



Building a Better Internet

Speaker: Colton White

If you do not have brains you follow the same route twice. — Greek proverb

What is a meshnet?

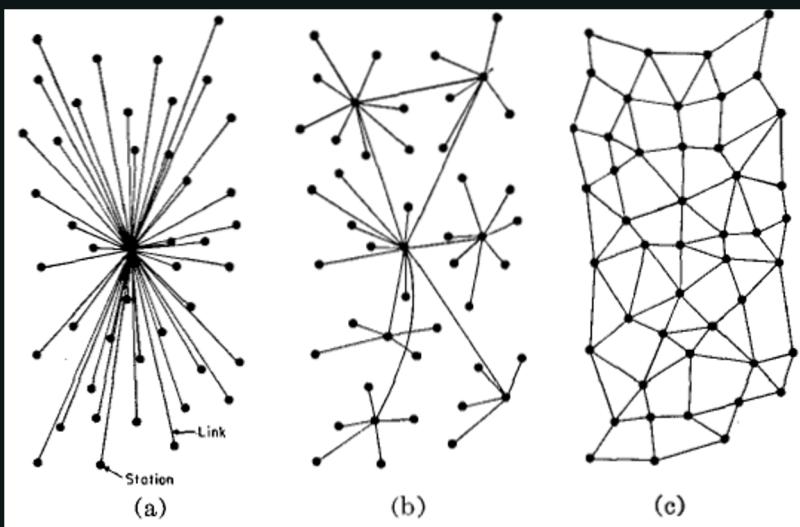


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

What is a meshnet?



<https://www.youtube.com/watch?v=1tEkyLOh-tY>

Why use a meshnet?

- Who owns the data passing through the “pipes?”
 - Responsible for spam or illegal content? (SOPA, EARN IT)
- Is digital privacy a basic human right? (4th Amendment)
- Should encryption be illegal? (EARN IT)
- Who draws the line between satire and propaganda?
- Choose between natural/government monopolies?
(Open Internet Order, Net Neutrality)

...self-evident with meshnets!



Assumptions

- Meshnets and otherwise distributed networks will improve many forms of communication, enabling freedom of information
- Distributing means of communication allows for some degree of autonomy for participants

History

- 2009: Bitcoin provides a method for decentralized banking and money transfer with a global currency (beginning of blockchain)
- 2010: China Telecom diverted 15% of world's Internet traffic for up to 18 minutes
 - BGP route leaks are a common enough occurrence to warrant change in infrastructure
- 2015: Ethereum introduces a global virtual machine as a blockchain
- 2015: IPFS provides global, distributed file storage
- 2017: Turkish gov blocks access to Wikipedia (subsequently hosted on IPFS to mitigate censorship)
- 2019: Mesh messaging app Bridgefy usage up 3685% amidst Hong Kong protests

Solutions: Application Layer

- Bitcoin: trustless consensus (proof of work)
 - Monero = crypto with zero-knowledge proof
- ZeroNet: merges blockchain & BitTorrent
 - Can serve dynamic websites (“zites”)
- Ethereum: Turing-complete VM over blockchain
 - Many “dapps” operate using Ether as “gas”
- IPFS for hosting static websites and files
 - Operates on Merkle DAG routed with DHT
 - Like a Git repository shared over BitTorrent
 - Content-addressed using hashes



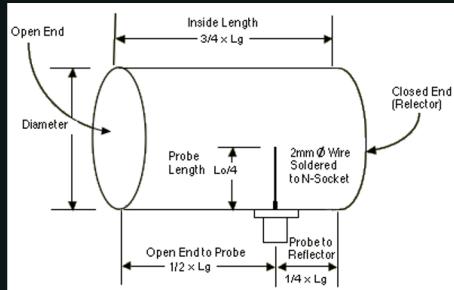
Solutions: Layers 2 & 3 (OSI)

- batman-adv
 - Layer 2 - Makes networked devices act as though part of the same switch -- parent protocol B.A.T.M.A.N. is layer 3
- cjdns
 - IPv6-addressed, e2e encrypted, load seeks “preferred nodes” in DHT (backhaul) -- still active but largely replaced by yggdrasil
- Yggdrasil
 - cjdns, but balances load equally and routes follow spanning tree
- babel
 - Optimizations to adjust to wireless/wired networks
 - Althea: babel + ether (pay-as-you-go service model)



Solutions: Layer 1 (OSI)

- <https://www.wikarekare.org/Antenna/WaveguideCan.html>
 - for the University Experience™

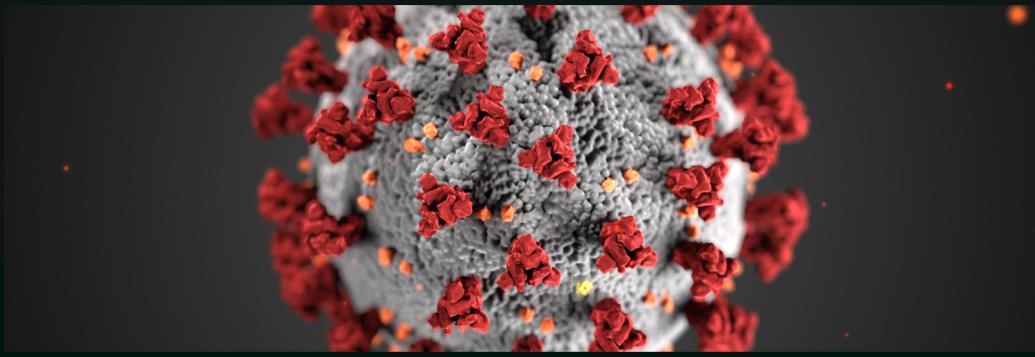


- <https://startyourownisp.com/posts/hardware-platform/>
 - more professional hardware (Ubiquiti routers are usually used)

Ethics

- With great power comes great responsibility
 - Greater potential for spread of reasonably illegal content
 - don't anonymize the network
 - Can still be vulnerable to DDoS attacks
 - require permission from **any participant** to enter network
 - require proof of work to send data over network
- On the other hand...
 - Censorship-resistant
 - Backed by community's interest, not corporate/legal
 - Democratic, promotes individual liberties

In Conclusion...



Low Barr: Don't give me that crap about security, just put the backdoors in the encryption, roars US Attorney General

I don't want to hear about hackers and keys, nerds – make it happen, or we'll pass a law making it happen

By Iain Thomson in San Francisco 23 Jul 2019 at 21:38

44 SHARE ▾



Sources

- Benet, J. (2014, July 24). IPFS - Content Addressed, Versioned, P2P File System. Retrieved November 11, 2019, from <https://github.com/ipfs/ipfs/blob/master/papers/ipfs-cap2pfs/ipfs-p2p-file-system.pdf>.
- Bulkin, A. (2016, May 3). Explaining blockchain - how proof of work enables trustless consensus. Retrieved from <https://keepingstock.net/explaining-blockchain-how-proof-of-work-enables-trustless-consensus-2abed27f0845?gi=3c4942d923f>.
- Chroboczek, J. (n.d.). Babel — a loop-avoiding distance-vector routing protocol. Retrieved November 10, 2019, from <https://www.irif.fr/~jch//software/babel/>.
- Cjdelisle. (2018, June 22). cjdelisle/cjdns. Retrieved November 11, 2019, from <https://github.com/cjdelisle/cjdns/blob/master/doc/Whitepaper.md>.
- Dale, B. (2018, February 6). Turkey Can't Block This Copy of Wikipedia. Retrieved from <https://observer.com/2017/05/turkey-wikipedia-ipfs/>.
- Eichler, A. (2013, October 26). Why Did 15 Percent of All Web Traffic Briefly Go Through China? Retrieved from <https://www.theatlantic.com/technology/archive/2010/11/why-did-15-percent-of-all-web-traffic-briefly-go-through-china/343377/>.
- Killeen, A., Killeen, A., & Pinterest. (2015, January 5). Distributed Networks. Retrieved from <http://venturehousela.com/2015/01/05/distributed-network/>.
- Mailonline, R. F. (2019, October 19). Hong Kong activists wear Joker and Winnie-the-Pooh masks. Retrieved from <https://www.dailymail.co.uk/news/article-7590823/Hong-Kong-activists-wear-Joker-Winnie-Pooh-masks.html>.
- Play: A P2P Distributed Torrent Site That's Impossible to Shut Down. (2016, March 1). Retrieved from <https://torrentfreak.com/play-p2p-impossible-shutdown-160301/>.
- Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: the brilliant technology changing money, business and the world*. Toronto: Penguin Random House Canada.
- Yggdrasil-Network. (n.d.). yggdrasil-network/yggdrasil-go. Retrieved November 11, 2019, from <https://github.com/yggdrasil-network/yggdrasil-go/blob/master/doc/Whitepaper.md>.