



# IETF standaarden, implementatie en deployment

Waar is de governance?

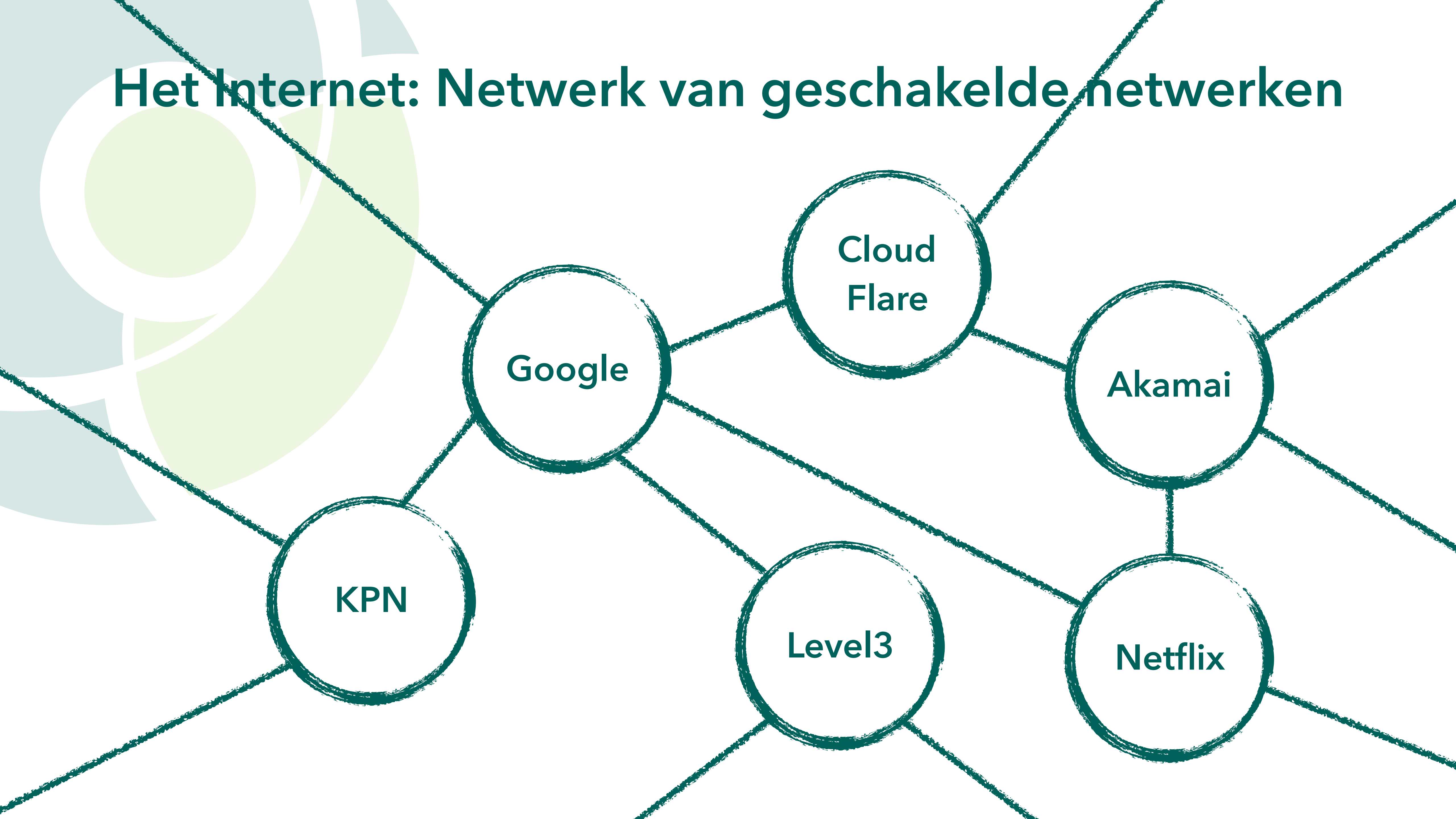
# 10.000 meter overzicht

- Waarom standaarden
- Route 53 hijack: waarom standaarden relevant zijn
- Het proces
  - open standaarden
  - open software
  - “deployment”: gebruik van open standaarden en open software

# Standaardisatie van Internetprotocollen

- Internet: netwerk van geschakelde netwerken
- Samenwerking tussen netwerken
  - naming: hoe benoem je diensten/services/... (DNS)
  - numbers: IPv4/IPv6 adressen etc.
  - routing: hoe bereik je de service
- Standaarden zijn essentieel om een netwerk van netwerken te realiseren

# Het Internet: Netwerk van geschakelde netwerken



Google

Cloud  
Flare

Akamai

KPN

Level3

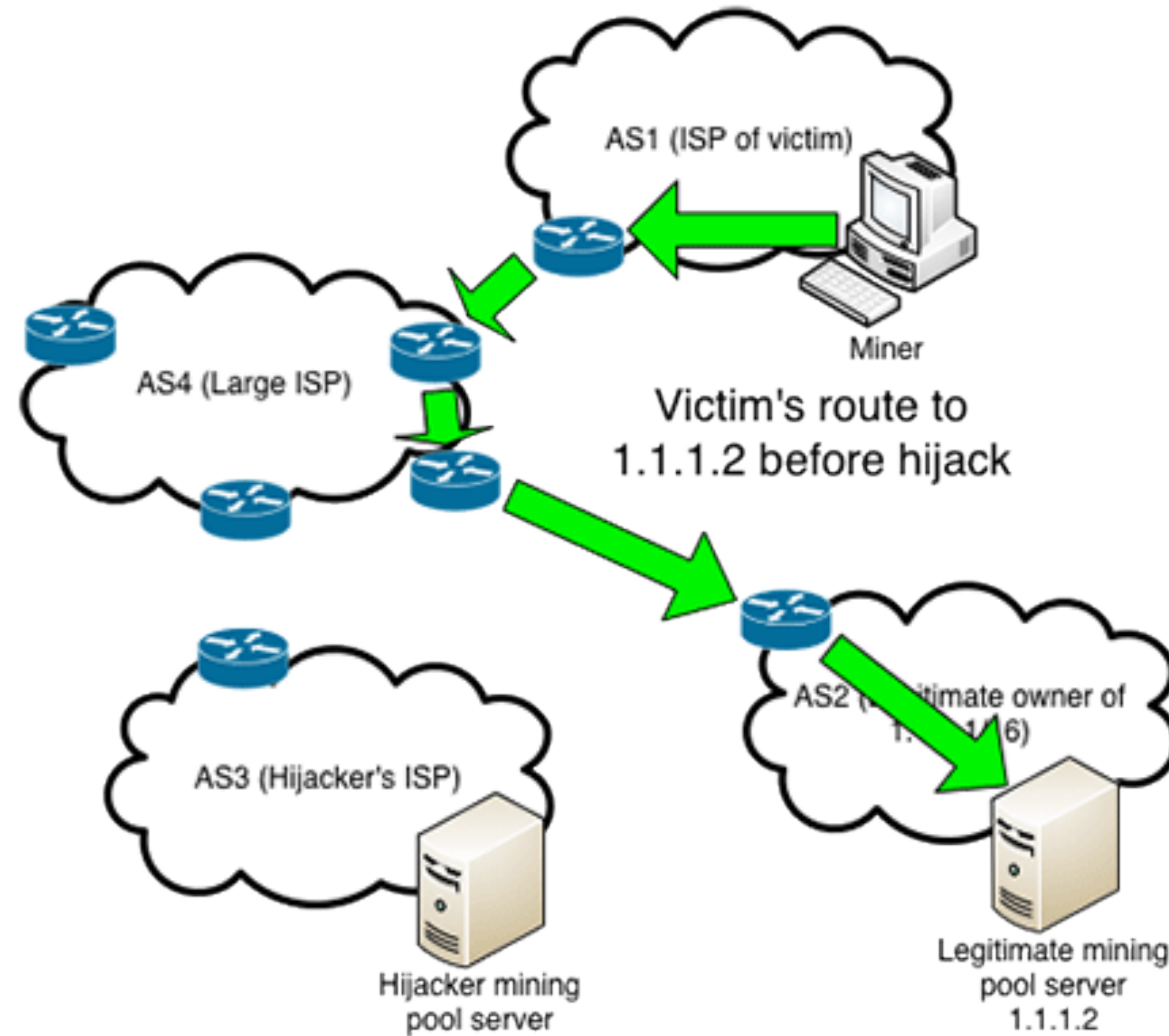
Netflix

# Amazon Route 53 Hijack

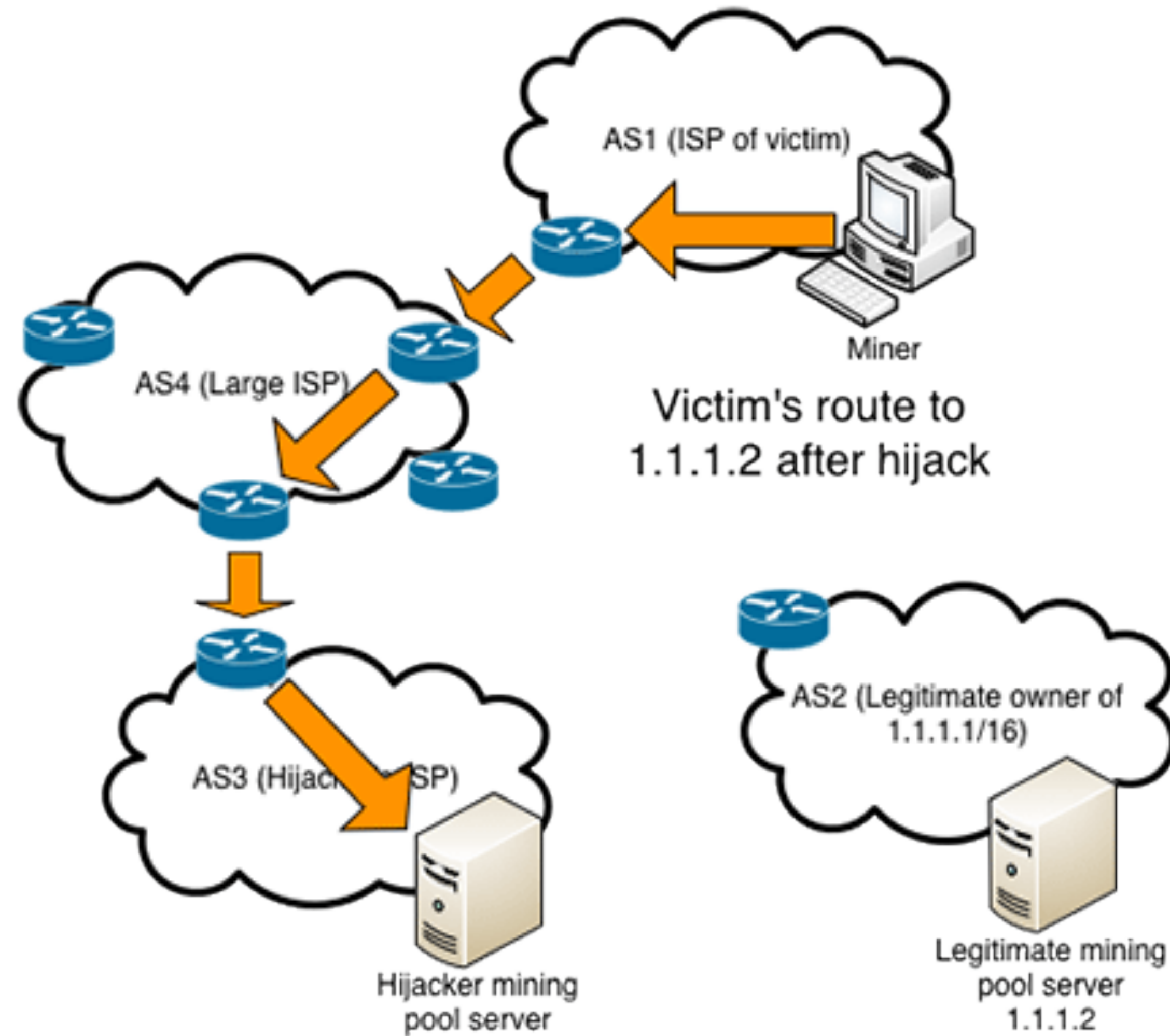
## Route 53 is DNS in the Amazon cloud

- Internet routing "hijack" om bitcoins te stelen
- Internet routing protocol BGP
  - routing protocol uit 1994
  - berekend netwerkbereikbaarheid en neemt routeringsbeslissingen
  - geen security, impliciete trust: "routing by rumour"

# Normale situatie



# Tijdens een route hijack

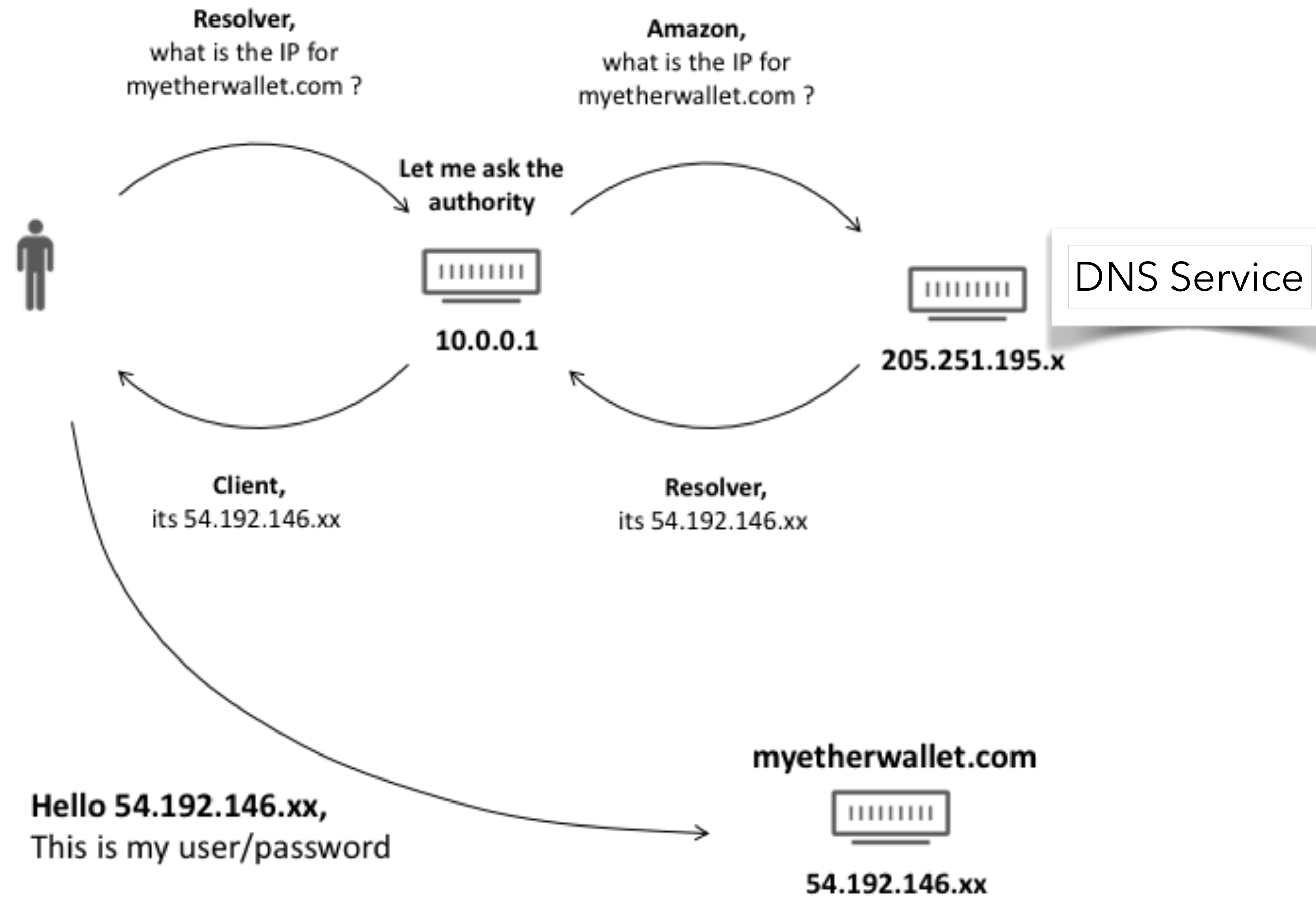


# Tweetraps aanval: DNS spoofing

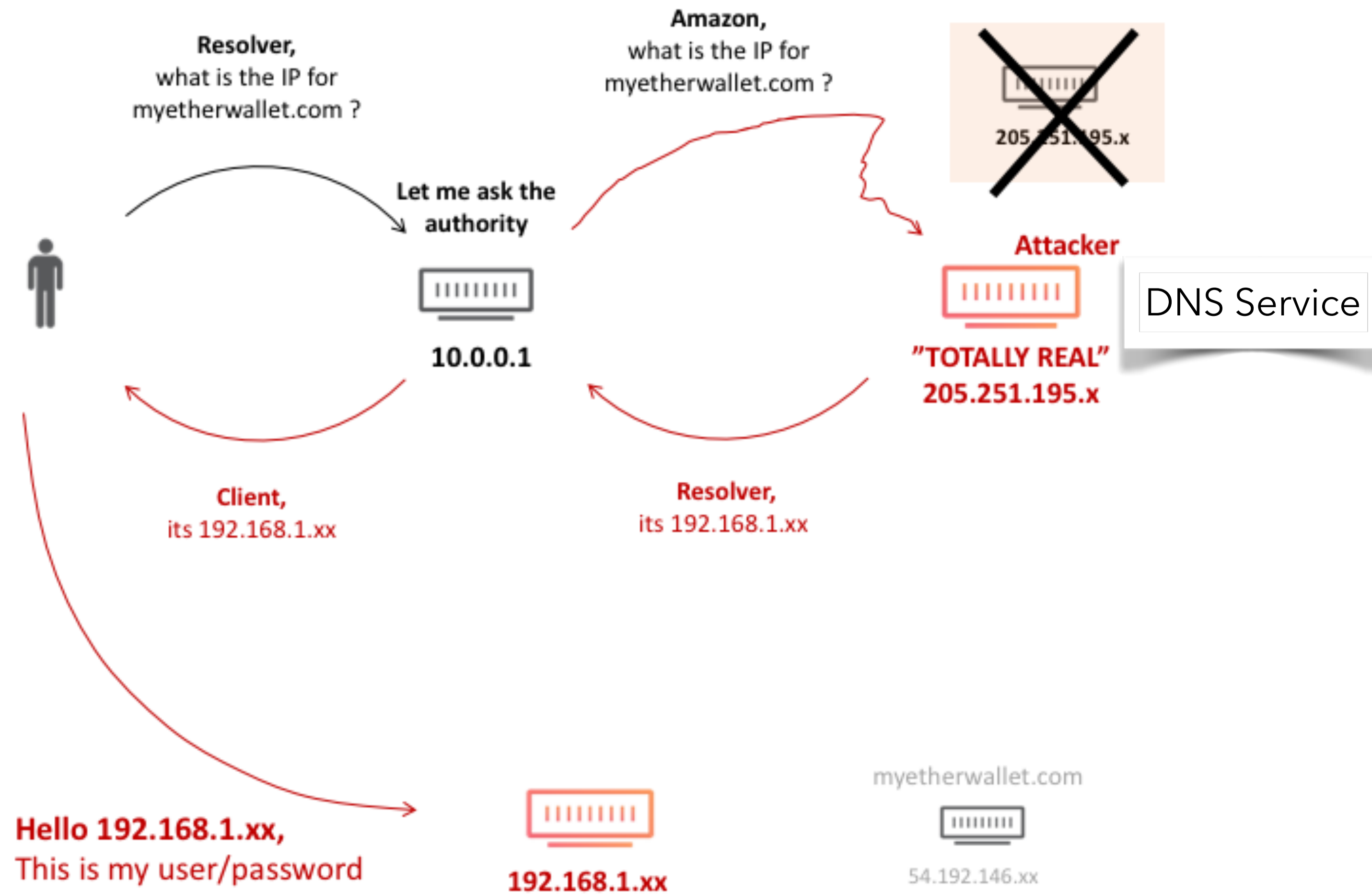
- Intentie van Amazon Route 53 hijack: DNS spoofing
- Valse DNS informatie
  - cryptocurrency digitale portemonnee: [myetherwallet.com](https://myetherwallet.com)
  - geen legitiem antwoord op [myetherwallet.com](https://myetherwallet.com), maar het IP adres van de aanvaller



# Amazon Route 53 DNS in normale situatie



# Amazon Route 53 DNS tijdens de route hijack



# Had dit voorkomen kunnen worden?

Voor dit soort aanvallen: ja

- BGP routing security standaarden
- RPKI: IETF RFC 6480, RFC 6481, RFC 6485-6489, ...
- DNS security standaarden
  - DNSSEC: IETF RFC 4033, RFC 4034, RFC 4035, ...

# IETF standaarden proces

- IETF is een open organisatie om Internet standaarden vast te leggen
  - geen leden of lidmaatschap
  - ieder die deelneemt heeft een gelijke stem in de standaardisatie
  - standaardisatieproces verloopt volgens het "rough consensus" model
  - standaarden (RFCs) zijn zonder kosten te gebruiken
    - intellectual property rights worden in proces meegenomen en vermeld

# Open source software

- Brede beschikbaarheid van open standaarden is essentieel, en open source speelt hierin een belangrijke rol
- Voorbeeld Stichting NLnet Labs: Open Source, Open Standaarden, Open Internet
  - Specialisatie in DNS & Routing: Security, Stability, Privacy
  - Core DNS Producten: NSD, Unbound, OpenDNSSEC
  - *Nieuw*: RPKI Routing security toolset
- Diensten: [internet.nl](https://internet.nl) – test op veilige, moderne Internetstandaarden

# Operationele implementatie van standaarden

- Waarom zijn de BGP en DNS security standaarden nog niet (breed) toegepast?
  - standaarden nog niet algemeen bekend (geaccepteerd als oplossing)?
  - operationele kosten en complexiteit?
- Stimulansen (prikkel) om toepassing te bevorderen
  - verantwoordelijkheidsgevoel ("good netizen") en reputatie
  - economische motivatie
  - of beleid (governance)?