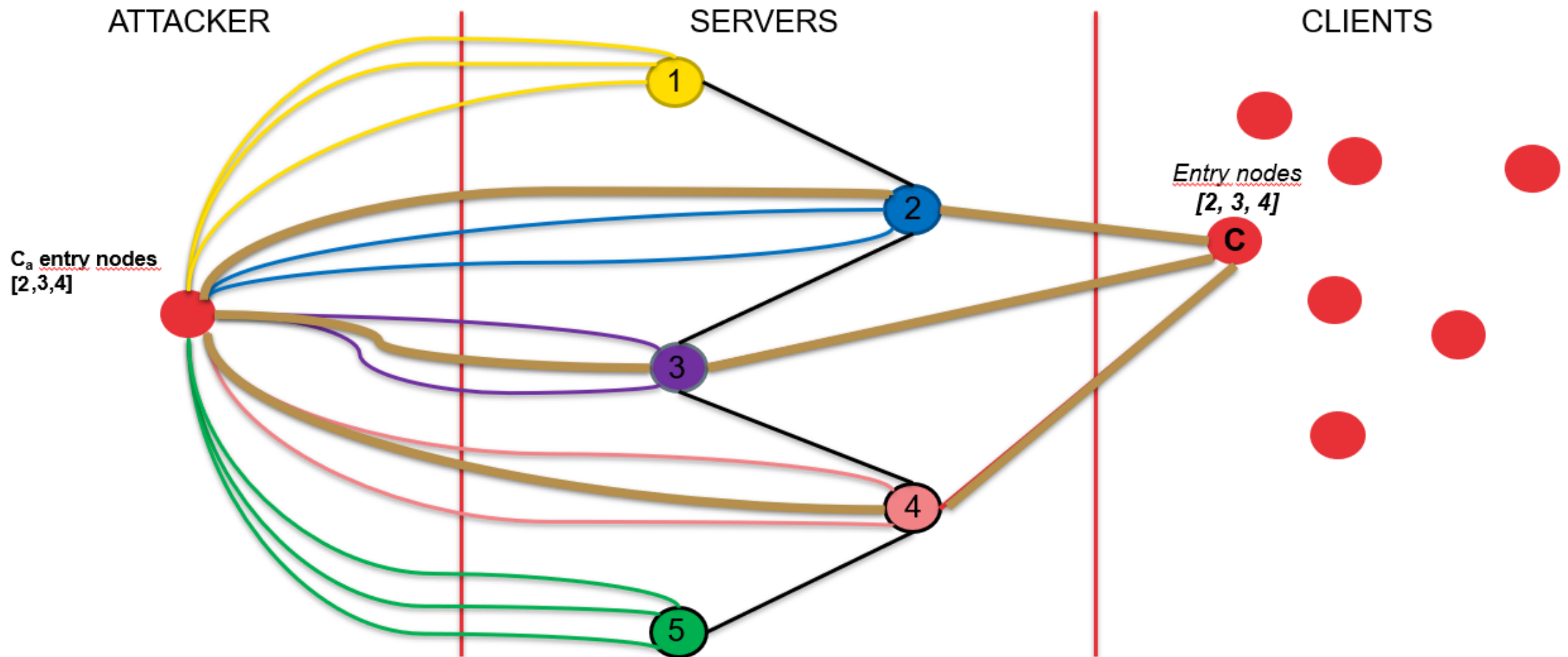


# Realtime Network Analysis

- "Attack" on the P2P Network
- Peers distinguished over set of its (8) entry nodes
- Linking inputs
- Tagging clusters

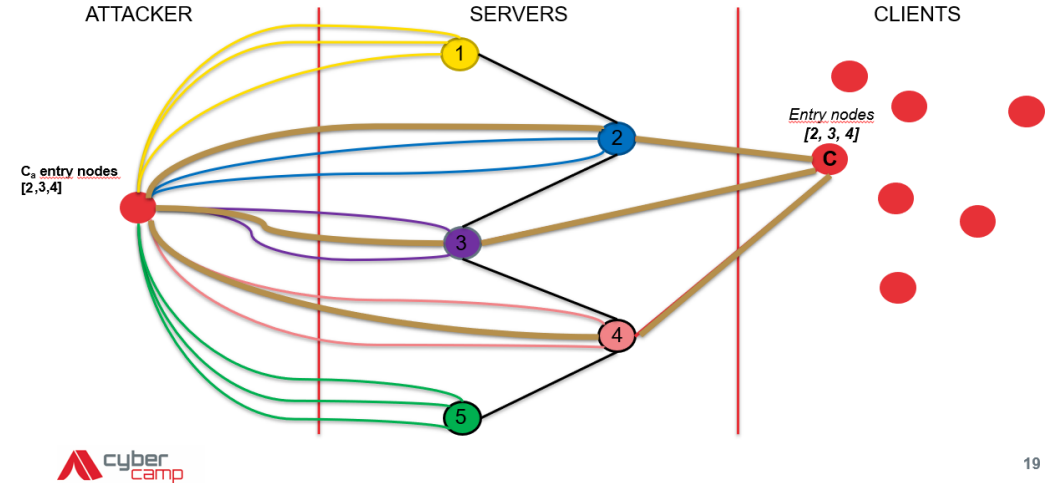


# Learning Entry Nodes



# Realtime Network Analysis

- Linking of different transactions to same user
- Each peer is trying to connect to *8 entry nodes*
  - *Network discovery*
- Servers
  - *Receive incoming connections*
  - *Max. 117 incoming connections*
- Clients
  - *8 outgoing connections*
- Peers are distinguished over set of it's entry nodes!

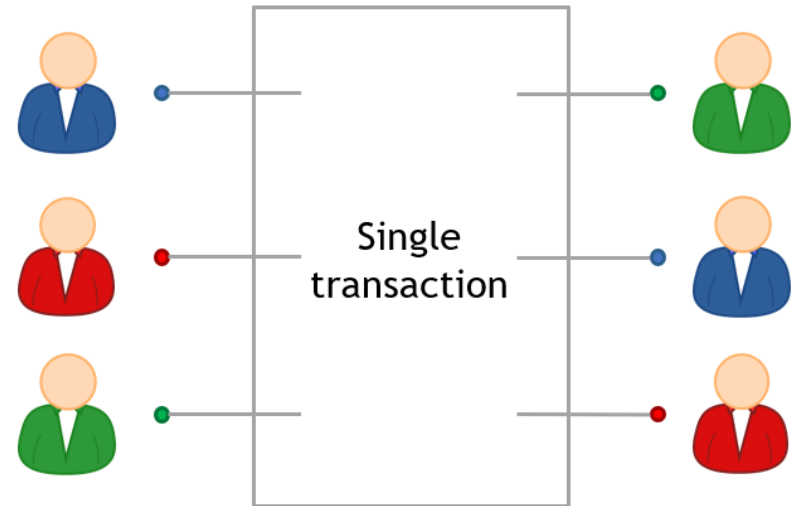




# Remediation

- Deterministic Address Pool Wallets
- Random Address Pool Wallets
- Tor
- Mixers
  - Who can we trust?
- Coinjoin
  - How to find Peers?
- Anonymous cryptocurrencies

## Coinjoin



# Anonymous Currencies

- Monero** - Ring signatures
- Dash** - Fork of bitcoin, coin-mixing service
- Zcash** - zk-SNARK, zero knowledge proofs
- Verge** - Tor and I2P network for privacy
- Komodo** - Fork of Zcash, zk-SNARK
- Pivx** - Fork of Dash, Zerocoin protocol

(Legitimate goods vs. legitimate worries;  
how can this be used for good or bad?)



Thank You!

# Resources

- <https://coincenter.org/entry/how-anonymous-is-bitcoin>
- <https://bitcoinmagazine.com/articles/is-bitcoin-anonymous-a-complete-beginner-s-guide-1447875283/>
- <https://www.coursera.org/lecture/cryptocurrency/how-to-de-anonymize-bitcoin-qnS76>
- <https://www.slideshare.net/bhaslhofer/bitcoin-deanonymization-and-money-laundering-detection-strategies>
- <https://pwlconf.org/2018/giulia-fanti/>
- <https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/>
- <https://decentralize.today/a-new-attack-vector-to-deanonymize-bitcoin-users-9c6dc433d4b6>
- <https://www.deepdotweb.com/2017/04/20/how-companies-are-deanonymizing-bitcoin/>
- <https://bitcoinsandblockchains.blogspot.com/2016/05/bitcoin-deanonymization.html>
- <https://btcmanager.com/u-s-department-of-homeland-security-create-bitcoin-deanonymization-tool/>
- <https://www.deepdotweb.com/2018/01/02/using-bitcoin-transaction-analysis-deanonymizing-users-tor-hidden-services/>
- [https://www.researchgate.net/publication/305423583\\_Listening\\_to\\_Whispers\\_of\\_Ripple\\_Linking\\_Wallets\\_and\\_Deonymizing\\_Transactions\\_in\\_the\\_Ripple\\_Network/download](https://www.researchgate.net/publication/305423583_Listening_to_Whispers_of_Ripple_Linking_Wallets_and_Deonymizing_Transactions_in_the_Ripple_Network/download)
- [https://www.youtube.com/embed/glyQy\\_e5LmM?](https://www.youtube.com/embed/glyQy_e5LmM?)