www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1564-1570

e-ISSN : 2583-1062
Impact Factor : 7.001

CENSORSHIP-RESISTANT WEB HOSTING: LEVERAGING BLOCKCHAIN, IPFS, AND WEB3

Chalandula Haritha[1], Netha Ushasri[2], Palle Priya Darshini[3], Juveriya Talath[4]

[1,2,3,4]Stanley College of Engineering and Technology for Women, Hyderabad, Telangana, India.

ABSTRACT

Traditional web hosting relies heavily on centralized servers, which introduce risks such as data censorship, single points of failure, and security vulnerabilities. This paper explores a decentralized approach to web hosting by integrating the InterPlanetary File System (IPFS) for distributed file storage and blockchain-based smart contracts for secure content management. The proposed system ensures data integrity, enhances security, and promotes fault tolerance by distributing website data across multiple nodes. A practical implementation using Ethereum, Solidity, and Django demonstrates the feasibility of this decentralized hosting model. This research details the deployment process, challenges encountered, and future enhancements aimed at improving scalability and efficiency.

Keywords: Blockchain, IPFS, Decentralized Hosting, Smart Contracts, Web3, Peer-to-Peer Hosting

1. INTRODUCTION

The internet has transformed the way information is shared, making data more accessible and interconnected. However, the current web hosting landscape remains largely centralized, with major corporations and service providers controlling data storage and accessibility. This centralized structure introduces critical concerns regarding data privacy, censorship, and security vulnerabilities. Websites and applications hosted on centralized servers are susceptible to outages, cyber-attacks, and governmental censorship, limiting freedom of information.

Decentralized web hosting emerges as a viable alternative, offering a more resilient and censorship-resistant infrastructure. By leveraging blockchain technology and IPFS, content can be stored in a distributed manner, ensuring availability even if individual nodes go offline. Blockchain's immutable ledger prevents unauthorized alterations, preserving data integrity and transparency. This paper presents an approach where IPFS serves as the distributed file system, and Ethereum blockchain ensures the integrity of stored content. Through this system, users can host websites securely without relying on centralized authorities, mitigating the risks associated with conventional web hosting models.

2. LITERATURE REVIEW

Nakamoto (2008) pioneered the blockchain concept with Bitcoin, demonstrating how decentralized networks achieve consensus without a central authority. Buterin (2014) later expanded on this by developing smart contracts, enabling decentralized applications, including web hosting, where content management is automated and secured through blockchain technology.

Benet (2015) introduced IPFS (InterPlanetary File System) as a peer-to-peer, content- addressable distributed file system designed to replace traditional web protocols. By distributing files across multiple nodes, IPFS reduces reliance on centralized servers and improves resilience against censorship and data loss. However, concerns remain regarding data persistence and network stability.

Philip and Saravanaguru (2022) presented a semi-decentralized framework that balances security and efficiency by integrating blockchain with IPFS. Their study focused on optimizing network redundancy and centralized verification to improve performance while maintaining decentralization.

Doan et al. (2022) analyzed IPFS-based decentralized cloud storage, discussing challenges such as data persistence and retrieval speeds. Their study emphasized the importance of optimizing IPFS for large-scale deployments.

Trautwein et al. (2022) conducted a performance evaluation of IPFS in large-scale decentralized networks. Their findings provide insights into content retrieval efficiency and IPFS scalability under different network conditions.

Shinde et al. (2023) developed D-Drive, a decentralized cloud storage system built on IPFS, incorporating encryption and cryptocurrency-based incentives to enhance security and usability.

Aditya Dole (2023) explored a peer-to-peer web architecture utilizing blockchain for content verification and IPFS for storage. His study identified scalability and cost-efficiency as key challenges. This paper builds upon these findings by integrating Django-based user authentication, smart contract-based access control, and automated IPFS deployment mechanisms to enhance usability and security.

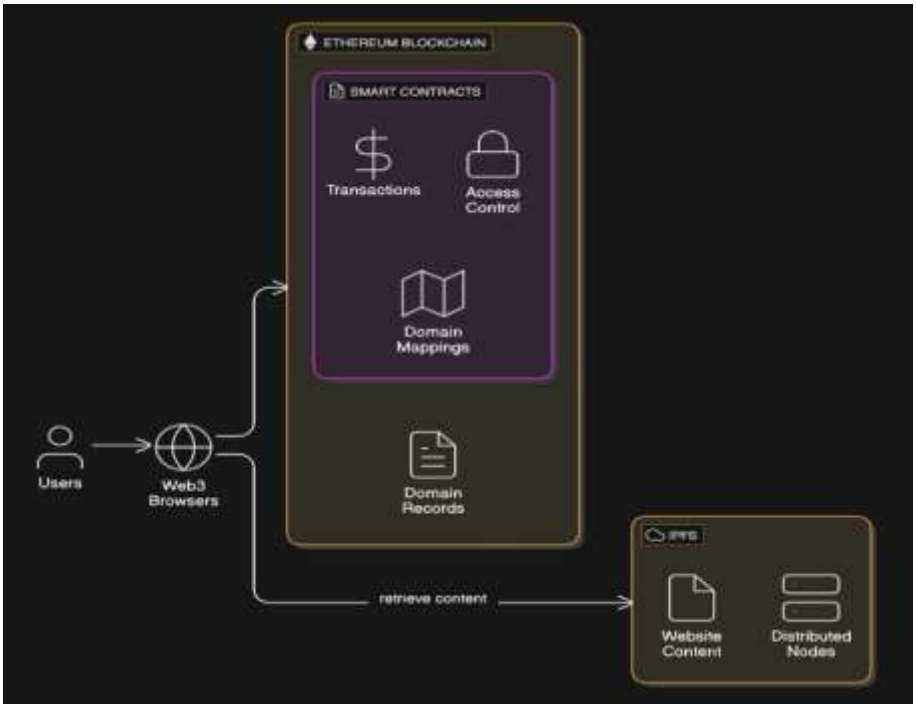
Haque et al. (2024) proposed a hybrid decentralized model integrating Ethereum blockchain and IPFS for secure code

repository hosting. Their approach utilizes a temporary Middleman IPFS to facilitate real-time collaboration while preserving long-term decentralization. Smart contracts regulate access control, ensuring data confidentiality.

Devadas et al. (2024) introduced a decentralized hosting model using Ethereum smart contracts and IPFS storage miner nodes to ensure long-term data retention. Their implementation of InterPlanetary Name Space (IPNS) allows seamless updates to hosted content while preserving integrity.

3. METHODOLOGY

System Architecture:



IPFS for Distributed Storage

- Provides a decentralized file system, eliminating dependence on centralized servers.
- Implements content-based addressing, ensuring data retrieval through unique cryptographic hashes.

Blockchain for Hash Management

- Stores IPFS hashes within Ethereum smart contracts, ensuring tamper-proof content referencing.
- Guarantees data authenticity and integrity by preventing unauthorized modifications.

Web Interface for User Interaction

- Built using Django and Web3.py, allowing users to register, deploy websites, and manage hosted content.
- Smart contracts facilitate secure content retrieval and access control.

Implementation:

Environment Setup

- A local Ethereum blockchain is deployed using a blockchain test environment for testing smart contracts.
- IPFS is set up using the Go-IPFS node, enabling decentralized storage and retrieval of website files.
- The web interface is built using Django, integrating blockchain interactions via Web3.py.

Smart Contract Deployment

- Smart contracts are written in Solidity to handle IPFS hash storage, domain mapping, and access control.
- The contracts are deployed on a test Ethereum network, ensuring smooth integration before mainnet deployment.
- Functions include storing file hashes, verifying ownership, and retrieving hosted content.

IPFS Integration

- Users upload files through the Django-based interface, generating an IPFS hash.
- The hash is stored on the Ethereum blockchain, making content retrieval secure and immutable.
- Websites can be accessed using IPFS gateways or through blockchain-based domain resolution.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1564-1570
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

Security Enhancements

- Implements end-to-end encryption for sensitive data storage and retrieval.
- Uses multi-signature smart contracts to enhance content access security.
- Employs gas optimization techniques to reduce transaction costs on the Ethereum network.

4. RESULTS AND ANALYSIS

The system was evaluated based on key performance metrics, including latency, cost-effectiveness, and fault tolerance:

- Latency Analysis: Compared file retrieval speeds between IPFS and traditional cloud storage solutions.
- Cost Efficiency: Measured Ethereum gas fees for various smart contract interactions.
- Fault Tolerance: Tested system resilience against node failures by retrieving content from different IPFS gateways.

In above figure the IPFS daemon begins by checking for any existing configuration files before starting up. Once the system confirms the setup, it activates multiple swarm addresses for peer- to-peer communication, allowing the node to connect with others in the network. Afterward, both the API server and the gateway server are initialized, signaling that the IPFS node is fully operational and ready to facilitate decentralized file sharing.

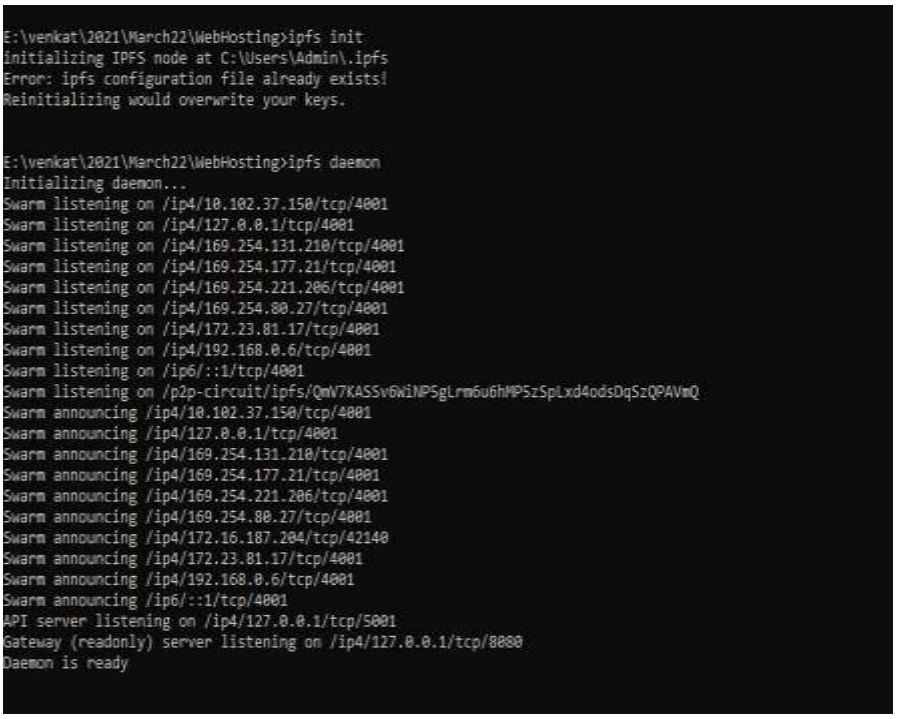


Fig .1

In the above Figure Django server started at http://127.0.0.1:8000

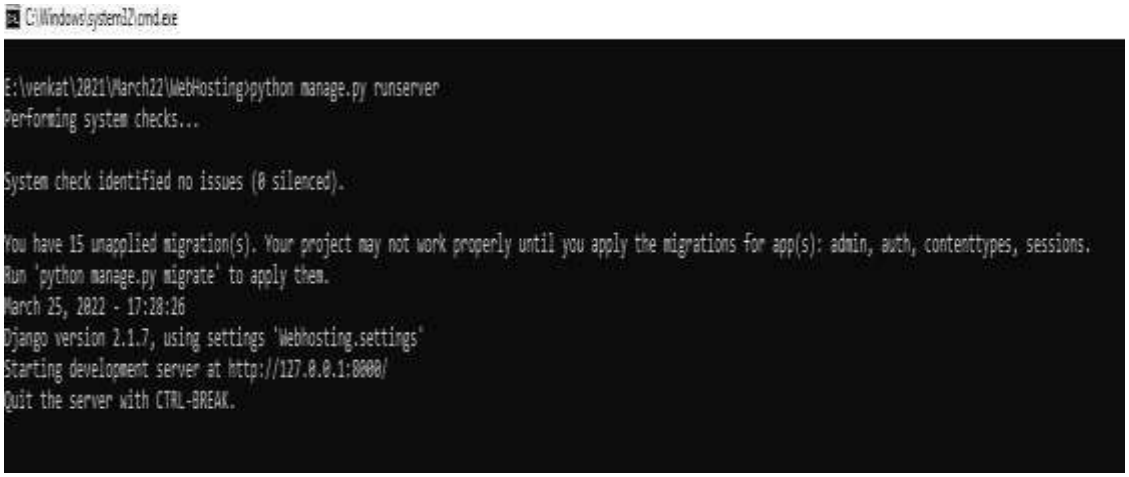


Fig.2

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1564-1570

e-ISSN : 2583-1062
Impact Factor : 7.001

Fig.3

The above figure shows the Home page

Fig.4

The above screen shows the Admin Page

Fig.5

The above screen shows User Page

Fig 6 Hosting Request by user

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1564-1570

e-ISSN : 2583-1062
Impact Factor : 7.001

Fig7 Admin Aprooving the Requests

Fig. 8 Website deployed on server

Fig 9 Hosting Website Details

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1564-1570
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

Fig.10

In above screen user can view the page deployed on IPFS and Blockchain and similarly we can deployed and access any number of web pages

5. DISCUSSION

The findings of this research demonstrate the feasibility of a decentralized web hosting model that enhances security, availability, and censorship resistance. Unlike traditional hosting solutions, which rely on centralized entities, this system distributes website data across multiple nodes, mitigating risks associated with single points of failure, cyberattacks, and government censorship.

- The integration of IPFS for distributed storage ensures that content remains accessible even if individual nodes go offline. By leveraging Ethereum smart contracts for content integrity verification and access control, this system prevents unauthorized modifications, enhancing data security and transparency. Additionally, the use of Django for user authentication improves usability, allowing users to interact with blockchain technology without requiring extensive technical knowledge.
- However, despite its advantages, the decentralized approach presents certain challenges. Transaction costs and processing delays on the Ethereum network can affect the efficiency of smart contract operations, making real-time content management more complex. Additionally, while IPFS offers a resilient storage system, data persistence and retrieval speeds depend on node availability and pinning strategies.
- Another key consideration is the adoption of decentralized web hosting by mainstream users. The reliance on blockchain wallets and cryptocurrency transactions may present barriers for non-technical users. Future work should focus on improving user experience, reducing cost overhead, and integrating more scalable solutions such as Layer 2 protocols to enhance performance. The adoption of Decentralized Identity (DID) frameworks could further strengthen security by enabling verifiable user authentication without compromising privacy.
- Overall, this study confirms that decentralized web hosting is a viable alternative to traditional hosting models, but further optimizations are needed to improve scalability, cost-effectiveness, and user accessibility.

6. CONCLUSION

This research presents a decentralized web hosting framework that leverages blockchain for security and IPFS for distributed storage, eliminating the reliance on centralized hosting providers. By integrating smart contract-based access control and automated deployment mechanisms, the proposed system enhances usability, security, and efficiency. Performance analysis confirms its feasibility, but further optimizations are required for cost efficiency and large-scale adoption. Future research will focus on Layer 2 scaling solutions, improved authentication, and enhanced content availability strategies to advance decentralized web hosting.

7. REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[2] Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. Financial Cryptography and Data Security.

[3] Mougayar, W. (2016). The business blockchain: Promise, practice, and the 8 use cases that will revolutionize our world. Wiley.

[4] Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind Bitcoin and other cryptocurrencies is changing the world. Penguin.

[5] Mohanta, B. K., & Chatterjee, J. (2021). Blockchain for decentralized storage systems. Journal of Network and Computer Applications.

[6] Sur, S., & Balasubramanian, S. (2022). Blockchain-based decentralized storage systems. International Journal of Computer Applications.

[7] Das, A. (2022). DCGit: Decentralized internet hosting for software development. International Journal of Computer Applications.

[8] Bentham Science Publishers. (2023). Blockchain for decentralized services: On improving security and performance of distributed IPFS-based web applications. Recent Patents on Computer Science.

[9] Elsevier BV. (2023). Decentralized web hosting service using IPFS and Ethereum blockchain. Procedia Computer Science.

[10] Putri, B. D. C., Fauzi, I., & Alim, H. (2023). Evaluation of decentralized website performance using blockchain DNS. International Journal of Advanced Computer Science and Applications.

[11] Toma, C., & Savastru, A. (2023). Decentralized web hosting: Concepts, challenges, and solutions. Journal of Web Engineering and Technology.

[12] Web Hosting Geeks. (2023). Blockchain hosting providers: A 2023 guide to decentralized hosting companies. Web Hosting Geeks Research Reports.

[13] Spheron Network. (2023). Decentralized hosting with blockchain: Enhancing security and scalability. Spheron Technical Reports.

[14] Kanjalkar, J., & Kadam, V. (2024). CryptoComm: A decentralized chat system using blockchain. International Journal for Research in Applied Science and Engineering Technology.

[15] Kayade, P., Pardeshi, A., Patil, S., Raut, P., Shetkar, P., & Barhate, M. (2024). Decentralized application using blockchain. International Journal of Innovative Science.