Research topics in Crypto Currencies

Alex Biryukov
University of Luxembourg

Our research on cryptocurrencies

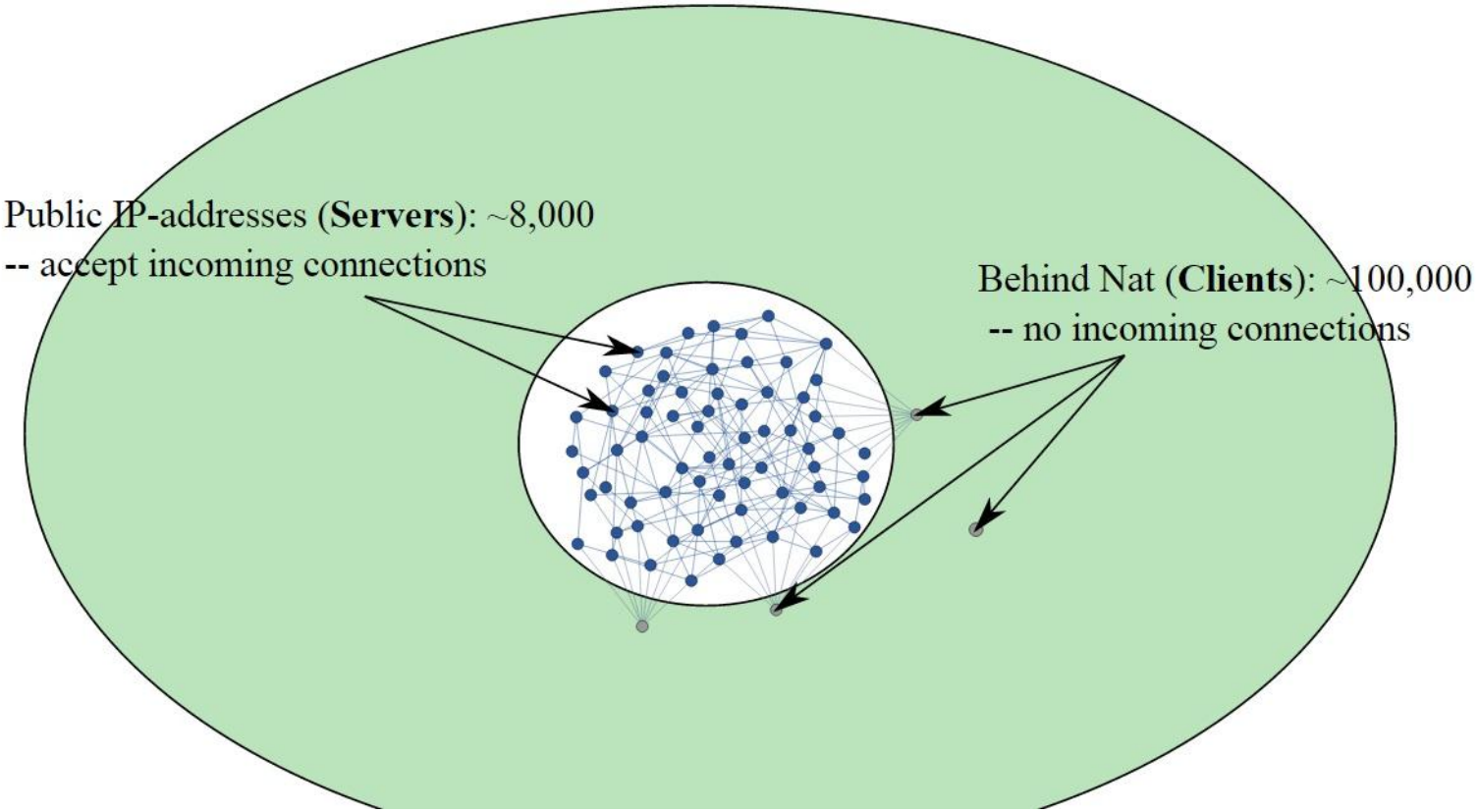
- Security and Privacy of Bitcoin (BC)
- Anonymous micropayments
- Customizable Proofs of Work (PoW)

Security of Bitcoin P2P Network

- Methods to discover Peer2Peer topology
- Address cookies for client fingerprinting
- Deanonymization of clients

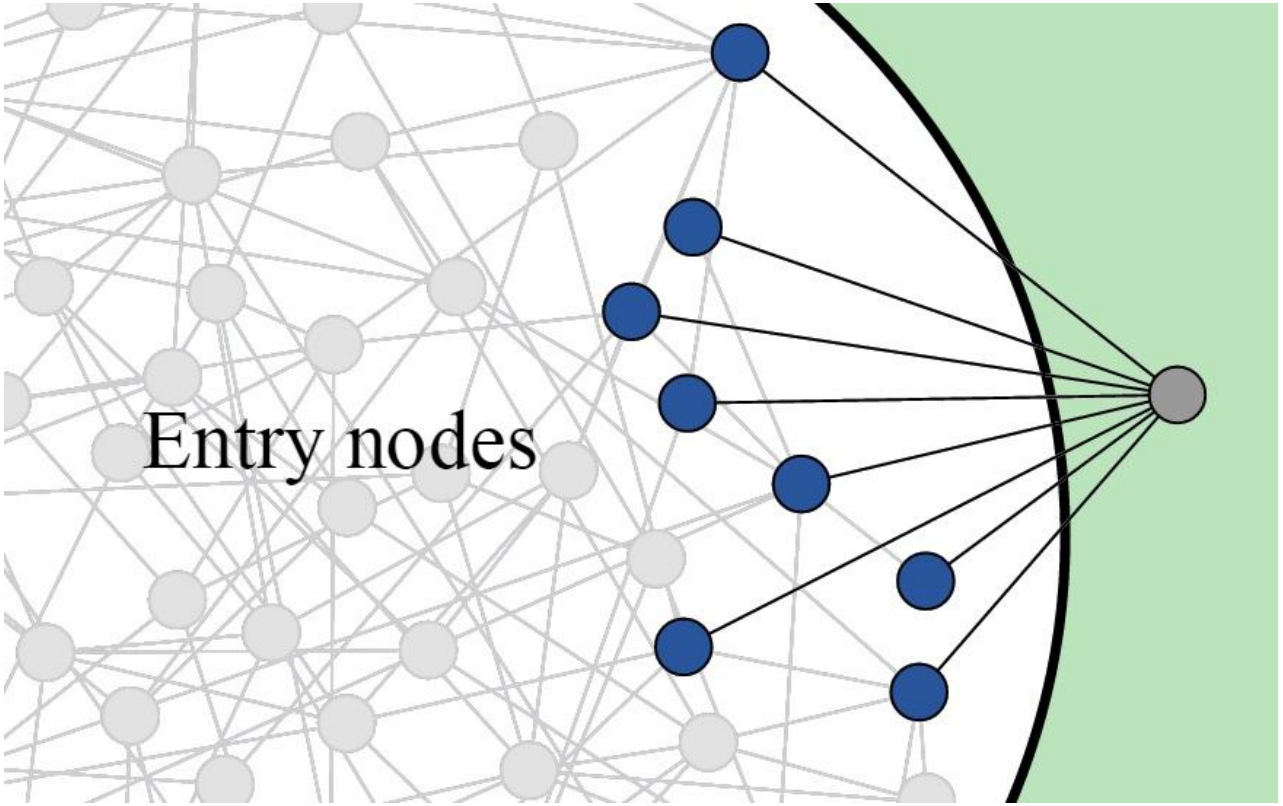
Deanonymiation of BC

Bitcoin P2P topology



Deanonymiation of BC

- Idea: 8 entry nodes – unique ID of the client



Deanonymiation of BC

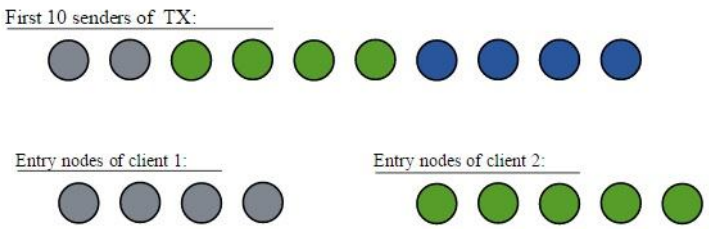
Advertising of IP address

- A client advertises its IP address to all entry nodes
- Each server forwards the address to two neighbors
- Bitcoin server has 125 connection slots
- Attacker connects to all **m** free slots
- Each server forwards tx to (some) neighbors
- Probability to be the first to catch tx is **m**/125

Matching rules

- Assumption: we can establish 50 connections to each server
  - => The probability to catch an entry node is 34%
- 3-tuple matching gives a unique candidate
- 2-tuple matching gives 4 candidates but has higher success rate

# of entries among first 10	Success rate	False positives
1	72%	1249
2	35%	3
3	11%	0
4	2.2%	0
5	0.2%	0



- 60% peers allowed 50+ connections
- 35% tx catch rate for 2 entry nodes

Features/Countermeasures

- Costs less 2000 eur per month
- Drawback: Many connections – noticeable
- Will work even if peer traffic is encrypted
- Complementary to tx graph analysis

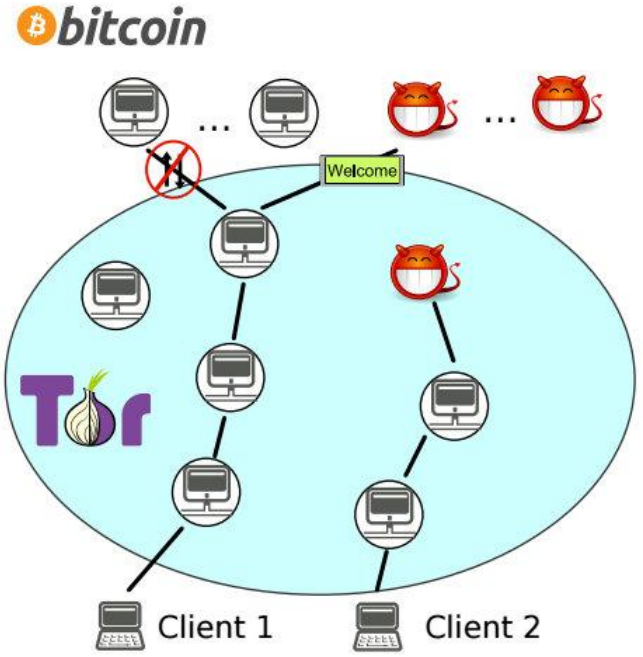
Countermeasures:

- Fewer entry nodes
- Rotation/decay of entry nodes
- Relax anti-DOS protections

More in "*Deanonymisation of clients in Bitcoin P2P network*", ACM CCS'14
https://orbilu.uni.lu/handle/10993/18679

Bitcoin over Tor

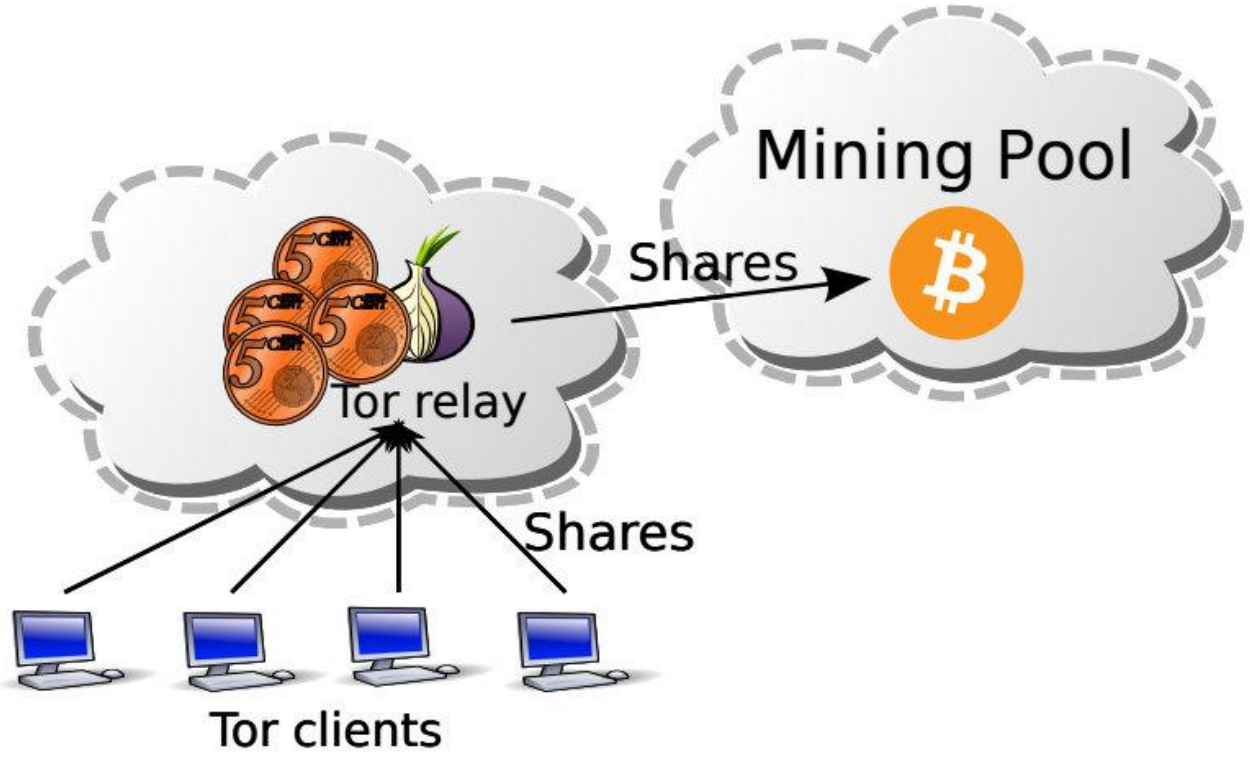
- Tor can be banned using DoS countermeasures (send malformed tx)
- Tor can be used for MitM attacks
- Address cookies - fingerprinting



More in "*Bitcoin over Tor isn't a good idea*", ACM CCS'15
https://orbilu.uni.lu/handle/10993/18751

Mining as Micropayment

- Alt-currency mining can be used as micropayment for news sites, blogs, video streaming, gaming sites or social media



Mining as Micropayment

Hash rates

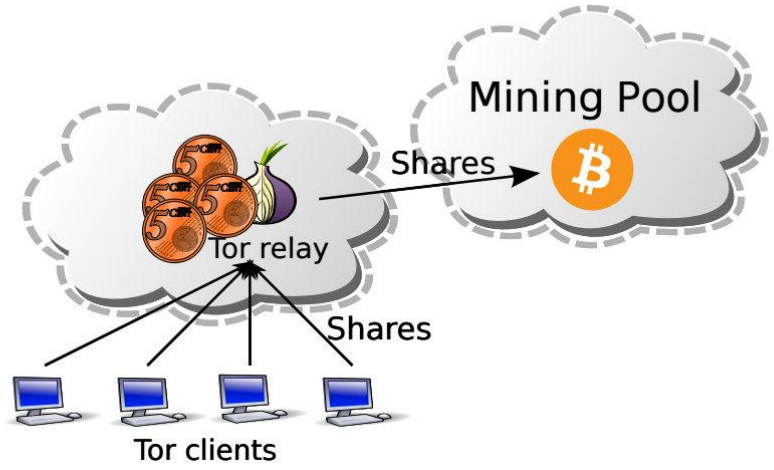
Hashing algorithm	Rate on Intel Core i7-2760QM	Currency	Revenue per day
Blake-256	9,6 Mh/s	Blakecoin	n/a
Groestl	1 Mh/s	Diamond	2.1
HEFTY1	128 Kh/s	Heavycoin	n/a
JHA	308 Kh/s	Jackpotcoin	2.2 cents
Keccak	5.2 Mh/s	Maxcoin	0.7 cents
Quark	300 Kh/s	CNotes	3.8 cents
Scrypt	40 Kh/s	42	0.8 cents
		Litecoin	0.65 cents
		Dogecoin	0.26 cents
Scrypt-N	20 Kh/s	Vertcoin	2.3 cents
Scrypt-Jane	360 h/s	Yacoin	n/a
SHA-256d	9.6 Mh/s	Peercoin	0.01 cents
		Bitcoin	0.008 cents
X11	360 Kh/s	Smartcoin	3.8 cents
		Darkcoin	2.5 cents
X13	104 Kh/s	Marucoin	n/a

Table 2. Hash rates of the proof-of-work algorithms on Intel Core i7-2760QM

- Résumé: We need ASIC-resistant PoW

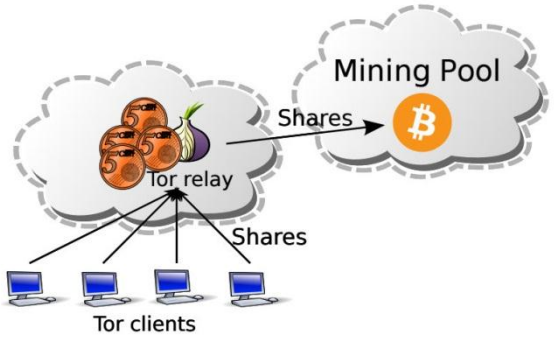
Mining as Micropayment

- Users can donate 10-20% of their CPU power if they like  the content
- Content provider can expand, give access to more services
- May help to boost crypto-currency economy



Mining as Micropayment

- Barter of CPU power for services
- Secure
- can be anonymous and private
- Inherently limited to micropayments – hard to steal or use for money laundering



More in "*Proof-of-Work as Anonymous Micropayment: Rewarding a Tor Relay*", Financial Crypto'15
http://orbilu.uni.lu/handle/10993/19655

Custom PoW

Features

- ASIC resistance, Botnet resistance
- Prover/Verifier asymmetry (hard work to mine, easy to verify)
- Owner/User asymmetry (designer of PoW can have mining advantage over regular user) – harder to mount 51% takeover attack

More in Dmitry's presentation, and in "*Fast and Tradeoff-Resilient Memory-Hard Functions for Cryptocurrencies and Password Hashing*" http://eprint.iacr.org/2015/430