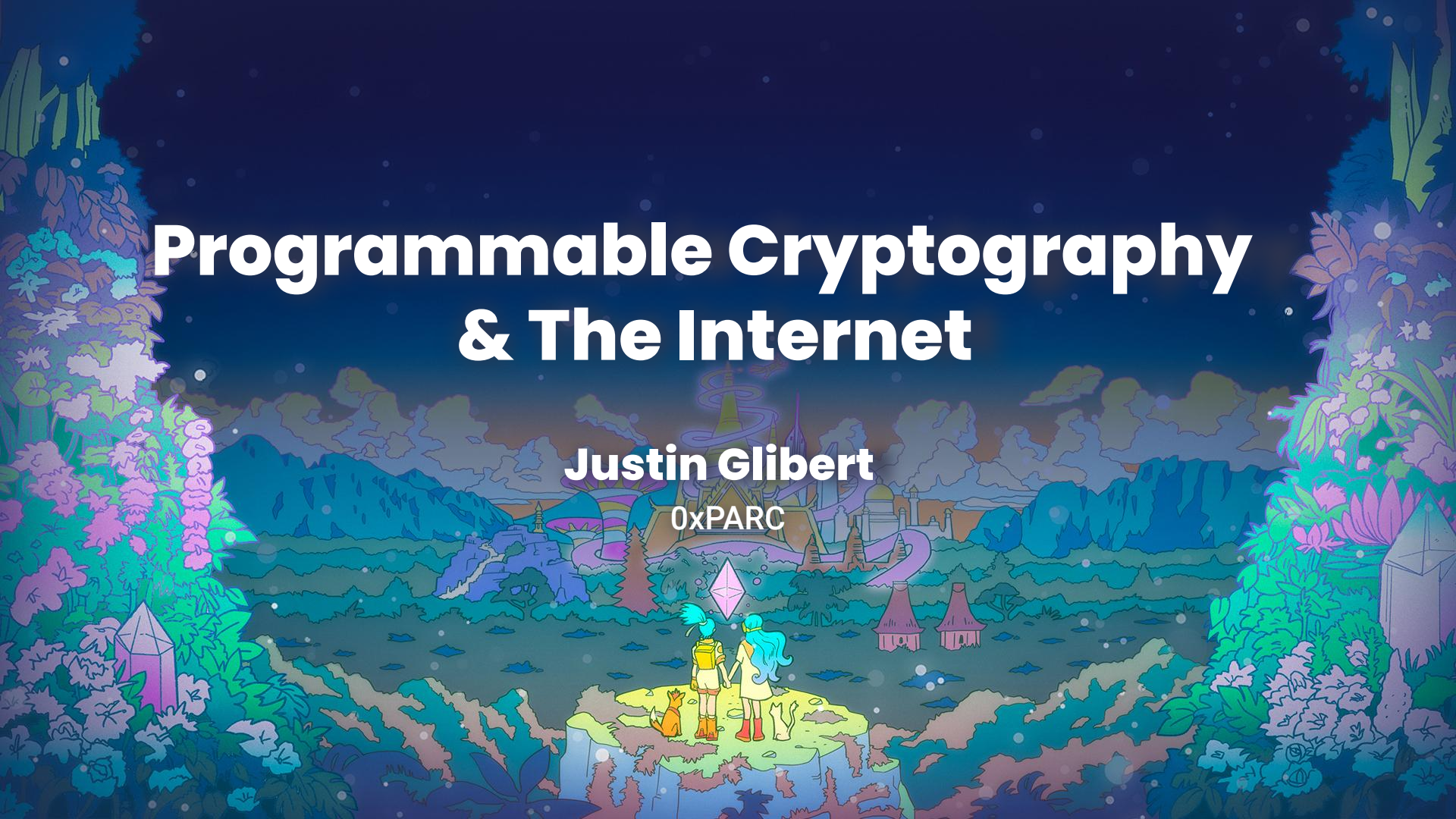
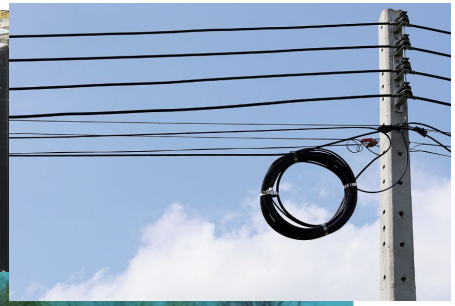
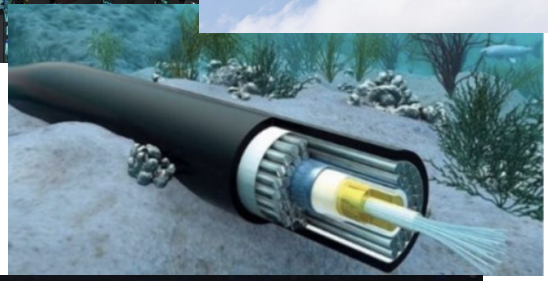
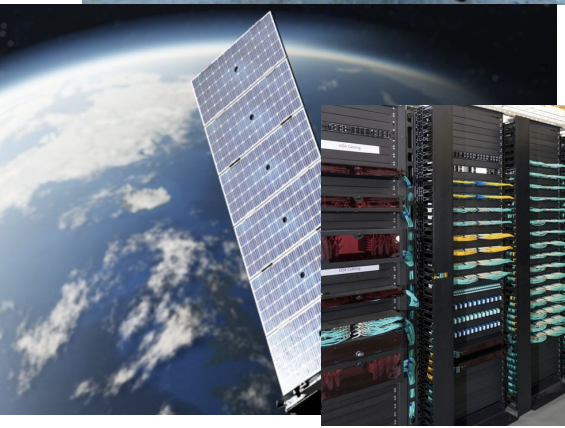
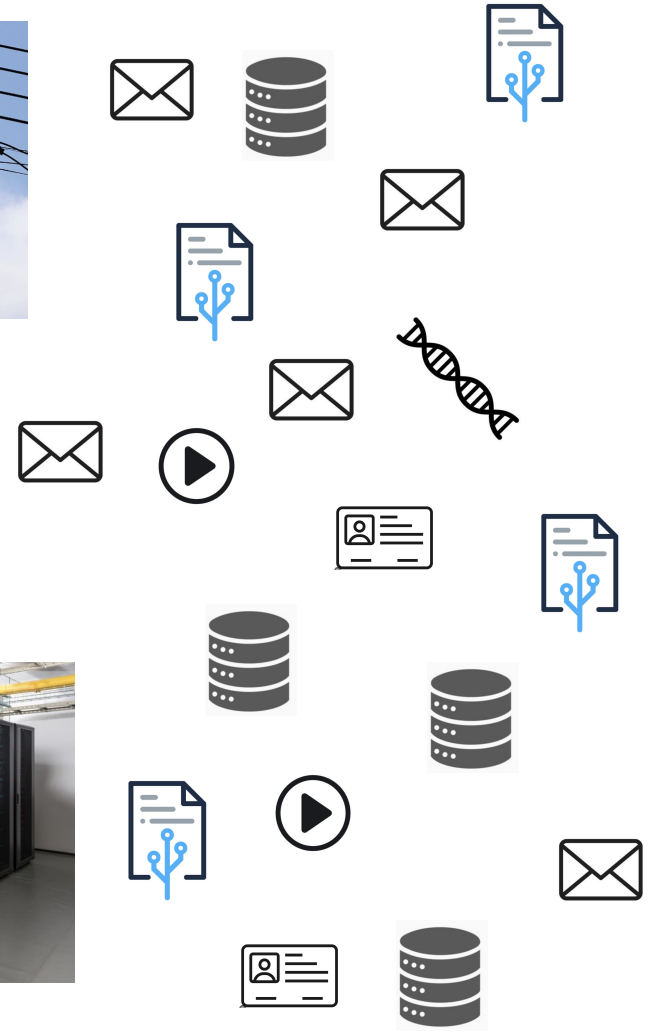
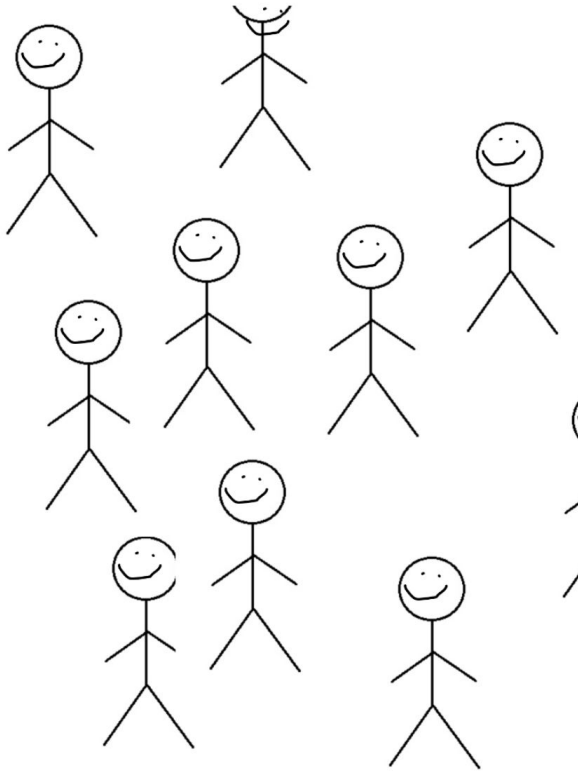
Programmable Cryptography & The Internet



Justin Glibert

0xPARC

Choose the problems you care about

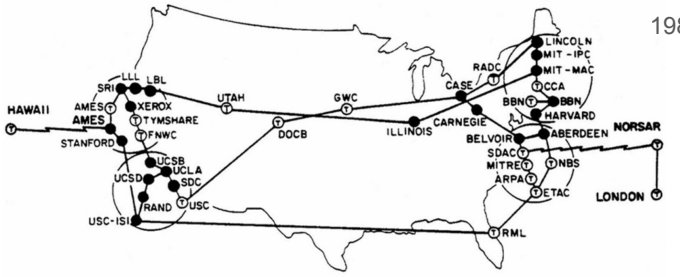
- Vendor lock-in
- Data Silos
- Lack of interoperability
- Lack of decentralization
- Biases
- Friction monetizing most content
- Poor compute / networking utilization
- Lack of transparency
- Barrier to entry
- Etc

How did we get there?

Brief history of the Internet & the Web

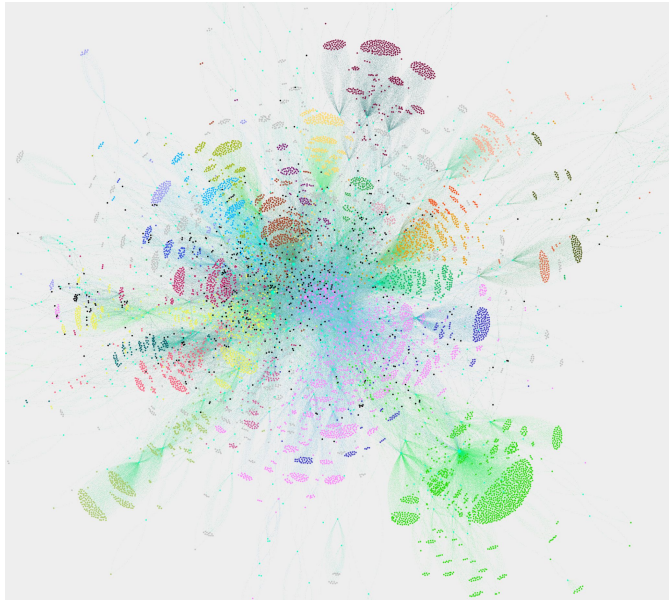
The Internet

Network of Networks



~20 Networks

1983: TCP/IP standardized



Global System Statistics

1203 Exchanges
30831 Networks
5461 Facilities
52 Campuses
181 Carriers
55100 Connections to Exchanges
50745 Connections to Facilities
7167 Automated Networks
44427 Registered Users
28699 Organizations

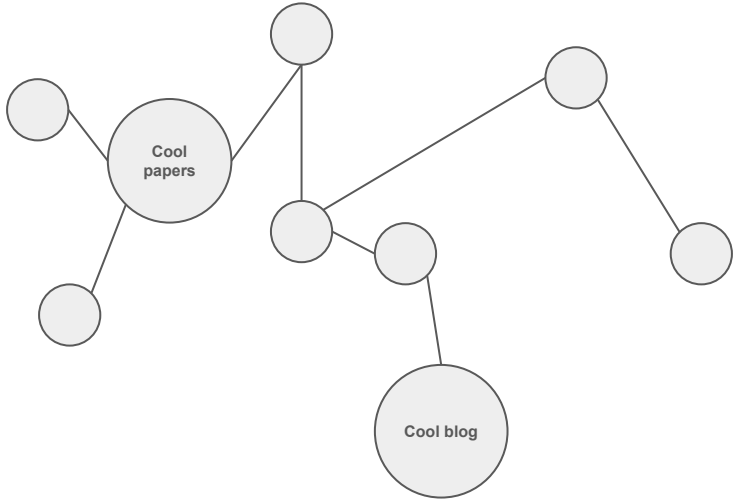
The Internet

- **Connect any two Nodes with each other**
- Peer-to-peer and completely **symmetric**
  - No node is “more important” than the others
- Get an IP address & start sending and receiving packets

The Web (1.0)

1990: Interlinked hypertext documents accessed via the internet

Interlinked: URL + Link (<a/>)
Hypertext: HTML
Documents: Browser rendering



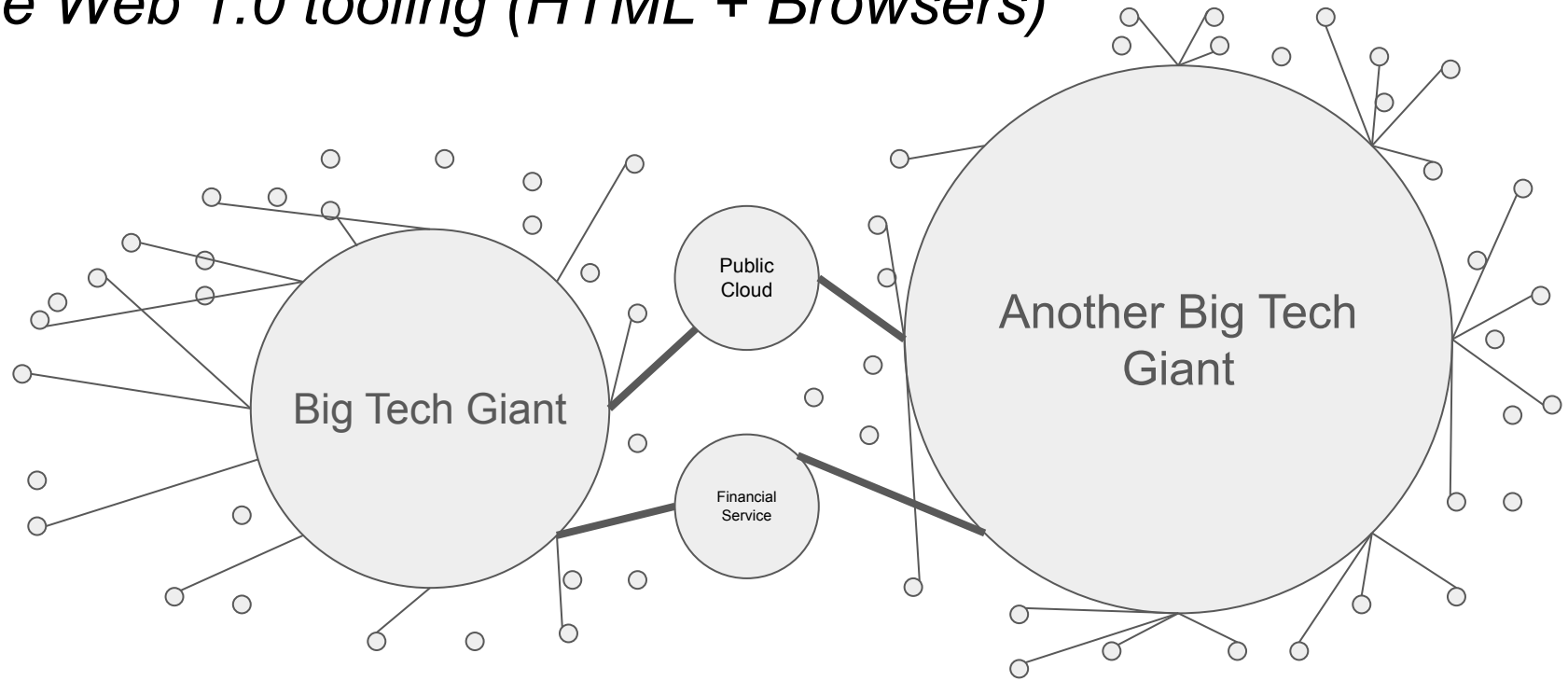
The Web (1.0)

- **Connect hypertext documents with each other**
- Peer-to-peer and completely **symmetric**
  - Anyone can host hypertext documents, anyone can browse them
  - Trivia: Operating systems came bundled with HTML servers! Producer and consumers were the same

The Web (2.0)

Tools, content, and networks (social, financial, etc) accessed via the Internet and The Web 1.0 tooling (HTML + Browsers)

Web 2.0	Client / Server
Web 1.0	HTML/Browser/HTTP
Internet	TCP/IP



The Web (2.0)

- **Back to time sharing: lots of dumb terminals and a few big important computers**
- Client-server -> **asymmetric**
  - We have ~hundreds of very important nodes: “The Client-Server Supernode model”
  - Everybody else is a dumb client
- Extreme centralization of {data, computation, power, infrastructure, economic}

Two Lenses

Downside prevention:

“Centralization of {data, computation, power, infrastructure, economic} is bad” -> We want to reduce {bias, abuse, censorship, anti-competition, lies}

Upside creation:

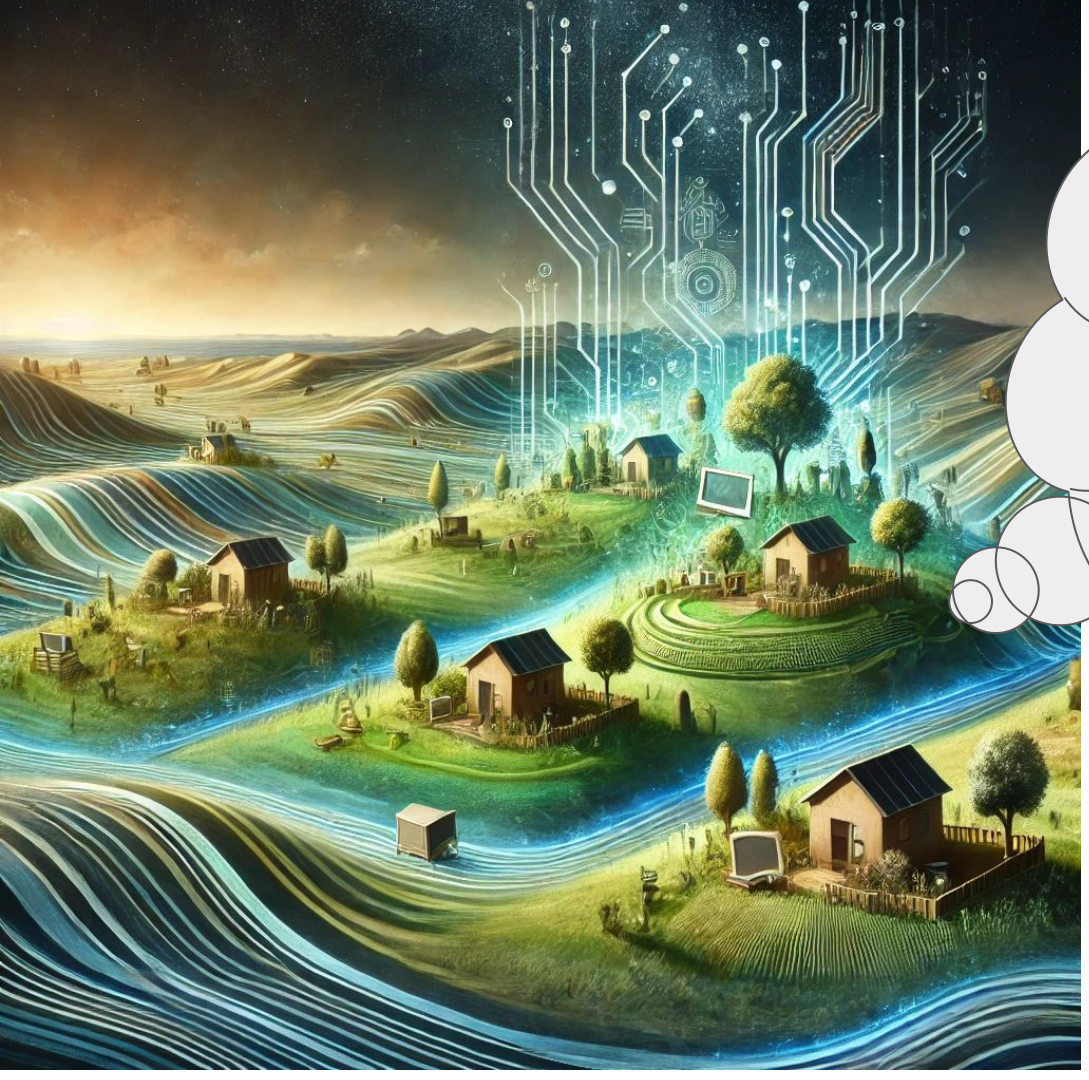
Most interactions and computations that *could* be possible on the Internet DO NOT happen.

Coefficient of friction is **very high**, if you are not part of the aggregators you can’t add new “features” to the Internet…

…Unless “you go through Y Combinator and build a company”

The Internet:
The primordial digital sea

The Web (1.0):
We climbed out of the primordial sea and built small digital villages



The Web (2.0):
We are stuck in the
Theme Parks

The Web (1.0)

The Theme Parks

> YOU ARE HERE <

The Metropolis

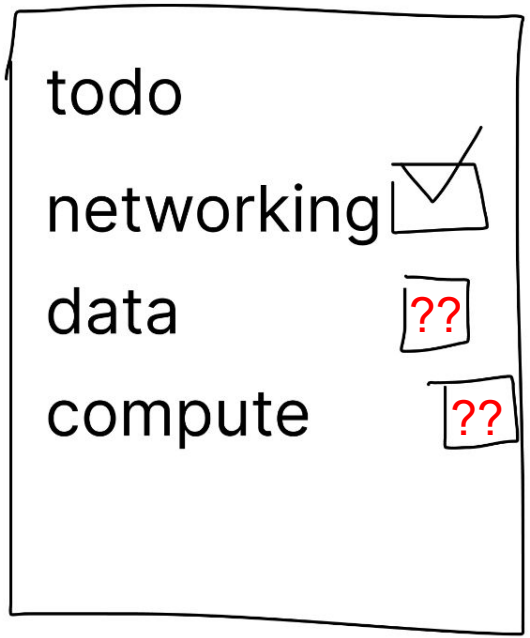
Rewind

- We were on such a good path!
- What happened?

The Internet created the **Perfect Pipe**

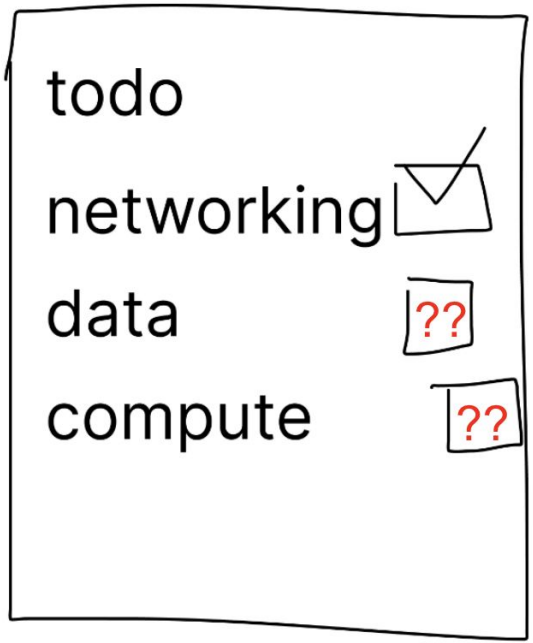
- **Delivers packets securely across the entire world**
- Peer to peer
- Fully encrypted point-to-point
- Symmetric: works for all nodes!
- Civilization Scale
- Built entirely with Gen 1 Cryptography
  - Asymmetric encryption (identity)
  - Symmetric encryption (hiding traffic)
- Email, SSH, Torrent all built *only* with the pipe

civilization dashboard



Trust in the Networking

How do we tick the other checkboxes?



- How do we build beyond P2P data transmission systems? (ie: Email, SSH, Torrent)
- How can we compute over mutually private data?
- How do we authenticate the origin, transformation, and aggregation of data?
- We Trust the networking, now how can we trust the data and the compute?

=> HACK: Client Server architecture + Institutional Hardness

We connected The Perfect Pipe to *what we had*

- Blackbox / Opaque servers
- Default (without accumulation of brand / iterated game) is abuse, data leak, downtime, etc
  - That’s why we (usually) don’t give our data / payment details / etc to random websites and apps!
- Some nodes did better than others and started accumulating power

“Trust me bro” as a fallback

- We merely started *believing* Compute and Data with client-server architecture
  - Compute in these servers and store your data there. Believe in what comes out. Accept what you cannot ask for.
- Rarely hear about abuse / friction / hacks / downtime / antitrust at the networking layer
- **Often** hear about these issues in the data / compute layer
  - Hacks
  - Censorship
  - Downtime
  - “API not supported”
  - Abuse of monopoly and power

After all, we could not have done better

- 0xPARC believes it is **impossible** to do better than the Perfect Pipe without Generation 2 cryptography
  - (we are trying to mathematically prove it!)
- The Perfect Pipe is as best as we could do with asymmetric encryption (cryptographic identities), hashes, and transport layer security

Networking

Compute

Data

0xPARC believes we can collectively add new dimensions to the Internet with Programmable Cryptography

Networking

Compute

Data

PC can be used to construct the **Perfect Packet Of Data**

- **Cryptographically authenticated:** API, a camera, the government, etc: integrity can be verified.
- **Verified transformation**: Operation on the data can be verified.
- **Information asymmetries:** Properties can be hidden and transformed just in time

Advanced form of PC – FHE, MPC, iO – can deliver the **Perfect Computer**

- **Fully encrypted**: Input, Compute, Output
- **Always online** – perfect liveness
- **Permissionless**: anyone can use it.
- Public data is really public. Private data is really private.
- Leverages The Perfect Pipe to operate as a network, consumes and produces Perfect Data

Networking

Compute

Data