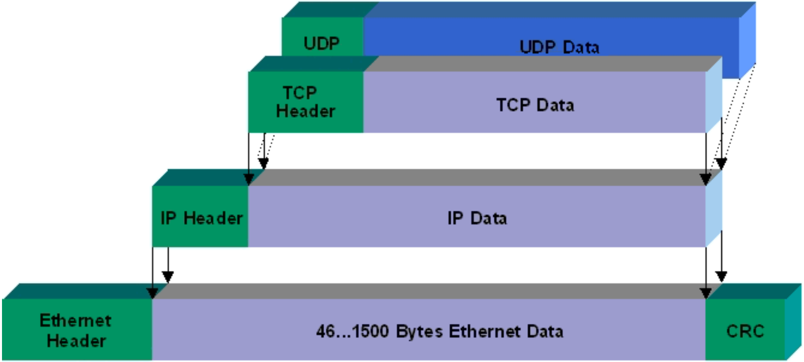
Escaping the Ossification Trap with GNUnet

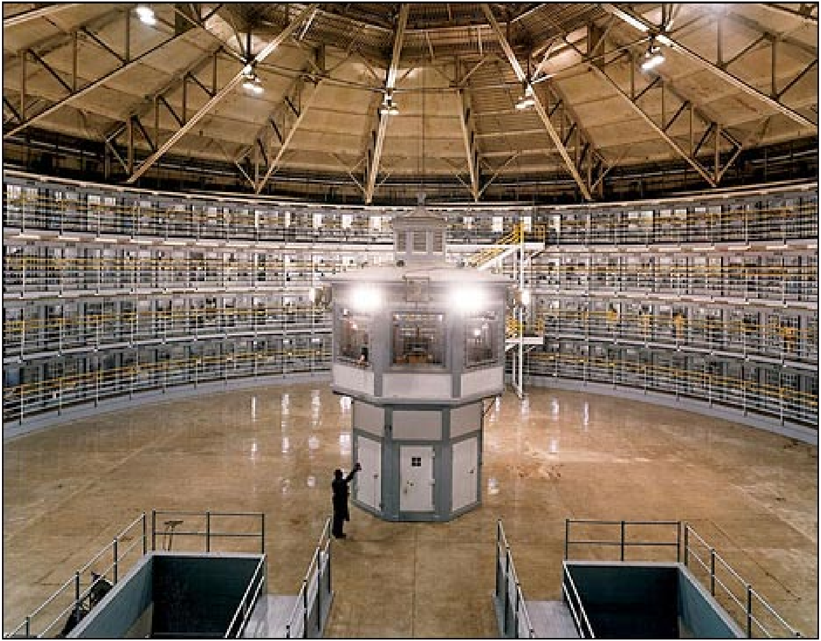
Christian Grothoff

BFH & The GNU Project

25.1.2018

“We shape our tools, and thereafter our tools shape us”. –John Culkin


UDP
UDP Data
TCP Header
TCP Data
IP Header
IP Data
Ethernet Header
46...1500 Bytes Ethernet Data
CRC



doug duBois & jim goldberg NYTImes 9-22-2002

facebook

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?

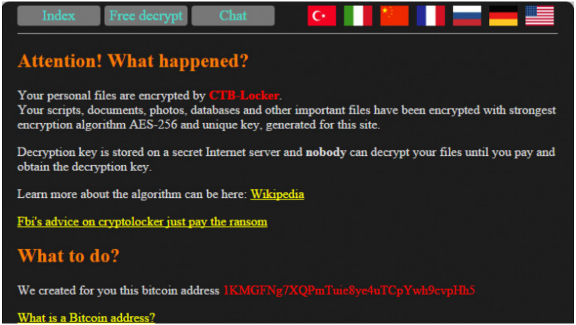
Better Technology!

Data protection!

Decentralization!

Self-Organization!

ZCASH



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

Fbi's advice on cryptolocker just pay the ransom

What to do?

We created for you this bitcoin address 1KMGFNg7XQPmTuie8ye4uTCpYwh9cvpHh5

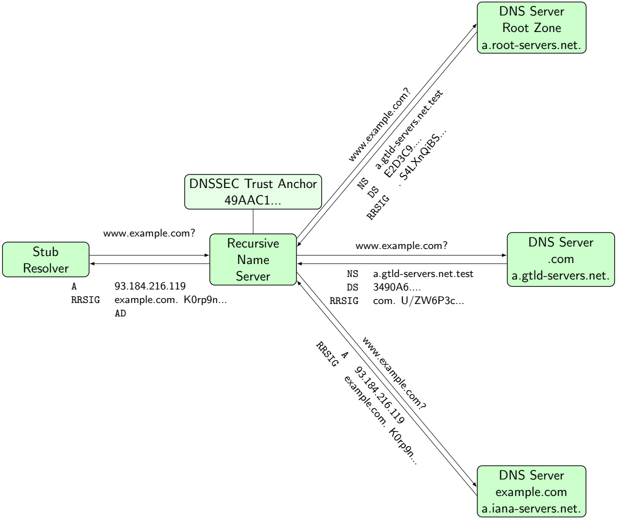
What is a Bitcoin address?

Technological impact assessment![1]

[1] Difficult, but better than design-by-buzzword!

Technological impact assessment case-study: Name systems

DNS/DNSSEC



DNS Server
Root Zone
a.root-servers.net.

www.example.com?

NS a.gtld-servers.net.test
DS E2D3C9....
RRSIG . S4LXnQiBS...

DNSSEC Trust Anchor
49AAC1...

Stub
Resolver

www.example.com?

A 93.184.216.119
RRSIG example.com. K0rp9n...
AD

Recursive
Name
Server

www.example.com?

DNS Server
.com
a.gtld-servers.net.

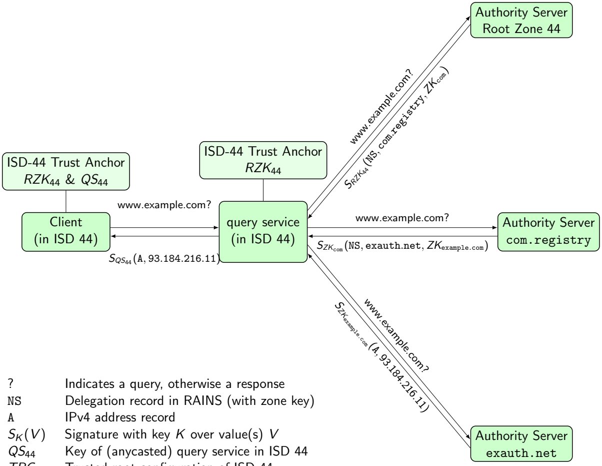
NS a.gtld-servers.net.test
DS 3490A6....
RRSIG com. U/ZW6P3c...

www.example.com?

A 93.184.216.119
RRSIG example.com. K0rp9n...

DNS Server
example.com
a.iana-servers.net.

RAINS



ISD-44 Trust Anchor
RZK_{44} & QS_{44}

Client
(in ISD 44)

www.example.com?

$S_{QS_{44}}(\texttt{A}, 93.184.216.11)$

ISD-44 Trust Anchor
RZK_{44}

query service
(in ISD 44)

www.example.com?

$S_{RZK_{44}}(\texttt{NS}, \texttt{com.registry}, ZK_{\texttt{com}})$

Authority Server
Root Zone 44

www.example.com?

$S_{ZK_{\texttt{com}}}(\texttt{NS}, \texttt{exauth.net}, ZK_{\texttt{example.com}})$

Authority Server
`com.registry`

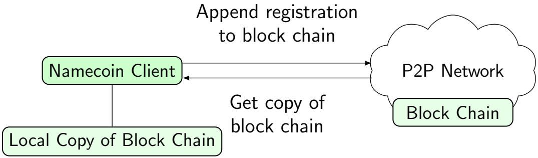
www.example.com?

$S_{ZK_{\texttt{example.com}}}(\texttt{A}, 93.184.216.11)$

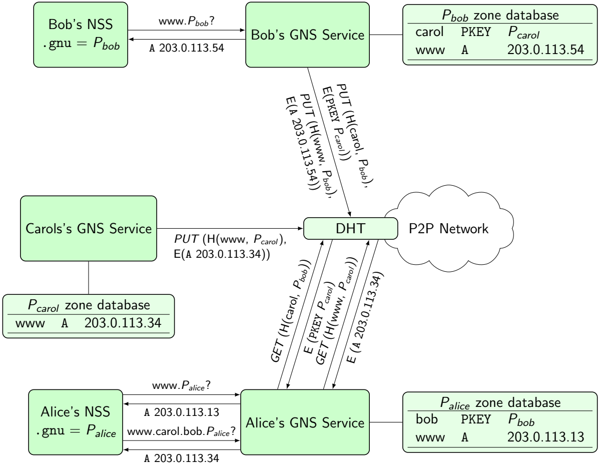
Authority Server
`exauth.net`

?	Indicates a query, otherwise a response
`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


Append registration
to block chain
Namecoin Client
P2P Network
Get copy of
block chain
Block Chain
Local Copy of Block Chain

The GNU Name System (GNS)



P_{bob} zone database

carol	PKEY	P_{carol}
www	A	203.0.113.54

P_{carol} zone database

www	A	203.0.113.34

P_{alice} zone database

bob	PKEY	P_{bob}
www	A	203.0.113.13

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 priviledged 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)

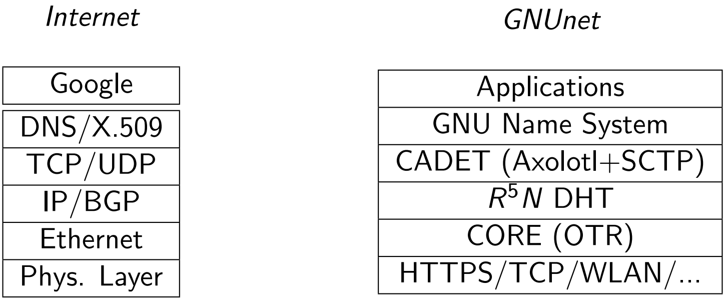
Overlay P2P networks

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

Full-Stack P2P networks

- GNUnet

Full Stack



Internet

Google

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Phys. Layer

GNUnet

Applications

GNU Name System

CADET (Axolotl+SCTP)

R^5N DHT

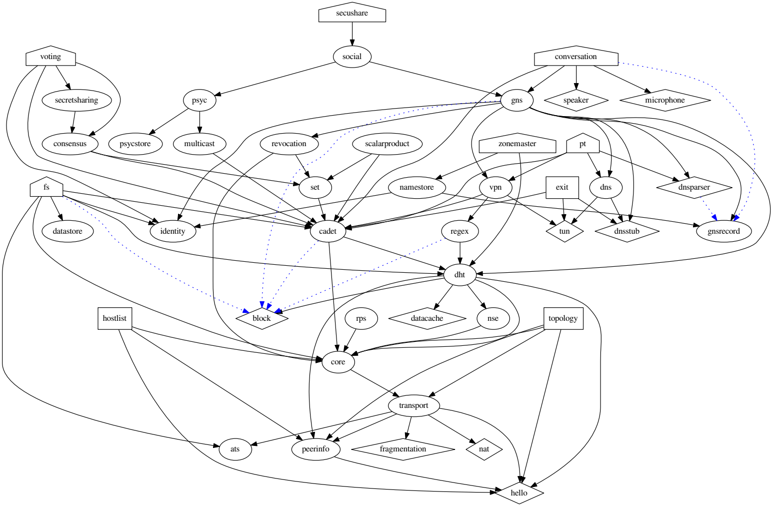
CORE (OTR)

HTTPS/TCP/WLAN/...

Raised Abstraction Level

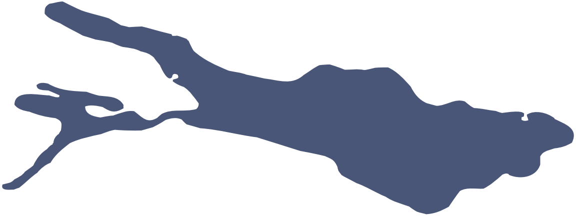
SecuShare	p≡p		Reuters	
Social	Lake		CRDT-Git	IP
PSYC	GNU Taler	Xolotl	Scalarproduct SMC	PT/VPN
Multicast	Fog-of-Trust	RPS	Set intersection	RegEx
GNU Name System				
CADET (Axolotl+SCTP)				
R^5N DHT				
CORE (OTR)				
HTTPS	TCP	WLAN	IP	...

Reality is messy[2]

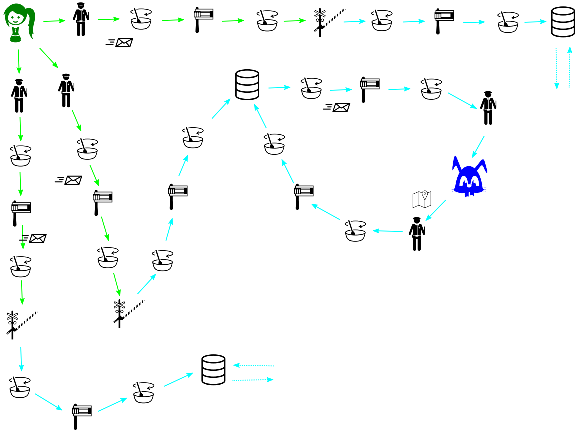


[2] But this applies to the Internet as well.

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!