PCMJ

Progress in Computer and Mathematics Journal (PCMJ)
volume 3 [November, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

PEER TO PEER FILE SHARING SYSTEM USING IPFS AND BLOCKCHAIN

AMMAR ARIEF AINOL AHMAM
2022949491@student.uitm.edu.my

NOR ADORA ENDUT*
noradora@uitm.edu.my

Article Info

Received: March 2025
Accepted: September 2025
Available Online: November 2025

Abstract

This paper presents a peer to peer (P2P) file sharing system designed on top of Interplanetary File System (IPFS) and blockchain. Decentralized storage solutions that enable programmatic file accessibility, security and reliability as well as eliminating bottlenecks, scaling problems, and user experience limitations in web based P2P application are explored.

It integrates IPFS to store and retrieve the files using content-based addressing and. Pinata is also used for file pinning and keeping the file in the network free availability, and Helia is a JavaScript based interface for web application to communicate with IPFS. To increase security and transparency, decentralized verification is conducted via smart contracts on Ethereum by permanently logging a file hash record. With MetaMask and Web3 technologies for secure payment, users can handle storage and access payment to services effectively. Despite these advancements, web based P2P programs have considerable challenges. Since they can run on limited processing power, storage, and fragile net stability, the processing is carried out in the client side, and that means slow file transfers and high latency. Moreover, the acceptance of decentralized applications is also hindered by the fact that users must understand the cryptographically based transactions and other complex concepts such as IPFS hashes. In this paper, we attempt to find approaches to improve performance on cryptographic computations using WASM, cache adaptive for faster download, and Ethereum Layer 2 solutions like rollups reducing transaction costs and improving scalability. Aside from that, associating with the Filecoin to facilitate growth of the distribution storage is considered to support the system growth

Keywords: Enter; P2P, peer to peer, IPFS, blockchain, ethereum

INTRODUCTION

In a P2P network, every participant contributes a portion of their hardware resources—such as computing power, storage capacity, network bandwidth, and printers—to provide services and content to the network. These shared resources are then made accessible

to other peers within the network. Moreover, P2P systems possess distinct attributes that set them apart from traditional distributed systems. Despite variations in architecture among different systems, they exhibit shared characteristics. Delving into the specific advantages offered by a P2P file system, alongside potential performance impacts such as the failure of one system will not affect the others, the potential on saving money by eliminating the need to purchase and maintain a server, and lastly peer-to-peer network does not require a network operating system so no network operating system is needed for a peer-to-peer network (Vidya et al., 2023).

LITERATURE REVIEW

P2P technicalities

"Peer-to-peer systems offer an alternative to traditional client/server systems that solve bottleneck problems but need complex algorithm" (Pourebrahimi B., 2005). As mentioned before, peer to peer is a decentralized system that uses users or clients for communicating data between each other without any centralized system or administration. A typical client-server model can be bottlenecked by the hardware used on the network that administrate the network flow. As mentioned by (Pourebrahimi B. et al., 2005), to provide content and services, client-server model act as the central registering unit.

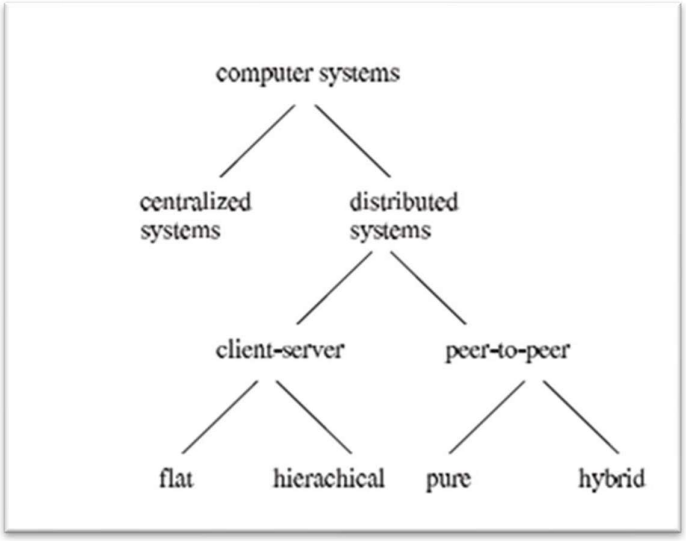
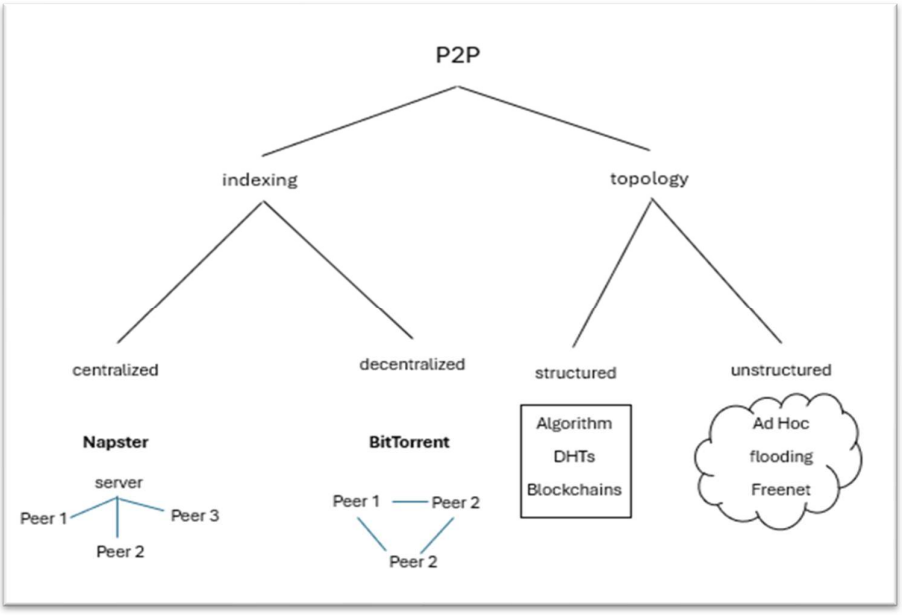


Figure 1 *Computer systems* (https://profile.iiita.ac.in/bibhas.ghoshal/lecture_slides/distributed/P2P%20Network%20Survey.pdf)

P2P network (structured & unstructured)

P2P network system can be classified as either structured or unstructured. In structured networks, the topology is managed, and information about the resources, for example, shared content and its location is consistent. This makes sure data queries can be directed to peers efficiently, even for rarer data (Thampi M., S., 2009). The primary role of these systems is to create and maintain an efficient mapping between data and its location, promising a quick response to data queries. There are examples of these network typologies based on real life examples such as KaZaA, Gnutella, Napster, and BitTorrent. One of the most common indexing methods used in structured P2P systems is Distributed Hash Tables (DHTs) (Suo, D., n.d.). In DHT, a lookup table containing key-value pairs is maintained, allowing peers in the P2P network to efficiently retrieve the value associated with a given key. Example of DHT-based system are Chord, Pastry, and Tapestry, each of the example have their own system of routing and data object/key management strategies. Although DHT-based P2P enhance performance, they may also lead to higher communication overhead compared to unstructured P2P network systems (Ramzan, N., Park, H., Izquierdo, E., 2012).



. ***Figure 2*** *P2P structure*

Impact on society

Human beings are social animals that constantly communicate with each other. Humans need to share their thoughts and information constantly so technology such as file sharing systems provide that means (Kavitha et al., 2022). As discussed above, the common file sharing system right now is BitTorrent. BitTorrent is a peer-to-peer software that makes sharing files between the user possible. In this era, a lot of people across the world have access to the internet so generating data transfer through BitTorrent does seem like a good idea. As mentioned, there are a lot of issues regarding P2P file sharing system such as copyright infringement, sharing copyrighted files between peers have brought up some major ethical and legal problems (Chan et al., 2020).

Napster old architecture

Napster popularizes the use of P2P communication by giving users the ability to share music (Kvetko, 2020). Napster causes a lot of legal issues regarding copyright infringement. Napster works by establishing between the presence of client and host. As mentioned, Napster is considered as centralized P2P communication by managing communication between host and client. The label of host and client depends on the current state of the network, both can change its status between host and client.

A central server is hosted among the P2P network to store information of the metadata that is served by the host. This server is called a broker. The broker contains the metadata or information regarding the host previously served files (Howe, 2002). The broker can act as a database for the client to query a particular file and send back a list of requested files and peers that have the said files. The image below shows computer “A” querying a file from the broker and the broker sets the file exchange between the peers.

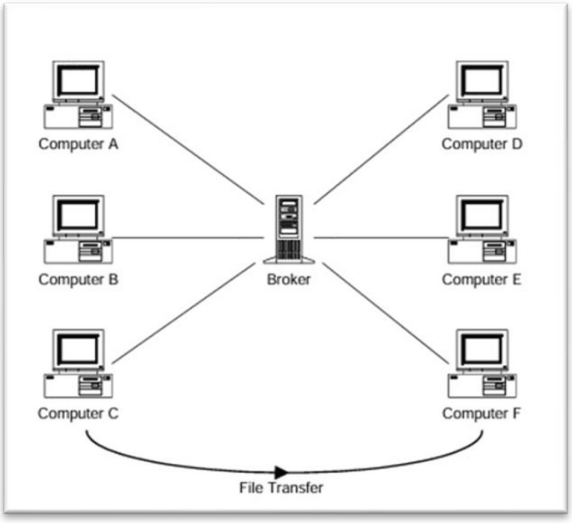


Figure 3 *Broker coordinate between peers*
(http://members.tripod.com/ahowe_ca/pdf/napstergnutella.pdf)

BitTorrent architecture

BitTorrent is a decentralized P2P file sharing system. It relies on other peers to download and upload files, the same as Napster. The main difference is BitTorrent not only shares music files but also any files uploaded by the user, and it does not have a server broker to manage uploaded files and network management among peers. The architecture of BitTorrent is much simpler than Napster in that it does not rely on a lot of other important role entity. BitTorrent system can be assessed by a few systems or entity such as:

- A torrent file
- A tracker
- An original downloader called *seed*
- The end user downloader called *leecher*

First and foremost, to upload a file or use files in the BitTorrent network one must turn it into a torrent file. A torrent file consists of information like its filename, size, hashing information and the URL of the tracker. Torrent files can be distributed through the web (http), e-mail, and IRC. A torrent client is used to convert files into functional torrent files, this is usually provided in the BitTorrent client. All torrent clients may have different features among each other, but the core concept is kept the same.

A seed can be downloaded in the BitTorrent architecture with the help of a tracker. The

difference between tracker and server broker is that tracker only stores a list of peers and how to connect to said peers based on content the user wants to download. The tracker does not store the content itself as a broker does. This communication all was done through an easy protocol on top of HTTP (Johnsen, 2005).

Ethereum Blockchain

In 2008 research interest in blockchain technology began after Satoshi Nakamoto published a document discussing protection from repeated payment mistakes in a decentralized system. Blockchain technology gained wide acceptance after its discovery because industries and governments now evaluate their value in system operations (Kushwaha et al., 2022). The consensus method in blockchain transactions replaces the requirement of reliable third-party agents. Smart contracts exist at the top level of blockchain technology systems. After Nakamoto published his white paper blockchain technology became popular because it demonstrated how to protect transactions. Ethereum has become the leading platform for implementing blockchain networks today. The system is fully functional according to Turing patterns therefore programmers can build their contracts while setting rules for actions. When programmed for blockchain purposes the agreement automatically performs its functions after meeting necessary conditions. The parties involved stick to set rules during their interaction so that when all conditions meet automatic actions begin. The use of smart contracts brings full visibility to the system without relying on third-party messengers.

IPFS

Protocol Labs created IPFS as several networking protocols. Its main purpose is to make the Web run faster with distributed networks that stay online through any disruption. Instead of tracking data positions IPFS finds data through its specific content. This method together with its duplicate removal system saves space on storage devices (Daniel & Tschorsch, 2022). IPFS lets users distribute content across multiple decentralized storage systems, so they have better protection from censorship

Helia is a library that works with Internet Protocol File System (IPFS) within JavaScript server and browser applications. The system depends on libp2p open-source code because developers use it to create IPFS applications that allow peers to connect with each other (Natarajan, n.d.).

PCMJ
Progress in Computer and Mathematics Journal (PCMJ)
volume 3 [November, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

METHODOLOGY

Project approach on methodologies is important to finish the development of the project's functional entities and to deliver the result as fast and good as possible. Each phase explains the approach in maintaining the stated objectives. Based on the project and current development styles and research the Agile methodology is chosen. The Agile methodology phases consist of requirements, design, development, testing, deployment and review.

Project Flowchart

The software itself as mentioned is going to be on the website and going to be hosted on a web server so that people can interact with it not just in the local network.

A URL will be provided when the system is finished developed with a constant domain name to avoid confusion. After the web application uploaded to the user device, it will show two inputs as to ask user the file they wanted to upload. The file uploaded can be various of type of file and the user needs to click on the button and choose the desired file. As for now, it only allows for one file per transfer. Next, the user has the option to choose whether to implement blockchain or only using IPFS. The user then can generate the file CID. The link is generated by IPFS to create spontaneity and to evade any prying listeners. Other peers can use the link generated. If the user only uses peer to peer or IPFS then the URL generated can only be shown

in the browser memory otherwise the URL is stored and can be fetch by using MetaMask's wallet ID.

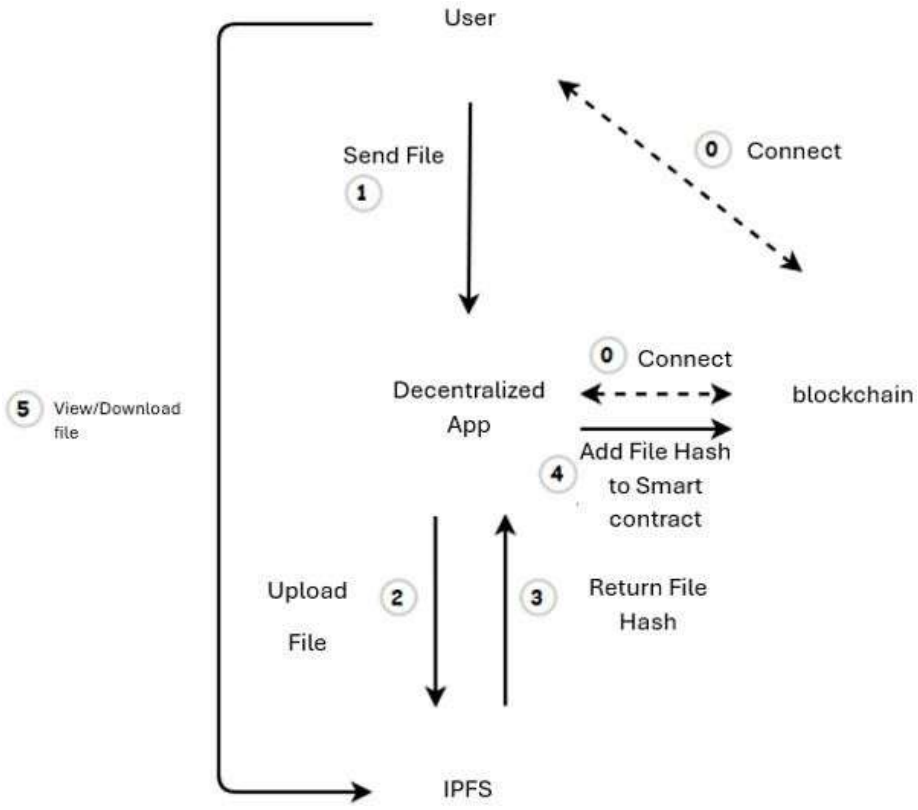


Figure 3 *Flowchart of the system*

System Architecture

The system architecture consists of some major entities like Helia nodes and the server. The web server holds the web application to make communication between other devices in the internet possible. After the application is ready to deploy, the main server can act as the mediator to host the web application for other client to share their files. The file that needs to be uploaded does not need any conversion for example into a torrent file because it uses peer to peer connections through the main server. The IPFS gateway resembles the

content storage where the people all the round the world can access content through the internet. Note that the server is based on Infrastructure as a service rather than a full-on server.

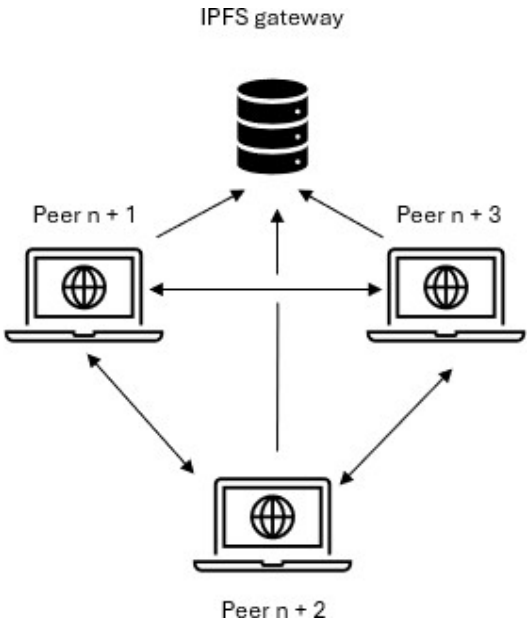


Figure 4 *System architecture*

RESULT AND DISCUSSION (HEADING 1)

This chapter consists of results and findings of this project's file sharing system that is constructed by using IPFS, blockchain via web application. During uploading files to the IPFS (content) and blockchain (content id) the user will be able to retrieve back their content based on IPFS distributed system.

Setting Up File Persistence

Pinata helps access IPFS features by providing essential tools to pin and store content within its platform. API keys or tokens from Pinata is needed to access and perform tasks after

setting up your account. Pinata simplifies IPFS work by its easy-to-use decentralized storage management tools. It offers pinning of files for persistent storage on IPFS and provides API tools for automated IPFS interactions while supporting big data storage needs and busy applications

After gathering all the API token, the web app can now interact with IPFS network, and the file content is accessible by using the URL **https:/ipfs.io/ipfs/<your-ipfs-hash>.** All files uploaded to the IPFS gateway in pinata are automatically pinned so there is no issue regarding files persistence

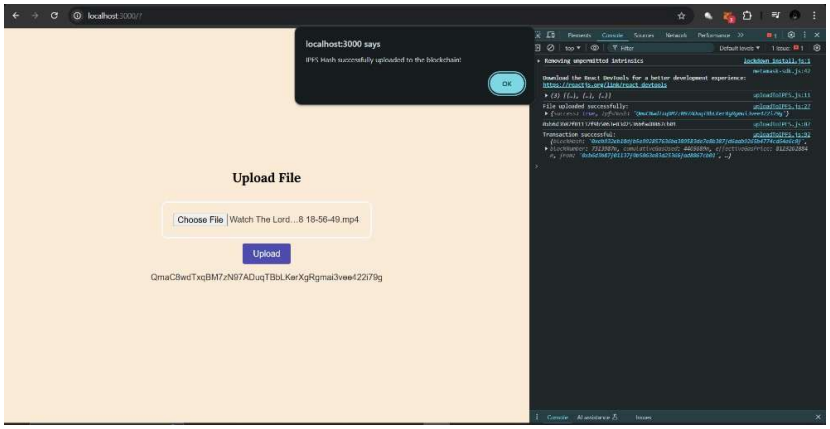


Figure 5 *Video file uploaded to IPFS network*

Figure 6 *Transaction details*

Progress in Computer and Mathematics Journal (PCMJ)
volume 3 [November, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

Figure 7 *Retrieve video file using URL + IPFS hash*

Identifying Transactions and Verifying IPFS Hashes on Etherscan

Once you add an IPFS hash to the blockchain the related transaction shows up on Etherscan for everyone to see. People can confirm smart contract transactions by entering their address or transaction ID into Etherscan. Etherscan provides a comprehensive view of the transaction, including:

1. Transaction Hash: Every transaction receives a special number to identify it.
2. Sender and Receiver Addresses: The transaction started from its wallet address and sent funds to the smart contract address that received it
3. Gas Fee: Users pay this payment to make their transaction possible.
4. Input Data: The smart contract received encoded information along with the IPFS hash when this data was submitted.
5. Block Number: The transaction received confirmation in this blockchain block.

Users can check if the IPFS hash made it onto the blockchain by looking at this data. They can check both the transaction date and verify if the smart contract worked correctly after processing.

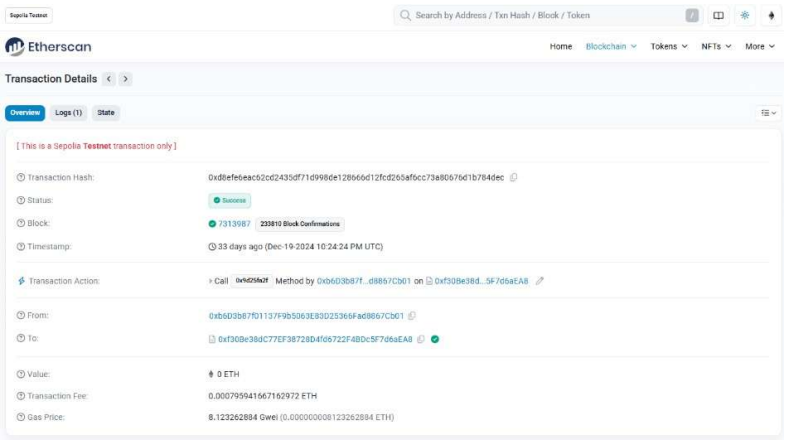


Figure 8 *Identify transaction using transaction hash*

Functionality Test

Function	Action	Pass	Fail
Main webpage	Connect to MetaMask account	✓	
Upload file button	Open prompt to choose file from local storage	✓	
Submit button	Shows a prompt that shows file successfully upload to IPFS	✓	
Blockchain integration	After clicking "ok" on the pop-up prompt it shows the MetaMask account to pay for transaction	✓	
Error handling	Throw an error through the prompt or through the console	✓	
Search & File retrieval	Show file CID based on owner of account transaction	✓	
Peer to peer between end devices	End devices can share files without IPFS gateway	✓	

CONCLUSION

In conclusion, a decentralized P2P file-sharing system that leverages IPFS, blockchain, and smart contracts to enhance security, reliability, and scalability. By integrating technologies like Pinata for persistent storage, Helia for web-based IPFS interactions, and Ethereum-based verification, the system ensures transparent and secure file access. However, challenges such as client-side processing limitations, high latency, and the complexity of cryptographic transactions remain barriers to widespread adoption. These advancements aim to enhance the efficiency and usability of decentralized file-sharing applications, paving the way for broader acceptance and adoption.

REFERENCES

Al-Enizi, Z. K., & Naser, M. (2022). The law applicable to P2P networks on national and international bases for violating intellectual property rights. *International Journal of Cyber Warfare and Terrorism*, *12*(1), 1–10. https://doi.org/10.4018/ijcwt.311419

Anthal, J., Choudhary, S., & Shettiyar, R. (2023). Decentralizing File Sharing: The Potential of Blockchain and IPFS. *International Conference on Advancement in Computation & Computer Technologies (InCACCT)*. https://doi.org/10.1109/incacct57535.2023.10141817

Argyropoulos, V., Alepis, E., & Patsakis, C. (2022). Semi-Decentralized File Sharing as a Service. *2022 13th International Conference on Information, Intelligence, Systems & Applications*. https://doi.org/10.1109/iisa56318.2022.9904336

Bhisikar, S., Taneja, S., Yadav, O., & Srivastava, S. (2023). Peer-to-Peer File Sharing WebApp. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(8), 21–35. https://doi.org/10.17762/ijritcc.v11i8.7920

Blanco, N., & Blanco, N. (2024, February 29). *How do P2P botnets work | Robots.net*. Robots.net. https://robots.net/fintech/how-do-p2p-botnets-work/

Bonguet, A., & Bellaiche, M. (2017). A survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud computing. *Future Internet*, *9*(3), 43. https://doi.org/10.3390/fi9030043

Buono, A. (2020). *A PRACTICAL GUIDE TO FAIR USE*. Gides. https://www.gides.com/alex/a-practical-guide-to-fair-use

Campidoglio, M., Frattolillo, F., & Landolfi, F. (2009). The Copyright Protection Problem: Challenges and Suggestions. *2009 Fourth International Conference on Internet and Web Applications and Services*. https://doi.org/10.1109/iciw.2009.84

Carlsson, B., & Gustavsson, R. (2001). The rise and Fall of Napster - an evolutionary approach. In *Lecture notes in computer science* (pp. 347–354). https://doi.org/10.1007/3-540-45336-9_40

Chan, M., Gong, M., Naha, R. K., & Mahanti, A. (2020). Piracy on the Internet: Publisher-side Analysis on File Hosting Services. *IEEE*. https://doi.org/10.1109/isncc49221.2020.9297276

Christin, N. (2010). Peer-to-peer Networks: Interdisciplinary Challenges for Interconnected Systems. *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives*. https://www.andrew.cmu.edu/user/nicolasc/publications/p2p_web.pdf

Congleton, R. J., & Yang, S. Q. (2016). A comparative study of education exemptions to copyright in the United States and Europe. *Athens Journal of Law*, *3*(1), 47–60. https://doi.org/10.30958/ajl.3-1-4

Dahal, R. K., Bhatta, J., & Dhamala, T. N. (2013). Performance analysis of SHA-2 and SHA-3 finalists. *International Journal of Cryptography and Information Security*, *3*(3), 1–10. https://doi.org/10.5121/ijcis.2013.3301

Damola, A. (2005). *Peer to peer networking in Ethernet broadband access networks*. http://www.diva-portal.org/smash/record.jsf?pid=diva2:513162

Danaher, B., Smith, M. D., & Telang, R. (2014). Piracy and copyright enforcement mechanisms. *Innovation Policy and the Economy*, *14*, 25–61. https://doi.org/10.1086/674020

Daniel, E., & Tschorsch, F. (2022). IPFS and Friends: A Qualitative comparison of next generation Peer-to-Peer data networks. *IEEE Communications Surveys & Tutorials*, *24*(1), 31–52. https://doi.org/10.1109/comst.2022.3143147

DHT-based Communications Survey: Architectures and Use Cases This work has been submitted to the IEEE for possible publication. Copyright may be transferred without notice, after which this version may no longer be accessible. (n.d.). Ar5iv. https://ar5iv.labs.arxiv.org/html/2109.10787

Geiger, C. (2014a). Challenges for the enforcement of copyright in the online world: Time for a new approach. In *Edward Elgar Publishing eBooks*. https://doi.org/10.4337/9781781955802.00027

Geiger, C. (2014b). Challenges for the enforcement of copyright in the online world: Time for a new approach. In *Edward Elgar Publishing eBooks*. https://doi.org/10.4337/9781781955802.00027

Gillis, A. S. (2020, March 17). *dynamic IP address*. WhatIs. https://www.techtarget.com/whatis/definition/dynamic-IP-address

Goel, S., Miesing, P., & Chandra, U. (2010). The impact of illegal Peer-to-Peer file sharing on the media industry. *California Management Review*, *52*(3), 6–33. https://doi.org/10.1525/cmr.2010.52.3.6

Gulihar, P., & Gupta, B. B. (2020). Cooperative Mechanisms for Defending Distributed Denial of service (DDOS) attacks. In *Springer eBooks* (pp. 421–443). https://doi.org/10.1007/978-3-030-22277-2_16

Hadzhiev, V., & Rashidov, A. (2021). A hybrid model for structuring, storing and processing distributed data on the internet. *2021 International Conference Automatics and Informatics (ICAI)*. https://doi.org/10.1109/icai52893.2021.9639240

Harjula, E., Ylianttila, M., Ala-Kurikka, J., Riekki, J., & Sauvola, J. (2004). Plug-and-play application platform. *Department of Electrical and Information Engineering*. https://doi.org/10.1145/1052380.1052390

Hildebrandt, M. (2019). Digital security and human rights. In *Routledge eBooks* (pp. 259–270). https://doi.org/10.4324/9781351025386-18

Howe, A. J. (2002). *Napster and Gnutella: a Comparison of two Popular Peer-to-Peer Protocols*. http://members.tripod.com/ahowe_ca/pdf/napstergnutella.pdf

Hunter, S. D., & Spitz, D. (2003). The social construction of Napster. *Social Science Research Network*. https://doi.org/10.2139/ssrn.469283

Huynh, T. T., Nguyen, T. D., Hoang, T., Tran, L., & Choi, D. (2021). A reliability guaranteed solution for data storing and sharing. *IEEE Access*, *9*, 108318–108328. https://doi.org/10.1109/access.2021.3100707

IJMTST | UGC Journal ID: 43137 | Vol 8 Issue 01 January 2022. (n.d.). http://www.ijmtst.com/vol8issue01.html

Kamil, I. S. M., & Azmi, I. M. B. a. G. (2020). Gatekeepers Liability for Internet Intermediaries in Malaysia: Way Forward. *International Journal of Business, Economics and Law*. http://eprints.ums.edu.my/26478/

Kavitha, V., Sruthi, G. S., Thoshinny, B., & Riduvarshini, S. R. (2022). Stagchain – A Steganography based Application Working on a Blockchain Environment. *2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC)*. https://doi.org/10.1109/icesc54411.2022.9885394

Klampanos, I. A., & Jose, J. M. (2012). Searching in peer-to-peer networks. *Computer Science Review*, *6*(4), 161–183. https://doi.org/10.1016/j.cosrev.2012.07.001

Kothari, R., Jakheliya, B., & Sawant, V. (2020). Implementation of a distributed P2P storage network. *2020 IEEE International Conference for Innovation in Technology (INOCON)*. https://doi.org/10.1109/inocon50539.2020.9298375

Kvetko, P. (2020, May 1). *How the Democratization of Music Changed the Industry*. http://hdl.handle.net/20.500.13013/768

Leung, H. H. (2012). Yi-Chieh Jessica Lin, Fake Stuff: China and the rise of counterfeit goods. *Journal of Consumer Culture*, *12*(3), 379–381. https://doi.org/10.1177/1469540512456941

Lindgren, S., & Linde, J. (2012). The subpolitics of online piracy: A Swedish case study. *Convergence*, *18*(2), 143–164. https://doi.org/10.1177/1354856511433681

Ma, D., Wang, X., Chen, W., Yang, S., & Ma, L. (2012). A research on dynamic allocation of network resources based on P2P traffic planning. *Peer-to-peer Networking and Applications*, *7*(4), 511–524. https://doi.org/10.1007/s12083-012-0163-5

Mangal, L., Singh, P. P., Gupta, K., Kumar, J., & Gupta, S. (2022). File Transferring Web Application Using Node JS. *nternational Journal for Modern Trends in Science and Technology*, *8*.

Martino, R., & Cilardo, A. (2019). A flexible framework for exploring, evaluating, and comparing SHA-2 designs. *IEEE Access*, *7*, 72443–72456. https://doi.org/10.1109/access.2019.2920089

Mehr-Un-Nisa, N., Ashraf, F., Naseer, A., & Iqbal, S. (2019). Comparative Analysis of Unstructured P2P File Sharing Networks. *Association for Computing Machinery*. https://doi.org/10.1145/3325917.3325952

Miller, J. P. (2018). Why the Pirate Bay remains at sea while Napster 1.0 now rests in Davy Jones's locker. *ResearchGate*. https://doi.org/10.13140/RG.2.2.36731.62242

Morin, O. (2018a). Cultural transmission. *The International Encyclopedia of Anthropology*, 1–10. https://doi.org/10.1002/9781118924396.wbiea1882

Moureau, N. (2016). Droit de Suite. *Springer eBooks*, 1–8. https://doi.org/10.1007/978-1-4614-7883-6_7-2

Musthafa, M. M., Vanitha, K., Rahman, A. Z., & Anitha, K. (2020). An Efficient Approach to Identify Selfish Node in MANET. *2020 International Conference on Computer Communication and Informatics*. https://doi.org/10.1109/iccci48352.2020.9104076

Naseer, M., Rusdi, J. F., Shanono, N. M., Salam, S., Muslim, Z. B., Abu, N. A., & Abadi, I. (2021). Malware Detection: Issues and challenges. *Journal of Physics. Conference Series*, *1807*(1), 012011. https://doi.org/10.1088/1742-6596/1807/1/012011

Natarajan, P. B. (n.d.). *Exploring decentralized computing using SOLiD and IPFS for social media applications*. ScholarWorks@UARK. https://scholarworks.uark.edu/csceuht/135/

Oesch, S., & Schuchard, M. (2019). *Nation Scale Mobile Ad Hoc Network for Normally Isolated Topologies*. https://doi.org/10.1109/ithings/greencom/cpscom/smartdata.2019.00047

Osborne, C. (2017, September 25). How much does The Pirate Bay's cryptocurrency miner make? *ZDNET*. https://www.zdnet.com/article/how-much-does-the-pirate-bays-cryptocurrency-miner-make/

Parsons, J., Winslow, J., & Tseng, L. (2023). Demo: Velox: Enhancing P2P Real-Time Communication in Browsers. *2023 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events*. https://doi.org/10.1109/percomworkshops56833.2023.10150343

Pourebrahimi, B., Bertels, K., & Vassiliadis, S. (2005). A Survey of Peer-to-Peer Networks. *Computer Engineering Laboratory*, 570–577. http://ce-publications.et.tudelft.nl/publications/868_a_survey_of_peertopeer_networks.pdf

Raj, U. a. S., & Maheswaran, C. P. (2023). Secure File Sharing System Using Image Steganography and Cryptography Techniques. *International Conference on Inventive Computation Technologies (ICICT)*. https://doi.org/10.1109/icict57646.2023.10134163

Rampon, J., Perillat, R., Torres, L., Benoit, P., Di Natale, G., & Barbareschi, M. (2015). Digital Right Management for IP Protection. *Information, Communication & Society*. https://doi.org/10.1109/isvlsi.2015.127

Ramzan, N., Park, H., & Izquierdo, E. (2012). Video streaming over P2P networks: Challenges and opportunities. *Signal Processing. Image Communication*, *27*(5), 401–411. https://doi.org/10.1016/j.image.2012.02.004

Salim, A. (2024). Applying software engineering based on Peer to Peer Communication. *Türk Bilgisayar Ve Matematik Eğitimi Dergisi*, *15*(1), 75–80. https://doi.org/10.61841/turcomat.v15i1.14385

Samarasinghe, N. H. L. C. (2019). *Peer-to-peer cached data distribution network as an alternative for the client-server model*. https://dl.ucsc.cmb.ac.lk/jspui/bitstream/123456789/4431/1/2016MCS099.pdf

Sánchez-Patiño, N., Gallegos-Garcia, G., & Rivero-Angeles, M. E. (2023). Teletraffic Analysis of DoS and Malware Cyber Attacks on P2P Networks under Exponential Assumptions. *Applied Sciences*, *13*(7), 4625. https://doi.org/10.3390/app13074625

Sganga, C. (2014). EU copyright Law between Property and fundamental Rights: A proposal to connect the dots. In *Springer eBooks* (pp. 1–26). https://doi.org/10.1007/978-3-662-44648-5_1

Sharing resources — Computer Networking : Principles, Protocols and Practice. (n.d.). https://beta.computer-networking.info/syllabus/default/principles/sharing.html

Sheriff, L., & Sheriff, L. (2024, February 29). *What is P2P Network | Robots.net*. Robots.net. https://robots.net/fintech/what-is-p2p-network/

Singh, S. K., Kumar, C., & Nath, P. (2021). Replication scheme for Structured P2P system applications in Wireless Mesh Networks (WMNs). *2021 Asian Conference on Innovation in Technology (ASIANCON)*. https://doi.org/10.1109/asiancon51346.2021.9544948

Sinnreich, A. (2014). Sharing in spirit: Kopimism and the Digital Eucharist. *Social Science Research Network*. https://doi.org/10.2139/ssrn.2437233

Spognardi, A., Lucarelli, A., & Di Pietro, R. (2005). A methodology for P2P file-sharing traffic detection. *2005 Second International Workshop on Hot Topics in Peer-to-Peer Systems*. https://doi.org/10.1109/hot-p2p.2005.2

Stern, R. (2000). Napster: a walking copyright infringement? *IEEE MICRO/IEEE Micro*, *20*(6), 4–5, 95. https://doi.org/10.1109/40.888696

Stevens, M., Bursztein, E., Karpman, P., Albertini, A., & Markov, Y. (2017). The first collision for full SHA-1. In *Lecture notes in computer science* (pp. 570–596). https://doi.org/10.1007/978-3-319-63688-7_19

Taddeo, M., & Vaccaro, A. (2011). Analyzing Peer-to-Peer Technology using information Ethics. *˜the œInformation Society/˜the œInformation Society*, *27*(2), 105–112. https://doi.org/10.1080/01972243.2011.548698

Tanha, M., Sajjadi, D., Tong, F., & Pan, J. (2016). *Disaster Management and Response for Modern Cellular Networks Using Flow-Based Multi-Hop Device-to-Device Communications*. https://doi.org/10.1109/vtcfall.2016.7880960

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive review. *Sensors*, *23*(8), 4117. https://doi.org/10.3390/s23084117

Thampi, S. M. (2009). Introduction to distributed systems. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.0911.4395

Thampi, S. M., & K, C. S. (2010). Survey of search and replication schemes in unstructured P2P networks. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1008.1629

Tran, Q., Vo, N., Nguyen, Q., Bui, M., Phan, T., Lam, V., & Masaracchia, A. (2021). D2D Multi-Hop Multi-path Communications in B5G Networks: A survey on models, techniques, and applications. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, *7*(25), 167839. https://doi.org/10.4108/eai.7-1-2021.167839

Vaidya, C., Takalkar, K., Ghosekar, A., Nimgade, S., & Ghode, V. (2023). Decentralized file sharing. *2020 IEEE International Students' Conference on Electrical,Electronics and Computer Science (SCEECS)*, 1–6. https://doi.org/10.1109/sceecs57921.2023.10062977

Valauskas, Edward J. (2001). *The Napster music community*. https://firstmonday.org/ojs/index.php/fm/article/download/1458/1373?inline=1

Van Der Sar, E. (2021, August 23). The Pirate Bay Earned Millions in Bitcoin Donations (If it HODLed). *Torrentfreak*. https://torrentfreak.com/the-pirate-bay-earned-millions-in-bitcoin-donations-if-it-hodled-210823/

Vanakamamidi, R. K., PMSS, C., Ponkumar, D. D. N., & Senkamalavalli, R. (2023). Peer to Peer Information Inter-Change and Network Coding to Improve Transmission Efficiency in Wireless Mesh Network. *Second International Conference on Augmented Intelligence and Sustainable Systems*. https://doi.org/10.1109/icaiss58487.2023.10250464

Vinaykumar, D., Vishal, Venakat, P., Vivek Yadav, J. N., & Naveen Chandra, G. (2024). Efficient file sharing system utilizing MongoDB and Node.js. *Zenodo*. https://doi.org/10.5281/zenodo.10634569

What is malware? Definition and types | Microsoft Security. (n.d.). https://www.microsoft.com/en-us/security/business/security-101/what-is-malware

Zhan, D., Lin, X., Wang, W., Gan, X., & Bi, S. (2023). A Design of File Sharing System. *IEEE 13th International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)*. https://doi.org/10.1109/cyber59472.2023.10256639