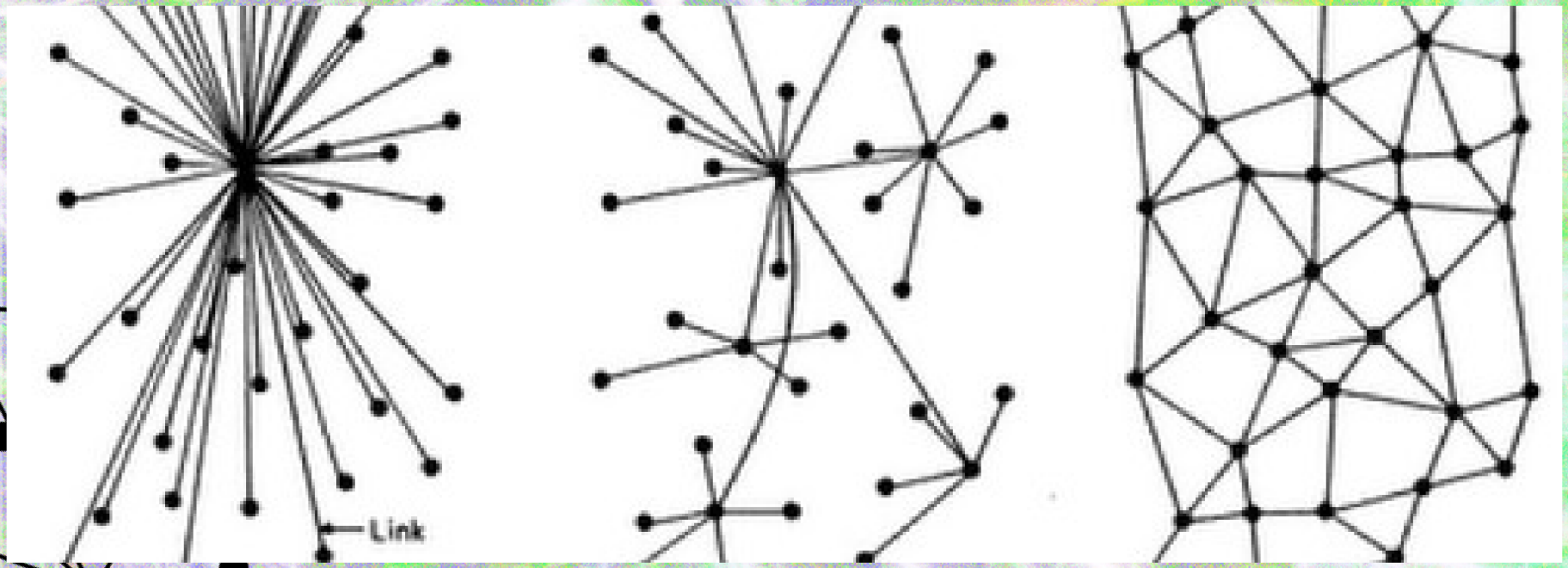
WELCOME TO SESSION 01

Introduction to Decentralized Web and Its Cultural Foundations

Since Sir Tim Berners Lee invented the World Wide Web in 1989 as a "universal linked information system" the web has grown to become the world's dominant interface with the Internet. Throughout the web's evolution, one of its core tenets has been "decentralization" – that this global network should allow anyone anywhere to create, share, and access digital content. In the 35 years since its inception, the web has fulfilled this promise in many ways. And yet some of its basic features have also proven to be vulnerable to powerful concentrated interests, enabling private and state actors to capture or censor the web.

This session will explore the history of the internet and the World Wide Web while analyzing the technologies, organizations, legislations, and ideologies that shaped the web over the past three and a half decades. We will look at examples of decentralized systems designed and implemented by humans long before the digital age up to the birth of the internet and until the period of time just before the introduction of cryptocurrencies.

OVERVIEW



HOW DO YOU DEFINE DECENTRALIZATION?

Power Distribution

Distributed Ownership

Tech centered around human needs

No Central Processor

Network of Nodes that are self sufficient but has agreed protocols

Not Like our Internet

Horizontal Structure

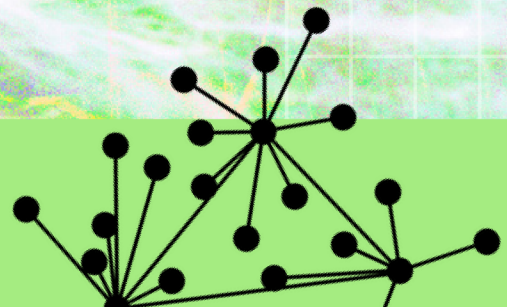
Distributed Knowledge

Community

Group Policymaking

Co-Creation

Participation vs Consumption



THE DIFFERENCE BETWEEN

Decentralized

- Each node acts as a router and a server
- All nodes have equal power and can work independently of each other
- Decisions are made by consensus
- Examples: Blockchain, p2p protocols, git

Distributed

- Data and processing power are shared across all nodes
- There can be a hierarchy of nodes, with some coordinating the actions of others
- Nodes coordinate together so as to act like a single unit
- Examples: bit torrent

OFFLINE EXAMPLE 01

THE IROQUOIS CONFEDERACY

The Confederacy wasn't a single, unified nation but a league of six sovereign Iroquois nations – Mohawk, Oneida, Onondaga, Cayuga, Seneca, and Tuscarora (joined later). Each nation maintained its own internal governance and cultural identity.

Decisions impacting the entire Confederacy were made through the Grand Council, a representative body with 50 sachems (chiefs) from each nation. This council operated on a consensus basis, requiring agreement from all nations before taking action.

OFFLINE EXAMPLE 02

THE !KUNG SAN

- The !Kung San lack formal leadership positions or hierarchies. Decisions are made through consensus among all adult members of the community, regardless of gender or age. This fosters a horizontal power structure where no individual holds absolute authority over others.

Disputes within the community are addressed through discussion and mediation rather than relying on a central authority figure to impose solutions. This reinforces the principle of collective decision-making and discourages the concentration of power for conflict resolution.

UNITED STATES MOTIVATIONS

THE COLD WAR

- Centralized systems are vulnerable: A single point of failure, like a physical attack or technical breakdown, could cripple the entire network.
- Potential for censorship and control: A centralized system could be easily controlled by a government or other authority, limiting information flow and communication.
- The US Government wanted to create a network that could withstand nuclear attack

ARPANET COMPETITORS AND OTHER NETS

OGAS (USSR)

A nationwide cybernetic network for monitoring the nation’s economy

MINITEL (FRANCE)

the world's most successful online service prior to the World Wide Web

CYBERSYN (CHILE)

A workforce maintained cybernetic network also for monitoring the nation’s economy

"THE GALACTIC NETWORK" WHAT WAS ARPANET?

1958

The US Government launches the Advanced Research Projects Agency (ARPA) Launches to compete with the USSR

1966

Bob Taylor, inspired by the vision of J.C.R. Licklider initiates ARPANET. Larry Roberts begins implementation in 1967.

1969

ARPANET successfully connects a terminal at UCLA to a terminal at Stanford.

ARPANET

Advanced Research Projects Agency Network

was the first wide-area packet-switching network with distributed control and one of the first networks to implement the TCP/IP protocol suite. Launched in 1969, it laid the foundation for the internet by connecting academic and research institutions across the United States.

When the National Science Foundation (NSF) took over from ARPANET, it evolved into the NSFNET in the mid-1980s. NSFNET served as a major backbone to connect universities and research institutions across the United States at higher speeds, significantly expanding the network's reach and capacity.

In 1995, when NSF decided to no longer fund the NSFNET, The responsibility for providing the internet's infrastructure shifted to the private sector. Multiple commercial networks took over, interconnecting through Network Access Points (NAPs). This led to the concentration of ownership over network infrastructure that we are left with today.

INTERNET ENGINEERING TASK FORCE (IETF)

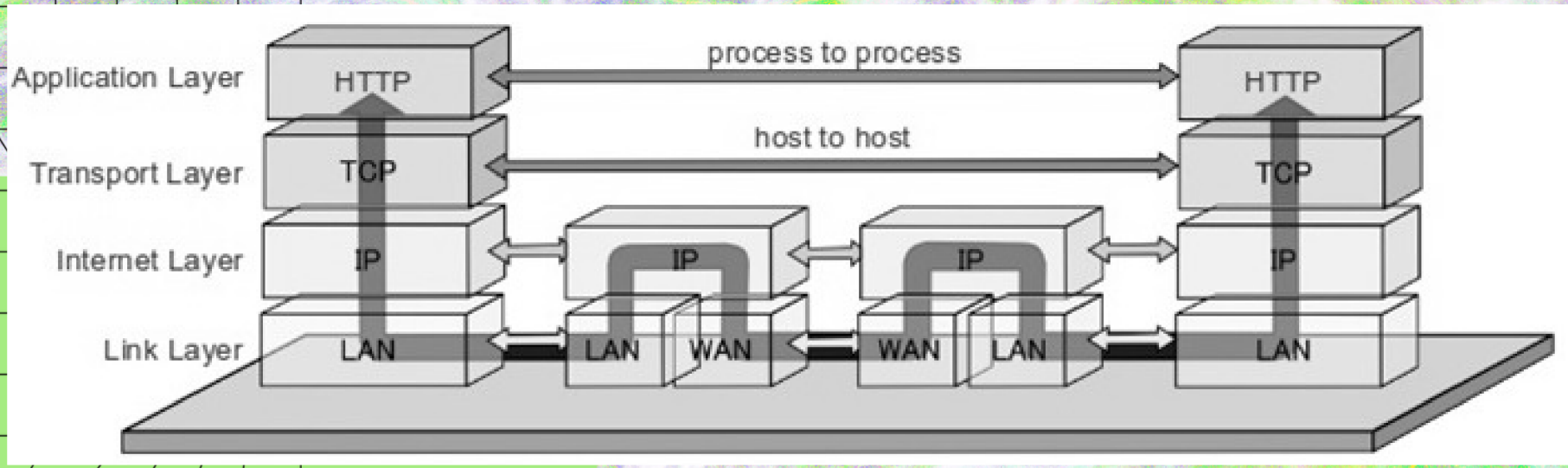
"little to do with the technology that's possible, and much to do with the technology that the IETF chooses to create."

The IETF, founded in 1986, is a standards development body that voluntarily creates standards for all functionality on the internet - including network hardware, routing, network security, internet and transport protocols, media applications, and more.

The IETF is also home to the Request For Comments (RFC) archive: https://www.rfc-editor.org/rfc-index-100a.html

Per the IETF's website, approximately 7,000 individuals may be actively contributing to the organization's mission by drafting standards, engaging in email discussions, or attending live meetings.

THE INTERNET PROTOCOL SUITE



INTERNET PROTOCOL (IP)

Also known as the 'Network Layer' or "layer 3', this protocol is responsible for assigning internet protocol addresses (think - 192.168.2.1) to our sending and receiving machines on across the network of networks, the internet. It is also responsible for figuring out the best routes for a packet to take across the internet.

TRANSMISSION CONTROL PROTOCOL (TCP)

Also known as the 'Transport Layer' or "layer 4', this protocol is responsible for making sure packets reach their destination intact and are able to be reassembled into the original text or binary file that it was originally a part of. Think - a puzzle broken up into its pieces, mailed to another address, and then reassembled into the original puzzle.

E-MAIL && SMTP

THE ORIGINAL KILLER APP OF THE INTERNET

Sending an electronic message was possible as early as the 1960s, when people could send messages via time-shared mainframe computers. The first ARPANET email was sent in 1971, followed by several proprietary attempts by IBM, Compuserve, Hewlett-Packard, and others. In the same year, a "Mail Protocol" was suggested, but not actually implemented until 1983.

SIMPLE MAIL TRANSPORT PROTOCOL (SMTP)

is this standard "Mail Protocol" that was finally implemented on the ARPANET, designed to be the standard protocol for exchanging electronic mail in lieu of the many proprietary systems that had come before it. It also replaced the File Transfer Protocol (FTP) as the preferred method for fetching mail.

ICANN AND DNS

ICANN

Oversees the Domain Name System (DNS), which translates domain names into numerical IP addresses that computers can understand.

DNS: DOMAIN NAME SYSTEM

DNS allows us to use user-friendly domain names so we aren't all having to remember IP addresses to access web pages.

TIERS OF THE INTERNET

TIER 1

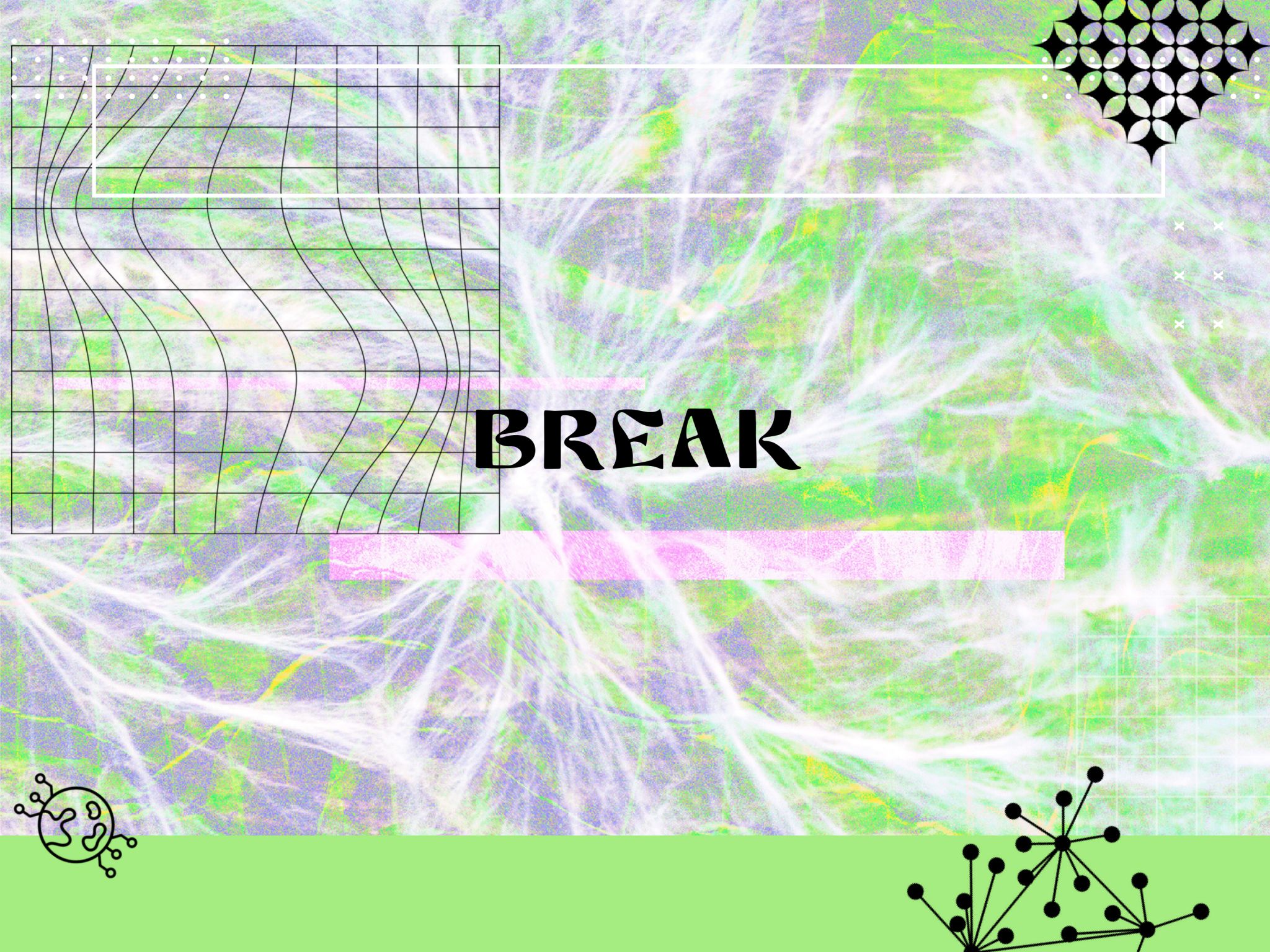
Tier 1 networks peer to each other at no cost. They are the landlords of the internet.

TIER 2

Tier 2 networks can sometimes peer to each other, but also need to lease infrastructure from Tier 1's

TIER 3

Tier 3 networks are dependent upon leasing infrastructure from Tier 2 networks


BREAK

COMMUNITY-CREATED NETWORKS

Freifunk (Germany)

guifi.net (Spain)

NYC Mesh (USA)

Athens Wireless Metropolitan Network (Greece)

TOR, VPNS, SCRAMBLING

THE ONION ROUTER (TOR)

is a decentralized system that enables anonymous communication across the internet. It directs internet traffic through a worldwide, volunteer-operated network consisting of more than seven thousand relays. By encrypting the data, including the destination IP address, multiple times and sending it through a series of relays, TOR masks a user's location and usage.

VIRTUAL PRIVATE NETWORK (VPN)

is a service that creates a secure, encrypted connection over a less secure network, such as the internet. It allows users to send and receive data across shared or public networks as if their computing devices were directly connected to a private network. By routing the data traffic through VPN servers, the originating IP address of the user is masked.

PEER-TO-PEER (P2P)

"Peer-to-Peer" (P2P) refers to a decentralized network architecture where each participant (node) in the network shares a part of their resources, such as processing power, disk storage, or network bandwidth, directly with other participants. These resources are shared without the need for centralized coordination by servers or stable hosts. Instead, each node in a P2P network acts as both a "client" (consuming resources) and a "server" (providing resources), with equal privileges and responsibilities.

Examples include: Git, Interplanetary file system (ipfs), Secure Scuttlebutt (SSB), Hyphanet (formerly Freenet), and Napster

FEDERATED NETWORKS

A federated network is a group of independent entities working together to achieve a common goal, but each entity maintains individual control over its own data and operations.

Mastodon: Text-based social media similar to Twitter

Pixelfed: Image-sharing platform similar to Instagram

PeerTube: Video platform similar to YouTube

EARLY SOCIAL NETWORKS

THE WELL (CA)

(The Whole Earth 'Lectronic Link)

THE ECHO NYC

USENET VS. BBS

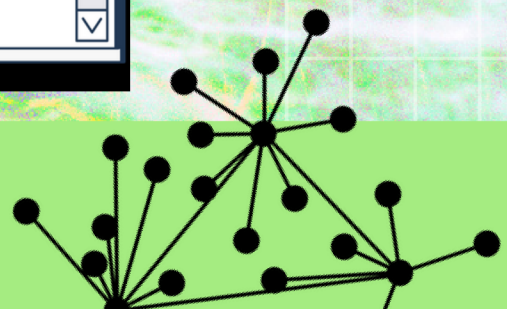
(Decentralized Newsgroups) (Bulletin Board Service)

THE CENTRALIZED WEB : ISPS

MCI MAIL

COMPUSERVE

AOL INSTANT MESSENGER

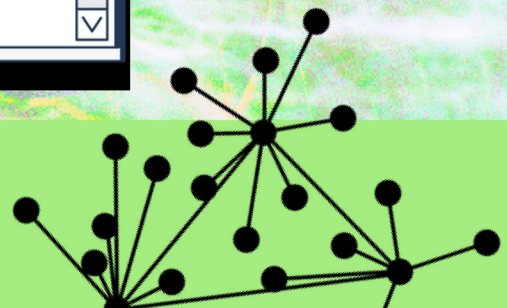


THE CENTRALIZED WEB : WEB 2.0

ALPHABET
(GOOGLE)

META

AMAZON



SUBMARINE CABLE MAP 2024

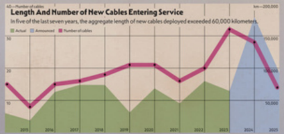
TeleGeography

Designed and produced by TeleGeography
One Thomas Circle NW, Suite 360, Washington, DC 20005, USA
www.telegeography.com +1 202 741 0020

telecomegypt®

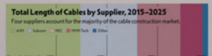
Sponsored by Telecom Egypt
B7 Smart Village, K28 Cairo-Alex Desert Road, Giza 12577, Egypt
www.te.eg ibu@te.eg

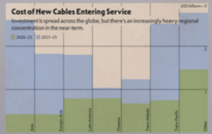
From SEA

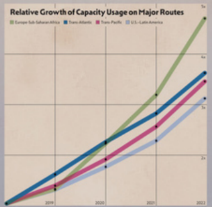


CABLE CONSTRUCTION

Between 2023 and 2025, a new cable boom valued at a record $10 billion will bring an estimated 78 systems online measuring over 300,000 kilometers in length, a level of growth not seen in over 20 years.

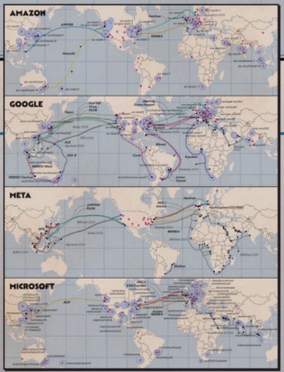






CABLE INVESTMENTS

Since 2018, content providers have added capacity at a faster rate than other bandwidth users. To date, Google and Meta—driven by their bandwidth-intensive requirements for search, video, and social media—have invested in 26 and 15 submarine cable systems, respectively.



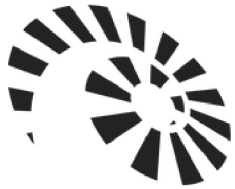
To CLOUD

CLOUD INFRASTRUCTURE

After a three-year slump, both mature and emerging markets are rebounding in cloud region expansion. These rollouts can be traced back, in part, to submarine cable routing decisions. Cables land near locations prime for cloud region growth, so cable routes show where inter-data center bandwidth growth is expected.

Production Team Larry Lairson, Markus Krisetya, Alan Mauldin, Lane Burdette, and Jon Hull ISBN 978-1-7363527-8-8

BLOCKCHAIN



In his 1982 David Chaum proposed a concept he called "blind signatures." and mentioned a "cryptographically secured chain of blocks" for timestamps".

In 1991, Haber and Stornetta published a paper titled "How to Time-Stamp Digital Documents." They proposed a system for securing and timestamping digital documents using cryptographic techniques.Their system involved creating a chain of "cryptographic hash functions," where each block in the chain linked back to the previous one, forming a tamper-proof chain.

Neither proposed system was envisioned as decentralized in infrastructure

BITCOIN

Broadly Speaking...

Transaction data is not stored on a single server controlled by a central authority, but rather on a distributed ledger replicated across a network of computers (nodes) worldwide.

nodes in the network constantly verify and agree upon the validity of transactions using a process called proof-of-work. This eliminates the need for a central authority to validate transactions and ensures a secure and transparent system.

- Hardware: The type of mining hardware used plays a significant role. High-powered, specialized mining rigs designed for efficient PoW problem solving are expensive compared to using personal computers.
-
- Electricity: The computational power required for PoW consumes significant electricity, and the cost varies depending on location and electricity rates.
-
- Mining difficulty: The difficulty of the PoW puzzle is adjusted automatically to maintain a specific block creation rate. As more miners join the network, the difficulty increases, requiring more computing power and consequently, higher electricity costs.

ETHEREUM

dApps (Decentralized applications) don't rely on a single entity to control their operation. The code, data, and governance mechanisms are distributed across the network of nodes running the Ethereum blockchain.

Proof of Stake or PoS validators are selected to create new blocks and verify transactions based on the number of coins they hold and are willing to "stake" as collateral. The likelihood of being chosen to validate transactions correlates with the size of one's stake, thus incentivizing validators to act honestly to avoid losing their stake as a penalty for malicious actions. This mechanism reduces energy usage by eliminating the need for competitive, computationally intensive mining.

TEZOS

Designed for forkless upgrades through a built-in on-chain governance mechanism. This allows the network to evolve and improve without splitting, offering greater stability and predictability.

Utilizes a delegation system where XTZ holders can delegate their staking rights to bakers. This allows even those with smaller holdings to participate in securing the network.

Node operators staked currency is liquid

lower gas fees

COSMOS

Cosmos allows developers to create independent blockchains tailored to specific needs. This promotes decentralization by fostering a multi-chain ecosystem where each chain can have its own governance model and consensus mechanism.

Allows developers to choose from various pre-built functionalities, increasing customization and flexibility.

Enables the creation of specialized blockchains for diverse use cases, contributing to a more decentralized and interoperable blockchain landscape compared to single-chain solutions like Ethereum and Tezos.

SIDE CHAINS AND LAYER 2S

The two-way peg mechanism that facilitates asset transfer between the main chain and the sidechain can be a security risk. If the peg is compromised, it could allow attackers to mint new assets on the sidechain without actually depositing them on the main chain. This could lead to inflation and a devaluation of the sidechain's assets.

Bridges are the communication channels between the main chain and the sidechain, facilitating asset transfers. These bridges can be complex and present potential security vulnerabilities if not implemented correctly. Hackers might exploit these vulnerabilities to steal assets being transferred between the chains.

CUSTODIAL CHAINS

Custodial chains, like Flow and Solana, differ from prominent blockchains like Bitcoin, Ethereum, and Tezos in their approach to decentralization. While they leverage blockchain technology for features like transparency and immutability, they incorporate centralized elements in their governance and consensus mechanisms. These chains often have a limited number of validators controlled by the platform operators, raising concerns about centralization and potential censorship. However, this approach can offer faster transaction processing times and lower fees

BLOCKCHAIN NODE PROVIDERS

- INFURA
- ALCHEMY
- ANKR
- HETZNER
- DIGITAL OCEAN
- AMAZON

FINAL QUESTIONS?

Anna Katrina