PriMera Scientific Engineering
Volume 8 Issue 2 February 2026
ISSN: 2834-2550

Ransomware Resilient Architecture for Healthcare Using Blockchain and IPFS

Type: Research Article
Received: January 12, 2026
Published: February 03, 2026

Citation:
Abdulaziz Alkhajeh., et al. "Ransomware Resilient Architecture for Healthcare Using Blockchain and IPFS". PriMera Scientific Engineering 8.2 (2026): 25-34.

Abdulaziz Alkhajeh*, Sara Alhashmi, Alya Al Ali, Rakan Alhosani, Suhail Alshehhi, Deepa Pavithran and Joseph Anajemba

Abu Dhabi Polytechnic, Abu Dhabi, UAE

***Corresponding Author:** Abdulaziz Alkhajeh, Abu Dhabi Polytechnic, Abu Dhabi, UAE.

Abstract

Healthcare has always been a crucial part of human life, with people investing resources to get the best services available. Ensuring patient confidentiality has always been crucial, but the digital era introduces new security risks. Hospitals now store patient information in computerized databases, which are vulnerable to cyberattacks. One major threat is ransomware attacks, where hackers capture sensitive and confidential patient data and demand large sums of money to prevent it from being leaked or sold. This puts patient privacy at risk and can disrupt healthcare services. Also, unauthorized access to the patients' information compromising the data confidentiality has been a growing concern because health care has always been sensitive and personal information that should not be utilized for commercial purposes. Blockchain technology offers a solution by providing a secure way to store patient files. Using an Interplanetary File System (IPFS) on the blockchain, healthcare providers can save patient records in a decentralized and protected system, reducing the risks linked to traditional databases. This method helps protect patient information from cyber threats, ensuring privacy and security. In this paper, we are using blockchain-based architecture coupled with pinata IPFS cloud to secure the patient's valuable information from any kind of cyber-attack, including ransomware.

Keywords: Data breach prevention; Ransomware attacks; Blockchain technology; decentralized storage

Introduction

With the rapid digital transformation in healthcare, patient data stored in centralized systems has become a prime target for ransomware attacks. Cybercriminals gain unauthorized access, encrypt medical records, and demand ransom for data recovery. Despite ongoing efforts to strengthen cybersecurity, many healthcare providers remain vulnerable, leading to significant breaches of sensitive patient information.

Ransomware specifically poses a major threat by disrupting system operations and denying access to critical data. While encryption and access control are widely used, they often fall short in protect-

ing system availability—an essential aspect of continuous patient care [1, 2]. To address these gaps, this paper proposes a framework that combines blockchain technology with the InterPlanetary File System (IPFS) to improve data security, integrity, and resilience in healthcare environments [3]. By using Pinata Cloud with IPFS, the model further enhances data availability and long-term storage reliability, forming a more robust and decentralized infrastructure [4].

The rest of the paper is structured as follows: Section II reviews the background of ransomware and its impact on healthcare. Section III outlines current security practices and the role of blockchain and IPFS. Section IV presents the rationale for adopting decentralized models. Section V explains the proposed methodology. Section VI evaluates tools such as MetaMask, Solidity, and Remix-IDE. Section VII concludes the study and outlines future directions.

Background

Ransomware and its Impact on Healthcare

Ransomware has recently emerged as a common threat in health organizations across the world affecting large, centralized records bases that contain patients' complete records, including medical histories, diagnostics, and finances. These attacks lock data and request substantial ransoms for it to unlock, with the consequence of severe financial hits and interruptions in patient care for many healthcare organizations. For instance, ransomware attacks carried out against HCIs in the United States were about $21 billion in the year 2020 and therefore require more robust protection of the health data [1, 2].

The impact of ransomware therefore transcends mere monetized losses to productivity lags, where hospitals for example have admitted to returning to pen and paper during cyber-attacks. Such delays in the attainment of EHRs may result in the detriment of patient safety and care, especially in the case of an emergency [3]. Moreover, ransomware attacks on rural hospitals exacerbate the problem, as these facilities often lack sufficient funds for proper cybersecurity measures [1].

Bare essentials like backup and antivirus have not been able to stem the rising tide of ransomware waves with new improved strains. The theme of the paper is the healthcare industry that ought to adopt advanced strategies to boost the ability to sustain disruptions and to maintain accessibility to sensitive information [4, 6]. Ransomware attacks the system through the following means:

- Phishing emails.
- Malicious website/ads.
- Exploiting vulnerabilities.
- Drive-by downloads.
- Remote desktop protocol.
- USB drive/network sharing.

There are different kinds of ransomware available in the market. The most common types are as follows:

- ***Locker Ransomware:*** this attack locks the drive and prevents the user from using their devices.
- ***Crypto Ransomware:*** this attack encrypts the files through some code and then demands money to decrypt it.
- ***Double extortion ransomware:*** Encrypting data and then threatening to leak it.

Blockchain technology in healthcare

Blockchain offers a decentralized and cryptographically secure solution for managing sensitive healthcare data. Unlike centralized systems, it eliminates single points of failure and ensures data integrity through linked cryptographic hashes [7]. Its structure supports regulatory compliance (e.g., GDPR) by giving healthcare providers control over patient data. Smart contracts further enhance security and transparency in data exchanges [8, 9].

Integrating blockchain with the InterPlanetary File System (IPFS) strengthens data management by decentralizing storage. IPFS assigns each file a unique Content Identifier (CID), ensuring immutability and enabling version tracking. Storing only CIDs on the blockchain optimizes performance while preserving data integrity and availability [10, 11]. This combined approach mitigates risks such as unauthorized access or data loss and enhances protection against ransomware.

The Binance Smart Chain (BSC) Testnet, using Proof of Staked Authority (PoSA), offers a fast, secure testing environment. It features a limited number of validators selected by stake and reputation, enabling 3-second block generation and high throughput. This makes it well-suited for developing and testing decentralized applications and smart contracts in a controlled setting [18].

Related Work

This related work explores the potential of using blockchain and IPFS to enhance data security within the healthcare sector, focusing on their combined role in preventing ransomware attacks. It begins by examining the impact of ransomware on healthcare, the limitations of traditional security measures, and the fundamental principles of blockchain and IPFS. A rising number of ransomware attacks have been recorded annually, focusing on healthcare companies. The healthcare industry in the United States has experienced a notable increase in these attacks, according to [1], as hackers have realized the importance of healthcare data and the industry's dependence on constant access to information for patient care.

The authors of [6] examine how blockchain technology might be used to secure healthcare data, emphasizing how it can improve patient privacy, confidentiality, and integrity. The study shows how blockchain offers a strong solution for immutable, decentralized data management while addressing issues like scalability. This is in line with the proposed paper, which combines blockchain and IPFS to strengthen the system's defenses against ransomware. Proactive storage techniques and effective access control measures are used to guarantee the security and accessibility of medical data.

The creators of [11] use IPFS and blockchain to safely store IoT data, but they do not emphasize proactive ransomware protection. This is enhanced by our paper, which stores the IPFS data hash on the blockchain. The decentralized structure of blockchain adds an additional level of protection while guaranteeing data integrity and resistance to tampering. Our system provides a more thorough security framework than mere storage by integrating data storage, hashing, and the decentralized backup technique, thus enhancing the protection of healthcare data from ransomware.

By showcasing blockchain's potential for improved security and ransomware mitigation through effective attack detection and response, [15] introduces the Ransomware Blockchain Efficient Framework (RBEF) for digital healthcare. With a significant difference, our paper proposes to strengthen healthcare data security against ransomware, whereas RBEF concentrates on blockchain- specific threat mitigation. Rather than just responding to an attack after it has already occurred, our strategy proactively aims to prevent data loss and improve resilience before one occurs. Compared to this paper, we enable decentralized storage and improved data availability by combining IPFS with blockchain, which is an important feature that RBEF does not address. This builds a stronger and more resilient platform for healthcare data management against ransomware.

In [16], the article suggests a blockchain-based architecture for safe medical data management that makes use of smart contracts to control access and guarantee data accuracy. This approach does not particularly address the rising problem of ransomware attacks in healthcare systems, even while it enhances security through decentralized access control. The proposed solution, in contrast, emphasizes a proactive backup method to ensure data availability and recoverability in the case of an attack in addition to integrating blockchain and IPFS for safe, unchangeable data storage. Because prevention and recovery are combined, the suggested solution is more effective and provides a thorough protection against ransomware in healthcare environments.

The authors of [17] suggest combining blockchain and IPFS in a decentralized manner to store medical data securely. Although their technology improves privacy and data integrity, ransomware attacks are not directly addressed by it. However, this paper goes above and beyond by combining IPFS and blockchain with a backup plan, guaranteeing that data can be recovered in the case of a ransom-

ware attack. The suggested method provides a more powerful and comprehensive defense against ransomware by combining safe storage with proactive data recovery techniques, which increases its applicability in actual healthcare environments.

There is limited literature on using blockchain for proactive ransomware prevention in healthcare. In contrast to previous studies that focus mainly on detection and reactive measures, our paper integrates blockchain and IPFS for secure storage with an advanced backup strategy that ensures data recovery and continuity. This comprehensive approach not only prevents data loss but also minimizes downtime, offering a more resilient framework for managing healthcare information.

Proposed Approach

The approach being proposed in this paper is that we will be using blockchain to store the hashes only. These hashes are generated by first translating the patient's information into JSON format and then uploading the same on the Pinata IFPS cloud. Upon uploading, IPFS Pinata cloud provides us a hash, which is then saved onto the blockchain. These decentralized file storage servers are specifically designed to support blockchain-based data storage. We will be using these servers for all the critical patient files, and since these files are non- existent on any server, these will not be exposed to the attackers.

System Design

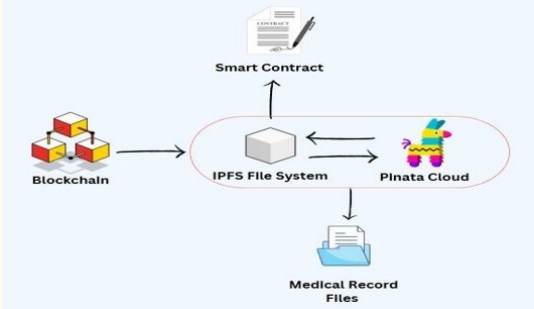

Figure 1: System Design.

Figure 1 illustrates how blockchain, IPFS, and Pinata Cloud work together to secure patient medical records. Blockchain ensures data integrity and availability, preventing unauthorized modifications. IPFS facilitates decentralized storage, while Pinata Cloud enhances security and accessibility for medical records. A smart contract governs interactions within the blockchain, ensuring only authorized access to patient files. This architecture assures that sensitive healthcare data remains tamper-proof, securely stored, and efficiently retrievable while maintaining confidentiality and access control for authorized personnel.

- ***Patient Visits Hospital***: The patient arrives and provides information to initiate their healthcare record.
- ***Receptionist Adds Patient's Information:*** The receptionist inputs the patient's data into the system, which creates a JSON file containing the patient's information.
- ***Create JSON File:*** The patient's details are saved as a JSON file, which will be uploaded to a decentralized storage system.
- ***IPFS Storage:*** The JSON file is uploaded to IPFS (InterPlanetary File System), a decentralized file storage platform, which stores the file and generates a unique file hash.
- ***Receive IPFS File Hash:*** The system receives the file hash generated by IPFS, which uniquely identifies the patient's file.

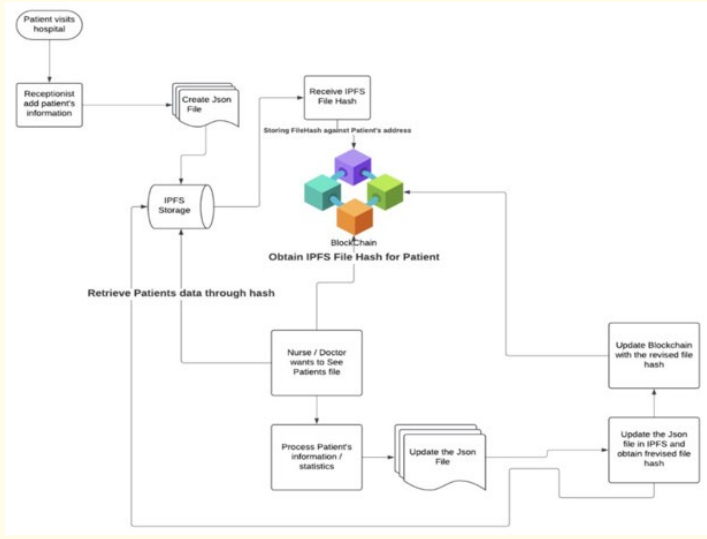

Figure 2: Workflow of Blockchain-based Healthcare Data Storage.

Check IPFS File Hash for Patient (Blockchain)

The IPFS file hash is stored on the blockchain, linking the patient's unique blockchain address with their data. This ensures secure, tamper-proof storage and retrieval of the patient's data.

- ***Retrieve Patient's Data Through Hash:*** Healthcare provider can access the patient's information by using the IPFS file hash to locate and retrieve the file from IPFS.

Process Patient's Information/Statistics

The healthcare provider reviews the patient's information, performs any necessary updates, and processes any new statistics or health records.

Update the JSON File

If there are updates or changes to the patient's information, the JSON file is modified with the new data.

- ***Update the JSON File in IPFS and Obtain Revised File Hash:*** The updated JSON file is uploaded again to IPFS, generating a new file hash that reflects the revised information.
- ***Update Blockchain with the Revised File Hash:*** The new IPFS file hash is updated on the blockchain, replacing the old hash with the revised one. This ensures the blockchain always points to the most recent version of the patient's file.

Decentralized Data Storage

Patient records are stored off-chain using IPFS, ensuring data availability and integrity. Each file is assigned a unique content identifier (CID) to maintain immutability. The blockchain stores only the CID and metadata, reducing on-chain storage overhead.

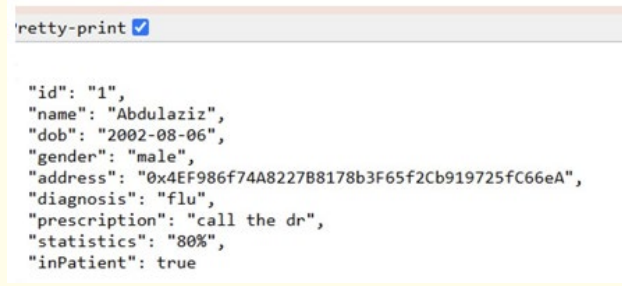

Figure 3: Json data-format from API.

Figure 3 shows the IPFS Pinata gateway through which we are able to see the data stored in IPFS Pinata. Only a few pieces of information like the address of the patient, the address of the doctor assigned, and the address of the nurse assigned are stored inside the blockchain, the rest of the information is not stored in the blockchain. That entire information is saved as a JSON file in the IPFS pinata cloud and a hash is generated from IPFS pinata. This cryptographic hash is then saved into the blockchain. So, no information can be fetched directly from the blockchain. Only authorized nurses and doctors can fetch this information. We chose to save this patient information in IPFS in order to save it from ransomware attacks.

IPFS uses a decentralized, peer-to-peer system where every node plays a role in storing and sharing data [19]. These nodes operate on libp2p, a networking layer that manages secure communication, peer discovery, and data exchange. To locate files, IPFS relies on a Kademlia-based Distributed Hash Table (DHT), allowing nodes to find where specific content—tagged with unique cryptographic hashes—is stored in the network. Files are split into smaller pieces and arranged in a Merkle DAG (Directed Acyclic Graph), where each chunk is hashed and linked to ensure consistency and immutability. Each node keeps a local blockstore, which contains the blocks it stores, referenced by Content Identifiers (CIDs). This architecture supports efficient, verifiable, and decentralized data sharing across the IPFS network.

Data Processing, updating and retrieval

Transactions include the patient's blockchain address, file hash (CID), and timestamp. Each transaction is validated by network nodes to maintain integrity.

Role-Based Access Control (RBAC) has been implemented to ensure that data access and retrieval are restricted based on predefined user roles and responsibilities. This access control system uses the private keys stored inside MetaMask and verifies the authenticity of users through web3 injection of private keys. If verified, the system will allow access to the information assigned to that address. Only authorized people can retrieve and access the information. For example, only those doctors and nurses can access the information who are assigned to the patients during their tenure in the hospital. After discharge from the hospitals, none of them will have any access to the information.

Figure 4: Smart contract access control.

Nurses and doctors who are not assigned to a particular patient will not be able to access the information.

We have also provided the responsibility of assigning roles to the receptionist role only. Only he can create the file and provide access to the patient's information to the respective nurse and doctor but cannot access it by himself/herself.

Admin of the hospitals are given the right to designate users at the roles of receptionist, nurses, or doctors based on their public key.

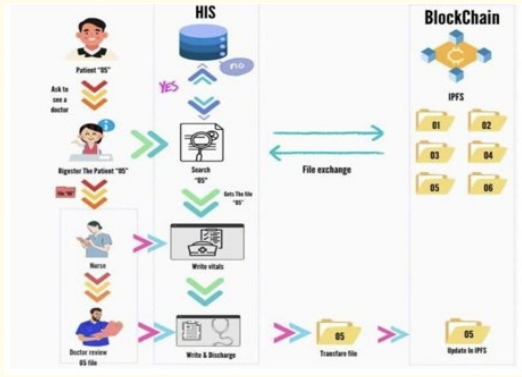

Figure 5: Blockchain structure of the proposed approach.

When entries are modified, new JSON files are created for storing new records and uploaded based on IPFS. The file hash is updated and remains on the blockchain with the new hash value; prior values are, therefore, not changed.

Ransomware Resilience

By uploading the information onto IPFS pinata, the files are not saved onto our own servers. Rather these files are saved on decentralized file servers in the form of IPFS. The project is saving the patient's data into the IPFS servers which are not subject to ransomware attacks. Similarly, the blockchain in which the IPFS hashes are stored also not susceptible to ransomware attack. The only thing which is susceptible to ransomware attack is the front end which is currently on ReactJS. We have placed this repository in our github cloud and in case of ransomware attack we can easily change our branch setting to pre hacking through which the front end setting will again connect to IPFS and blockchain where actual data resides.

Implementation

Our proposed framework required us to create and run a blockchain system for medical record management. We tested our blockchain system using Binance Smart Chain's test environment and protected patient data in IPFS storage outside the chain.

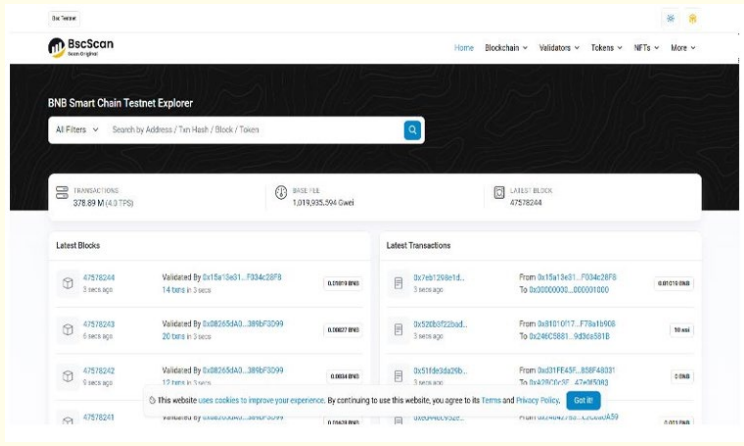

Figure 6: Block Explorer of BSC tesnet as blockchain.

Implementation Detail
Technology Stack

- ***Blockchain Network:*** Binance Smart Chain Testnet for deploying and testing smart contracts.
- ***Smart Contracts:*** Managed patient record hashes (CIDs) using Solidity.
- ***Frontend & Backend Tools:*** ViteJS for UI and MetaMask for secure wallet integration.
- ***Decentralized Storage:*** Patient records stored as JSON files in IPFS. These hashes are generated by first translating the patient's information into JSON format and then uploading the same on Pinata IFPS cloud. Upon uploading, IPFS Pinata cloud provides us a hash which is then saved onto blockchain.
- ***Development Environment:*** Remix-IDE for writing, testing, and deploying Solidity smart contracts efficiently.
- ***Security & Authentication:*** MetaMask ensures only authorized users can sign transactions and access patient records.
- ***Data Integrity & Updates:*** Each record update generates a new IPFS hash, maintaining a verifiable and immutable history on the blockchain.

Function	*Traditional Centralized Systems*	*Proposed Blockchain-Based System (This Paper)*
Data Storage	Centralized database vulnerable to ransomware attacks	Decentralized storage using IPFS, enhancing security and resilience
Data Integrity	Prone to data tampering and single-point failures	Blockchain ensures immutability and verifiability
Data Access	Limited to centralized server access	Distributed access through IPFS and blockchain nodes
Data Backup	Requires external or periodic manual backups	Data redundancy inherent in decentralized architecture
Resilience	High risk of downtime during ransomwa re-attacks	Continuous data availability due to distributed storage

Table 1: Comparison with traditional centralized systems.

When doctors and hospitals use blockchain and IPFS together, their data stays secure, accessible, and real, helping them create stronger defenses against ransomware attacks.

Conclusions and Discussion

Ransomware attacks severely impact healthcare systems by encrypting patient data, demanding ransom payments, and disrupting medical services. This paper proposes a blockchain-based framework integrated with IPFS and Pinata Cloud to mitigate ransomware risks by decentralizing patient data storage. By eliminating reliance on centralized databases, our approach ensures data integrity, availability, and resistance to encryption-based attacks.

The proposed system achieves ransomware resilience by storing patient records securely in IPFS while recording only cryptographic hashes on the blockchain. This prevents direct access or modification of sensitive data by attackers. Smart contracts enforce strict access controls, allowing only authorized medical personnel to retrieve and update records, reducing the risk of unauthorized tampering. Additionally, the decentralized nature of IPFS ensures that patient records remain accessible even if one node is compromised, minimizing downtime and ensuring continuity of care.

This paper demonstrates a secure, tamper-resistant framework that protects healthcare data from ransomware threats. Future enhancements may include AI-driven anomaly detection and zero- knowledge proof cryptographic techniques to further strengthen the system against evolving cyber threats.

References

1. Neprash HT., et al. “Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021”. JAMA Health Forum 3.12 (2022): e224873.
2. Leventhal. “Report: Ransomware attacks cost healthcare organizations $21B in 2020”. Healthcare Innovation, (2021). https://www.hcinnovationgroup.com/cybersecurity/data-breaches/news/21214314/report-ransomware-attacks-cost-healthcare-organizations-21b-in-2020
3. AHA News. “Study documents regional impact of hospital ransomware attacks”. American Hospital Association (2023). https://www.aha.org/news/headline/2023-05-19-study-documents-regional-impact-hospital- ransomware-attacks
4. B Siegel. “Free ransomware help for Coronavirus healthcare organizations”. Coveware: Ransomware Recovery First Responders (2020). https://www.coveware.com/blog/free-ransomware-assistance-to-healthcare-coronavirus
5. CC McGlave., et al. “Characteristics of short-term acute care hospitals that experienced a ransomware attack from 2016 to 2021”. Health Affairs Scholar 1.3 (2023).

6. AK Noon., et al. "Implementation of blockchain in healthcare: A systematic review". Proc. 2021 Int. Conf. Innovative Computing (ICIC) (2021): 1-10.
7. P Esmaeilzadeh. "Benefits and concerns associated with blockchain-based Health Information Exchange (HIE): A qualitative study from physicians' perspectives". BMC Med. Informatics Decis. Making 22.1 (2022).
8. P Zhang., et al. "FHIRCHAIN: Applying blockchain to securely and scalably share clinical data". Comput. Struct. Biotechnol. J 16 (2018): 267-278.
9. J Benet. "IPFS - content addressed, versioned, P2P file system". arXiv preprint (2014).
10. D Trautwein., et al. "Design and evaluation of IPFS: A storage layer for the decentralized web". arXiv preprint (2022).
11. M Bin Saif, S Migliorini and F Spoto. "Efficient and secure distributed data storage and retrieval using Interplanetary File System and Blockchain". Future Internet 16.3 (2024): 98.
12. TV Doan., et al. "Toward decentralized cloud storage with IPFS: Opportunities, challenges, and future considerations". IEEE Internet Comput 26.6 (2022): 7-15.
13. J Jayabalan and N Jeyanthi. "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy". J. Parallel Distrib. Comput 164 (2022): 152-167.
14. H Taherdoost. "Privacy and security of Blockchain in healthcare: Applications, challenges, and future perspectives". Sci 5.4 (2023): 41.
15. Lakhan A., et al. "RBEF: Ransomware Efficient Public Blockchain Framework for Digital Healthcare Application". Sensors 23.11 (2023) 5256.
16. Azbeg K, Ouchetto O and Andaloussi SJ. "BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security". Egyptian informatics journal 23.2 (2022) 329-343
17. Mittal S and Ghosh M. "A three-phase framework for secure storage and sharing of healthcare data based on blockchain, IPFS, proxy re-encryption and group communication". The Journal of Supercomputing 80 (2024) 7955- 7992. [Online].
18. Binance Academy. Proof of Staked Authority (PoSA). [Online]. https://academy.binance.com/en/glossary/proof-of-staked-authority-posa
19. J Benet. "IPFS - Content Addressed, Versioned, P2P File System". arXiv preprint arXiv:1407.3561 (2014). [Online]. https://arxiv.org/abs/1407.3561