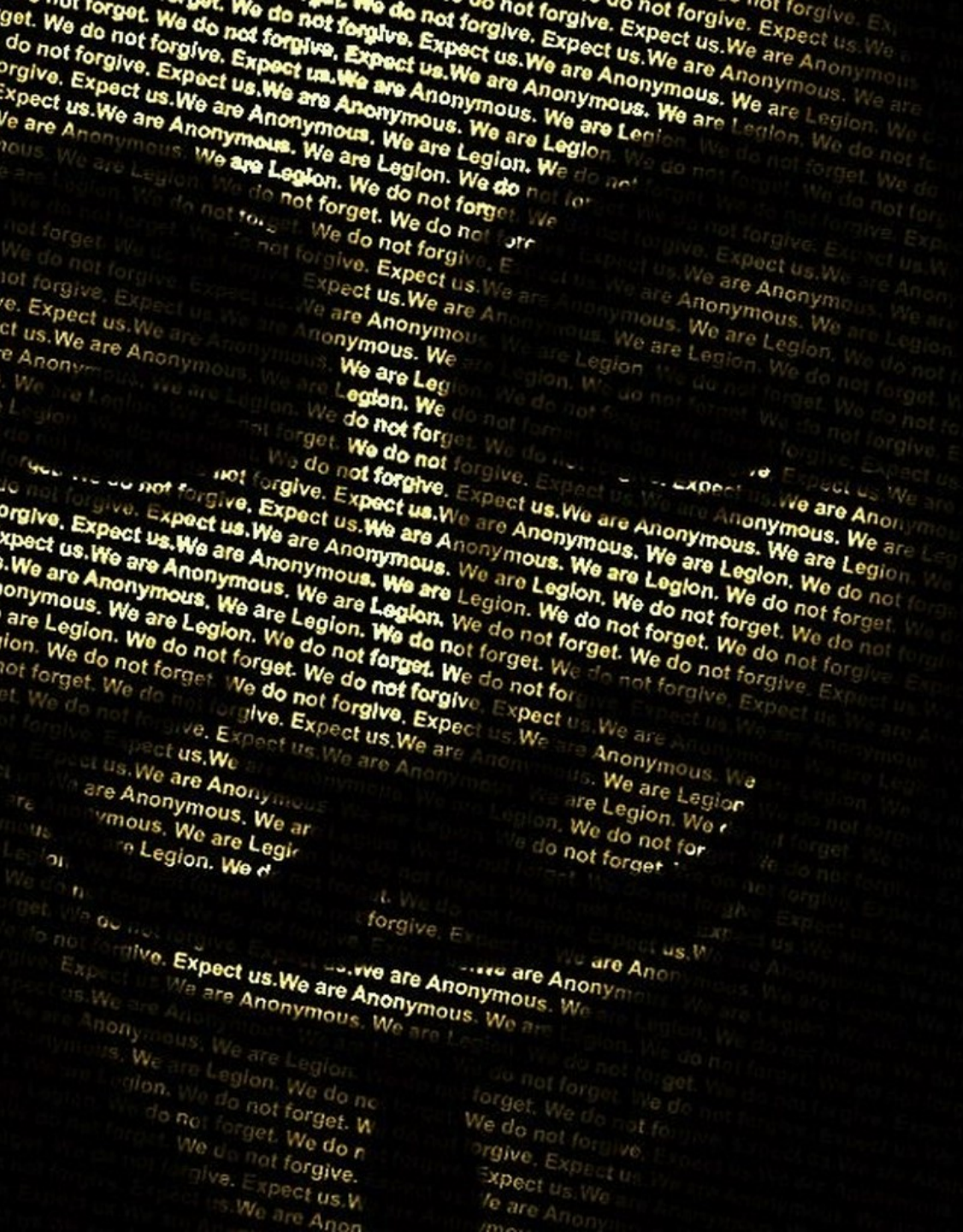


Not so Anonymous - Deanonymization of Blockchain Users

Johannes Ahlmann

Cork Blockchain Meetup

2018-11-13

https://www.dailydot.com/news/anonymous-opfullerton-kelly-thomas/

Lightning Talk - Agenda

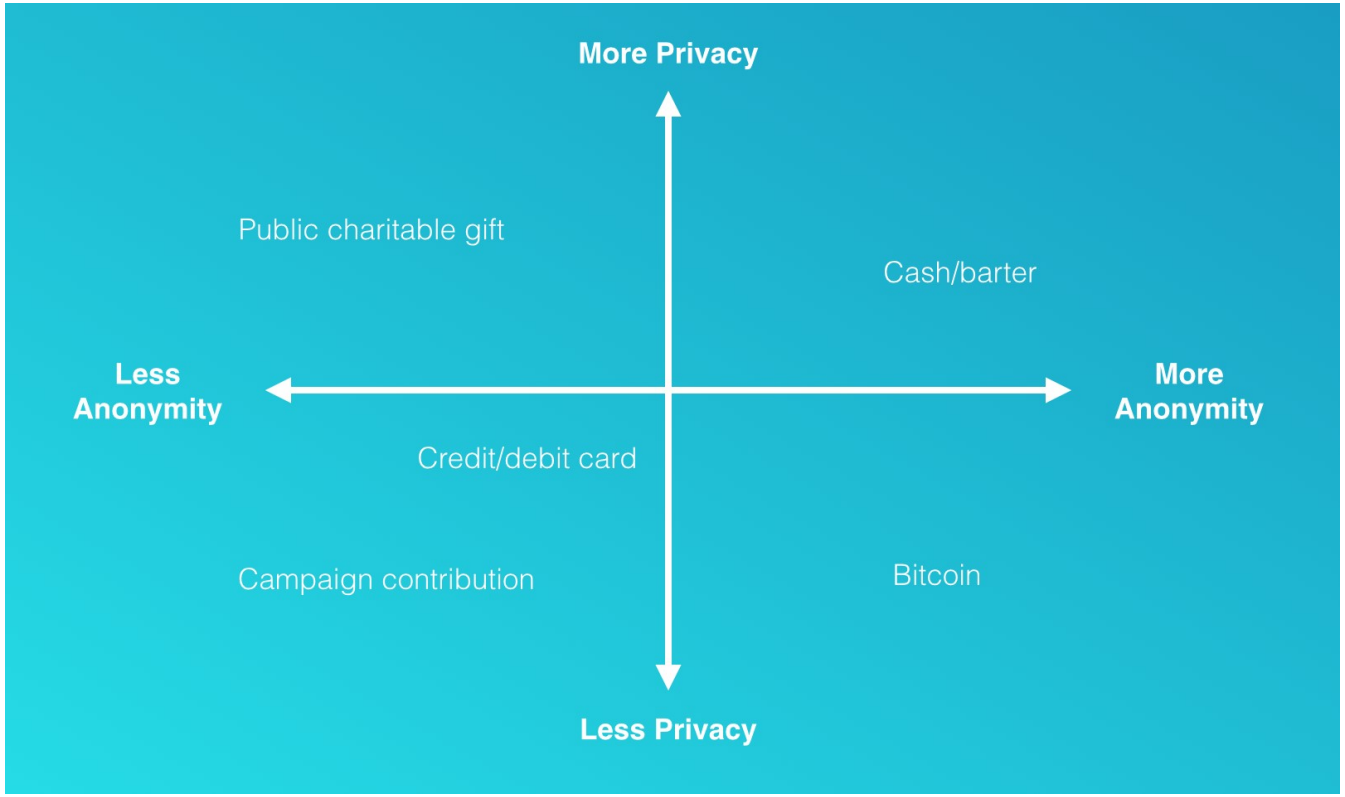
- Is Bitcoin anonymous?
- What is Deanonymization?
- Why should I care?
- What can I do about it?
- Where to get cryptos?
- Alternatives

Anonymity & Privacy

Anonymity
"They" can see what you do, but not **who you are**

Privacy

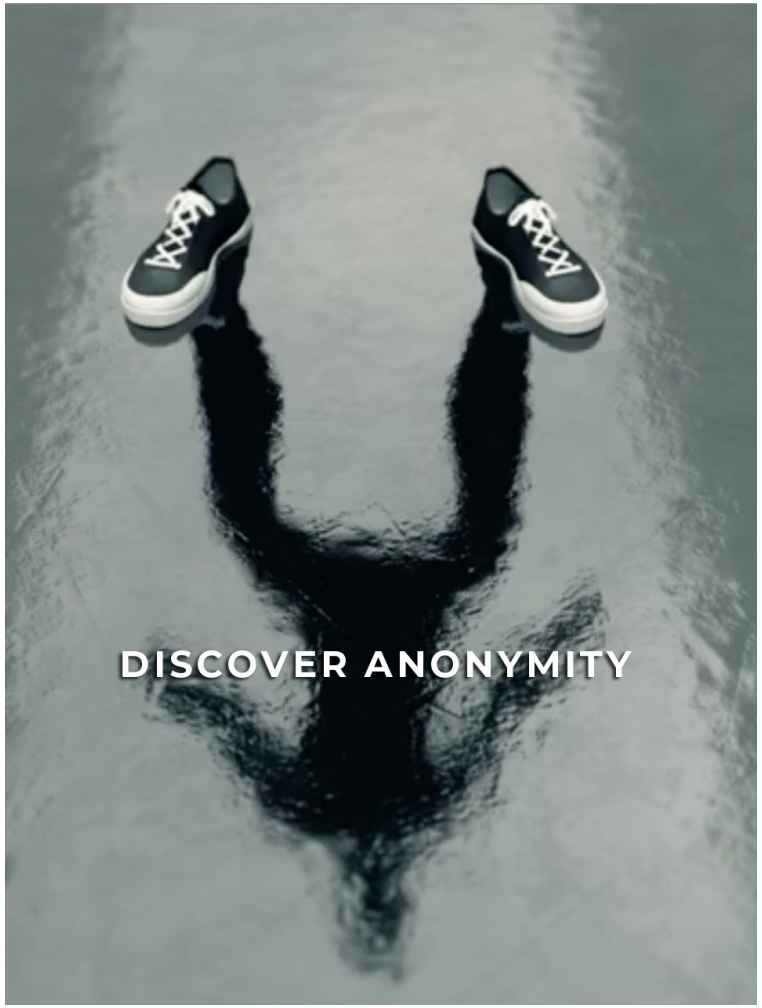
Controlling who sees what **activities you engage in**



https://d262ilb51hltx0.cloudfront.net/max/1610/1*d0KdwdeKDi5m8n-sZdr-_A.png

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



source: Prof. Murtuza Jadliwala

Anonymity 2/2

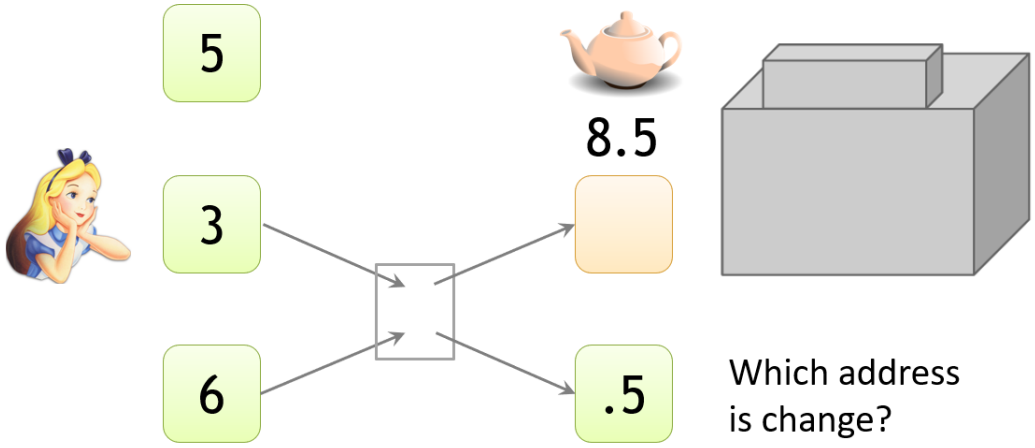
- Privacy vs. Decentralization
  - Public Ledger is core component in consensus and sharing state of the world
- Bitcoin is pseudonymous, not anonymous
  - public addresses = pseudonyms
  - much less anonymous, private than cash
- Many Bitcoins are acquired through Exchanges or Mining Pools
- Relatively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

What is Deanonymization

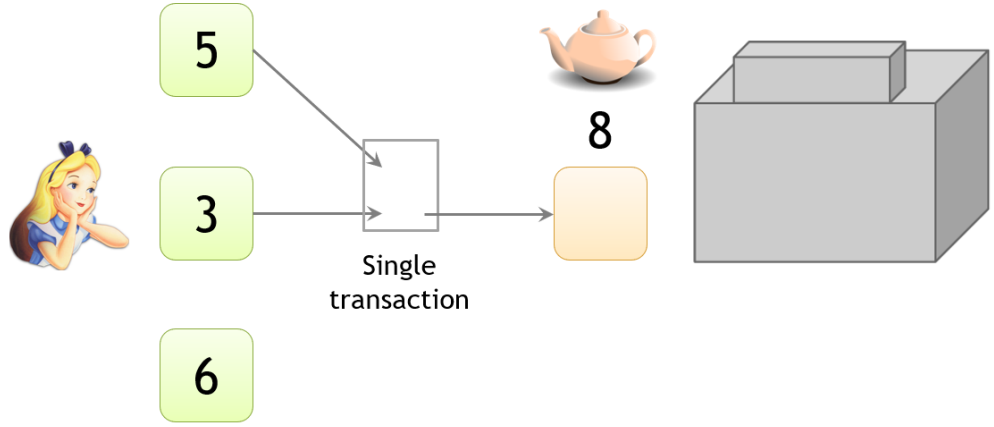
- Linking you to your addresses
- Linking you to your transactions
- Tagging, clustering of totality of addresses, transactions
- Approaches
  - Transaction Graph Analysis
  - Realtime Network Analysis of P2P network

Transaction Graph Analysis 1/2

Change Address

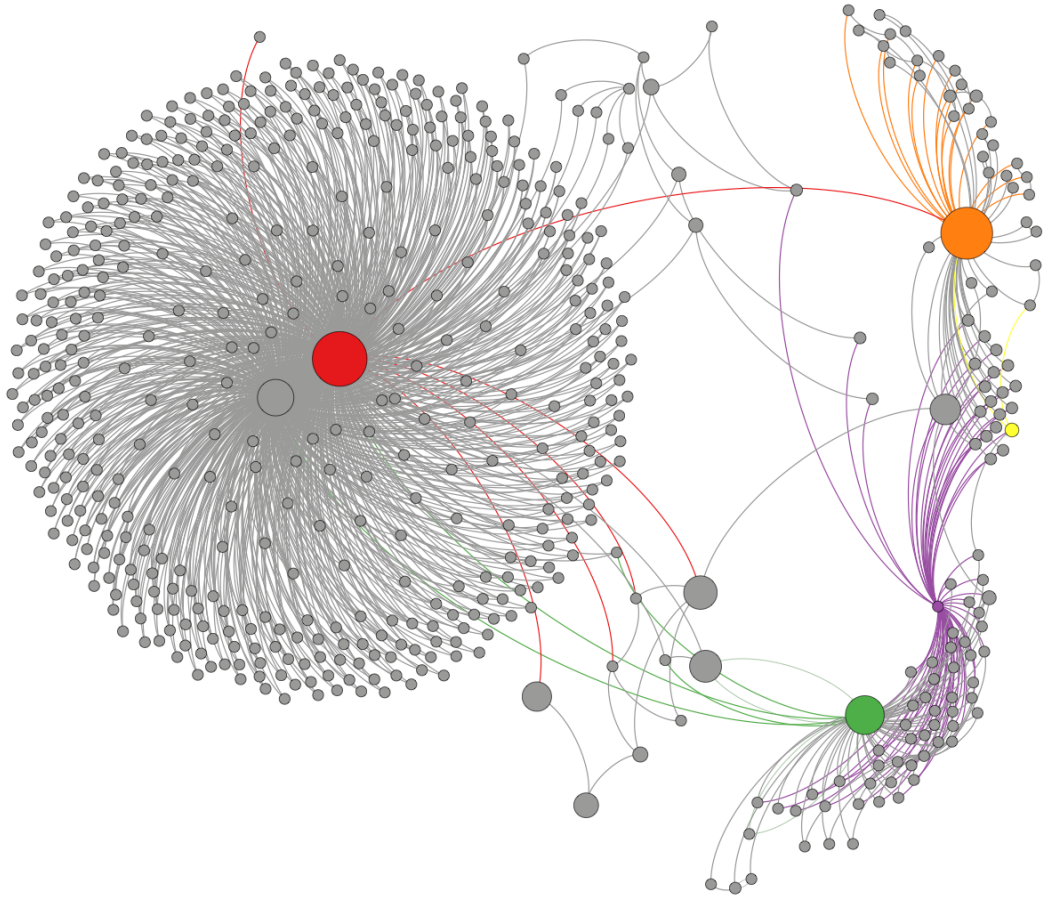


Combined Addresses



Transaction Graph Analysis 2/2

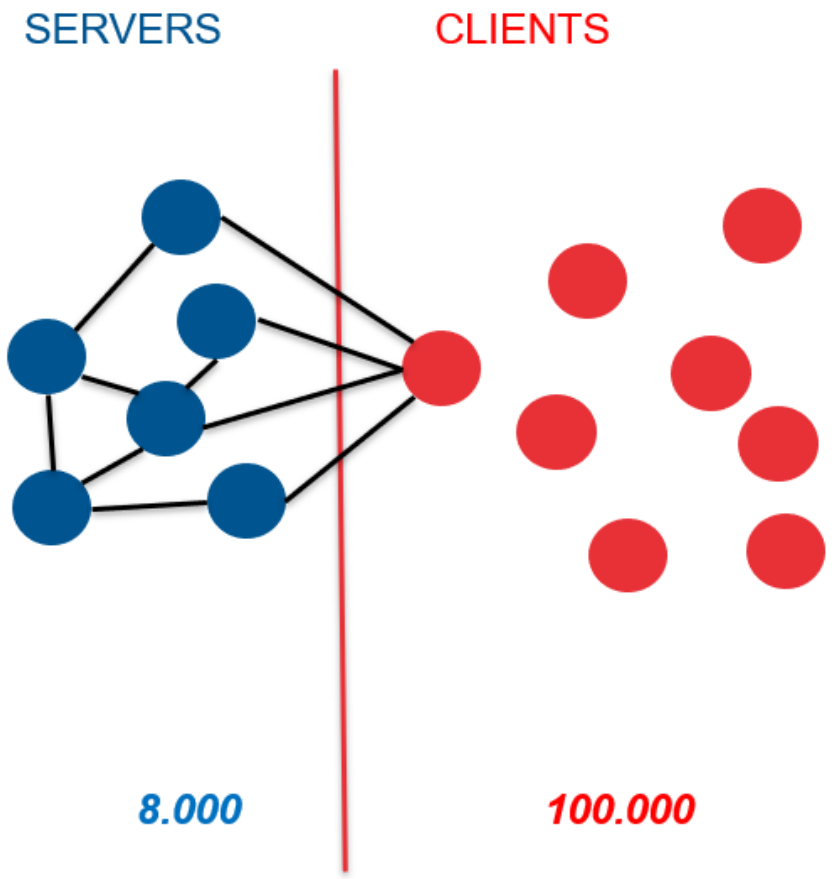
- Bitcoin transactions are public
- Active collecting
  - Mining pools
  - Online wallets
  - Exchanges
  - Merchants
  - Gambling
- Tagging clusters
  - One tagged address in cluster tags all cluster
- Bitcoin address should only be used once



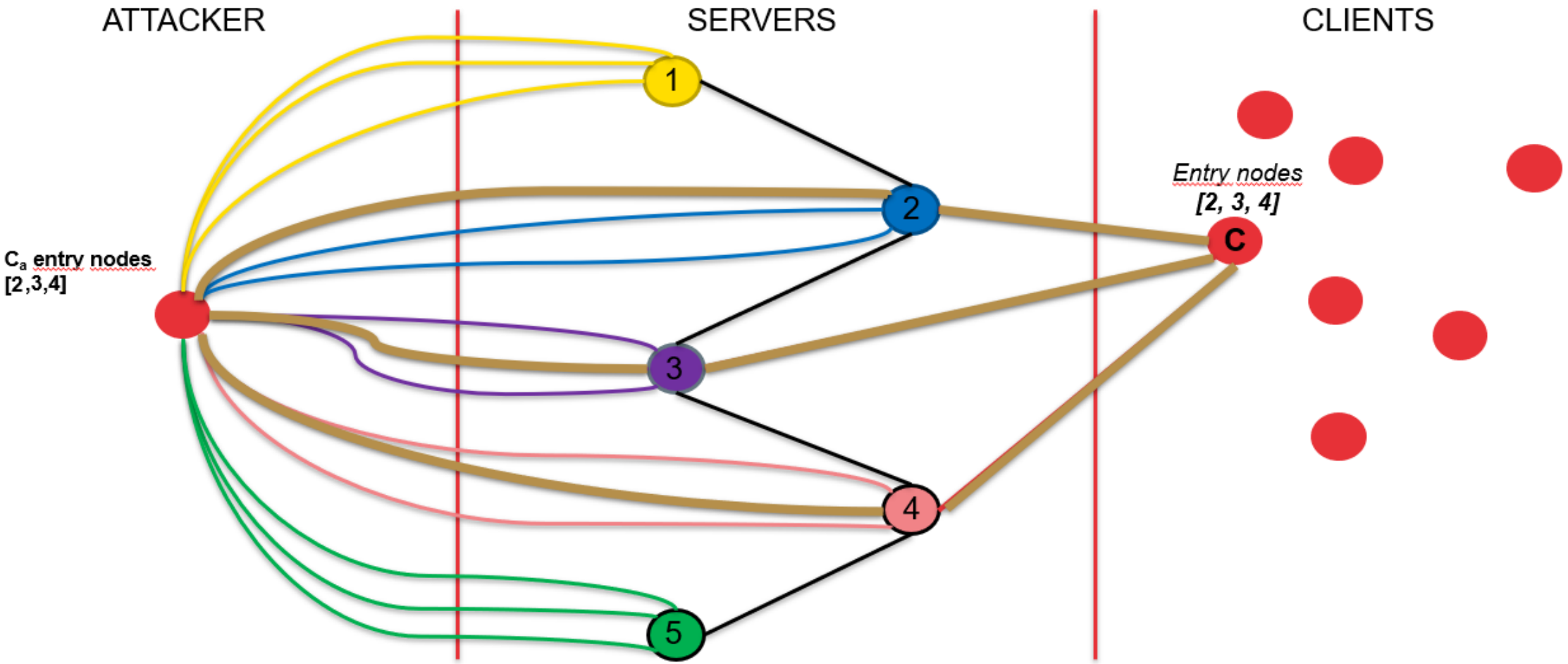
An Analysis of Anonymity in the Bitcoin System
F. Reid and M. Harrigan, PASSAT 2011

Realtime Network Analysis

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

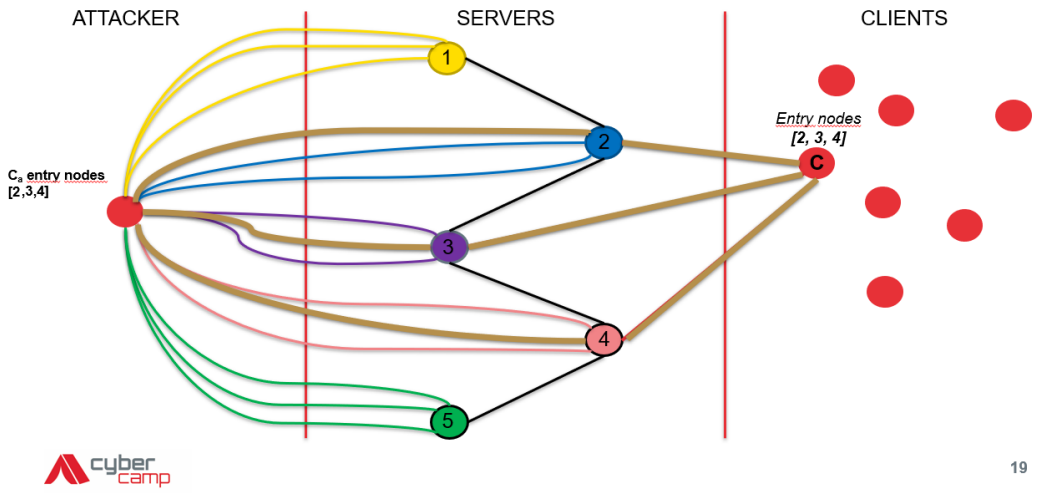


Learning Entry Nodes



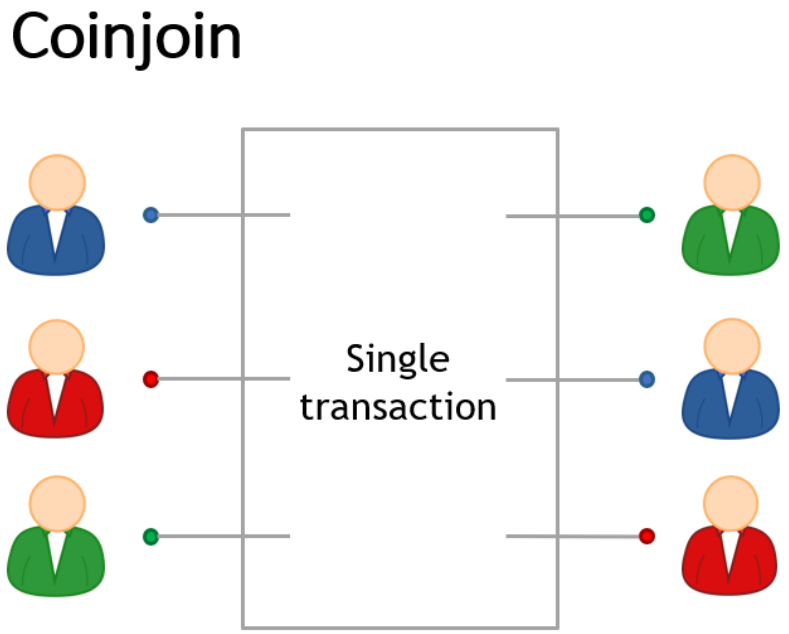
Realtime Network Analysis

- 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

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



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://www.slideshare.net/bhaslhofer/bitcoin-deanonymization-and-money-laundering-detection-strategies
- 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/