

Facebook on blockchain?

Reinventing the Internet spectrum:

build a bunch of own middleware ... throw out L2

Example: Istvan NSDI '16

- Ethereum
- TON

...

- Freenet
- I2P
- Tor
- GNUnet

:3 ==> example.com

MAC, DHCP, IP, TCP src, DNS spoofing

...

Made into “merely” leaks
by “universal” TLS (oh, OCSP!)

Tor ain't enough

- GPNO
- generally narrow scope:
 - limited anonymization,
 - even more limited distribution strategies possible

1. Lock-in
2. • content distribution
 - native monetization
 - security by default
3. Ridding of central authority (DNS, X.509)
4. Privacy and censorship resistance

Example: IPNS a month ago

Privacy and censorship-resistance

- BFT routing
- Resilient naming
- Private dot product
- **Efficient multicast** + subscriptions as cover traffic
- Transports indistinguishable from random packets

P2P social networks:
why and how viable?