Decentralized Internet

Zhanglong Peng, zhanglongpeng@wustl.edu (A paper written under the guidance of Prof. Raj Jain)

Download

Abstract:

Decentralized internet is a people-powered kind of internet that makes the web more democratic as there is no hosting company. This research looks into the various platforms offered by protocols that adapt to the decentralized networks and their aim to contribute to the shift from the current centralized network. There are benefits alongside the decentralized network that act as proof for the need to change. Initially, the internet was not designed to be centralized. This paper analyses why there is a need to change back to a decentralized system through the analysis of how the network protocols work. Through the analysis of the underlying protocols, it is possible to find the motivation towards a free and secure network that is not controlled or owned by tech giants. This paper investigates the reasons behind the need for a decentralized network. Focus is also directed towards the applications of the architecture based on research and how the present decentralized applications and protocols have adopted the technique and put it to use to combat the challenges faced by the centralized system.

Keywords

Decentralized internet, centralized internet, secure network, IPFS, SSB, IoTeX, BitTorrent, Privacy, Dat

Table of Contents

1. Introduction

The internet started with the Advanced Research Projects Agency Network (ARPANET) during the year 1969 where a successful network connection between UCLA and Stanford Research Institute was achieved. The two computers were able to send a message from one node to the other making it possible to establish a unique transmission. The American Department of Defense pioneered the main intention of creating the internet to create an impenetrable communications network hence the need for it to remain decentralized [Tabora18]. In terms of security, the decentralized network was more secure since each node was independent without reliance on another - peer-to-peer connectivity. The extra dependency of people on the internet paved the way for it to be commercialized when the tech companies realized that they could make money out of the venture. Through the development of TCP/IP, WWW and HTML, Browser, Search Engines, and ISPs, the internet would not have achieved mass adoption [Tabora18]. Hence, ARPANET and NSFNET were decommissioned to make way for the current tech giants.

Recently, the internet has become part of ordinary people's lives, whether they are aware or unaware of its existence. Society seems to be networked by an invisible wire considering the rate at which information is disseminated nowadays and the ease to reach out. From social media influencers, gamers, and content creators, more people rely on the internet for their daily needs or the paycheck at the end of the month. This shows just how the internet has transformed as compared to a few decades ago, where people had to rely on the traditional approach to careers and handling information. The internet suddenly shifted from being decentralized to being centralized. However, networking back is not impossible in a world full of stand-alone appliances [Zittrain08]. There are several decentralized networks that are achieving success during this era.

2. Reasons why the Web is Centralized

The internet adopted a centralized network [Hindman18],. There are two websites with almost similar content and many interested consumers who visit both sites equally. Both sites will then try to bridge any possible gaps in losing their consumers by finding the mutual interests that their consumers prefer. Once the topics are identified, the sites will tend to strengthen their references by making the consumers' interest readily available through the analysis of the data both sites share on the client. This is a typical marketing approach that is adopted by most monopolies for the sake of directing traffic to one network and reaping the most profits.

Currently, people are becoming conscious of the internet monopoly that has influenced how services are delivered online. Platforms such as Google, Amazon, and Facebook are among the tech giants that have taken over the internet, making users dependent on them for information or entertainment. They make their content quite appealing to the extent of pulling in a large crowd of consumers. According to Tabora [Tabora18], the problem is that these tech giants have monopolized the market, making their sites the only options for the items of preference. The principle concept of Net Neutrality points out that all websites should be given equal opportunities by service providers to compete for consumers [Hindman18]. However, it seems that users always end up on the tech giant's sites since they offer better quality and reception.

3. Disadvantages of the Centralized Network

Users have begun to gradually notice the negative impacts and challenges of the centralized internet. Centralized networks tend to be a single entity that is aware of the full network and resource state of the multi-domain network [Aracil09]. This means that the centralized network is not safe from a breach and neither is there guaranteed privacy. The owners of the platforms people use may decide to retrieve information concerning clients in an easy way. It is also possible to manipulate the decisions of people online through the information provided unconsciously when browsing the internet. As a result of data mining, firms can predict behaviors of consumers through the trails of patterns they leave behind as they search the internet [Aracil09]. This has led to a lot of controversy especially from a legal aspect since companies are illegally using consumer data to make more profit from the results gained.

Despite the fact that the centralized system is easy to implement and reconfigure, it faces the challenge of failure in case the main servers are corrupted. This makes the approach not scalable for use in a large network such as the internet today [Aracil09]. A centralized network is much easier to attack compared to a decentralized one. Networks with several nodes that support various operating systems offer better protection since it's difficult to hit both nodes at the same time and paralyzing operations. Decentralized networks offer better security and acts of fairness as opposed to the centralized system that does not offer transparent democracy.

4. Methodology

This research paper aims to answer the question: Why is decentralization useful? The approach used for the research is qualitative, thus giving deeper insight into the reasons, opinions, and motivations to pursue decentralized internet in networking. The study focuses on the "why" of the decisions made to support this type of architectural network. The research is based on a collection of past materials that address the same issue in the hope that a holistic view will be achieved to help understand the need for decentralization of the internet.

5. Analysis of Decentralized Internet Systems

5.1. BitTorrent

BitTorrent is a protocol that supports peer-to-peer file sharing to distribute large amounts of data around the world. Essentially BitTorrent takes the stress of transferring data files from one massive server to every user over an extremely robust network and splits it up to multiple normal PCS and multiple smaller networks. A study conducted ten years ago showed that P2P file-sharing contributed to 66% of traffic in South Africa, 65% in South America, 70% in Eastern Europe, 55% in Southern Europe, and 54% in Southwest Europe [Kong12]. This goes ahead to show the popularity in the communications protocol among users of the internet. Unlike the client-server approach where users depend solely on the file's original distributor, BitTorrent is a form of decentralized network that allows adequate mirroring.

Users can then enjoy fast downloads since there are no bottlenecks, and the host does not incur bandwidth charges due to popular downloads [Fehily13]. BitTorrent downloads continue downloading from the moment they were interrupted once they are reconnected back to the internet. The download is not lost in the case of a power failure, system crash or lost connection [Sia06]. That is one of the reasons why BitTorrent has gained so much popularity over the years leave alone its ability to download large data files.

The steps in BitTorrent are:

1. One Seeder: For the first time a file is shared, there is a single seed for the user who is uploading a file for the first downloader. So a torrent will relatively be slow when it is first created. When the file is first saved on the storage media, it is known as a torrent file. However, when it comes to sending over the file, the metadata is usually sent but not the file itself. The metadata contains information about the file that details the type of content on the file and the location to the storage media to retrieve the file in case the receiver requires to download it [Sia06]. The user will then choose a tracker to follow up on the file-sharing.
2. One seeder or One leecher: at this point, the first leecher is still downloading from the seeder but has not yet completed the download when a new leecher joins in and starts downloading as well. Now, this is where the whole idea of decentralization comes in. Unlike in a server-client network where users do not communicate and wait upon the server to give them the file, BitTorrents allow users to share the bits and pieces of files they already have. Therefore, the new leecher may receive pieces of the file that the first leecher does not yet have and then share them with the first leecher [Sia06]. A connection is formed where the users are all sharing bits and pieces of information hence creating a more reliable and stable independent network.
3. Two seeders/many leechers: once a leecher has acquired the whole file, they move up the chain and become a seeder, enabling other leechers to download from them.
4. Many seeders/many leechers: at this point, most of the users have the complete file and are no seeders. The original seeder does not play a critical role anymore and can quit without affecting the operations of the others. Leechers can also pause downloads and continue during another time [Sia06]. The tracker monitors the communications in the absence of the original seeder.
5. Few seeders/few leechers: as time passes on, the swarm decreases, but this all depends on the popularity. Torrents may have seeders for a long time, depending on the need for people to acquire that specific information. However, as the swarm shrinks, download speeds slowly die down.
6. Death: the death of a torrent is considered as the point where there are no seeders.

5.2. InterPlanetary File System (IPFS)

The main aim of IPFS is to create a decentralized file-sharing system while at the same time storing records on those files so that they are never lost. Protocol Labs are responsible for the development and maintenance of IPFS. One can say it is similar to BitTorrent, but then it is also similar to Kademlia. In real sense, it is a combination of both. Users can store and refer to files using their hash [Rajput19]. As much as this network system may sound convincing as a decentralized network, it may not apply to all applications and mostly gains popularity with information sites such as Wikipedia and academia. In the future, it may come in handy as a way to store information critical for historical purposes or research making it a reliable tool for educational systems.

Structures of IPFS

IPFS is the result of the combination of Git, BitTorrent, and Hash Tables. Git is a distributed version control that is mostly used all over the world. Programmers prefer to use Git because of its adaptability to Integrated Development Environments [Kempen18]. IPFS uses the Merkle Directed Acyclic Graph (MDAG) that allows for communication among independent nodes within a non-cyclic graph. The IPFS MDAG consists of blobs, lists, trees, and commits commands. All these controls rely on the BitTorrent protocols to communicate, upload and download information. A blob is a set of bytes that may represent anything from a file, image, or code. A tree represents a hierarchy or some form of a directory that may be connected to other trees or blobs. A Git commit points to who committed the previous changes through the email address or name. There is also the structure of BitTorrent, but the difference is that there are not trackers in IPFS [Kempen18]. The developers of IPFS consider trackers to be centralized hence beating the whole purpose of creating a decentralized network. The network then uses distributed hash tables instead.

Introduced in the early 21st Century, Distributed Hash Table has gained popularity as the Mainline DHT is the most used method to find peers without relying on a third party. Such a method gives users complete control or reliance on a centralized system. The DHT system used on IPFS is a combination of both Coral and Kademlia, which originate from the parent Kademlia DHT system [Kempen18]. The combination of these two systems offers better security as well as improved look uptime. The diagram below shows the difference in the network architecture between IPFS and current HTTP.

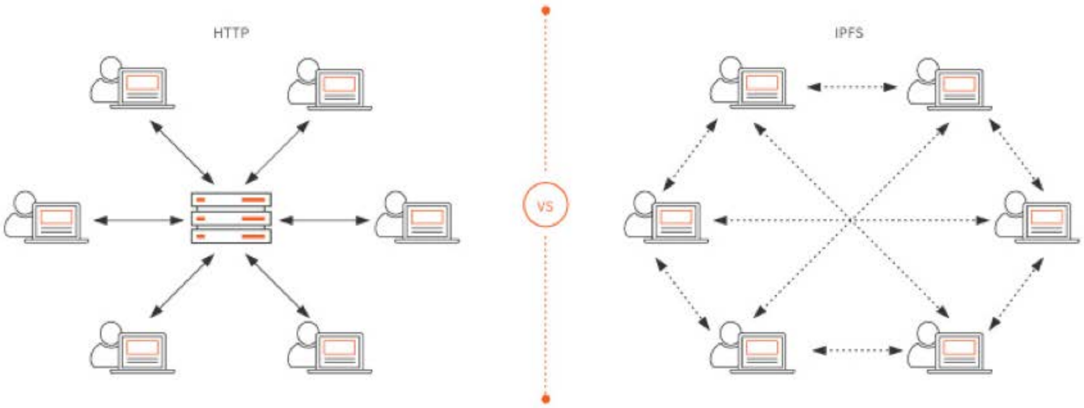

Figure 1: The difference in the network architecture between IPFS and current HTTP.

Shortcomings of IPFS

The main problems to IPFS are immutability and hash collisions. IPFS prefers to reference data rather than duplicating it. Whenever a user creates a file, the file is broken down to portions of 256kB. If any of those portions is similar to an already existent blob, the user will be required to reference that blob. No two files contain the same data independently. The problem comes in with the referencing since it may prove difficult to refer to the latest version available. This requires that the users allocate a lot of time and practice to get it right [Kempen18]. The solution to this problem includes the use of IPNS and DNSLink. Hash collisions, on the other hand, occur when two blobs with the same hash are received during a request over the network. This is because the system fails to have a hash check, and there have not been any implementations regarding this issue. The probability of a collision according to the SHA-256 algorithm is relatively low at the moment, but soon, it may be possible for a collision to occur [Kempen18]. This problem may be dealt with through the use of the built-in "multi hash" system where the hash system can be easily changed until another problem occurs.

5.3. Secure Scuttle Butt(SSB)

SSB is a distributed social network that is responsible for replicating messages for the users connected to the internet. Each node is referred to as a Scuttleverse giving the impression of a networking universe that the system intends to create. The network uses Patchwork technology through the implementation of the commands found in its library. Mainly, Patchwork is more relevant for the desktop versions, while Manyverse is often used for mobile applications [Tarr19]. The fascinating idea behind SSB is that it can function offline. When it comes to decentralized networks, the whole idea is to detach from the centralized system including internet providers. SSB offers exactly this since the users can perform functions without network connectivity. Similar to IFPS, SSB also uses similar techniques such as Git, where there is a distributed version control system. When offline, the users can perform all kinds of activities supported by their Git repository. Users can go online through connections over the Wi-Fi, Ethernet or Bluetooth where they can send other users' images or files [Tarr19]. Another advantage of SSB is that it allows users to discover each other over the local network.

How SSB Works

Each user on the SSB has a unique private key allocated to them. These private keys allow for the users to write to their logs and determine who gets to see their messages. They also have the authority to determine who can write on their log as well. When a message is sent, it must reference the message it is written in response to while at the same time, each new message is allocated a sequence number [Tarr19]. The ID represents the original message and links the messages through the chain. It is because of the hash and signature that the ID is unique. Through these interlinked messages, otherwise known as a feed, authorized users can read through the chain of messages and understand the message being conveyed [Mota19]. Once a user authorizes another to send or receive messages from their feed, they can verify that the messages sent belong to the authorized user through the identifications of their signatures on the sent messages. The figure below represents the high-level structure of a feed example.

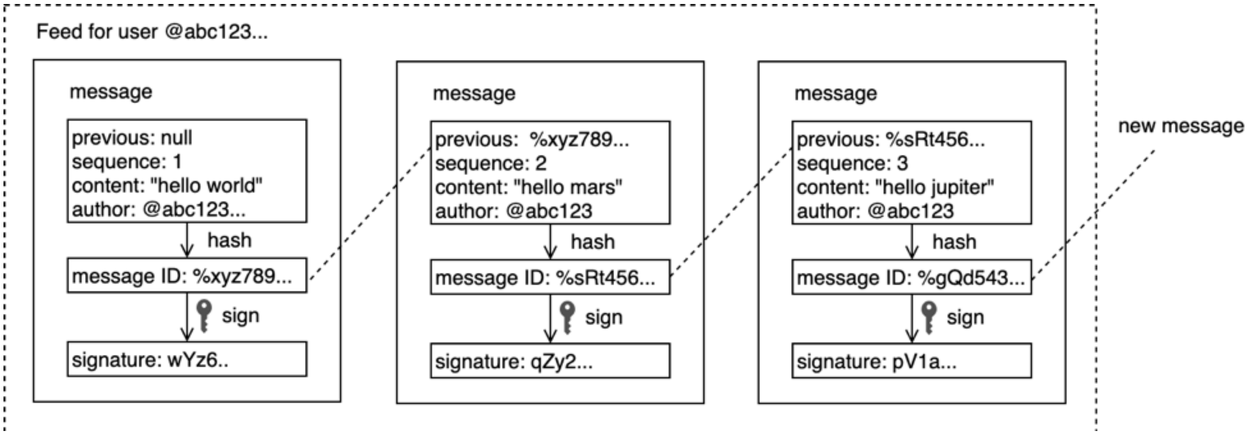

Figure 2: The high-level structure of a feed example.

There is also the use of Pubs that resemble real-life experiences. SSB aims to give the decentralized network a platform similar to the social media platforms that are available on the centralized web today. However, this network is free from dependency on the third party and relies on the interests of people to pass information in a secure and less controlled environment. What pubs do is, they allow people to communicate in large groups through invitations to join the group [Tarr19]. Some groups require more than an invite and request verification through emails. Another definition of SSB Pubs is through the connection of people who are within the same vicinity. Pubs are large nodes that allow people to connect even when they travel. Users can send messages to their friends or colleagues, and they are relayed through the users connected to SSB until they reach their destination. However, clients who are not following the sender may decide to filter out the message such that it never gets to the receiver. In terms of security, SSB is reliable since it uses cryptographically signed keys to send the messages over the peer-to-peer network [Mota19]. Even though a user may filter out a message passing through their node, they are not able to view the details of the message. Once the private message gets to the receiver, it is decrypted by the same key.

5.4. Dat/Hypercore/Beaker

Just like the others, Dat is a data distribution system that allows for tracking and making changes to data sets. However, Dat is slightly different from IPFS and SSB in that it does not use the hash system but rather implements the use of Public Key Addressed file archives such as zip files [Farmer18]. The good thing with Dat that sets it apart from other decentralized network protocols is its ability to accommodate multiple writers, at the same time enable them to merge sites. Dat protocol focus on enabling analysts to make changes to data through collaboration over the network. With their initial release dating back six years ago, Dat has been able to release a more stable version just a few months ago on 17th April 2019. The protocol supports Linux, macOS, and Windows operating systems making it easy for most users to be a part of the decentralized web. The protocol is written in JavaScript and is funded as a non-profit under the United States of America [Farmer18]. Dat registers among the fastest-growing decentralized networks that have the potential to support future applications. The protocol aims at giving researchers the chance to share large files of data with each other, which is helpful to the world of learning and education. Another major point that has gained popularity for Dat is that it allows users to create their websites without the use of a web hosting service. This eliminates the middleman which is the main aim of the decentralized web [Robinson18]. Rethinking how data is owned, preserved and managed is the motivation to pursue a decentralized architecture.

Properties of Dat

Dissemination of information has made developers rethink the structure of the internet even though most of it remains centralized. Dat can archive dynamic datasets of any size while a unique identifier tracks the folder for the package [Robinson18>]. Even though the content may change, the identifier remains the same, unlike the case of IPFS where the change in content changes the unique key. However, the changes are noted, and Dat allocates a changelog to the item that was changed. This gives the users a chance to view previous records such that they can make comparisons or deduce why the version was updated. There is also a transparent log of the history of the object [Robinson18]. Another property of Dat is that creators are allowed to authorize downloads to other users making the object readily available in various locations. Link rot is reduced since organizations can download and store valuable files.

In the case of Hypercore and Beaker, these are the storage content and browser of Dat. Hypercore involves the networking rules that govern Dat as well as the storage and content of the protocol. The hypercore is the backbone that is fundamental to the building of Dat since dat-related modules can work off it. Understanding the Hypercore gives more insight on Dat and how the feeds work. The protocol is defined by buffers, while feeds are binary append-only [Robinson18]. The protocol implements the use of hash and signatures within cryptographical keys that give the users read keys when messages are sent. Through understanding hypercore, one can realize that Dat is relatively safe and secure from a breach. Beaker is the browser that supports Dat and acts as an interface for users who are looking for files or need to edit and publish objects. Beaker uses the Dat protocol to run its features and benefits from the protocol due to its security and efficiency [Robinson18]. The relationship between Beaker and Dat has created a way for people to interact on the decentralized web in a much more advanced and easier way as opposed to other network architectures that fail to provide an easy to use interface for their users.

5.5. IoTeX Mainnet Alpha

IoTeX is a blockchain solution that connects the Internet of Things in a network environment such that information can be passed around. The aim is to integrate Internet of Trusted Things and privacy within the blockchain, which happens to be the most trusted crypto company. IoTeX Mainnet implements Root Chain on which new Layer 2 chains, tokens, Apps, and businesses will be launched. The main aim is not only to add trust to IoT but to also create a decentralized network that will promote trust from node to node. IoTeX is the biggest firm that focuses on the integration of blockchain technology with large scale IoT devices, and they believe that they will transform the world through the implementation of privacy and trusted computing [Reilly19]. IoTeX aims to be the tech giant in the future since their vision is to power all things to fit a decentralized economy.

How Mainnet Alpha works

The Root Chain employed by the L2 chain by Mainnet is reliable in terms of security, and transparency since it implements the use of Roll-DPoS. Like any other decentralized network, the Mainnet uses peer-to-peer technology that is provided by the Root Chain. Another feature that makes the Root Chain advantageous is that it gives developers the freedom to customize their L2 chains [IoTeX19]. Developers are also able to communicate with each other thanks to the Root Chain that supports L2 intercommunications. These L2 chains can be changes and serve various purposes. Therefore, developers are not limited and can execute their ideas such as permissioned vs. permissionless, storage vs micro-transaction focused, privacy vs. transparency centric [IoTeX19]. IoTeX remains to be open source with the hope that developers will learn from it, experiment, and collaborate on the network. Through the Mainnet Alpha, IoTeX has introduced the IoTeX Native Token that will be used for decentralized governance where user will be able to vote in regard to how the network is run and the rules/laws that govern it. Users will also be able to transact over the network using the tokens.

There are key components that come along the Mainnet Alpha, and they include Roll-DPoS Consensus, Ethereum-to-IoTeX Bridge, Extensible State Transition, SDK, and Explorer and EVM-compatible execution unit. These components allow for secure scalability, interoperability, extensibility, advanced developer ability, and portability. As IoT devices are increasing in the population, the need for data privacy is also dire. The devices in the IoT ecosystem tend to be resource-constrained and lack security measures to protect the users [Boncea19]. At the top of IoTeX is blockchain, which is open, distributes and single shared tamper-evident ledge for maintaining permanent records of transactional data [Boncea19]. IoTeX uses cryptographical blocs that entail hash, timestamps and transactional data. IoTeX is also relevant to real-life examples making it stand a chance in popularity in the near future as people get more familiar with IoT and AI. Through the integration of IoT and blockchain, users can control and authorize use of their smart homes in a fully P2P fashion [Kim19]. The consensus algorithm implemented in the blockchain technology enables users to transmit information through the connection of nodes. Since the network is a distributed database, people may have control over their IoT through the network even when they travel.

6. Findings/Results

From the research through various sources to determine the usefulness of a decentralized network, it is possible to come up with some reasons that justify these needs. At the top of the list, developers encourage a decentralized system because of fault tolerance, attack resistance, and collusion resistance. This goes ahead to show that a large number of developers do not have faith in the current network since it may cause chaos in the case of a collapse of the main serves. Most of the decentralized network protocols tend to rely on distributed systems or peer-to-peer networks because it offers a more reliable approach to preserving the data online [Ramaswamy05]. The fault tolerance of a centralized system seems to be quite low, and people are more likely to lose their data on such a system. That is why most of the decentralized networks used the peer-to-peer BitTorrent methods to store files in more than one location. For a centralized system, the files are all stored on a server that required backing up, or else files are lost in case the server fails. Fault tolerance means that a network continues with its operations in the case of a component failure [Fehily13]. In the case of a centralized system, all operations are doomed to come to a standstill in the event of failure. That is not the case with peer-to-peer networks, where only the affected component stays out of service. Information continuity is possible with decentralized systems such that it's not possible to notice that there is a fault within the network.

In the case of attack resistance and collusion resistance, decentralized systems exhibit the best characteristics in resisting manipulation or collusions. Recently, people have noticed that the tech giants controlling the internet are using personal information for financial or political benefits. Decentralized systems are not easy to attack since they are connected in a distributed manner. To attack such a system would require a significant amount of resources or capital [Singh05]. This would make it difficult to gather information about people for the sake of manipulating them. A decentralized system is more secure since they lack sensitive central points. Attacking such a system would mean attacking all the nodes that support the target station, which is extra work. In terms of collusion, it is nearly impossible that users on the decentralized system would collude to benefit from other members on the network. In most government networks, the leaders may collude to benefit themselves from the members of the network. This is not the case with decentralized networks since they promote high privacy for individuals hence making them resistant to attacks such as phishing for information or manipulation.

Even though a number of nodes may be compromised, the perpetrators may only influence a number of nodes before being noted and censored. These are some of the reasons that stood out to support the need for a decentralized system. Developers feel that they need to create a working environment that supports privacy and is faultless at the same time. The current manipulation by the big tech companies through data mining portrays the inefficiency of the centralized network in terms of data protection. Adopting the decentralized system enables users to experience data protection and break free from the manipulation from governments and corporates [Choffnes08]. Developers are hoping to take back the internet to its original use of free and fair communication that is free for all without reliance on a middleman.

7. Discussion

The debate among network analysts that focuses on decentralization of the internet in a networking aspect is more than just security. It also focuses on the need for fewer responsibilities for the sake of addressing latency problems and the issue of mass adoption. These are but a few of the major hurdles to be dealt with the introduction of the system. Even though people's desire for transparency is increasing with the ongoing privacy scandals by tech giants, the introduction of the decentralized system may not be as smooth as most people think [Choffnes08]. An example is the issue of mass adaption. It is quite easy to understand how decentralized internet works and learn how to work around the applications the same way people learned how to use centralized networks. However, as long as nobody is using the network yet, people will most likely shy away from it making it hard to implement. According to Hindman [Hindman18], there has been an increase in feelings towards breaking up tech giants that promote anti-competitive behavior. That may motivate people to move towards the decentralized internet options. Issues such as votes may also force people to think of decentralization as an option due to the fact that they are less manipulated. But until then, people will still use a centralized network.

Issues of decentralized systems also come in the fact that there are no servers to counter the latency issues. From the research, most of the protocols rely on the P2P method to transmit information across the network. The lack of a server may prove as a challenge to the current generation that is already used o fast internet processes. The requests processed per second are lesser when compared to decentralized systems [Choffnes08]. It is a good approach, but it offers a number of downsides when the developer considers the milestones achieved by the centralized system. However, the same developers still fight centralized systems since they feel that no one should own the internet fully. Richard Stallman says, "imagine you bought a house and the basement was locked and only the original building contractor had the key. If you need to make any change, repair, anything, you have to go to him. If he was too busy doing something else, he tells you to get lost, and you would be stuck" in 2:59:3:04[Reason19]. This is the exact definition of what the internet has become today - leaving less room for developers to make changes or work in freedom over the internet. The only option is to work on the decentralized internet but still face issues such as slow problems due to the lack of a server.

As appealing as the decentralized system sounds, people do not need more responsibilities added to their daily routines. The peer-to-peer network may not be favorable as people have already created an attachment to third party applications that make everything easy. The decentralized internet, however, is great for tech geniuses and political agendas due to its freedom from corruption [Ramaswamy05]. However, a worldwide implementation may not be the friendliest way to approach the shift in networks. The network displays a number of young aspects that need growth before implementation to the real world is achieved on a large scale.

8. Conclusion

The research paper was able to answer the question of the usefulness of decentralization. Some of the uses that stood out were file sharing, archiving and preservation of files through a secure and control free channel. Through the analysis of various protocols, the uses of the decentralized web were easy to depict and understand. However, the implementation and the use of the decentralized web is where the challenge manifested itself. As easy as it is to understand the need for decentralization and why most developers are after it, it was possible to tell that the network is complex and would require people to learn how to use it. The complexities of the system make it only useful to tech-savvies or interested parties, but for the ordinary person, it may prove a challenge getting used to. There are still gaps to bring the decentralized internet closer to people so that they may interact on the web without intermediaries. The benefits that this type of network architecture has to offer is quite appealing and has the potential to take over the future of the internet. The internet was meant to be open and decentralized, and it is in the hope of developers that one day, the system will be accepted at a global level. The peer-to-peer network may be the answer to government censorship and monopoly posed by the giant tech companies. It is also possible to preserve a lot of information relevant to humanity through the centralized system. As the masses garner for democracy over the internet, decentralization may be the only way to achieve this. A network on its own, giving people the freedom they desire online.

9. References

1. [Aracil09]Aracil, J. (2009). Enabling Optical Internet with Advanced Network Technologies (pp. 151). Springer Science & Business Media. Retrieved 14 October 2019, https://books.google.co.ke/books?id=qrjXk08gaNkC&pg=PA151&dq=disadvantage+of+centralized+internet&hl=en&sa=X&ved=0ahUKEwjE-J_I7JvlAhXCiFwKHW0wDysQ6AEIWzAH#v=onepage&q=disadvantage%20of%20centralized%20internet&f=false
2. [Boncea19]Boncea, R., Petre, I., & Vevera, V. (2019). Building trust among things in omniscient Internet using Blockchain Technology. Romanian Cyber Security, 1(1). Retrieved 15 October 2019, https://www.researchgate.net/profile/Radu_Boncea/publication/336284645_Building_trust_among_things_in_omniscient_Internet_using_Blockchain_Technology/links/5d999acf92851c2f70eeda52/Building-trust-among-things-in-omniscient-Internet-using-Blockchain-Technology.pdf
3. [Choffnes08] Choffnes, D. R., & Bustamante, F. E. (2008, August). Taming the torrent: a practical approach to reducing cross-isp traffic in peer-to-peer systems. In ACM SIGCOMM Computer Communication Review (Vol. 38, No. 4, pp. 363-374). ACM.
4. [Farmer19] Farmer, C. (2018). Five Projects that are decentralizing the web in slightly different ways. Retrieved 15 October 2019, https://medium.com/textileio/five-projects-that-are-decentralizing-the-web-in-slightly-different-ways-debf0fda286a
5. [Fehily13] Fehily, C. (2013). Cancel Cable: How Internet Pirates Get Free Stuff. Questing Vole Press. Retrieved 15 October 2019,https://books.google.co.ke/books?id=XYN5AQAAQBAJ&pg=PT17&dq=understanding+bit+torrent+basics&hl=en&sa=X&ved=0ahUKEwjY5qv365zlAhWoyYUKHfqJA1cQ6AEINDAC#v=onepage&q=understanding%20bit%20torrent%20basics&f=false
6. [Hindman18] Hindman, M. (2018). The Internet Trap: How the Digital Economy Builds Monopolies and Undermines Democracy (pp. 75-76). Princeton University Press. Retrieved from https://books.google.co.ke/books?id=hmmYDwAAQBAJ&printsec=frontcover&dq=monopoly+of+the+internet&hl=en&sa=X&ved=0ahUKEwj6483N3ZvlAhWIh1wKHTTqAIkQ6AEIJzAA#v=onepage&q=monopoly%20&f=false
7. [IoTeX19] IoTeX. (2019). Everything You Need to Know About IoTeX Mainnet Alpha. Retrieved from https://medium.com/@iotex/everything-you-need-to-know-about-iotex-mainnet-alpha-b8d790e0bd55
8. [Kempen18] Kempen, V. (2018). An Introduction to IPFS (pp. 3-14). Retrieved 15 October 2019,https://nvankempen.com/wp-content/uploads/2018/12/paper.pdf
9. [Kim19] Kim, S. (2019). Advanced Applications of Blockchain Technology (p.12). Springer Nature. Retrieved 15 October 2019, https://books.google.co.ke/books?id=77yxDwAAQBAJ&dq=IoTex+network&source=gbs_navlinks_s
10. [Kong12] Kong, J., Cai, W., & Wang, L. (2010, February). The evaluation of index poisoning in BitTorrent. In 2010 Second International Conference on Communication Software and Networks (pp. 382-386). IEEE.

11. [Mota19] Mota, M. (2019). Getting Started with Secure Scuttlebutt (SSB). Retrieved 15 October 2019, https://medium.com/@miguelmota/getting-started-with-secure-scuttlebut-e6b7d4c5ecfd
12. [Rajput19] Rajput. (2019). Transforming Businesses With Bitcoin Mining and Blockchain Applications (pp. 216-218). IGI Global. Retrieved 15 October 2019, https://books.google.co.ke/books?id=UMexDwAAQBAJ&pg=PA218&dq=IPFS&hl=en&sa=X&ved=0ahUKEwiYrIStzp3lAhUq5uAKHWjWA7gQ6AEILDAB#v=onepage&q=IPFS&f=false
13. [Ramaswamy05] Ramaswamy, L., Gedik, B., & Liu, L. (2005). A distributed approach to node clustering in decentralized peer-to-peer networks. IEEE Transactions on Parallel and Distributed Systems, 16(9), 814-829.
14. [Reason19] Reason. (2019). The Decentralized Web Is Coming [Video]. https://www.youtube.com/watch?v=R1ccwyP6fjc&t=625s
15. [Reilly19] Reilly, E., Maloney, M., Siegel, M., & Falco, G. (2019, April). A Smart City IoT Integrity-First Communication Protocol via an Ethereum Blockchain Light Client. In Proceedings of the International Workshop on Software Engineering Research and Practices for the Internet of Things (SERP4IoT 2019), Marrakech, Morocco (pp. 15-19).
16. [Robinson18] Robinson, D., Hand, J., Madsen, M., & McKelvey, K. (2018). The Dat Project, an open and decentralized research data tool. Scientific Data, 5(1). DOI: 10.1038/sdata.2018.221
17. [Sia06] Sia, K. C. (2006). DDoS vulnerability analysis of BitTorrent protocol. UCLA: Technical Report.
18. [Singh05] Singh, K., & Schulzrinne, H. (2005, June). Peer-to-peer internet telephony using SIP. In Proceedings of the international workshop on Network and operating systems support for digital audio and video (pp. 63-68). ACM.
19. [Tabora18] Tabora, V. (2018). The Evolution of the Internet, From Decentralized to Centralized. Retrieved 14 October 2019, https://hackernoon.com/the-evolution-of-the-internet-from-decentralised-to-centralized-3e2fa65898f5
20. [Tarr19] Tarr, D., Lavoie, E., Meyer, A., & Tschudin, C. (2019, September). Secure Scuttlebutt: An Identity-Centric Protocol for Subjective and Decentralized Applications. In Proceedings of the 6th ACM Conference on Information-Centric Networking (pp. 1-11). ACM.
21. [Zittrain08] Zittrain, J. (2008). The Future of the Internet -And How to Stop It (pp.19-21). Yale University Press. Retrieved on 14th of October 2019 https://books.google.co.ke/books?id=NiATs-C6nlQC&printsec=frontcover&dq=history+of+centralized+internet&hl=en&sa=X&ved=0ahUKEwjP0s_a05vlAhVOQ8AKHQwuCGUQ6AEIRzAE#v=onepage&q=history%20of%20centralized%20internet&f=false

10. List of Acronyms

- ARPANET - Advanced Research Projects Agency Network
- DHT - Distributed Hash Table
- DNS - Domain Name System
- HTML - HyperText Markup Language
- HTTP - Hypertext Transfer Protocol

- IoT - Internet of Things
- IPFS - InterPlanetary File System
- IPNS - Inter-Planetary Name System
- MDAG - Merkle Directed Acyclic Graph
- NSFNET - The National Science Foundation Network
- Roll-DPoS - Roll-Delegated Proof of Stake
- SSB - Secure Scuttle Butt

Last Modified: December 10, 2019
This and other papers on latest advances in computer networking are available on line at
http://www.cse.wustl.edu/~jain/cse570-19/index.html
Back to Raj Jain's Home Page