



IJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** X **Month of publication:** October 2023

DOI: <https://doi.org/10.22214/ijraset.2023.56408>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Blockchain Based Decentralized Web Hosting System

Aditya Dole

Department of Electronics and Telecommunication Vishwakarma Institute of Technology

Abstract: *In today's digital era, the internet heavily depends on a centralized framework where powerful servers support content on well-known platforms such as Facebook and Twitter. Although this centralization is proficient in content delivery, it comes with significant drawbacks, including a single point of failure and vulnerability to censorship. The need for a decentralized web hosting structure is growing due to its promise of content accessibility regardless of a user's geographical location, while still maintaining the speed and reliability of conventional web services.*

Currently, the internet's structure is defined by centralization, introducing risks related to cyber-attacks and service disturbances. For example, even a brief disruption to a large platform like Facebook can leave millions without internet access. Additionally, large corporations and government bodies possess significant control over the internet, enabling them to alter and censor content. To confront these problems, it becomes essential to develop a decentralized web structure that is publicly owned. This study delves into the issues arising from the centralized internet and investigates potential solutions by utilizing blockchain technology to decentralize web structure, subsequently improving traditional web services and fortifying the internet's robustness and accessibility.

Keywords: *Block chain, decentralized architecture, centralization of web architecture, peer-to-peer web hosting, web2*

I. INTRODUCTION

The Internet and the emergence of the WWW put an end to sharing of information through physical mediums (like floppy disks, pen drives etc.) by providing a data transmission protocol – TCP/IP – that made the transfer of data faster and massively reduced the transaction costs of information exchange [4]. Ten years later, the Internet became more mature and programmable [4]. We saw the rise of the so-called “Web2” architecture, which brought us social media and e-commerce platforms. The Web2 revolutionized social interactions, bringing producers and consumers of information, goods, and services closer together, and allowed us to enjoy P2P (Peer to Peer) interactions on a global scale, but always with a middleman which a platform acting as a trusted intermediary between two people who do not know or trust each other, which mainly were giant MNCs and governments. Although these platforms have done an amazing job of developing a peer-to-peer (P2P) economy with a sophisticated content discovery and value settlement layer, they also own all user data and determine all transaction rules. [3]. In this context, block chain seems to be a driving force of the next-generation Internet, what some refer to as the “Web3”. Block chain reinvents the way data is stored and managed. It offers a distinct collection of data that is controlled collectively (a universal state layer). For the first time, a value settlement layer for the Internet is made possible by this special state layer. It allows us to send files in a copy-protected way, enabling true P2P transactions without intermediaries, and it all started with the emergence of Bitcoin. Web2 brought with it a revolution in the frontend, it is the Web3 which now is trying to remap the wiring of the unseen stuff. While the surface of the Internet or Web as we call it will remain the same, it is the backend where all the revolution will take place.

A. Vision

Our vision is anchored in the reshaping of the web hosting environment. We are driven to establish a decentralized web hosting system that surpasses the existing centralized paradigm. Our chief objectives in this vision are to boost efficiency and dependability while drastically reducing the constant risk of security infringements.

The centralization of web hosting, wherein potent corporations and governmental bodies hold dominion over the majority of data, has sparked worries about user privacy, data protection, and censorship. Our vision endeavors to remedy these issues by dispersing data across a network of linked nodes, removing the power concentration from a select few. This decentralization not only strengthens security but also guarantees that sensitive data is not exclusively in the hands of these powerful players.



By diverging from the conventional model, we aim to provide a more fair and robust internet infrastructure. This vision signifies our dedication to a safer, more open, and inclusive digital realm where users can access and host information without excessive dependence on a small number of dominant entities.

B. Scope of the project

A decentralized web hosting system, based on blockchain technology, revolutionizes the internet infrastructure by offering multiple benefits. Foremost is security, as the distributed ledger of blockchain is resistant to tampering and cyber threats. It promotes efficient peer-to-peer exchange of information, reducing the need for intermediaries. Transaction logs allow for transparency and chronological tracking, streamlining auditing processes and increasing accountability. Redundancy assures accessibility even when individual nodes fail, and the immutability of data ensures its integrity. User privacy is enhanced, giving individuals control over their own information. User ownership and control are emphasized, decreasing dependency on major corporations. The system's scalability meets the increasing demands of the web. This innovative model prioritizes security, efficient information exchange, transparent data recording, accessibility, and user control, positioning it as a robust and user-focused alternative to traditional centralized web hosting systems.

C. Goals and Objective

Our project is focused on a transformative mission: to transition web hosting from a single centralized entity to a distributed system of multiple peers. This innovative strategy is inspired by the emerging "Web3" architecture that underscores decentralization and user empowerment.

At its core, our objective is to democratize the control of web servers by distributing it among various users. This shift towards decentralization is critical in reshaping the operation of the internet. It bestows users with more influence and ownership over their digital domains.

Drawing upon the principles of Web3, our objective is to break away from the conventional, top-down structure of web hosting, where a single entity holds significant power and responsibility. Our vision, instead, is a dynamic ecosystem where users collectively partake in hosting and managing web content. This methodology not only amplifies the system's resilience and security but also cultivates a more equitable and user-centric online space.

II. LITERATURE REVIEW

A. Blockchain

Blockchain operates as a decentralized system where nodes interact directly via a peer-to-peer network. Some nodes maintain a ledger made of a series of blocks that have been agreed upon through consensus. Blocks are interconnected using the hash of the preceding block, a value that also serves to confirm the integrity of the previous block's content. The first block in the chain is referred to as the genesis block[8]. Each block consists of a block header, which contains the management information for both the block and the chain, and a block body, which houses a set of transactions. To ensure synchronization of data on the ledger among miner nodes, blockchain technology utilizes consensus algorithms[9]. Blockchain technology has numerous potential applications. Cruz et al. suggested leveraging smart contracts for role-based access control. The authors of [14] suggested utilizing blockchain to control permissions for access to medical data. There are further suggested applications in the fields of agriculture, finance, Internet of Things, and transportation [5]. A new category of accountable systems has arisen in recent years. The first such system was Bitcoin, which uses a publicly verifiable open ledger (also known as a blockchain) to enable users to transfer money (bitcoins) safely without the need for a centralized authority. Since then, other initiatives have shown how these blockchains can do additional tasks requiring trusted computation and auditability (referred to as Bitcoin 2.0 [17]).

B. Blockchain for decentralization of internet: prospects, trends and challenges

The research paper studied, plans to implement a technique to use blockchain for decentralization of web hosting. This includes studying different web architectures, like Web 1.0, Web 2.0 and ongoing Web 3.0 as well as learning the advantages and disadvantages of these architectures. This contains learning various algorithms about how the data is stored, transferred and received by the user. This study provides us with numerous comparisons between different technologies, which elaborate the need of decentralization thus, putting forward a simplistic way to decide the solution for solving the Internet problem.

C. Blockchain technology for internet decentralization: opportunities, trends, and difficulties

Recent studies have shown how similar strategies can be used to de-anonymize anonymized datasets [18], [19], even with a limited number of data points or high-dimensional data. As the purpose this study is to focus on problems of centralized web architecture and investigate the block chain's potential for decentralized web architecture capable of improving conventional web services. Internet was created as decentralized architecture interconnected with several computer networks to exchange information across trusted participants.

With the development of web2 it has led to the centralization of web architecture. The causes of all these services are provided by the giant tech companies, they control vast amounts of users' data. But the original concept of the internet was not like that. The giant companies are organizing and monetizing information through their centralized web services. So due to centralization of web services internet is undergoing through lots of issues which are getting worse day by day. The paper proposes to come up with a solution where the Identity Management System (IDMS) is based on self- sovereign identity (SSI) management architecture. Leading businesses in the sector have decided to put into place their own proprietary authentication software based on the OAuth protocol [16], where they act as centralized trusted authorities.

D. A Decentralized Solution for Web Hosting

This paper proposes a solution for decentralized web hosting using mainly 2 technologies i.e., IPFS (Interplanetary File System) and Ethereum blockchain. The proposed solution provides 3 huge advantages compared to the current one that are - Confidentiality, Integrity and availability. The authors in [12] provide a survey of decentralized access control mechanisms in distributed file systems intended for large-scale environments. Within the realm of blockchain technology, numerous research efforts [12], [13] explore the potential of using blockchain as an access control manager for distributed systems, such as cloud computing. Zyskind et. al. and his team [13] suggest a decentralized platform for personal data that is gathered and managed by a third party. This solution is made possible by integrating a blockchain with an off-chain storage method. Interplanetary File System - Is a peer-to-peer distributed file system [5].

It is very similar to the Bit Torrent protocol, where the content is stored and provided by and to the users, by the users themselves. Unlike the traditional system where information is requested based on Location Based Addressing, IPFS uses Content Based Addressing, where the information is requested on the basis of the content availability rather than the address of the server. Nodes in the IPFS communicate with each other through peer-to-peer network with asymmetrically encrypted data. The data to be served is stored in an IPFS object, which includes 2 fields: - data and link. The data contains binary data, and the link contains links to other pieces of the same data.

E. Ethereum Blockchain

Vitalik Buterin proposed Ethereum is a new distributed blockchain network [10]. In relation to the IPFS, Ethereum blockchain contains smart contracts, where information about the web hosting services and the nodes in the network can be stored, which can provide access control to the admins and clients. This paper leverages the Ethereum blockchain [11] to provide an access controlled IPFS. An Ethereum smart contract stores and allows dynamic modification of the access control list.

III. SPECIFIC REQUIREMENTS

A. Functional Requirements

- 1) Constant ledger state – All the ledgers in the distributed machines should have the same version. These ledgers should contain a variable list of transactions with accurate timestamps. The transmission of these ledgers between nodes will be controlled by transaction protocols known as Smart Contracts. It is also needed that the ledgers be only appended within the database to make sure that without the need of central verification, transactions can be tracked securely.
- 2) Maintaining Immutable Storage – The nodes used within the network will be unalterable or immutable. Each database created is retained in every node in the interconnected network along with having a reference of itself in the Blockchain as part of unchangeable history. To maintain the integrity of ledgers within the nodes, the immutable storage will provide an encryption function, which will establish trust and increase in incentives within the Blockchain.
- 3) Automated update of hashes - Developers should have an automated process to update the hashes of the node content after they make updates, changes to their applications, so that every node in the network knows that a new version of the object (explained above) is published. This process for now has to be done manually after every update/change on the IFPS.

- 4) Storage incentives for all the users who give their storage spaces in order to be used as storage nodes in the network, should be given some kind of crypto currency or equivalent assets as incentive so that they continue doing so and encourage others to do the same.
 - a) Upload Data - Users or node managers should be able to upload new data. And a copy of the old data should be maintained for future references. (Somewhat like way back machine).
 - b) Remove node on will - Users can choose to opt in or out from becoming a retrieval miner node or storage miner node.
 - c) Register and manage node - Node provides should have ability to manage their own nodes. Some operations may include - registering, stopping, pausing operations for some time, removing.
 - d) Easy sharing of user's public key - The public key should be easily transferred between clients.
 - e) Watching ads - Ads are the single major source of generating revenue of many companies, hence disabling them isn't an option. Instead, clients will be shown ads based on certain parameters which keep their privacy and identity hidden, but at the same time show relevant ads.

B. Non-Functional Requirements

- 1) Tackling Blockchain's Challenges- Blockchain, though revolutionary, isn't without its flaws, including concerns about privacy, performance, and energy-intensive mining. Our goal is to fuse blockchain with advanced web technologies such as the Internet of Things (IoT), Cloud Computing, and Peer-to-Peer (P2P) systems to mitigate these issues. This integration paves the way for a more flexible and resilient network that utilizes the advantages of these technologies while minimizing blockchain's shortcomings.
- 2) Enhancing Scalability and Availability- For blockchain networks to achieve mainstream acceptance, their scalability and availability are of utmost importance. Hence, we are dedicated to finding solutions that bolster the fundamental features of blockchain, such as increasing the block size limits and decreasing the time taken to verify blocks. We are investigating well-known Layer 1 scalability solutions like sharding, segregated witness (SEGWIT), and hard forking to ensure the blockchain can cater to an expanding user base.
- 3) Ensuring Reliability- Conventional client-server models are vulnerable to single points of failure, which can cause network or system downtime. By incorporating Peer-to-Peer (P2P) technologies into a Web 3.0 blockchain-based structure, we strive to eradicate such weak points. In this decentralized framework, services are more resilient to outages and bottlenecks, guaranteeing reliability for users.
- 4) Prioritizing Security and Privacy- Shielding essential user data from harmful cyber threats and maintaining network integrity are of the highest importance. Blockchain-based methods provide sturdy security measures, such as protection against Distributed Denial of Service (DDoS) attacks. This inherently enhances the security and privacy of user data, minimizing the risks tied to centralized networks.
- 5) Enforcing Strict Access Control- Upholding rigorous access control is vital to protect the information housed on the Interplanetary File System (IPFS). Nodes on the IPFS network should be incapable of interpreting object content or accessing information without the appropriate rights and permissions. This access control system aids in safeguarding data privacy and integrity.
- 6) Swift Content Delivery- Quick distribution of new application versions is key to keeping users current. We strive to ensure that when developers roll out new versions, these updates propagate swiftly within the network. At the same time, older versions should be stored for reference, striking a balance between providing the most recent content and maintaining access to past versions.
- 7) Transparency - Blockchain's built-in decentralization guarantees all transactions are open and can be publicly inspected. This transparency can be achieved via personal nodes or blockchain explorers, with transactions occurring in real-time, a level of openness that's challenging to attain in centralized systems. Each node keeps an updated copy of the blockchain as new blocks are incorporated, enabling anyone to follow transactions and modifications within the network. This level of transparency forms a crucial aspect of blockchain technology [2].

C. Hardware Requirements

The active engagement of users who donate their workstations to function as network nodes is this decentralized structure's primary reliance for operation.

This system’s adaptability is significant in that it can work with a variety of computer setups with the only prerequisites being an internet connection and a predetermined amount of storage.

D. Software Requirements

1) Internet Connection-

A. End users - To guarantee seamless access to the de- centralized network’s content, a minimum internet connection speed of 500 kbps or greater is advised.

B. Node providers - A somewhat faster internet connection speed is advised for individuals who decide to become node providers and provide resources to the network, particularly between 1.5 and 2 mbps. Effective network management and content exchange are made possible by this increased speed.

2) IPFS Installation- All participants must have the Interplanetary File System (IPFS) software installed on their computers, regardless of whether they want to create or consume content. At the center of this decentralized organization is IPFS, which makes safe distributed data sharing possible.

3) Ethereum Blockchain Dependencies- Users and node providers need to have certain software requirements in order to interact with the Ethereum blockchain. These comprise software development tools like Solidity, which are necessary for developing and deploying smart contracts. The decentralized network’s numerous functions are built on top of these smart contracts, which promote trust, security, and transparency in all dealings.

Participants can effectively contribute to and profit from this decentralized structure by making sure these software requirements are met. Regardless of their computer configuration, it offers users a flexible and inclusive framework that enables them to actively contribute to the network’s expansion and functionality.

IV. DIAGRAMS

Use case diagram

Blockchain Based Decentralized Web Hosting System

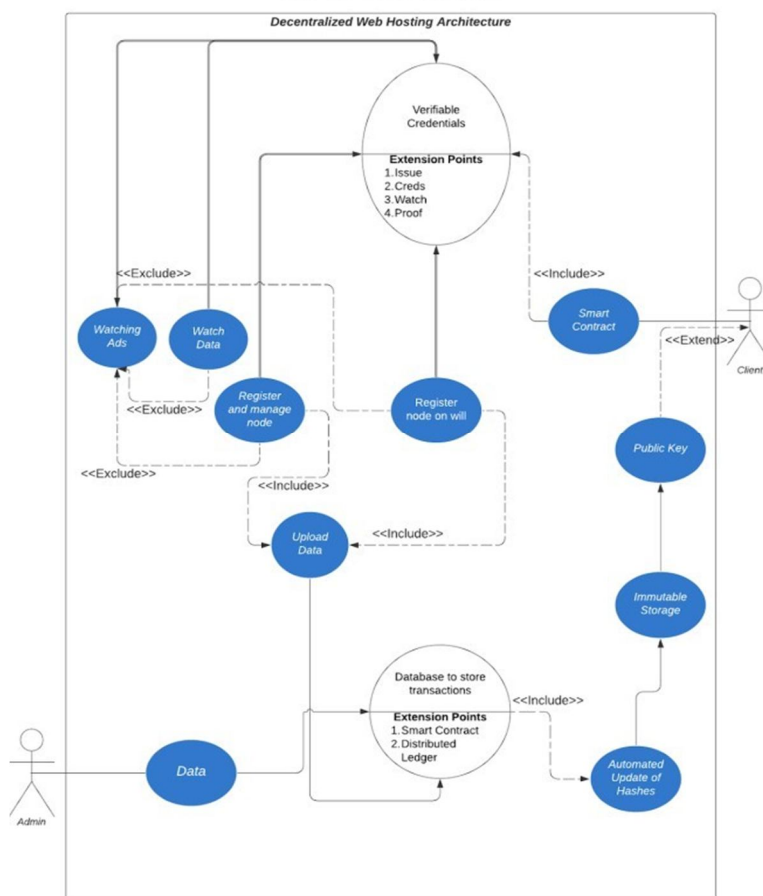


Figure 1: Use case Diagram

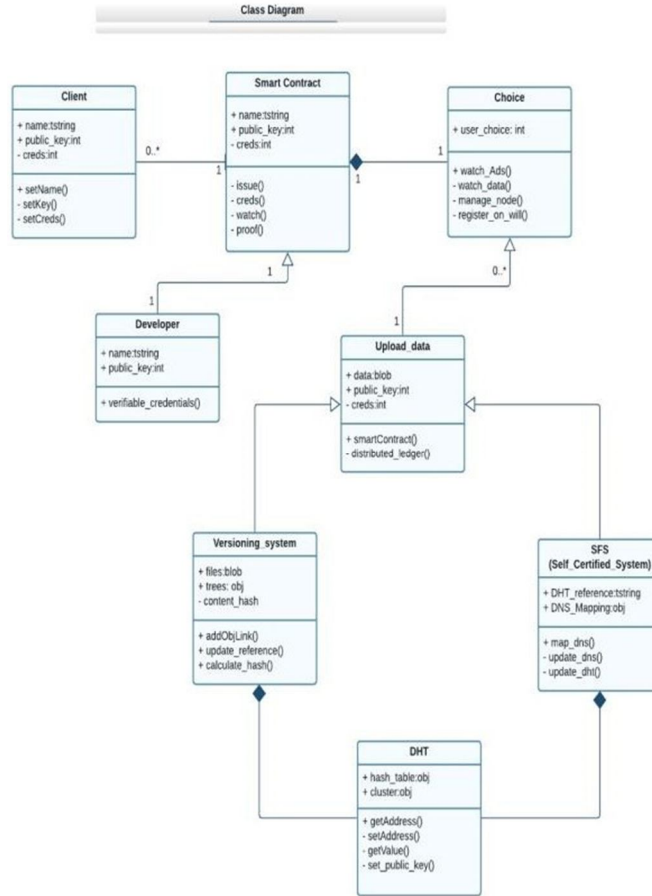


Figure 2: class Diagram

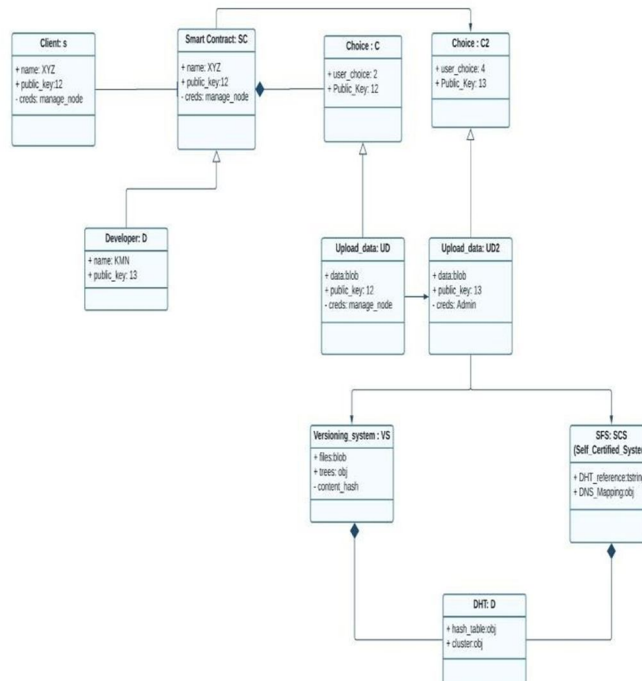


Figure 3: object diagram

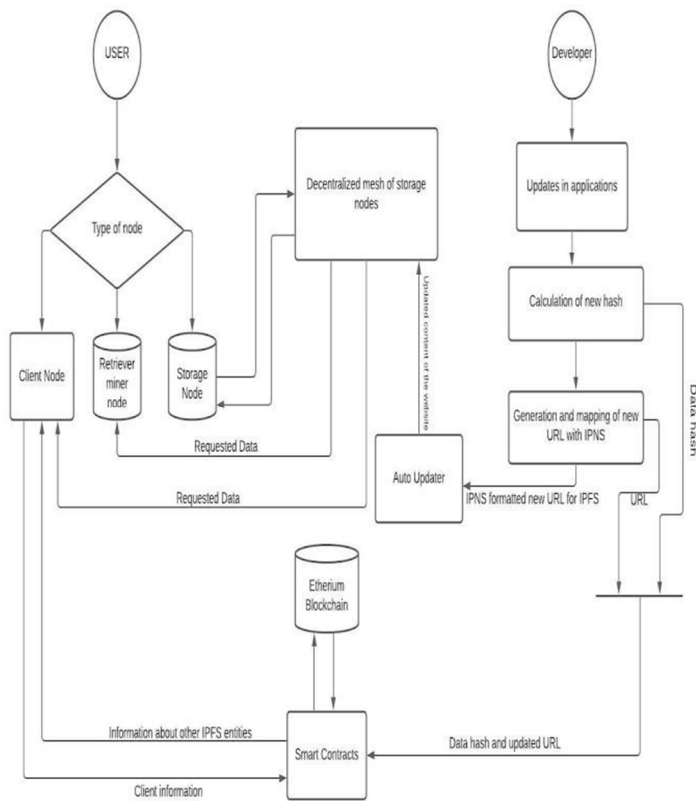


Figure 4: Activity diagram

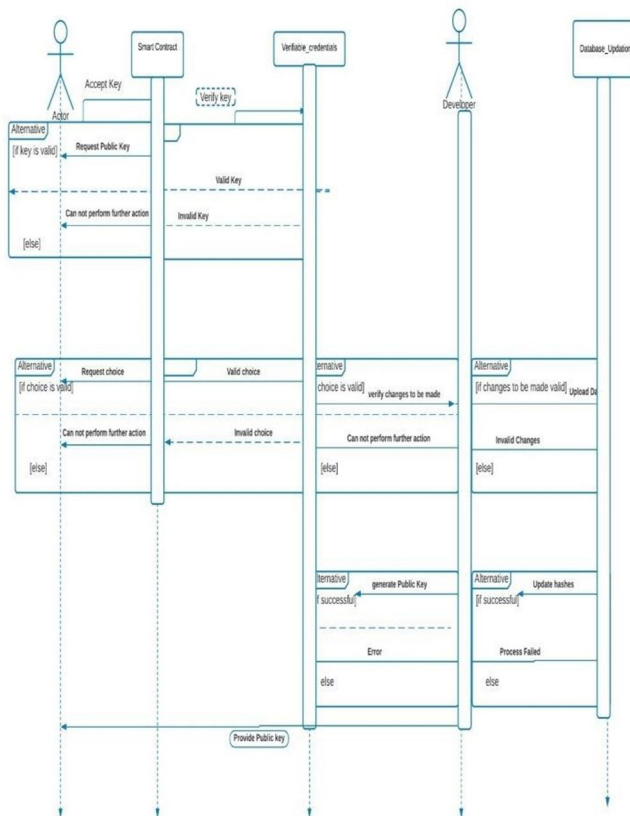


Figure 5: Sequence Diagram

| | I WANT TO | PRIORITY | STATUS |
|------|---|----------|--------|
| User | 1. Access the main page. 2.Introduce the correct information. 3. Smart contract 4. Able to sign in | 1 | Done |
| User | Able to monitor system | 1 | Done |
| User | 1.sign out 2.System destroys session | 1 | Done |
| User | Distributed resource sharing requirement | 1 | Done |

Figure 6: Product backlog

| | |
|-----|--|
| US1 | As client I want freedom of box like personal publishing system should be there |
| US2 | As client there should be improvement in storage system like distributed storage service with a proposed mechanism to incentivize resource sharing should be there |
| US3 | As client I want distributed platforms to shift towards user-controlled data, the ownership of a user's social graph and intellectual property should be created online. |
| US3 | "Decentralized" networks generally means anyone can join, which implies these systems have to take strong precautions to enforce security. |
| AD1 | As administrator there is requirement like linked-data protocol is there that could act as a back-end for data sharing between social media networks |
| AD2 | As administrator it is my request to Fund developers directly to create a diverse ecosystem of publishing platforms and curation websites is another place to make a difference. |

Figure 7: User Stories

V. CONCLUSION

We can use block-chain's potential to decentralize web architecture and can improve traditional web services. De- centralized applications, or Apps, run on a block chain — a decentralized digital ledger that is maintained by a network of computers rather than a centralized server. This allows the network to function without a single point of failure and provides users with the security and privacy they deserve. The decentralized web is a web that is built on a block chain, which allows users to store and share content without having to rely on a single service provider. Decentralization is the foundation of the new web. The web we all know, and love is centralized hosted on a small number of servers and accessed through a small number of websites. But most of the web we use today is centralized, built on a vast network of servers and accessed through thousands of websites. Data is hosted on a handful of websites, instead of being distributed across millions of users. So the decentralized web is the solution to the centralized web's major problems.

REFERENCES

- [1] International Journal of Internet, Broadcasting and Communication Vol.13 No.1 26-36 (2021) <http://dx.doi.org/10.7236/IJIBC.2021.13.1.26> Blockchain for the Trustworthy Decentralized Web Architecture
- [2] 2019 6th NAFOSTED Conference on Information and Computer Science (NICS) A Decentralized Solution for Web Hosting
- [3] IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3) Juan Benet juan@benet.ai
- [4] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. <https://bitcoin.org/bitcoin.pdf>.
- [5] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems" Future Generation Computer Systems, 2017.
- [6] Z. Xiao, S. Wen, H. Yu, Z. Wu, H. Chen, C. Zhang, and Y. Ji, "A new architecture of web applications-The Widget/Server architecture," in 2010 2nd IEEE International Conference on Network Infrastructure and Digital Content, IEEE, 2010, pp. 866-869.
- [7] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, "BlockchainBased, Decentralized Access Control for IPFS," in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 1499-1506.
- [8] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, "Bitcoin and cryptocurrency technologies: A comprehensive introduction," Princeton University Press, 2016.
- [9] Z. Zheng, S. Xie, H. N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," in International Journal of Web and Grid Services, 2016.
- [10] V. Buterin, "A next-generation smart contract and decentralized application platform," white paper 3, 2014, 37.
- [11] G. Wood. (2018) Ethereum: A secure, decentralised generalised transaction ledger. [Online]. Available: <http://yellowpaper.io/>
- [12] S. Miltchev, J. M. Smith, V. Prevelakis, A. Keromytis, and S. Ioannidis, "Decentralized access control in distributed file systems," ACM Comput. Surv., vol. 40, no. 3, pp. 10:1–10:30, Aug. 2008. [Online]. Available: <http://doi.acm.org/10.1145/1380584.1380588>
- [13] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in 2015 IEEE Security and Privacy Workshops, May 2015, pp. 180–184.
- [14] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in 2016 2nd International Conference on Open and Big Data (OBD), IEEE, 2016, pp. 25-30.
- [15] R. A. Popa, E. Stark, S. Valdez, J. Helfer, N. Zeldovich, and H. Balakrishnan, "Building web applications on top of encrypted data using Mylar," in 11th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 14), 2014, pp. 157-172.
- [16] Juan Perez. Facebook, google launch data portability programs to all, 2008.
- [17] Jon Evans. Bitcoin 2.0: Sidechains and ethereum and zerocash, oh my!, 2014.
- [18] Arvind Narayanan and Vitaly Shmatikov. How to break anonymity of the netflix prize dataset. arXiv preprint cs/0610105, 2006.
- [19] Yves-Alexandre de Montjoye, Cesar A Hidalgo, Michel Verleysen, and Vincent D Blondel. Unique in the crowd: The privacy bounds of human mobility. Scientific reports, 3, 2013.
- [20] Duffany, J. L. (2012). Cloud Computing Security and Privacy. In 10th Latin American and Caribbean Conference for Engineering and Technology (pp. 1-9)



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)