Escaping the Ossification Trap with GNUnet

Christian Grothoff

BFH & The GNU Project

25.1.2018

“We shape our tools, and thereafter our tools shape us”. –John Culkin
What can be done?
Regulation?

- Charles Stross (@34c4) warns: Companies are AIs that develop faster than the law
- Julia Reda (@IGF) warns: Regulation of platforms paradoxically can give them more power
Regulation?

- Charles Stross (@34c4) warns: Companies are AIs that develop faster than the law
- Julia Reda (@IGF) warns: Regulation of platforms paradoxically can give them more power
- Democracies are slow

⇒ Effective regulation of mega-corporations exists only under dictatorships

Dictatorship or Corpocracy?
Better Technology!

Data protection!

Decentralization!

Self-Organization!
CASH
Attention! What happened?

Your personal files are encrypted by **CTB-Locker**. Your scripts, documents, photos, databases and other important files have been encrypted with strongest encryption algorithm AES-256 and unique key, generated for this site.

Decryption key is stored on a secret Internet server and **nobody** can decrypt your files until you pay and obtain the decryption key.

Learn more about the algorithm can be here: [Wikipedia](https://en.wikipedia.org/wiki/Ransomware)

**Fbi’s advice on cryptolocker just pay the ransom**

What to do?

We created for you this bitcoin address: **1KMGFNg7XQPmTuucYe4uTCpYwh9cypHh5**

**What is a Bitcoin address?**
Technological impact assessment!\textsuperscript{1}

\textsuperscript{1}Difficult, but better than design-by-buzzword!
Technological impact assessment case-study: Name systems
RAINS

- **NS**: Delegation record in RAINS (with zone key)
- **A**: IPv4 address record
- **S_K(V)**: Signature with key K over value(s) V
- **QS_{44}**: Key of (anycasted) query service in ISD 44
- **TRC_{44}**: Trusted root configuration of ISD 44
- **RZK_{44}**: Root zone key of ISD 44
- **ZK_{name}**: Zone key of authority for “name”
Namecoin

Namecoin Client

Local Copy of Block Chain

P2P Network

Append registration to block chain

Get copy of block chain
The GNU Name System (GNS)
But you cannot change DNS!
In a peer-to-peer network nodes interact as equals.
Peer-to-Peer Network Classification

- What is the network designed to achieve?
- Do some peers have privileged or special roles?
- Can new nodes freely join?
Peer-to-Peer Networks

The Internet Protocol (IP) is a peer-to-peer protocol.
Peer-to-Peer Networks

The Internet Protocol (IP) is a peer-to-peer protocol.

Underlay P2P networks

- 802.11s
- Freifunk (B.A.T.M.A.N)

Overlay P2P networks

- Gnutella / Bittorrent
- Waste
- Freenet / RetroShare / I2P / Tor
- Bitcoin / Altcoins

Full-Stack P2P networks

- GNUnet
## Full Stack

### Internet

<table>
<thead>
<tr>
<th>Google</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS/X.509</td>
</tr>
<tr>
<td>TCP/UDP</td>
</tr>
<tr>
<td>IP/BGP</td>
</tr>
<tr>
<td>Ethernet</td>
</tr>
<tr>
<td>Phys. Layer</td>
</tr>
</tbody>
</table>

### GNUUnet

<table>
<thead>
<tr>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>GNU Name System</td>
</tr>
<tr>
<td>CADET (Axolotl+SCTP)</td>
</tr>
<tr>
<td>$R^5N$ DHT</td>
</tr>
<tr>
<td>CORE (OTR)</td>
</tr>
<tr>
<td>HTTPS/TCP/WLAN/...</td>
</tr>
</tbody>
</table>
## Raised Abstraction Level

<table>
<thead>
<tr>
<th>SecuShare</th>
<th>$p\equiv p$</th>
<th>Reuters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Social</td>
<td>Lake</td>
<td>CRDT-Git</td>
<td>IP</td>
</tr>
<tr>
<td>PSYC</td>
<td>GNU Taler</td>
<td>Xolotl</td>
<td>Scalarproduct SMC</td>
</tr>
<tr>
<td>Multicast</td>
<td>Fog-of-Trust</td>
<td>RPS</td>
<td>Set intersection</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GNU Name System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CADET (Axolotl+SCTP)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$R^5N$ DHT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CORE (OTR)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP</td>
<td>WLAN</td>
<td>IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Reality is messy

But this applies to the Internet as well.
Lake
Peers may not be all equal
Challenges

- Lack of business models: no control, no data, no property
- Self-organizing protocols achieving usability and robustness
- Fault-tolerance, scalability and decentralization
- Resource utilization, accounting and privacy
  (⇒ https://taler.net/)
- Public awareness about value of privacy and independence
Ossification

The older the Internet becomes, the harder it is to change!

Evolution can still happen in an overlay network!

It likely is now or never!
Join us and build it!