When Tor and Bitcoin meet each other

Alex Biryukov and **Ivan Pustogarov**

London
January 9, 2015

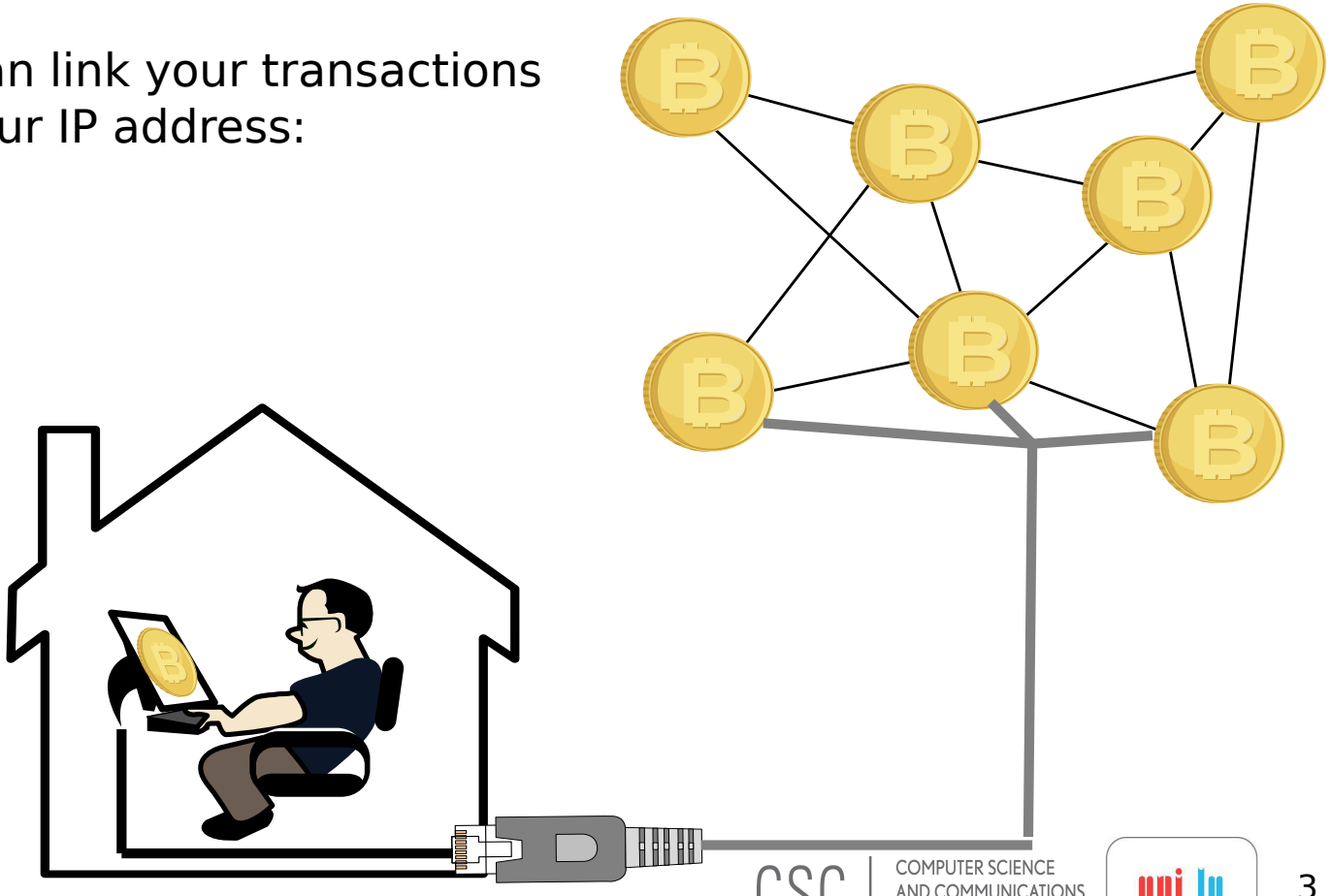
UNIVERSITÉ DU LUXEMBOURG

Outline

- Bad: Bitcoin over Tor isn't a good idea
  http://arxiv.org/abs/1410.6079
- Good: Bitcoin for Tor
  Proof-of-Work as micro-payment
  (to appear at FC 2015)

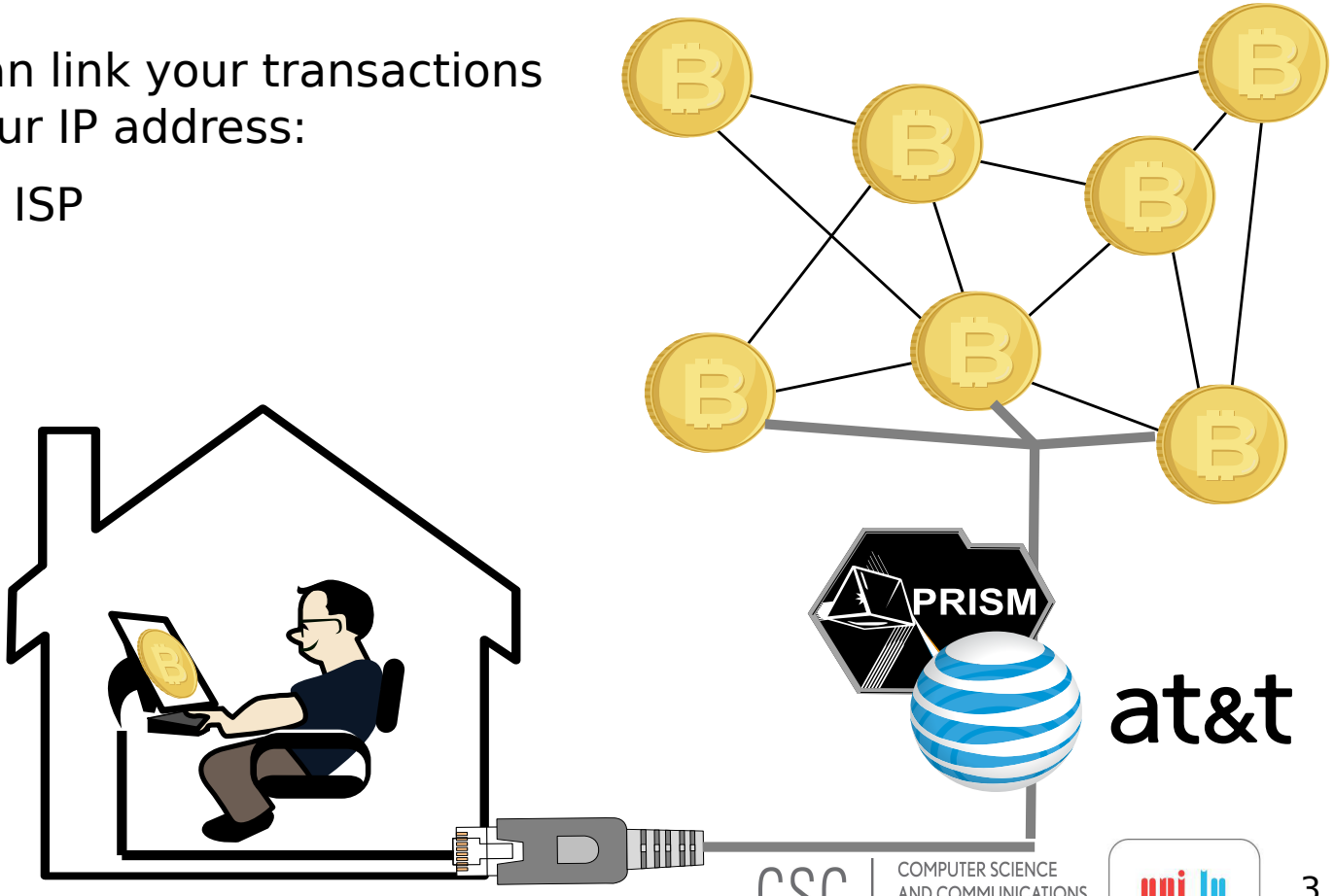
No encryption in Bitcoin

- They can link your transactions with your IP address:



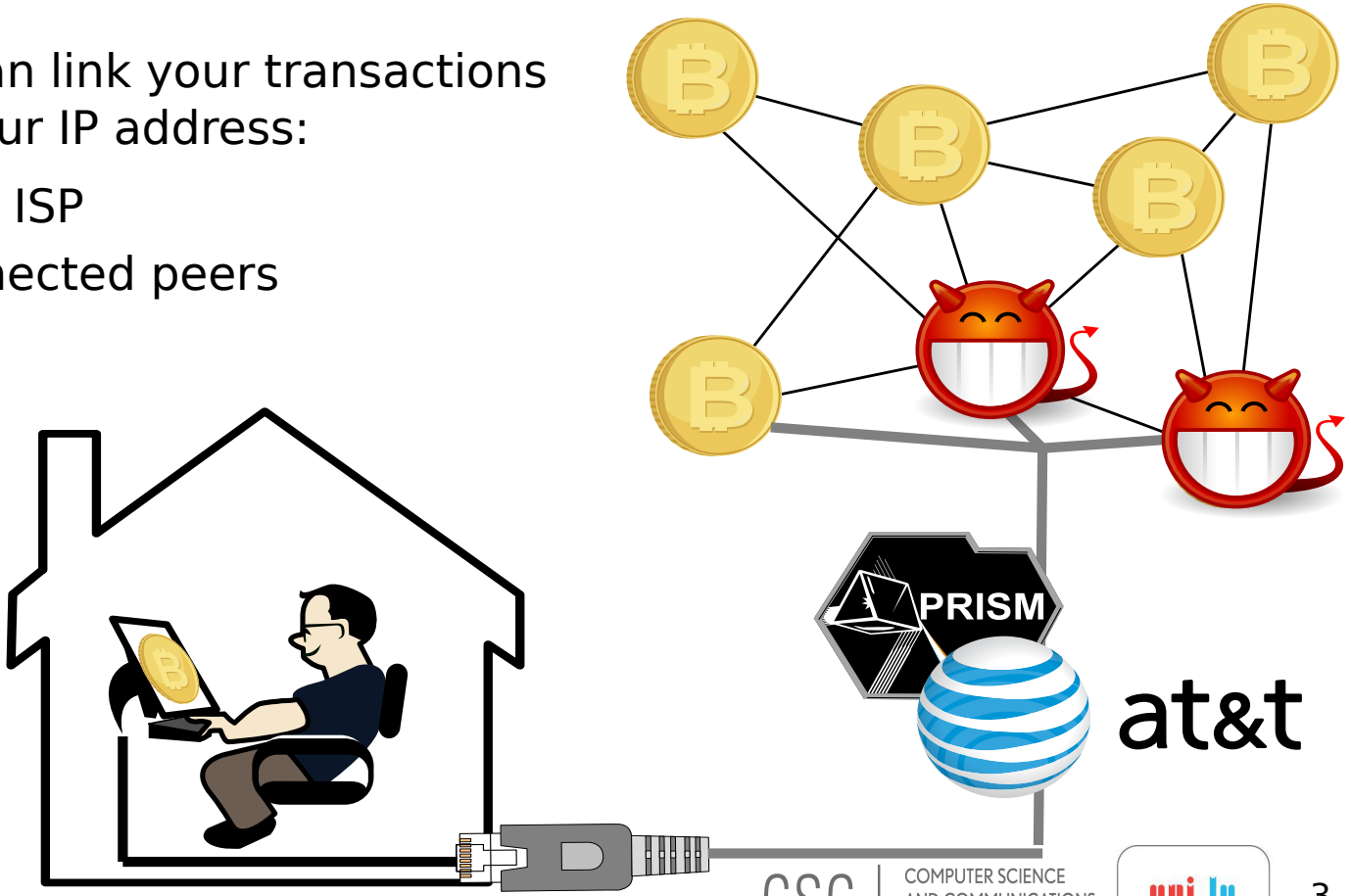
No encryption in Bitcoin

- They can link your transactions with your IP address:
  - NSA, ISP



No encryption in Bitcoin

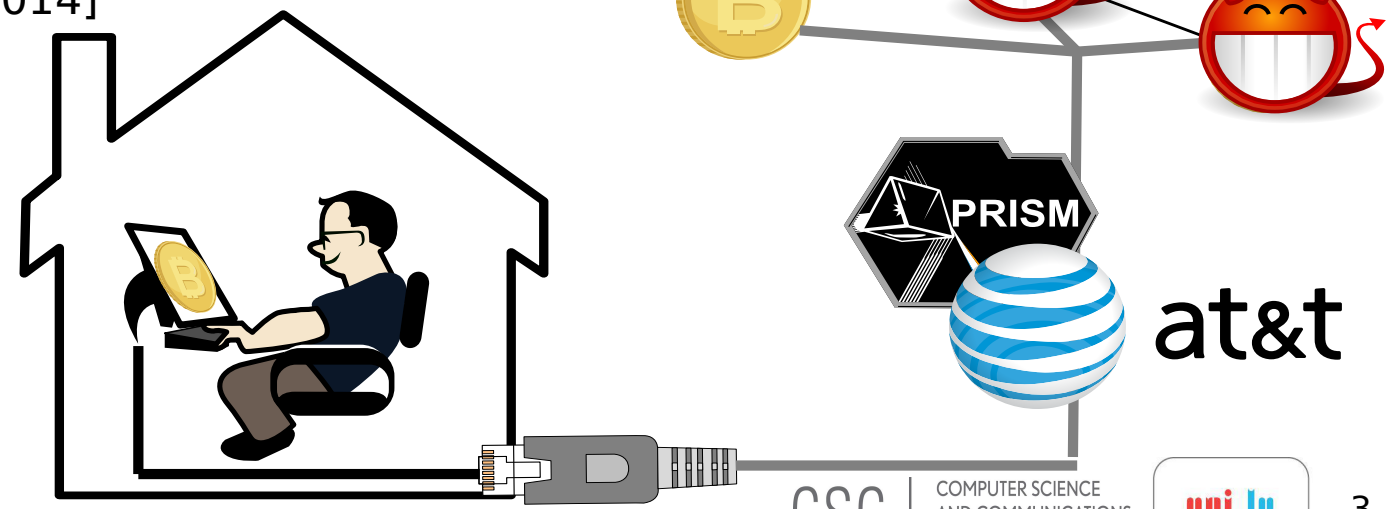
- They can link your transactions with your IP address:
  - NSA, ISP
  - Connected peers



No encryption in Bitcoin

- They can link your transactions with your IP address:
  - NSA, ISP
  - Connected peers
  - Remote Low resource attackers

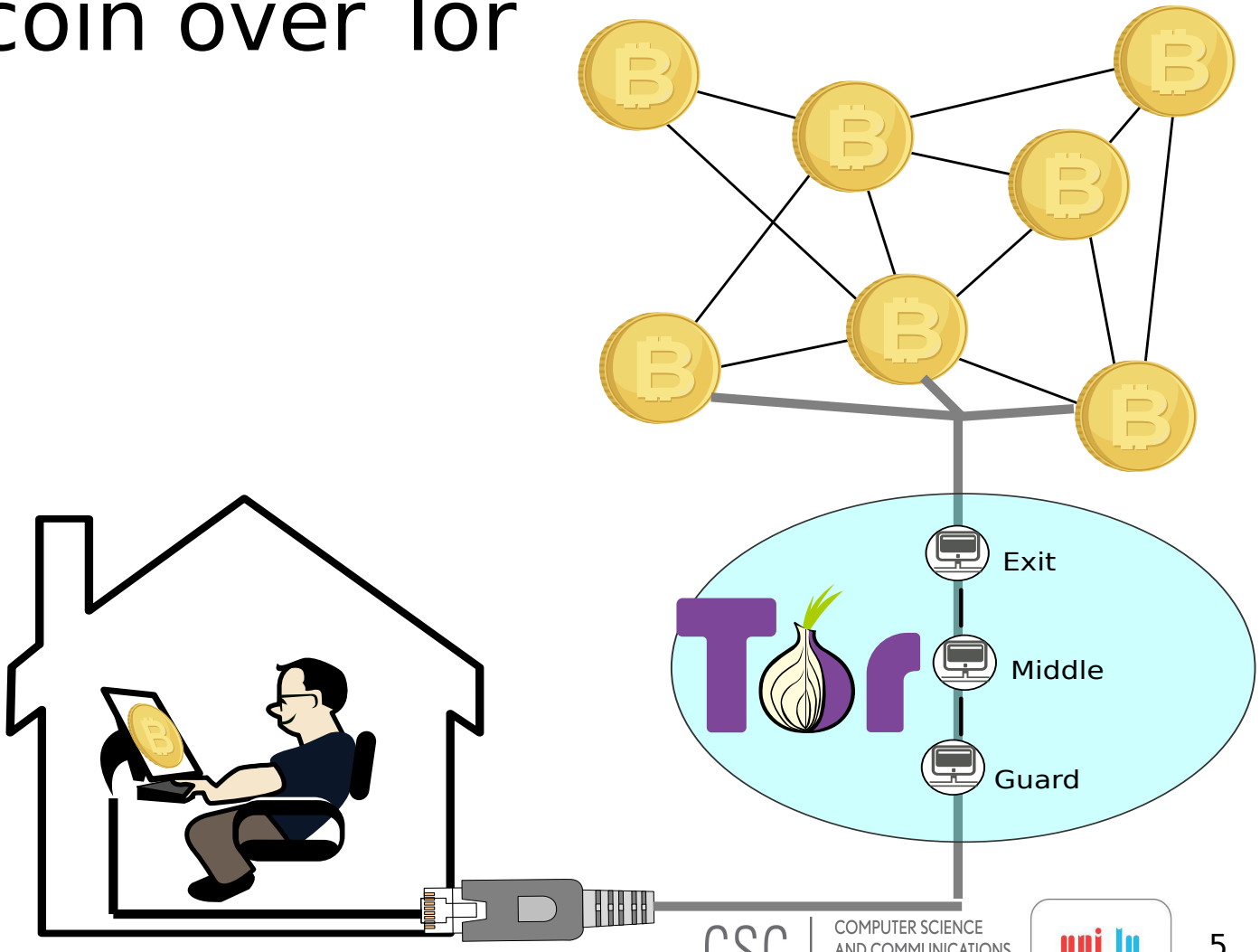
[CCS 2014]



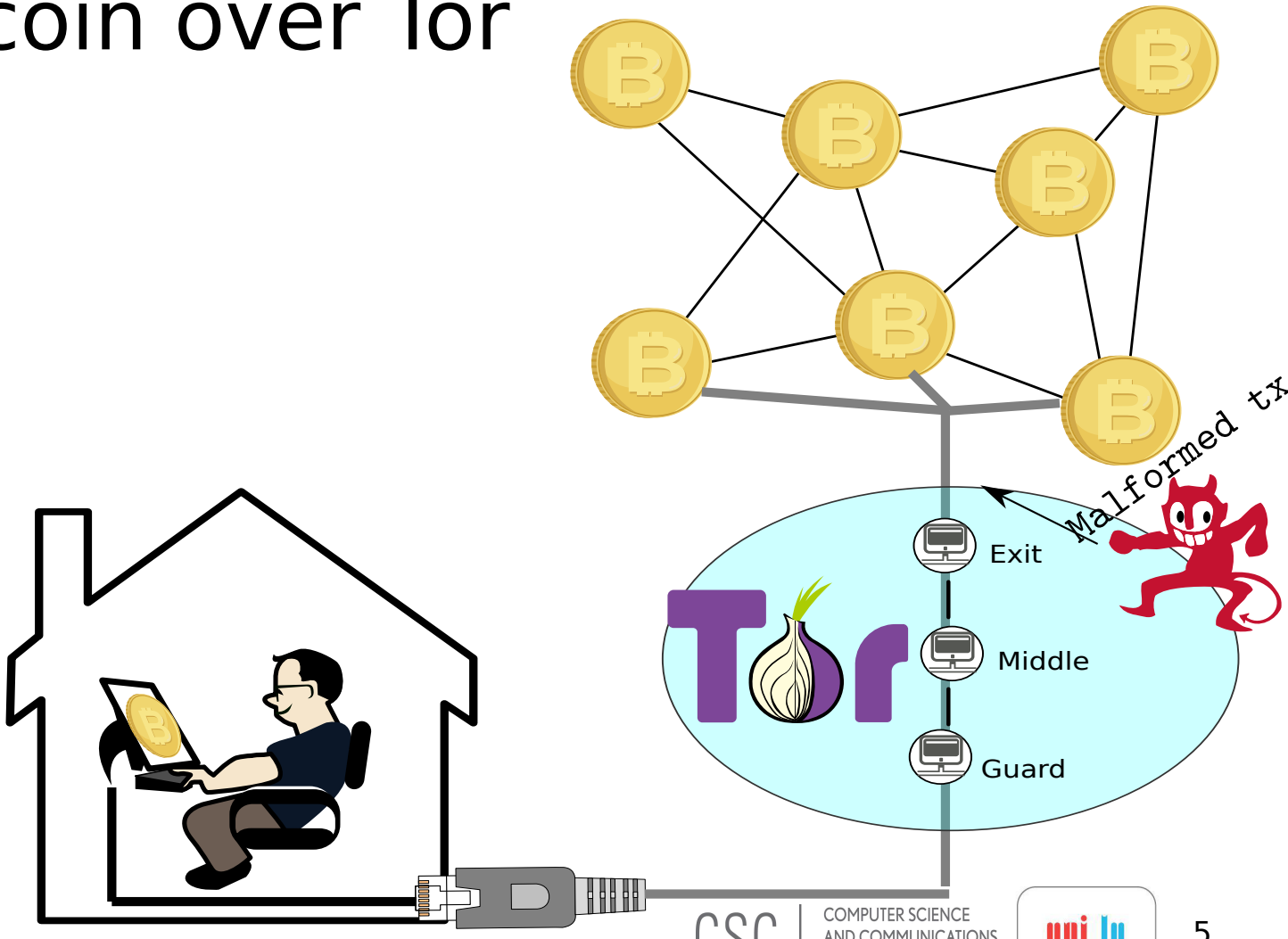
Bitcoin over Tor

- The recommended (by bitcoin.org) way to avoid IP leakage is to use Tor
- SVP clients are bundle with Tor (to avoid spoofing, e.g. when connecting through a public WiFi)

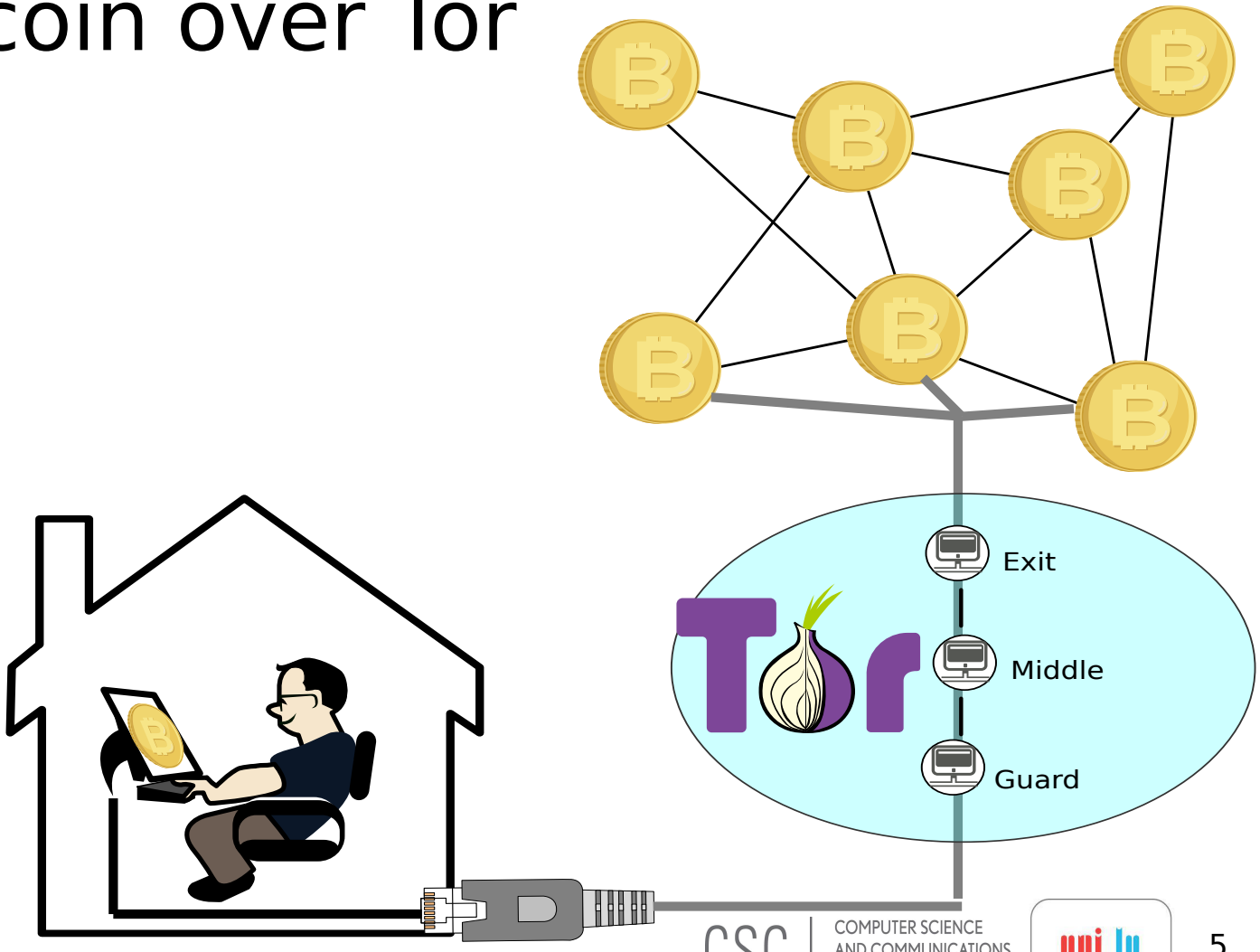
Bitcoin over Tor



Bitcoin over Tor

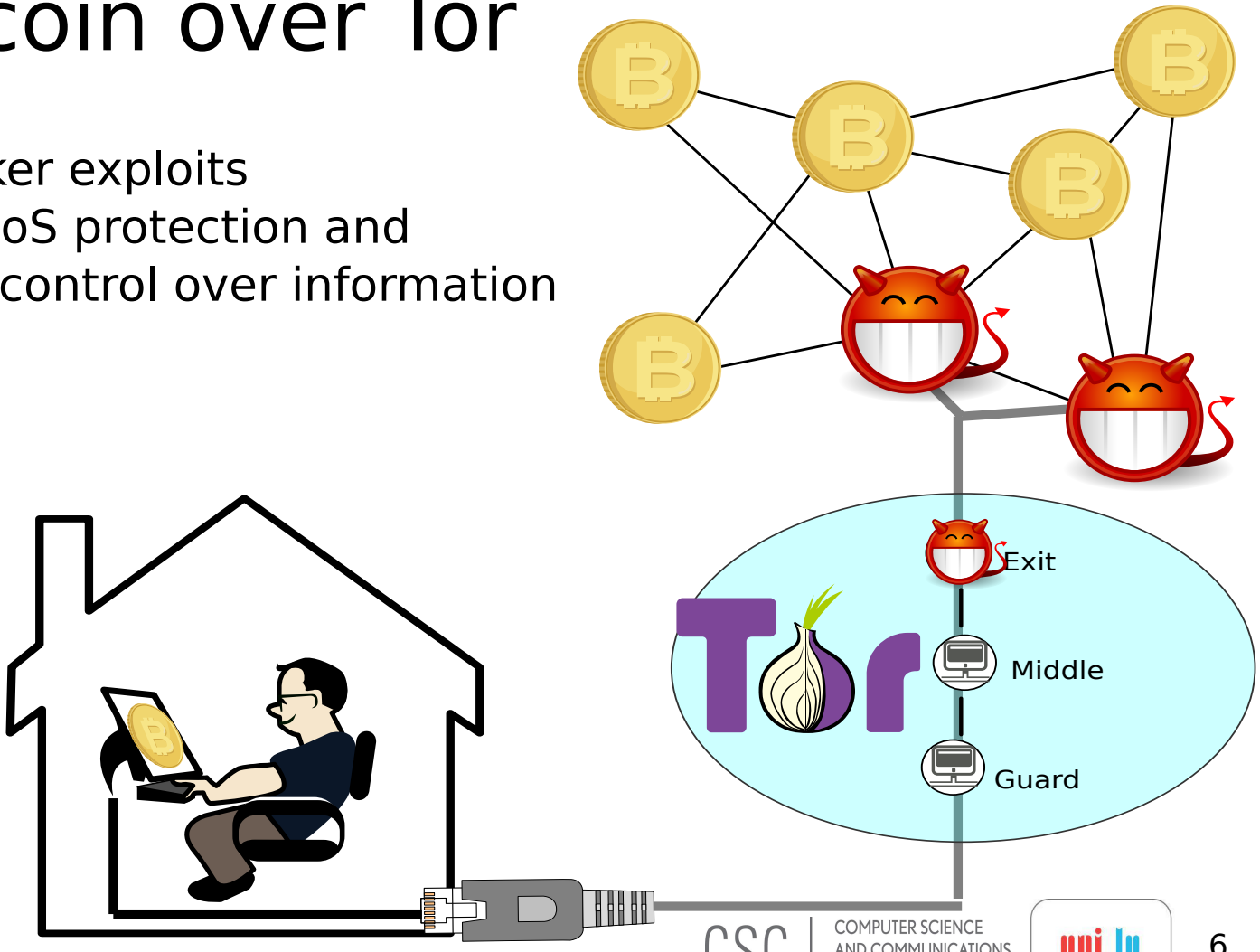


Bitcoin over Tor



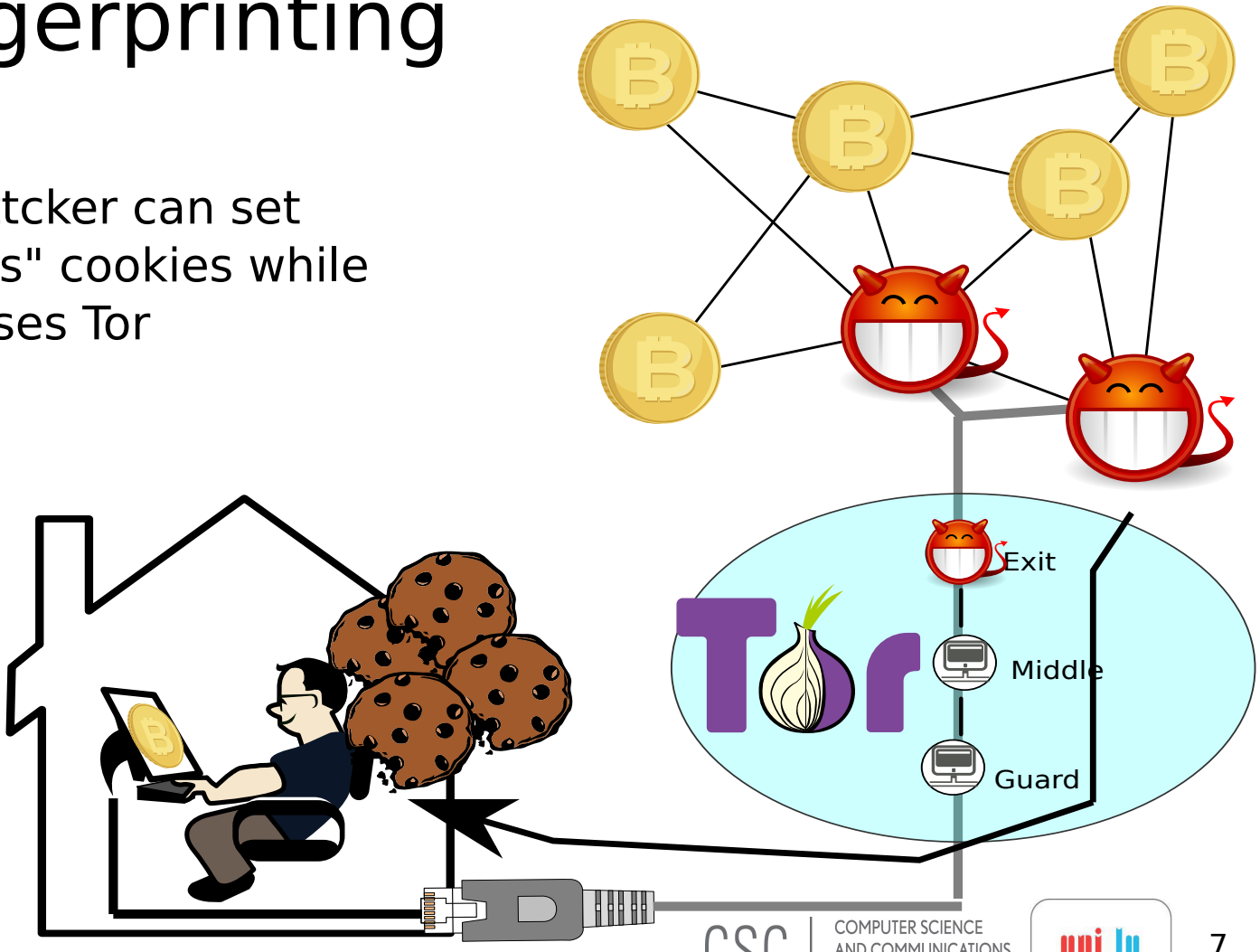
Bitcoin over Tor

1. Attacker exploits anti-DoS protection and gains control over information flows



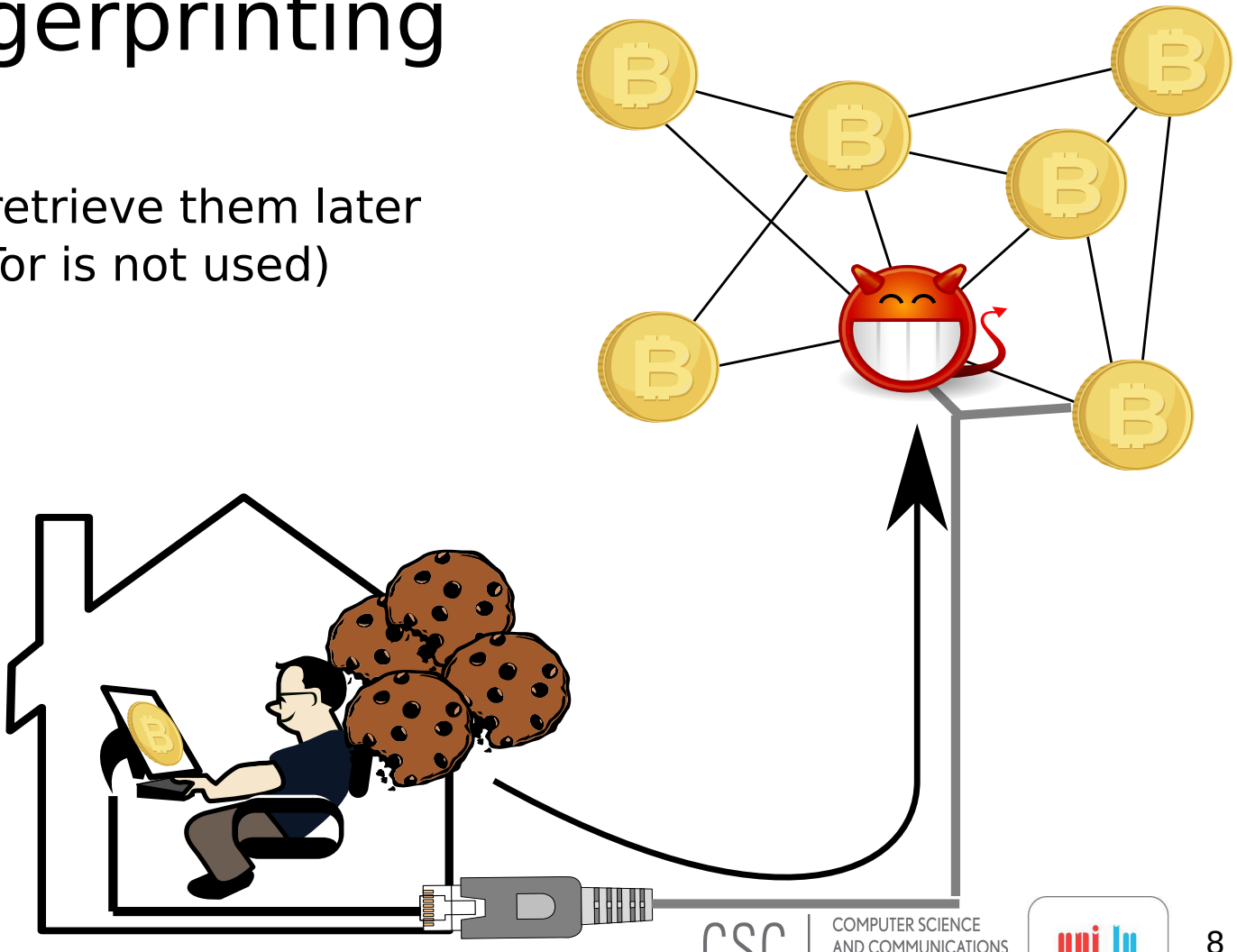
Fingerprinting

2. An attcker can set "address" cookies while client uses Tor



Fingerprinting

2. And retrieve them later
(when Tor is not used)



The good: PoW as payment

Incentivizing Tor relays

- Only limited number of Tor Exit relays provide decent bandwith while client base is large
- Problem 1: Tor users cannot contribute since they are behind NAT
- Problem 2: Many cryptocurrencies are not anonymous which is conflict with Tor goals

Mining pools

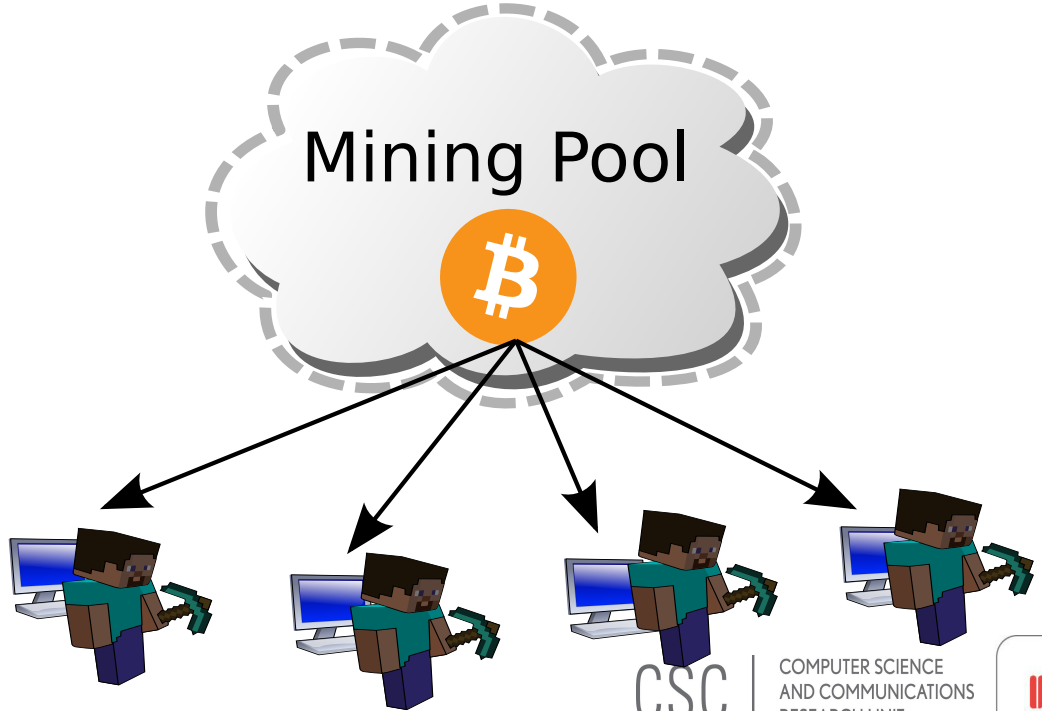
- For miners without powerful dedicated hardware it takes prohibitively long time (years) before they can make a return.

Mining pools

- For miners without powerful dedicated hardware it takes prohibitively long time (years) before they can make a return.

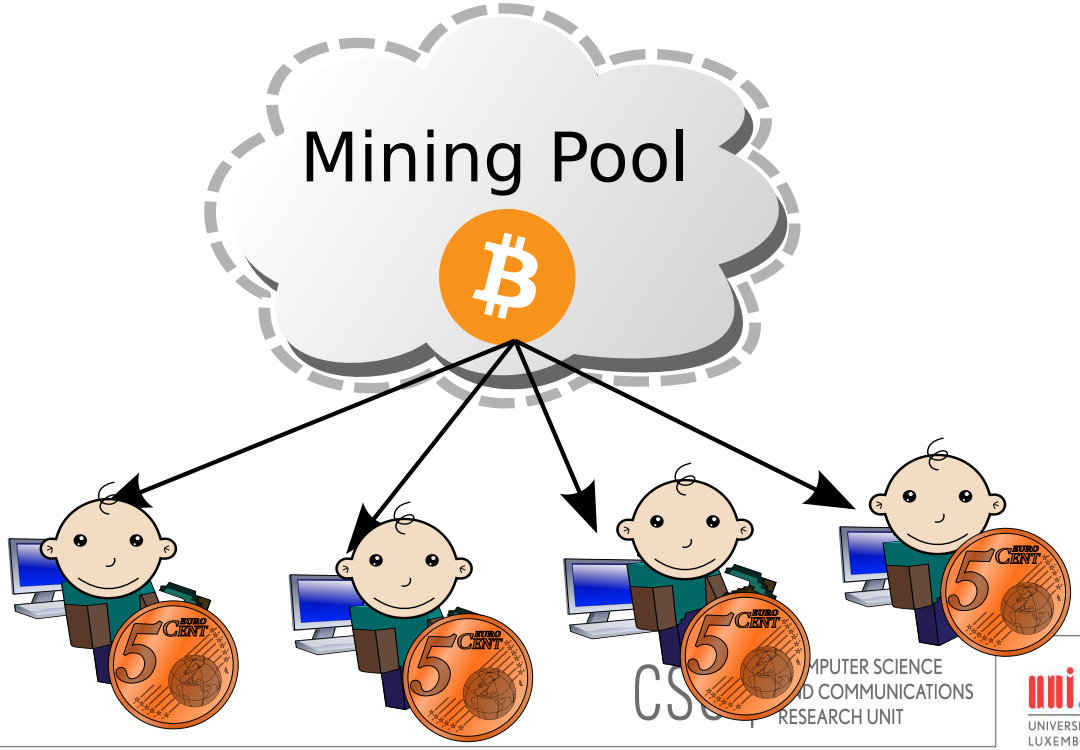
Mining pools

- Participants of a mining pool all together generate blocks much\ faster and receive a portion of the block reward.
- Each miner tries to solve a share.



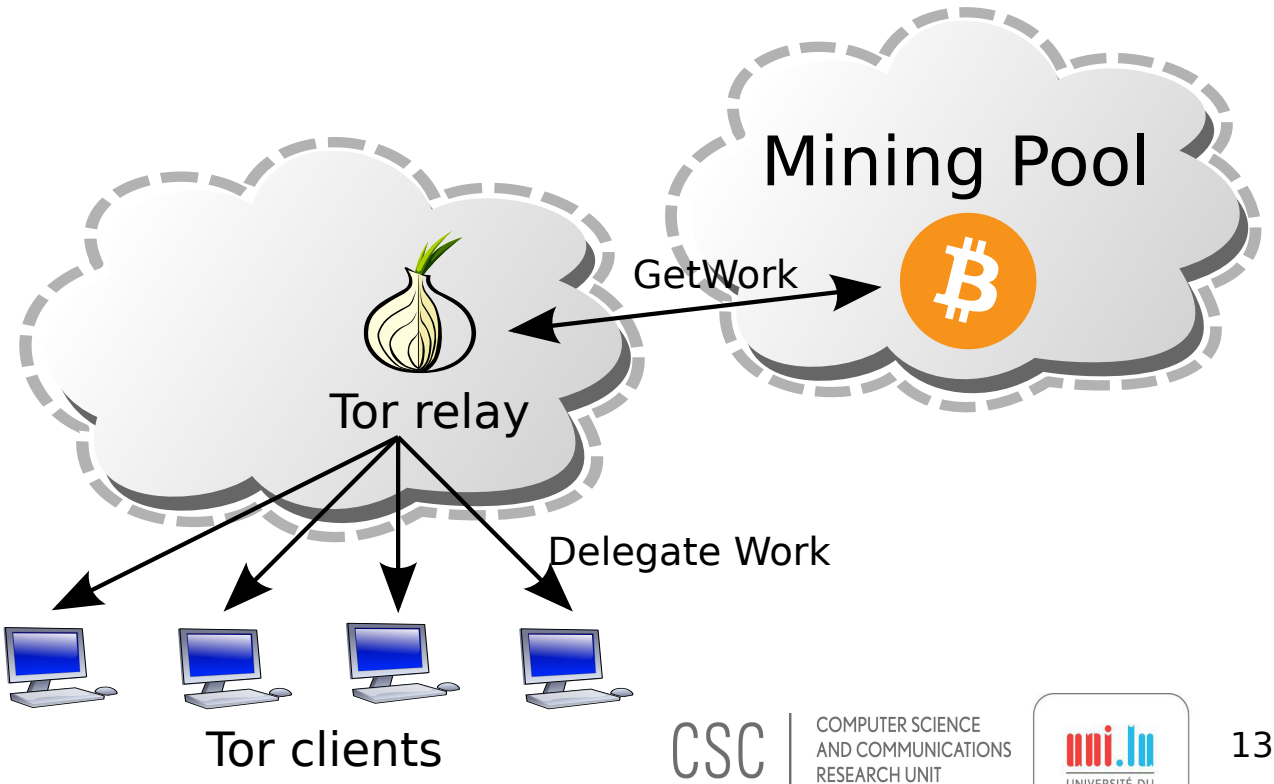
Mining pools

- Participants of a mining pool all together generate blocks much\ faster and receive a portion of the block reward.
- Each miner tries to solve a share.



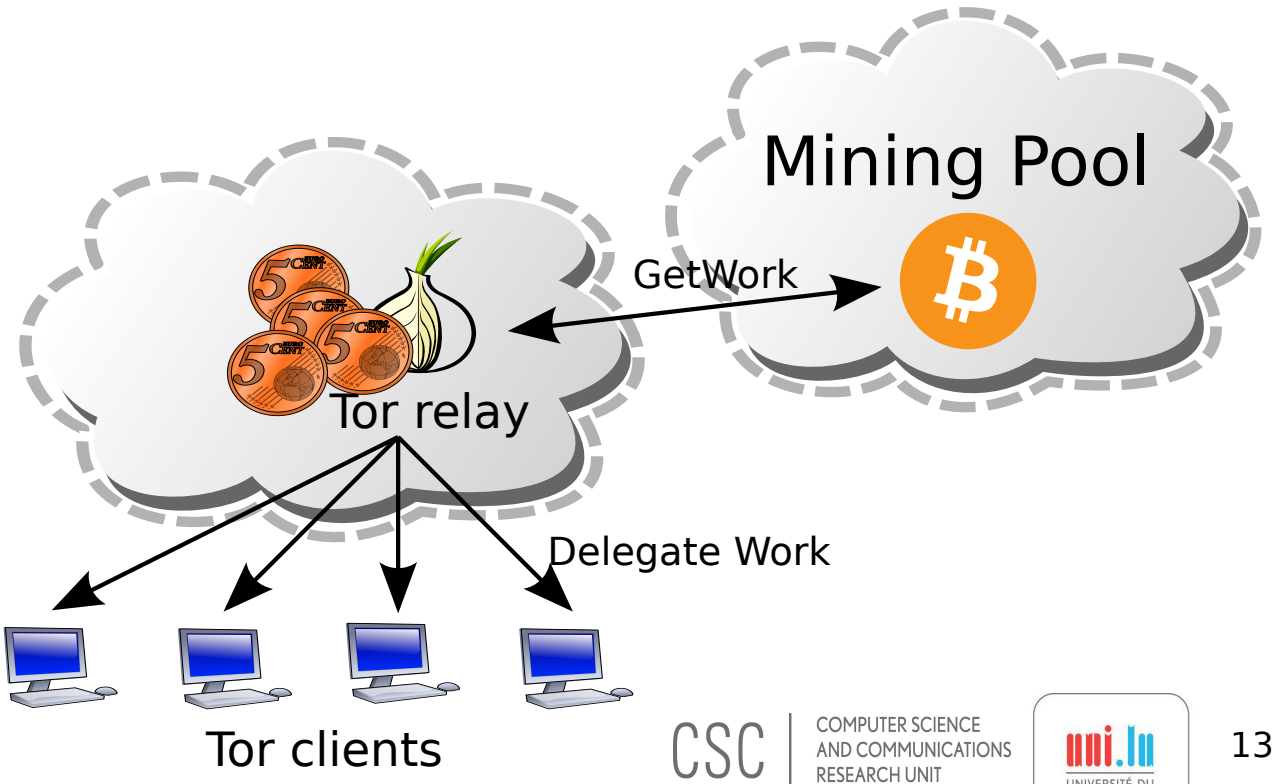
PoW as payment

- Let's add one more level of delegation



PoW as payment

- Let's add one more level of delegation



PoW as payment

- Tor clients do not pay directly but instead help relays to mine crypto-coins.
- Tor relays keep all coins
- Tor relays issus priority tickets in return

Questions?