The mass surveillance in Bitcoin and privacy coins

- Global surveillance disclosures.
- Blockchain analytics companies.
- Bitcoin and privacy.
- Pseudo-anonymous cryptocoins.
- Privacy coins.

Global surveillance programs

PRISM: NSA + GCHQ + ASD/DSD + AIVD

Microsoft, Facebook, Apple, Google.

Tempora: NSA + GCHQ

British Telecommunications, Interoute, Verizon, Viatel, Vodafone Cable.

Who spies on you?

Five Eyes → Nine Eyes → Fourteen Eyes + FATF + Key Disclosure

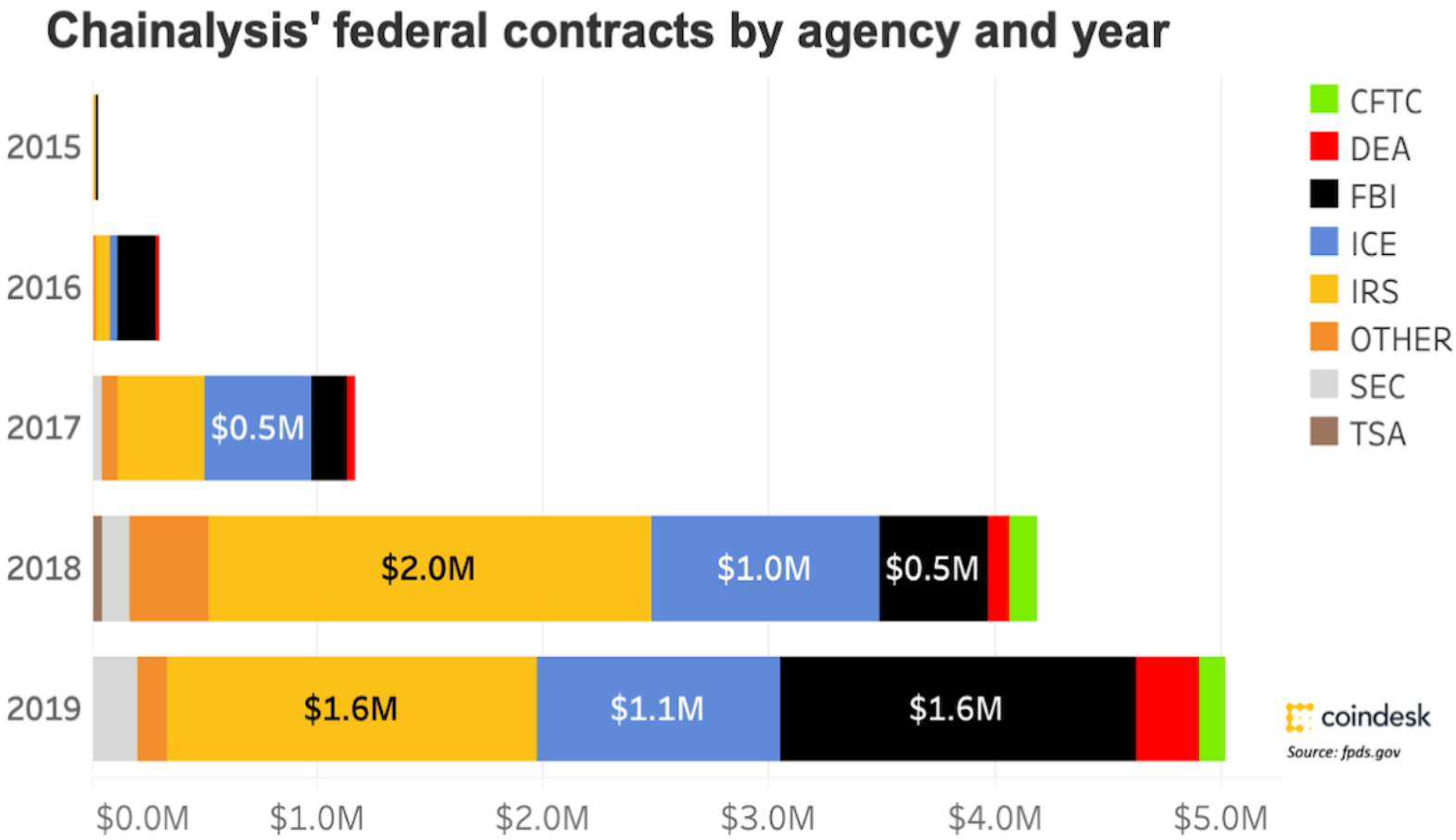
Australia, Canada, New Zealand, UK, USA + Denmark, France, Netherlands, Norway + Belgium, Germany, Italy, Spain, Sweden.

Intel Management Engine + AMD Platform Security Processor

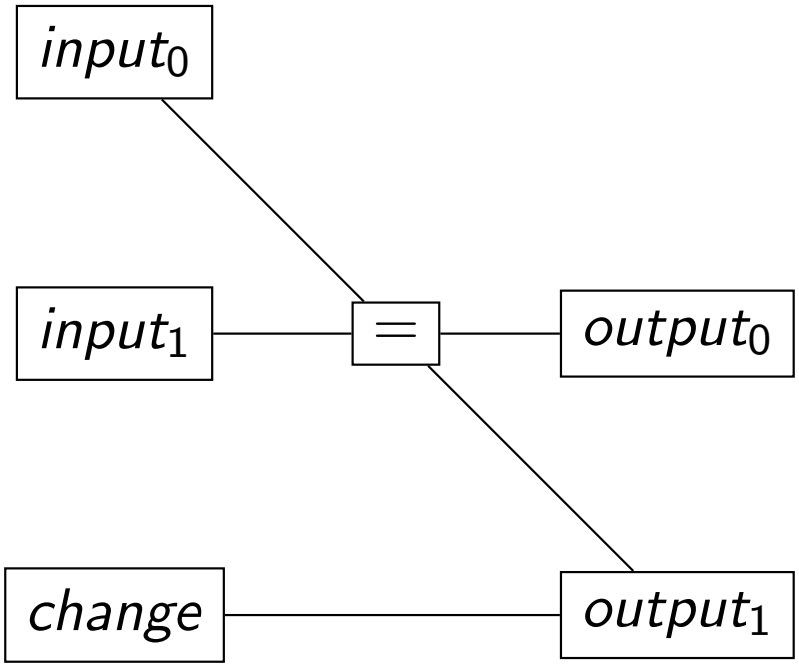
Intel ME, from 2008 + AMD PSP, from 2013.

Blockchain analytics companies

- CipherTrace, now owned by Mastercard since Sep 9, 2021.
- Chainalysis

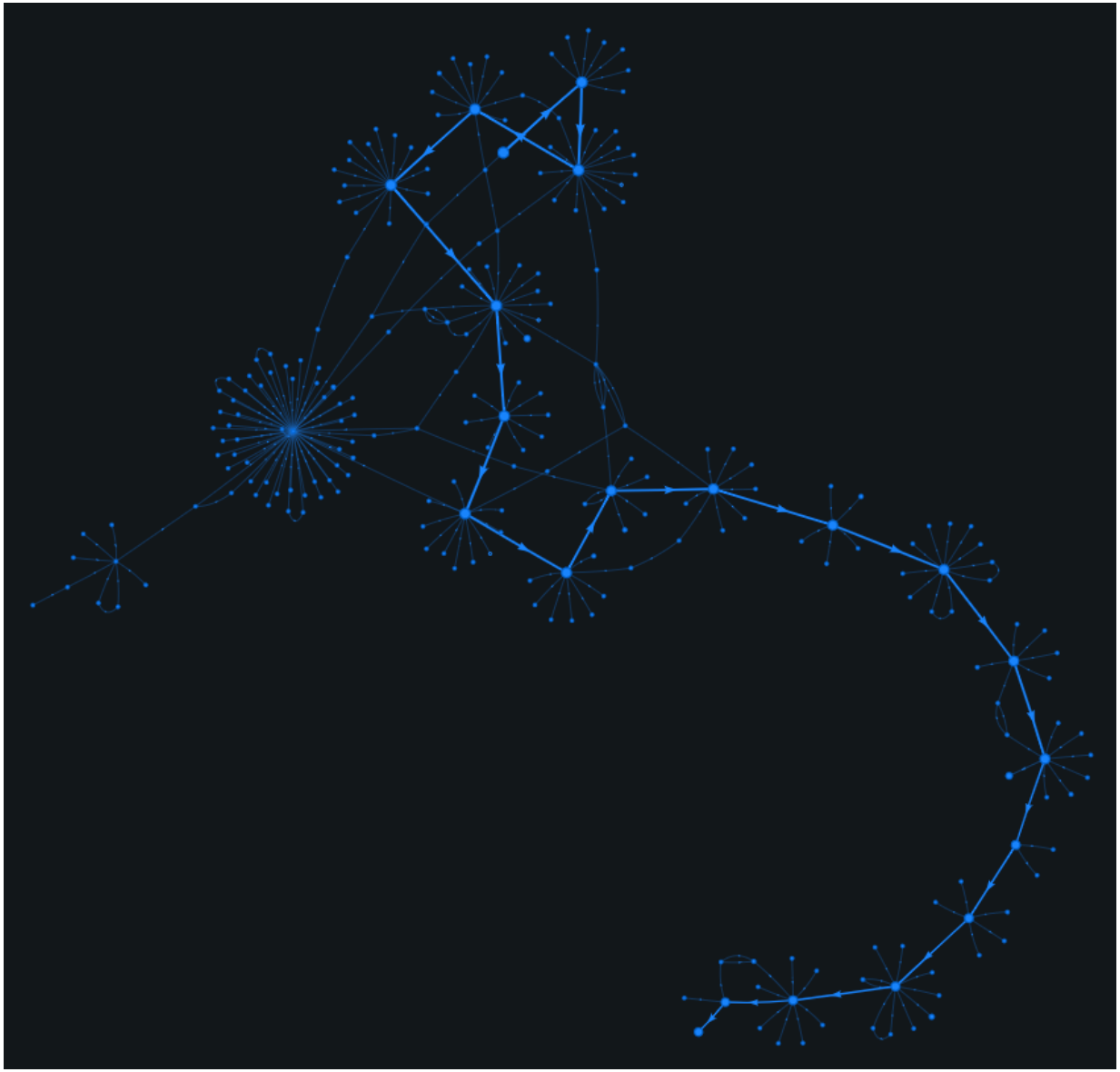


Bitcoin average transaction



- Alice's address is well known.
- Bobs's address is well known.
- The amount sent is public.
- Fee = sum(inputs) - sum(outputs), *not fixed*.
- N(outputs) is well known.

Bitcoin and privacy don't go together



Bitcoiners pay more and wait hours for privacy

Coinjoin (*trustless* version to centralized mixing services)

Combining outputs and inputs into a single transaction to make it difficult to determine which spender paid which recipients.

- Minimum an hour to *coinjoin*, can be a day.
- After mixing, it is recommended to do another mix.
- All potential metadata as addresses and amount is still public.
- Average fee for the service is not less than 0.15%.
- Huge size of a transaction = higher mining fee.
- Change tx is not recommended or not allowed.
- Difficult to use, no *incentives* to do so.
- Mixed txs can be marked as *stolen* by chain analysis.
- Low anonimity set per transaction, not network-wide.

Built-in mixing in Dash, still not private by default

PrivateSend (Coinjoin)

Built in Privacy feature that allows mixing coins with other anonymous people on the network.

- Nobody is using it.
- Only available in Dash Core wallet.
- False assumptions about privacy.

Dark web uses Monero

Optional privacy $\rightarrow$ 3 min ring size $\rightarrow$ 5 minimum $\rightarrow$ 7 $\rightarrow$ 11 for all

Ring Signatures is a group of signatures with at least one real participant.
RingCT hides the amount exchanged.
Stealth Addresses is a one-time address for every tx.

- Zero-decoy and chain reactions.
- Chain splits and key image reuse attack.
- Input selection algorithm.

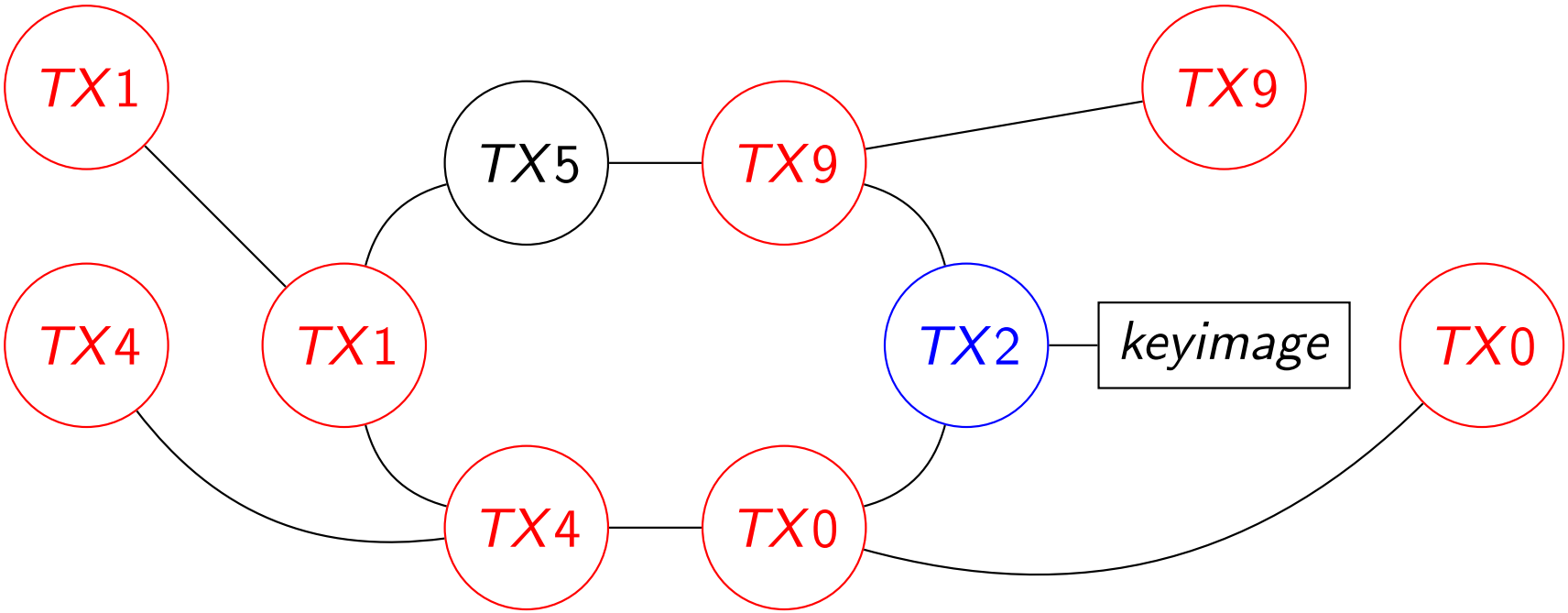
How to fix?

The ring size increase.

- Verification time.
- Transaction size.

Zero-decoy and chain reactions

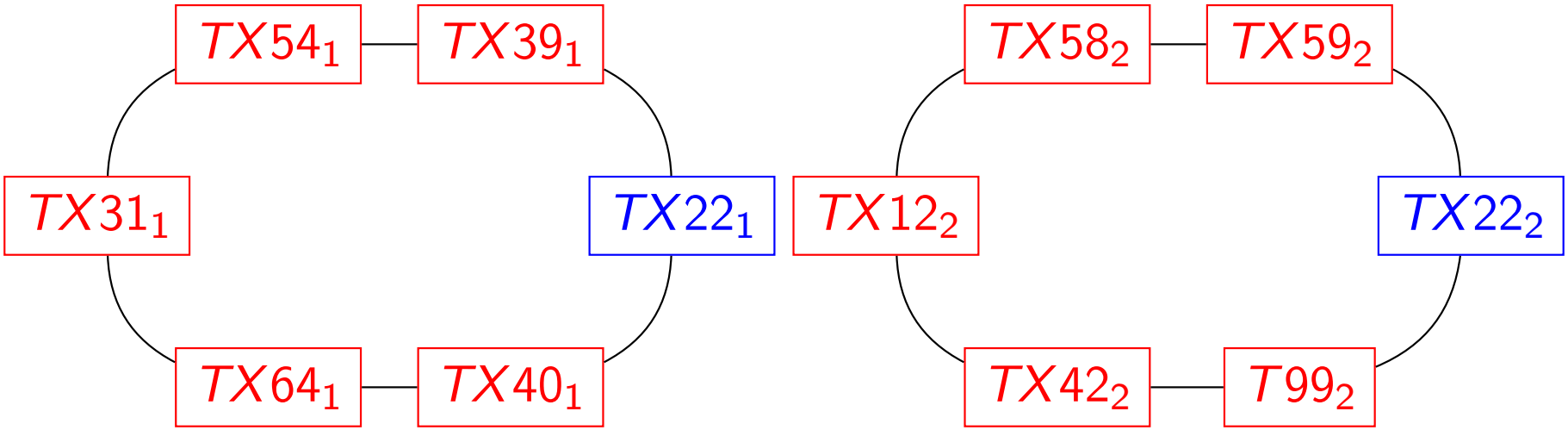
- TX2 is the output that we control and want to spend.
- We do not control other outputs, called decoys.



- 0-decoy txs (spent output) reduced the privacy for RS=3, 5, 7 and 11.
- The anonset decreases over time once the decoys were compromised.
- TX2 will decrease the privacy for other txs.

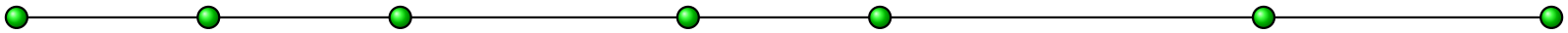
Chain splits and key image reuse attack

- Airdrops and forks stimulate the deanonymization
- Same key image use on both chains is not a good idea



Input selection algorithm

- The actual output that was spent is usually the most recent one.
- Decoys are most likely will be *behind*.



Significant decoy selection bug found and persists today

Minimum chance of selecting extremely recent outputs as decoys.

Zero-Knowledge Succinct Non-Interactive Argument of Knowledge

Shielded transactions are fully encrypted on the blockchain.
One can prove possession of certain information without revealing it.

Zcash is not a privacy coin, but has the best technology

- Optional privacy leads to serious consequences.
- 5% of zaddr usage.

Timerange(TX)	t $\rightarrow$ t	t $\rightarrow$ z	z $\rightarrow$ z
Past Hour	265	39	1
Past Day	5183	617	72
Past Week	32357	4372	668
Past Month	133784	19046	2987

Alt-coin traceability by Carnegie Mellon University

Shows that only 0.09% of ZEC txs in a 30-day period were shielded.

Anonymity sets of privacy coins

The anonset is the number of people you are hiding amongst.

anonset(H) = shielded_outputs(H) - shielded_inputs(H)

Name	Anonset	Velocity	At block	Shielded txs
Hush v3	631510	0.977	646229	99%
Piratechain	549337	0.351	1562222	99%
Zcash	187619	0.135	1385202	10%

A shielded transaction is protected by the network-wide anonset

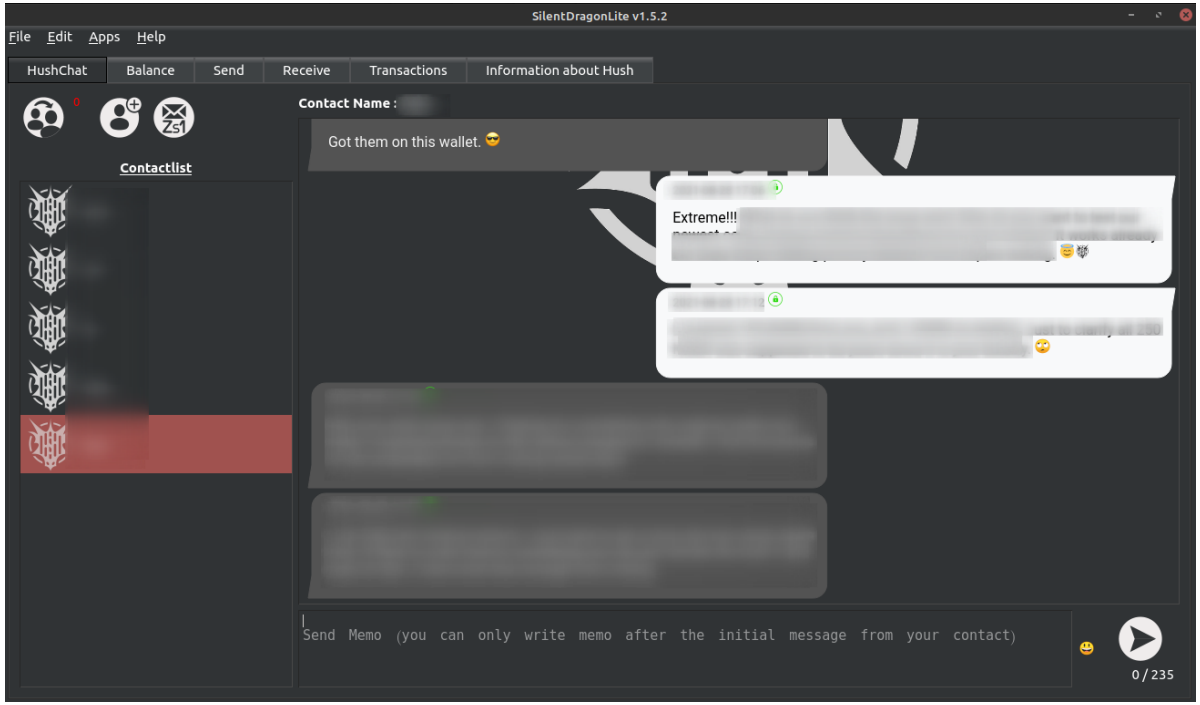
shielded_outputs(H) = number of shielded outputs at height H
shielded_inputs(H) = number of *spent* outputs at height H

- Monero has anonymity set per transaction, so 11.
- Even RS of 1000 cannot provide the same privacy as Zcash Protocol.

Largest anonymity set and anonset velocity

Sietch. Talking to 3 friends is not a problem

Hush *rounds up* the number of outputs to 8.



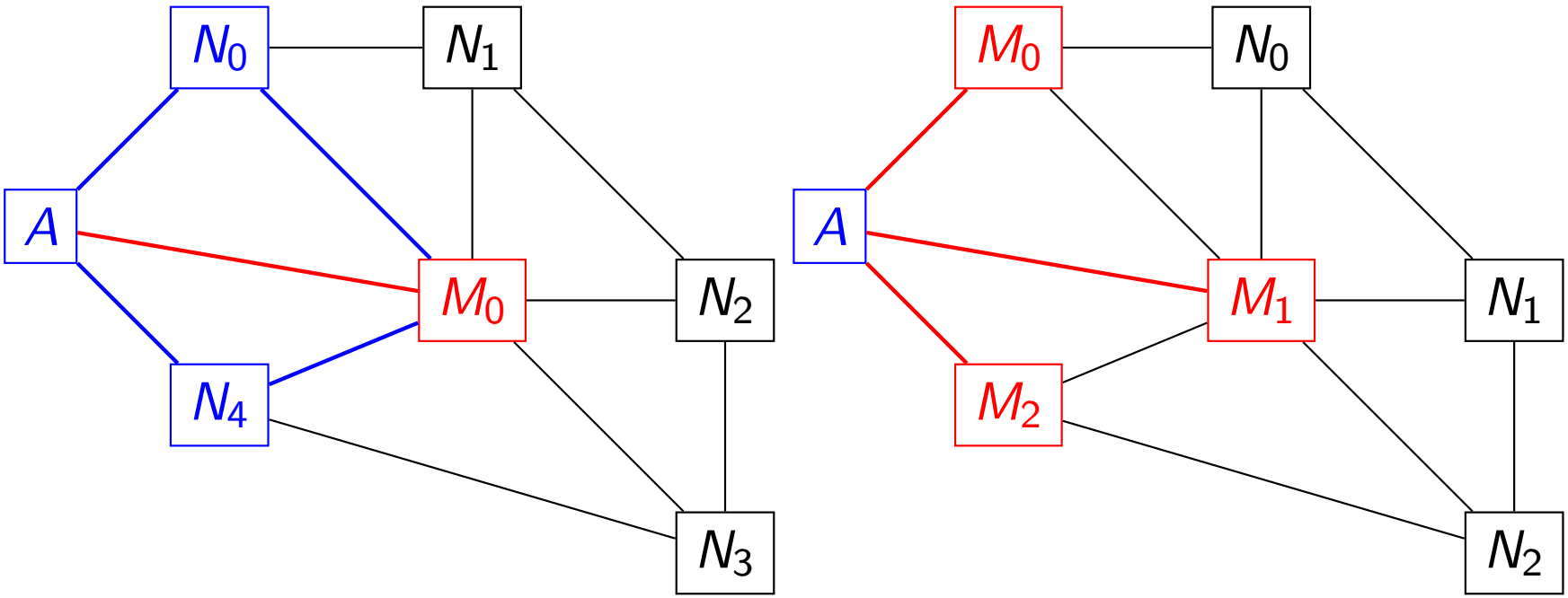
HushChat

Each HushChat memo increases the anonset size by 7.

Peer-to-Peer network anonymity

Public key → Bitcoin address → IP address → ISP → You

A Sybil operator runs multiple nodes to *spy* on newly created transactions.



Required conditions for privacy coins

- Zero-knowledge math instead of obfuscation.
- Privacy by default, z2z txs only.
- Not a company nor foundation.
- Alice's address must be private.
- Bobs's address must be private.
- Encrypted P2P connections, TLS 1.3 only.
- Sybil attack mitigation.
- The number of outputs should be *round up*.

Useful links

- onryo:matrix.lrn.fm
- hush:privacytools.io
- eprint.iacr.org/2020/627.pdf
- monerooutreach.org/breaking-monero
- git.hush.is/hush/anonsets
- oxt.me/graph/transaction/tiid/2830647161