Apparitions of the Internet That Once Was

How did the Internet become a space of total commercialization?

K. Kayra Banak

October 2024

Abstract

This paper explores the transformation of the Internet from its early decentralized and anarchic roots into a highly commercialized, centralized space dominated by corporate interests. By analyzing key moments in Internet history—from the early days of ARPANET and NSFNET to the rise of Web 2.0 and the advent of surveillance capitalism—the paper illustrates how the ideals of digital autonomy, peer-to-peer interaction, and lack of hierarchy were gradually eroded. Despite this commercialization, moments of "Internet Entropy" emerge in technologies such as BitTorrent, blockchain, and decentralized networks, revealing the Internet's persistent capacity for chaos and resistance against control. Drawing on anarchist political philosophy and technological case studies, this paper argues that while the Internet has largely been tamed, its inherent anarchy remains embedded in its structure, providing potential for future decentralized innovations, particularly with the rise of Web 3.0. Ultimately, the paper reflects on the tension between corporate control and digital freedom, seeking to understand how the Internet might evolve moving forward.

1 Introduction

> "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather." (Barlow)

A Declaration of the Independence of Cyberspace opens with strong, daring words that aim to set the route for the newly emerging digital space. The ideals of the text, although at times deemed "utopian" (Turner 3), spread around cyberspace like whispers of revolution. It influenced the Internet and its culture from the very beginning, inspiring inventions and movements that would attempt to profoundly alter the functioning not only of the digital, but also of the material world (Chun 37). However, almost 30 years later, the Internet has evolved into a space with a level of commercialization that would seem unthinkable to any cyberlibertarian from the 1990s.

In "The Master Switch" Tim Wu explains the centralization of the internet quite deterministically by claiming that any and all new media technology starts off as decentralized and then commercializes and centralizes over time due to the profit incentive.

While it is undeniable that the profit incentive pushes companies to try and centralize new technology, it's unintuitive to compare the internet to its predecessors such as the telephone or the radio. Considering both of these technologies required extensive and investment heavy infrastructure to function, they were inherently gatekept, which is a crucial flaw in Wu's argumentative process. Centralization has clearly taken place in the digital space, yet explaining it through deterministic false-equivalences would only harm discourse around Internet policy.

It would be unfair to name the anarchists of the Internet as unrealistic optimists. The idealist cyberlibertarians certainly had their reasons. There was an inherent anarchy to the internet as opposed to older forms of media, characterized by its decentralized, non-hierarchical technology. Rapid, and at times forced, efforts of commercialization attempted to tame the nature of the digital, nevertheless there remains a form of entropy embedded within the internet's structure. That inherent chaos gushes out in varying frequency, out of numerous new innovations of the digital world. Although commercialization and centralization distort the nature of cyberspace, it cannot fully suppress it, resulting in moments of entropy that reanimate the initial chaos to the Internet. This paper is written as a retelling of the history of the Internet through a lens of corporate greed, while searching for instances of internet entropy in its dark corners.

2 Anarchic Characteristics of Early Internet

> "In many ways the Internet is the world's largest experiment in anarchy." (Schmidt)

During the 1990s, a plethora of internet experts were talking about the Internet as though it was a potential anarchist utopia, a chance to create a better world clean of the sins of the material, and as a place of total freedom. Today, understanding their standpoints might seem harder, therefore before attributing an inherent anarchy to the Internet in agreement with Eric Schmidt and his peers, one must understand what anarchy means in the context of the digital, how it occurs, and where it stems from.

Defining anarchy, even when borrowing terms and ideas from political philosophy, poses challenges. There have been numerous definitions of anarchy and anarchism over the years ("On the Distinction Between State and Anarchy" 40). However, one thing is certain: Anarchy, in the political context and by its etymological roots, has an exclusionary definition. Anarchy has been defined to include the lack of central authority, lack of rulers, lack of states, lack of hierarchy... This understanding necessitates that in redefining anarchy in the digital sense, there are to be ideas borrowed from anarchist political philosophy, as well as exclusions to be thought of.

Then much like political anarchy, digital anarchy would be defined through a set of criteria. The following criteria have been curated with political anarchy, and early internet culture in mind. In order for any digital technology to be considered anarchic, it has to demonstrate these four properties:

1. **Decentralization and Peer-to-Peer (P2P) Autonomy**:Decentralization is a direct loan word from anarchist political philosophy, and it refers to the distribution of power and control away from a central authority and instead to independent actors to manage their own parts of the system (Kropotkin 110). P2P autonomy stems directly from decentralization and further emphasizes the independence of nodes in the network. It allows users to interact directly with one another without intermediaries or centralized control.

2. **Autonomous Self-Organization**:In the political framework, autonomous self-organization is defined as a network of people acting by and for themselves without central authority, which is required for the anarchical process to constantly generate itself (Landstreicher). Self-organization in the digital context stands for the ability of the network to constantly and spontaneously form and maintain structures and functionalities without centralized planning or control.

3. **Lack of Hierarchy**:Once again a direct loan-term from political philosophy, lack of hierarchy implies that every participant in the network has roughly equal power to contribute, share, or build, and that decisions are driven by collective participation.

4. **Lack of Barriers to Entry**:Openness might not be the first thing to come to mind when talking about political anarchy, but the material world is by nature free to enter and to roam. States and borders create barriers to traversal, both of which are opposed to in almost every definition of political anarchy. (Gary Chartier Chad Van Schoelandt 1) For a network to truly be anarchic, it must possess the inherent openness of the material world, and be free to enter and free to roam.

Having established general criteria, the next section will examine one of the earliest versions of the internet, NSFNET, and determine which technologies gave cyberspace its anarchic nature.

NSFNET was a key predecessor to publicly available Internet in its modern form. First established in 1985, NSFNET aimed to provide a more accessible alternative to the heavily regulated and exclusive ARPANET. While it adopted multiple features and protocols from ARPANET, NSFNET connected various self-organized regional networks and supercomputers, functioning as a backbone network across the United States (Leiner et al. 3). It was one of the first major networks to utilize packet switching technology, and it played a crucial role in transitioning to the TCP/IP protocol suite.

NSFNET was a decentralized backbone network that was essentially free of commercial barriers to entry (Lyon and Hafner 125). The network was government funded, and it was not available to the public and only accessible through universities or libraries. However, the NSFNETs barriers stemmed from lack of infrastructure, and although the NSFNET would not live long enough, plans for opening the network to the public were being considered since its dawn. In addition, the defining features of NSFNET which included packet switching, TCP/IP, the Domain Name System (DNS), and local area network (LAN) technologies, each carried one or more of the aforementioned anarchic principles.

1. **Packet Switching**:Packet switching is a turning point in the early years of computer network technologies, having enabled the creation of ARPANET and afterwards NSFNET. In packet switching, any information sent from one node to another gets split into packets, with each packet finding its own fastest route to the target node and the receiver node sorting the packets back in order. In contrast, circuit switching works by having a connection set between the two nodes, and sending the information as a whole through the set route. Packet switching enables further decentralization and P2P autonomy as sent information would be harder to intercept or be forced through a central node than in a circuit switching model. Packet switching is also constantly self-organizing, and lacks hierarchy, while neither of which would be the case for circuit switching.

2. **Transition Control Protocol/Internet Protocol (TCP/IP)**:TCP/IP are a set of standardized protocols that ensure no errors are made in the data transmission. While TCP determines how data is broken into packets and how it should be resorted, checking for any errors in the processes, IP ensures the packets know which node they're coming from and which node they're supposed to go to. TCP/IP protocols are decentralized in the sense that each node determines how to send the packets and that any device using the protocols can send and receive information peer-to-peer. It is also open protocol, meaning anyone can implement it without needing permission or special privileges, making the technology free of barriers to entry.

3. **Domain Name System (DNS)**:The DNS is essentially a translator between human-friendly domain names and computer-friendly IP addresses. It functions by attributing IP addresses to domains on five different levels. Although these levels are called the DNS hierarchy, the DNS in itself is not hierarchical, in the sense that the Root-TLD-Domain-Subdomain hierarchy is only effective in nomenclature, and does not influence the network's control or management structures. The hierarchy exists solely to organize domain names systematically, but each query is processed independently by various servers without a centralized governing body controlling the flow of requests. This allows DNS to maintain a decentralized nature, where any computer on the network can request a domain name resolution without needing approval from a central authority, in line with the

principle of distributed control.

4. **Local Area Network (LAN)/Ethernet**:LAN refers to a network that connects computers within a limited area, enabling them to communicate and share resources. LANs typically use Ethernet as the standard protocol for data transmission, which is achieved through cables. These regional LANs were essential to the NSFNET, which was only a backbone of the network, connecting various regional and institutional networks, most of which relied on LANs to link local computers to one another and to the NSFNET. Ethernet enables devices to be connected without hierarchy controlling the flow of data. Each device can independently initiate communication, in addition to being self-organizing in the sense that devices can dynamically join or leave a network. They also use protocols like CSMA/CD (Carrier Sense Multiple Access with Collision Detection) to manage data transmission, meaning devices autonomously detect and handle collisions without the need for a central coordinator

Having established the anarchic characteristics of NSFNET and its core technologies, the next logical step is to shift focus towards how commercialization began to shape and control this once free-flowing digital landscape. A good starting point would be examining the commercialization of internet access itself.

3 Commercialization of Internet Access

For the first half of its life of 10 years, NSFNET was a government funded, non-profit networking effort that was free to use through libraries, research institutions or universities. However, as the demand for a commercial Internet grew, NSFNET's non-commercial model increasingly came under fire. Companies seeking to profit off of the Internet saw NSFNET as an obstacle, and lobbying efforts to open the Internet to commercialization intensified. Their philosophy was simple:

3.1 The first step of commercialization is to gatekeep

Many companies saw the commercial potential of the digital realm, however NSFNET's acceptable use policy kept early ISPs (Internet Service Providers) from using the backbone commercially. This also created an understanding that if the Internet was to be commercialized, an alternative to the NSFNET would have to be created, and there was no reason for said alternative to be free to use. Therefore, although multiple ISPs like PSINet, ALTERNet and CERFNet were allowing commercial traffic on the NSFNET adhering to the acceptable use policy, it was only a matter of time before a commercial network would be formed.

The commercial internet long awaited by ISPs came in 1991 in two forms. The first was ANS CO+RE. From its formation in 1990 to 1991, ANSNet was

a non-commercial network that functioned on the same infrastructure as the NSFNET, overseen by the non-profit ANS formed by NSFNET's operators: Merit, IBM and MCI. In 1991, ANS decided to allow for commercial traffic under the name ANS CO+RE (Commercial+Research). NSF allowed for commercial traffic on the network as long as the NSFNET backbone wasn't diminished, the price of ANS CO+RE covered the average cost of traffic, and the profit would be put into an infrastructure pool that would be used for the expansion of the network.

The same year, ISPs PSINet, UUNET and CERFNet formed the CIX, or the Commercial Internet eXchange. This new network between ISPs was free of NSFNETs restrictions, and it grew rapidly. Its member ISPs felt the ANS CO+RE gave IBM, Merit and MCI an unfair advantage in the race, and refused to purchase a connection between ANS CO+RE and CIX, while ANS refused to connect to the CIX. Although some connection was established between CIX and ANS CO+RE after June 1992, conflicts went on as CIX demanded regional networks within the ANS CO+RE pay a 10.000$ fee. It was only in 1995 and after significant lobbying efforts by ISPs that NSF pulled out of the NSFNET, therefore lifting all restrictions and forming a truly commercial internet.

Why, then, did ISPs go to such lengths to commercialize internet access? It would seem that the profits from selling access alone, while lucrative, were not the endgame. There had to be something more significant driving this relentless push. One might think that beyond the immediate gains, the real value lay in the infrastructure and control they could secure—control over data, communication channels, and the ability to shape how people interact online. However, looking at how the next years of the Internet went, it seems ISPs acted first, and asked next.

4 Now That We Have the Internet, What Do We Do With It?

Since restrictions were lifted on who can use the internet and how, a digital space that encompassed the globe was being born. The Internet was becoming part of the lives of hundreds of millions of people, and cyberspace was expanding in both non-commercial and commercial ways. Evergrowing networks of computers were joining the Internet, forming a web of users around the world. The World Wide Web had arrived.

4.1 Web 1.0: The Read-Only Internet

The WWW (World Wide Web), invented by Tim Berners-Lee in 1989 and released to the public in 1991 was a completely different way for the Internet to function. Under WWW, the Internet was becoming a decentralized and hyper-connected global library (Berners-Lee 50). The idea introduced web pages as the building block of the Web, which are online documents that are connected to one another through hyperlinks. These pages were written in the consciously

designed easy-to-use HTML (Krol and Klopfenstein 12), and were designed to display text, images, video, audio and more.

The contents of the Internet were growing rapidly through the WWW, and access was getting easier for the public with the use of web browsers and search engines. However, the contents of Web 1.0 were drastically different from the content we come across on the Internet today. Most websites of the Web were static, as in documents written in HTML and CSS that couldn't be interacted with. The Internet was flooding with personal websites, company websites, and information repositories that were read-only.

4.2 Anarchy Spewing Out of the Digital: the Internet against the World

No matter the fact that internet access had been commercialized, the content and the technologies emerging from the Internet still reflected an inherent anarchy, especially in contrast to the material world. Eventually, there came a moment where the lawlessness of the digital started to affect industries of the real world, and the crusade to tame the Internet rejuvenated. This time, not only through ISP efforts but also with the help of media companies that were hurt by peer-to-peer file sharing technologies.

One of the first and most influential P2P file sharing platforms was Napster. Founded in 1999, it consisted of a central directory where users could upload music in the form of MP3 files, and other users would be able to download them. A significant traffic of the website was illegal distribution of copyrighted music, and it quickly gained popularity, drastically altering the way music was consumed by the general public. A sense that music consumption should be free, or cheap had been established. Media companies acted rapidly against Napster, leading to the shutdown of the platform in 2001. Nonetheless, Napster had left an undeniable effect on internet culture, and was followed by the similar Limewire, and later on by the BitTorrent protocol.

BitTorrent is not a platform like Napster and Limewire were. It is a file sharing protocol that works by segmenting the file into multiple small pieces, and having downloaders (leechers) receive the pieces from sharers (seeders) who have previously torrent the file. The protocol works through a .torrent metadata file that tells the leecher information about the pieces of data it should be looking for, and connects the leecher to a tracker server that finds seeders sharing the file. The leecher can download different pieces from multiple seeders at once, drastically increasing download speeds. The protocol can be used for any file transfer, but has become the standard on illegal distribution of copyrighted material such as films, music, video games, and even applications. The fact that BitTorrent is a file sharing protocol and not a centralized platform makes it near impossible to crack down on file sharing, with legal charging only being possible against users of the protocol who are actively engaging in copyright infringement.

4.3 The ISP Oligopoly

In the meantime, a more orderly and commercialized Internet was being slowly dominated by a number of ISPs seeking every method for increasing their profits. AOL and UUNET were some of the larger ISPs dominating internet access. AOL had grown its user base significantly by distributing free trial CDs, so much that at one point in the 1990s, 50% of all CDs produced worldwide were for AOL (Siegler). AOL then held onto its large user base by creating what is known as a "walled garden", limiting its users access to the internet only to sites owned by AOL itself, and in doing so closing off the internet.

ISPs started to form into an oligopoly as time went on, with very few companies controlling most commercial internet access. Especially after major mergers in the early 2000s, including those between AT&T and Comcast as well as AOL and Time Warner, the U.S. internet service provider market began to consolidate significantly. By the mid-2000s, the ISP landscape was dominated by a small group of major companies, including AT&T, Verizon and Time Warner, leading to an oligopoly. These companies controlled both the infrastructure for providing internet access and a significant portion of media content.

This consolidation created limited competition, with these few companies setting the standards for internet pricing, service quality, and access. It also allowed them to prioritize profit through tactics like data caps, throttling, and high subscription prices. As a result, they gained even more control over the growing digital landscape, making it difficult for smaller providers to compete. This oligopoly further solidified as the major ISPs increasingly acquired or merged with content companies, aligning their interests with the broader commercialization of the internet.

4.4 Commercial Creep

However, profiting off of selling internet access was seen by most as the tip of the iceberg of what was to come out of the Internet. Especially with traditional methods of profit-making deemed less useful by Napster and its likes, companies started to look at non-traditional ways of earning from the Internet.

The Internet had already started to be seen as a space of advertisement, and HotWired, the first commercial online magazine, brought forth the idea of banner ads. By 1994, companies like NetScape were already entertaining the idea of tracking user behavior to serve relevant ads through the use of cookies. Especially after Google's revolutionary approach to user tracking and data collection, the Internet had set route to a completely different future than the cyberlibertarians of the 1990s had imagined.

5 Web 2.0: The Social Web

Throughout the 2000s, companies found ways to protect themselves from getting hurt by the chaos of the Internet, and even profit off of it. While they successfully mitigated the damage to traditional media sales via subscription services, and

diminished the inexpugnableness of the internet with social media websites that create walled gardens and use content algorithms to keep users engaged, they exploited the lack of regulation by collecting incredible amounts of data from users to feed content algorithms curating both ads and content. Lawsuits against Napster and Limewire caused the platforms to shut down in 2001 and 2010 respectively, and streaming turned out to be profitable despite online piracy. The new age of the Web had begun.

5.1 Web 2.0: The Social Web

The new Web signified near-total corporate control over the Internet. Today, corporate and commercial websites make up more than 80% of global web traffic (Statista). Web 2.0 is defined as the read-write internet. Users were now allowed not only to read on the web, but also to create and interact with the websites, commenting on others, making their own content, all without leaving the initial website. User generated content became the driving force of the Internet with the new web, which then fueled the rise of social media and blogs. The newly risen social media giants looked at ads as the revolutionary source of revenue. They began collecting excessive amounts of data, often without user consent, and used it for targeted ads and for increasing screen time and keeping users on the platforms. Surveillance capitalism was afoot.

5.2 Big Data and Surveillance Capitalism

Surveillance capitalism, as defined by Shoshana Zuboff, is a new economic order that claims private human experience as free raw material for data extraction, prediction, and profit. As methods of collecting and storing data improved, almost every move anyone made on the internet became trackable and recordable. These large amounts of complex information were called "Big Data", and as methods of analyzing big data evolved, so did companies' ability to better profit off of it. Using these data, companies became able to target their ads better and increase screen time, limiting personal and collective futures by preempting behavior in the process.

In this new era of the digital space, owning as much of the internet as possible became drastically important. Of course, no one "owns" the Internet in the traditional sense, nor is it divided into parcels of bytes like pieces of land, however hosting as much internet traffic as possible became the goal for many companies. "User-friendly" search engines like Google, major physical server owners like Amazon, monopolistic ISPs, and most importantly intentionally and increasingly addictive social media websites like Facebook or Twitter thrived under surveillance capitalism.

5.3 Cookies and Tracking

A cookie, in its simplest definition, is a small piece of data that a website stores on your browser. It contains your activity on the website, such as your last

logged in account, items in your cart, your website setting, etc. They are crucial for lots of websites to work, and aren't necessarily used for surveillance and tracking, however most websites and third-party advertisers plant unnecessary cookies in browsers, gathering information on the sites you click on, ads you look at, posts you engage with, and even your cursor movements (Mims). This excessive amount of data creates "behavioral surplus", which could be defined as excess information on your behavior that could be used to better understand, preempt, and even manipulate how you act. These are then either used for targeted ads, or fed into content algorithms.

5.4 Content Algorithms

As stated, one of the major commercial goals during Web 2.0 is to "own" as much internet traffic as possible. That is done by getting users to use your website, and keeping them from leaving for as long as possible. Notifications are an obvious method for getting users back online, creating walled gardens that keep users from leaving the app is another, exemplified by social media apps launching "mini-browsers" inside their apps instead of sending you to your preferred browser when you click on a link. Yet, at the core of this goal lie content algorithms. Content Algorithms are, in the context of surveillance capitalism, machines that utilize large data sets and identify patterns to make decisions on what content to put on a person's feed to keep them on the website for as long as possible. These algorithms track and analyze a grotesquely large amount of data, so much so that their method is sometimes simplified as "creating a digital replica of a person, and experimenting on it". These algorithms have intentionally and unintentionally had manipulative real life consequences like the Cambridge Analytica scandal where they were used to alter voter behavior, or algorithmic radicalization which stands for the tendency of social media algorithms pushing people into the further corners of their corresponding political stances by creating filter bubbles and confirmation biases.

Although in many countries across the world there exist several restrictions on tracking and algorithms that enforce consent rules or even outright bans, like the EU's GDPR law, today the digital has become a land as vast as the material, and it has been subjected to near total commercialization. Persistent cookies ensure that even when visiting non-commercial websites, our preferences and actions are recorded to enhance targeted ad and content algorithms. What happened then, to the initial and inherent chaos of the Internet? Has cyberspace been tamed, and its idealists defeated? Not by a long shot. In fact, now more than ever, every piece of innovation to come out of the Internet reminds the world of Internet Entropy.

6 Instances of Internet Entropy

As argued in chapter one, the technology that makes the Internet work is inherently anarchic, and this anarchy leaves its traces in many pieces of technology

that comes out of the internet. Even the most commercial of innovations can have an uncontrollability to them, which causes companies to either gatekeep the full functions of new innovations, or shut down projects altogether. These traces of chaos are defined as Internet Entropy. They are a manifestation of the Internet's tendency to recreate its initial form of anarchic functioning, and it is the nature of the digital. To look for instances of Internet Entropy, one has to search for technology that is inspired either by the early technology of the internet and its four anarchic characteristics, or for movements and ideologies that have inherited from the ideas of early cyberlibertarians. Throughout internet history, an abundance of evidence is visible to the naked eye that shows how Instances of Internet Entropy shine in the past, in the now, and in the future.

6.1 Torrent and Online Piracy

Although Napster and Limewire paved the way, it was the Bittorrent Protocol that irreversibly altered the Internet's approach to media consumption. With it, online piracy had reached new heights. Online piracy existed decades before Napster, people would copy software onto floppy disks and share them with others without concern for copyright law. With the invention of the Bittorrent Protocol, illegal sharing of copyrighted material such as films, music, games and software skyrocketed. (U.S. Copyright Office)

Bittorrent works through basic peer-to-peer file sharing, and its idea of dividing files into bits of data to increase efficiency and flexibility is highly influenced by packet switching. With both ideas, the protocol became an innovation that leveraged and increased the anarchic backbone of Internet technology in its favor, and in that sense the technology behind it is an undeniable example of Internet Entropy.

6.2 Anti-Surveillance Resistance: VPNs, Tor, and the Dark Web

As governmental and commercial surveillance grew, the Internet replied with methods of preserving privacy and anonymity. These methods such as VPNs and Tor have been community driven, and many of them are open source and decentralized.

VPNs encrypt users' internet traffic, masking their IP addresses and locations. By rerouting connections through different servers, they enable users to bypass geographical restrictions and censorship, providing a degree of privacy in a monitored digital landscape.

The Tor network on the other hand, offers a more robust solution for anonymity by routing traffic through multiple volunteer-operated servers, encrypting data to make tracing nearly impossible ("The Tor Project"). This structure supports the Dark Web, which, while often associated with illicit activities, serves as a haven for free speech and activism, especially in oppressive regimes.

These anti-surveillance technologies play crucial roles in fighting for privacy in the commercialized internet, and embody internet entropy in recreating the

anarchic processes of the early internet.

6.3 Mesh Networks

A mesh network is a decentralized network structure where every device, or "node," connects with multiple other devices, creating a dynamic, web-like system. Unlike traditional networks, which rely on central routers or servers, mesh networks allow data to travel through any node, taking the most efficient route. This decentralized setup makes them highly resilient, as data can automatically reroute if one node fails. They are used in environments where traditional infrastructure is limited, like rural areas or disaster zones, and can even be set up for community-driven internet sharing.

Mesh networks embody the principle of internet entropy, a concept that reflects the internet's tendency toward decentralized, self-organizing systems. As they don't rely on centralized control or large ISPs and service providers, mesh networks offer a form of technological anarchy, where each participant contributes to the system's resilience. This unpredictability, where no single entity governs data flow, aligns with the early internet's chaotic, decentralized nature. Much like peer-to-peer networks and early file-sharing systems, mesh networks thrive on self-organization and resistance to central control, making them inherently entropic.

6.4 Blockchains, Cryptocoins, and DeFi

A more recent and more relevant instance of internet entropy is the creation and widespread use of blockchains in cryptocoins. Starting with Bitcoin, cryptocoins are digital currencies aiming to create a more private and decentralized alternative to traditional digital banking, essentially being the equivalent of "digital cash". The blockchain technology that helps the functioning of these currencies works in such a way that each node in the network keeps track of all transactions happening in the network, and in set time intervals one (or more) of the nodes are chosen to validate the new transactions. This validator is chosen via the use of different methods such as proof of work or proof of stake. These validators then create blocks, and that block is connected to all the blocks that came before it, creating a publicly available history of all transactions that have happened in the network. There are differences between each cryptocoins and proof systems functioning, but in essence, these systems allow the networks to stay resilient to attacks, private, yet still decentralized.

These blockchains also enable DeFi, or Decentralized Finance through the use of smart contracts. By enabling globally accessible, low cost, decentralized and transparent finance, they challenge traditional banking. Blockchains draw from the ideals of peer-to-peer connections and decentralization, and their entropy challenges to drastically alter the material world.

6.5 Web 3.0

Through blockchains and the technologies they enable like smart contracts and decentralized applications, some have predicted that the Internet is on the verge of another major transformation, this time in favor of decentralization. The decentralization that may come out of the transition into Web 3.0 holds increased privacy and user control over data, fewer intermediaries and reduced censorship, permissionless access across the web, and overall an Internet free of surveillance capitalism.

The feasibility of Web 3.0, however, is frequently challenged by Internet theorists. The promises of the new web are deemed too ambitious to keep, and the scalability and security of the systems are nowhere comparable to those of Web 2.0, yet. In addition, even trailblazers of the new cyberspace are pessimistic, saying that Web 3.0 would decrease the profitability of the Internet, and "Companies would have to change their structures dramatically to transition into Web 3.0". Nonetheless, the Internet and its newest innovations hold the potential to reestablish its decentralized, free to enter, non-hierarchical and autonomous youth. Web 3.0, is Internet Entropy. Here and now.

7 Conclusion

The Internet, once a wild and untamed frontier, was born from a spirit of freedom, anarchy, and idealism. It promised a digital landscape unbounded by the hierarchies and controls of the physical world—a space where decentralized, peer-to-peer networks could flourish, and autonomy reigned. Yet, like all things wild, it was inevitably captured, corralled, and commodified. The dream of an open cyberspace, free from corporate greed and government control, has dimmed, replaced by an oligopoly of tech giants, endless surveillance, and the monetization of our most intimate data.

But the spirit of the early Internet—the chaos and entropy at its core—has never truly died. It lingers in the dark corners of the digital world, in the rebellious lines of code that power torrents, blockchains, and decentralized apps. It whispers through mesh networks and anonymized traffic, in the users who still resist the ever-tightening grip of surveillance capitalism. The Internet's original anarchy, though diminished, pulses beneath the surface, ready to reemerge in unexpected ways.

Perhaps the future of the Internet lies in this tension—between the forces that seek to control and profit from it, and the entropy that defies such control. The rise of Web 3.0, with its promises of decentralized applications and user-driven governance, offers a glimmer of hope that the Internet may once again return to its roots. Yet this future is fragile, and the path forward is uncertain. Will the Internet finally succumb to total commercialization, or will its inherent chaos find new life in the technologies of tomorrow?

The Internet, after all, is not just cables, servers, and code—it is a reflection of human will, desire, and defiance. It is a mirror of our struggle for freedom in

a world increasingly bent on control. And as long as there are users who dream of an Internet unchained, there will always be moments of entropy, cracks in the system where the original chaos of cyberspace seeps through. In these moments, fleeting as they may be, the Internet that once was—the Internet that could still be—survives.

References

[1] Abbate, J. (2000). *Inventing the Internet*. MIT Press.

[2] Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Retrieved from `https://www.eff.org/cyberspace-independence`.

[3] Berners-Lee, T. (2008). *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*.

[4] Bookchin, M. (1974). *Post-scarcity Anarchism*. Wildwood House.

[5] Chun, W. H. K. (2006). *Control and Freedom: Power and Paranoia in the Age of Fiber Optics*. MIT Press.

[6] Czetwertyński, S. (2016). Opportunistic Behavior and Copyright on the Example of Bittorrent. *Studia i Prace WNEiZ*, 44, 59–72. doi:10.18276/sip.2016.44/2-05.

[7] Kıranoğlu, G. (2016). Copyright and the Internet: The Case of Napster. *Journal of Human Sciences*, 13(2), 2758. doi:10.14687/jhs.v13i2.3839.

[8] Krol, E., & Klopfenstein, B. (1996). *The Whole Internet User's Guide & Catalog*. O'Reilly Media.

[9] Kropotkin, P. (1990). *The Conquest of Bread*. Black Rose Books.

[10] Landstreicher, W. (2009). Autonomous Self-Organization and Anarchist Intervention: A Tension in Practice. *The Anarchist Library*. Retrieved from `https://theanarchistlibrary.org/library/anonymous-autonomous-self-organization-and-anarchist-intervention-a-tension-in-practice`

[11] Lanier, J. (2010). *You Are Not A Gadget: A Manifesto*. Penguin UK.

[12] Leiner, B. M., et al. (2009). A Brief History of the Internet. *ACM SIGCOMM Computer Communication Review*, 39(5), 22–31. doi:10.1145/1629607.1629613.

[13] Lyon, M., & Hafner, K. (1999). *Where Wizards Stay Up Late: The Origins Of The Internet*. Simon and Schuster.

[14] Mims, C. (2011). The Next Big Thing in Analytics: Tracking Your Cursor's Every Move. *MIT Technology Review*. Retrieved from `https://www.technologyreview.com/2011/05/20/259194/the-next-big-thing-in-analytics-tracking-your-cursors-every-move/`.

[15] Chartier, G., & Van Schoelandt, C. (2020). On the Distinction Between State and Anarchy. In *The Routledge Handbook of Anarchy and Anarchist Thought*.

[16] Pool, I. de S. (2009). *Technologies of Freedom*. Harvard University Press.

[17] Parvin, J. R. (2020). An Overview of Wireless Mesh Networks. In *Wireless Mesh Networks - Security, Architectures and Protocols*. IntechOpen. Retrieved from `http://dx.doi.org/10.5772/intechopen.83414`.

[18] Rheingold, H. (2000). *The Virtual Community, Revised Edition: Homesteading on the Electronic Frontier*. MIT Press.

[19] Schmidt, E. (1999). Internet World Trade Show.

[20] Siegler, M. G. (2010). How Much Did It Cost AOL To Send Us Those CDs In The 90s? 'A Lot!,' Says Steve Case. *TechCrunch*. Retrieved from `https://techcrunch.com/2010/12/27/aol-discs-90s/`.

[21] The Tor Project. (2024). *Anonymity Online*. Retrieved from `https://www.torproject.org/`.

[22] Turner, F. (2010). *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. University of Chicago Press.

[23] Wu, T. (2010). *The Master Switch: The Rise and Fall of Information Empires*. Atlantic Books.

[24] Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.