



**Decentralized File Storage using Blockchain: Implementation and**

**Proof-of-Work Analysis**

Yogesh P 22BPS1044, Vishwa D 22BPS1222, Dinesh Kumar M 22BRS1369

Vellore Institute of Technology Chennai.

**ABSTRACT** Medical diagnostics such as medical tests, x-rays etc. are stored in two ways- Physical records and Online records, which cannot be accessed by patients without authorized permission. Even doctors/medical professionals do not get this data during crucial times. This could be avoided by sharing medical data of patients to the doctors and patient directly. Present storage method is also at a security threat of being tampered and accessed by unauthorized. This paper proposes blockchain network to address the issues related to medical records system which is easily accessed by the patient or doctor to take better and effective decisions ensuring immutability. Doctors view/update past visits for a medical record, if given the permission to by the respective patients. We developed a web-based application for decentralized file storing using blockchain. In this application any user can upload as many files (one at a time) as he/she likes. All other peers and the user himself can download and access those files in their system. File can be of any type and any size. Refer to project demo link to see the detailed explanation. We are using randomly generated nonce in proof of work concept to achieve the required difficulty. Once peer uploads the file, the file is stored in a block including username, file size and file data. These block gets appended to the current blockchain, which makes it impossible to edit or delete the file/block. The reason to implement file storing using blockchain is its ability to avoid any modification or deletion. No one can delete or corrupt our files that are stored.

**KEY TERMS** Blockchain, Medical Records, SHA256, Proof of work.

1. **INTRODUCTION**

Blockchain technology serves as an expansive labeling framework for distributed electronic databases, authenticated through cryptography. This framework excels in demonstrating the time, integrity, and identity of both individuals and machines, independent of traditional systems. Unlike conventional databases reliant on a centralized validation framework, blockchain technology diverges by offering a decentralized and more flexible approach.

Traditional databases face challenges in accommodating multiple users simultaneously due to fixed capacity and a restricted number of credentials provided by centralized authentication. In contrast, blockchain operates as a distributed ledger, encrypting individual transactions into unalterable blocks through applicable encryption methods. These encrypted blocks become permanent additions to the ledger, creating an immutable record.

One key distinction lies in the verification process within blockchain. Instead of a centralized authority, the information is fundamentally authenticated by a linked list of encoded transactions utilizing a hash. The hash function plays a crucial role by encrypting the data fed into the blockchain, generating a unique hash that verifies the integrity of the information. This decentralized and cryptographic foundation sets blockchain apart from traditional databases, offering enhanced security, flexibility, and accessibility for users.

The field of World Health Care/Medical Science has witnessed significant progress, particularly with the transition from the paper/physical era to the digital age. Notably, platforms like Practo have contributed to the gradual migration of medical history storage to digital platforms. This shift is driven by the challenges associated with searching for individual records, often relying on Unique IDs and conventional record storage methods.

Digital platforms for medical history storage have gained widespread popularity due to their efficacy in managing comprehensive medical information, including x-rays, prescriptions, lab results, and more for individuals. While these platforms address the issue of cumbersome storage, they encounter challenges related to data protection against tampering and unauthorized access. Furthermore, a notable limitation is the lack of patient-centricity, meaning users are unable to share their medical history with others.

The necessity for safeguarding against tampering is particularly crucial in consulting and insurance fields, where the accuracy and authenticity of every record hold significant importance. Any instance of false information or tampered data poses a potential risk to clients and underscores the need for a solution that not only efficiently stores medical information but also ensures robust data protection and user-centric functionalities.

One notable feature of this blockchain is its focus on file information. Users can upload and download various file types from a publicly available website, transforming the blockchain into a decentralized and secure file storage system. To ensure the security of the blocks, the implementation utilizes the SHA256 cryptographic algorithm. This algorithm generates a fixed-size hash value unique to the input data, providing a robust level of security.

The consensus algorithm employed in this implementation is proof of work. Miners are required to solve a cryptographic puzzle, finding a hash value that starts with three 0's, before they can announce a new block on the chain. This proof-of-work approach adds a layer of security, preventing malicious actors from easily altering the blockchain.

1. **LITERATURE SURVEY**

* This paper explores a landscape of research related to decentralized healthcare record management and blockchain technology in medical data systems. It navigates studies discussing the advantages and challenges of decentralized systems in healthcare data management, emphasizing patient-centric approaches, access control, and interoperability. Additionally, it surveys the application of blockchain technology in ensuring data integrity, privacy, and transparency within medical record management. The survey extends beyond blockchain to encompass decentralized models for medical data, exploring peer-to-peer networks and distributed databases. Security and privacy considerations are highlighted across various studies, encompassing encryption methods, access control mechanisms, and privacy-preserving techniques within healthcare record management. Furthermore, it delves into comparative analyses between centralized and decentralized systems, evaluating performance, scalability, and security aspects. Lastly, it covers recent studies addressing adoption rates, challenges, regulatory compliance, interoperability issues, and technological barriers in implementing decentralized healthcare systems.[1]
* This literature survey navigates through diverse research domains pertinent to the integration of blockchain technology in healthcare information management, as highlighted in the paper by Martínez, Molina, and Subauste. It delves into the evolving landscape of blockchain applications within healthcare, focusing on its role in ensuring data security, integrity, and transparency in managing electronic medical records (EMRs). The survey explores existing studies elucidating the challenges and benefits associated with EMRs in healthcare organizations, addressing issues of interoperability, accessibility, and data security inherent in technology architectures tailored for healthcare information management. Furthermore, it investigates the feasibility and implications of integrating blockchain technology into EMR systems, aiming to understand the potential advantages and challenges presented by blockchain-based solutions compared to traditional EMR systems. Comparative analyses between these systems are considered, evaluating factors like data security, scalability, and efficiency to discern the transformative potential of blockchain in revolutionizing medical record management. Additionally, the survey extends to recent publications discussing emerging trends and future challenges in EMR management and blockchain adoption within healthcare, offering a comprehensive view of the research landscape surrounding the utilization of blockchain technology in healthcare organizations for electronic medical records management.[2]

Castellani et al., have proposed an

* architecture for a smart ofﬁce application [11]. Their main
* focus is only to interconnect wireless sensor networks and
* actuator networks to the Internet as a web service. Similarly,
* the EPC global IoT architecture has mainly focused on the
* RFID network and smart logistics system [12]. There is no
* suitable uniﬁed architecture till date that is appropriate for a
* global IoT infrastructure. The existing architectural proposals
* are deﬁned for a particular type of application. From a security
* perspective, these proposals list requirements for each type of
* application (e.g. identiﬁcation and usage control), but do not
* propose or adopt speciﬁc security frameworks
* Castellani et al., have proposed an
* architecture for a smart ofﬁce application [11]. Their main
* focus is only to interconnect wireless sensor networks and
* actuator networks to the Internet as a web service. Similarly,
* the EPC global IoT architecture has mainly focused on the
* RFID network and smart logistics system [12]. There is no
* suitable uniﬁed architecture till date that is appropriate for a
* global IoT infrastructure. The existing architectural proposals
* are deﬁned for a particular type of application. From a security
* perspective, these proposals list requirements for each type of
* application (e.g. identiﬁcation and usage control), but do not
* propose or adopt speciﬁc security frameworks
* This literature survey investigates the realms of electronic medical record (EMR) data sharing, encryption methodologies, and blockchain integration as presented in Zhang, Lin, and Zhao's research on SV-DEMR. Focused on enhancing the secure sharing of medical data, the paper centers on a scheme utilizing searchable and verifiable encryption within a consortium blockchain framework. The survey traverses through studies highlighting the challenges and pivotal role of secure data sharing in healthcare, emphasizing the need for robust encryption methodologies to safeguard sensitive patient information. It explores research elucidating various encryption techniques applicable to EMR systems, discussing their effectiveness in ensuring data confidentiality while enabling authorized searchability and verifiability. Additionally, the survey delves into the integration of blockchain technology, specifically consortium-based architectures, in facilitating transparent, tamper-proof, and decentralized data sharing mechanisms for EMRs. It aims to comprehend the practical implications and benefits of employing such a scheme, analyzing its potential in enhancing data integrity, accessibility, and privacy in healthcare settings. Moreover, it identifies emerging trends and future challenges in the fusion of encryption techniques and blockchain technology for secure EMR data sharing, contributing to the evolving landscape of innovative solutions aimed at fortifying medical data management and sharing practices.[3]
* This literature survey delves into the domain of secured digital health record management systems, centering on the paper by Nautiyal, Agarwal, and Sharma on Rechain. The paper emphasizes the integration of blockchain technology to fortify the security aspects of managing digital medical health records. It navigates through existing research discussing the challenges inherent in medical record security, emphasizing the criticality of robust systems for safeguarding sensitive patient information. The survey explores the application of blockchain technology within healthcare, elucidating its role in ensuring data integrity, immutability, and transparency in managing digital health records. Additionally, it investigates innovative systems like Rechain, aiming to understand their architecture, functionality, and impact on enhancing the security and accessibility of medical data. The survey further extends to discuss potential implications, advantages, and challenges associated with implementing blockchain-based systems like Rechain in healthcare settings. Furthermore, it identifies emerging trends and future prospects in the realm of secured digital health record management systems, contributing insights to the evolving landscape of technology-driven solutions aimed at fortifying the confidentiality and integrity of medical data.[4]
* This literature survey navigates through pertinent research domains associated with blockchain technology in healthcare, specifically focusing on the paper by V. B, S. N. Dass, S. R, and R. Chinnaiyan on a blockchain-based EMHR framework utilizing smart contracts. It examines existing studies elucidating the integration of blockchain in healthcare, emphasizing its role in ensuring secure, immutable, and transparent management of electronic medical records. The survey explores the concept and application of smart contracts within blockchain frameworks, highlighting their ability to automate and enforce agreements in EMHR systems. Additionally, it investigates the proposed framework's architecture, functionalities, and implications in enhancing the security, accessibility, and integrity of medical data. The survey aims to comprehend the potential advantages and challenges associated with utilizing smart contracts in EMHR frameworks powered by blockchain technology. Moreover, it identifies emerging trends, innovations, and future challenges in the domain of blockchain-based EMHR frameworks, contributing insights to the evolving landscape of technology-driven solutions aimed at revolutionizing medical data management and security.[5]
* This literature survey delves into the domain of secure medical record systems within the context of blockchain technology, particularly focusing on the Recchain Framework proposed by Widhawati, Royani, Khoirunisa, Santoso, and Apriliasari. The survey navigates through existing research elucidating the challenges and crucial aspects of securing medical records, emphasizing the imperative nature of robust systems for safeguarding sensitive patient information. It explores the integration of blockchain technology in healthcare, emphasizing its role in ensuring data integrity, immutability, and transparency in managing medical records. Furthermore, it investigates the Recchain Framework, analyzing its architecture, features, and implications in enhancing the security, accessibility, and integrity of medical data. The survey aims to comprehend the potential advantages and challenges associated with implementing the Recchain Framework, specifically designed to fortify medical record systems through blockchain integration. Additionally, it identifies emerging trends, future prospects, and potential advancements in secure medical record systems leveraging blockchain technology, contributing insights to the evolving landscape of technology-driven solutions aimed at fortifying the confidentiality and integrity of medical data.[6]
* This literature survey delves into the domain of blockchain-based medical record management systems, focusing on performance analysis as presented by Koushik, Jain, Menon, Lohia, Chaudhari, and B.P. The survey navigates through existing research elucidating the challenges and necessities of efficient medical record management within healthcare, emphasizing the need for systems that ensure data integrity, security, and scalability. It explores the integration of blockchain technology in healthcare, highlighting its role in enhancing transparency, immutability, and accessibility in managing medical records. Additionally, it investigates the performance analysis methodology employed in evaluating the blockchain-based medical records management system, analyzing factors such as transaction speed, scalability, and resource utilization. The survey aims to comprehend the findings, insights, and implications derived from the performance analysis, identifying strengths, weaknesses, and potential improvements in blockchain-based systems for medical record management. Furthermore, it identifies emerging trends and future directions in the realm of performance evaluation of blockchain-based medical record systems, contributing insights to the evolving landscape of technology-driven solutions aimed at optimizing medical data management within healthcare environments.[7]
* This literature survey traverses the landscape of blockchain technology's implementation, particularly focusing on the integration of hash methods in Java for medical record application development, as presented by Jaya, Nugraha, Davinsi, Moniaga, and Jabar. It navigates through existing research highlighting the significance of blockchain in healthcare, emphasizing its potential to ensure data security, immutability, and accessibility in managing medical records. The survey delves into the utilization of hash methods in Java for implementing blockchain technology, discussing their role in ensuring data integrity and cryptographic security within medical record systems. Additionally, it investigates the practical implementation and development aspects of utilizing Java-based hash methods for medical record applications powered by blockchain technology. The survey aims to comprehend the methodology, advantages, and challenges associated with implementing these technologies, identifying their potential impact on enhancing the security, efficiency, and reliability of medical record management systems. Moreover, it identifies emerging trends and future prospects in the realm of blockchain-based medical record applications using hash methods in Java, contributing insights to the evolving landscape of technology-driven solutions aimed at fortifying the confidentiality and integrity of medical data.[8]
* This literature survey delves into the domain of blockchain-based record management systems within hospital settings, focusing on the paper by Vernekar, Sakhare, Bhapkar, Jadhav, and Adhao. It explores existing research that underscores the challenges and essentiality of robust record management in healthcare, emphasizing the necessity for systems ensuring data integrity, security, and accessibility within hospitals. The survey navigates through the application of blockchain technology in healthcare, particularly in ensuring secure and transparent management of hospital records. Additionally, it investigates the proposed blockchain-based record management system, aiming to comprehend its architecture, functionalities, and implications in enhancing the security, accessibility, and efficiency of hospital record management. The survey seeks to understand the potential advantages and challenges associated with implementing blockchain technology in hospital record management systems, contributing insights to the evolving landscape of technology-driven solutions aimed at fortifying the confidentiality and integrity of medical data within hospital environments. Furthermore, it identifies emerging trends and future directions in the realm of blockchain-based record management systems in hospitals, providing valuable perspectives for improving record-keeping practices in healthcare settings.[9]

**III. PROPOSED SYSTEM**

In The proposed system, we have used SHA256 cryptographic algorithm to secure the block. As a consensus algorithm, proof of work is implemented, which requires miners to solve any cryptographic puzzle before they get to announce new block on chain. In our application, we require to find a hash value that starts with three 0's as part of a puzzle.

SHA-256 (Secure Hash Algorithm 256) is a widely used cryptographic algorithm that produces a fixed-length, 256-bit (32-byte) hash value. The purpose of the SHA-256 algorithm is to create a unique digital fingerprint of a piece of data, such as a message or a file.

The key features of the SHA-256 algorithm are message length, digest length, and irreversibility.

Message Length: The length of the plaintext (the readable text before it is encrypted) should be less than 264 bits.

Digest Length: The hash digest (the result of applying a cryptographic hash function to data) length should be 256 bits. When installing an SSL certificate on your server, you may select SHA-512 and bigger digests. While SHA-512 is more secure, it’s not recommended for most systems, as it requires more calculations and computer power.

Irreversibility: All hash functions such as the SHA-256 are irreversible by design. For each input, you have exactly one output, but not the other way around. Multiple inputs produce the same output. The output has a fixed size, but the input doesn’t have size restrictions.

1. **SHA256 CRYPTOGRAPHIC ALGORITHM:**
2. Data Preprocessing: To ensure a length that is a multiple of 512 bits, the input data undergoes padding and extension. This involves adding a one-bit followed by zeros and appending the original message's length in bits.
3. Message Expansion: The 512-bit input block is initially divided into 16 32-bit words. Through a series of logical operations, this block is then expanded into 64 32-bit words.
4. Message Compression: The expanded 64-word message block undergoes processing through 64 rounds, each comprising several steps:
5. Round Constant Determination: Each round entails generating a unique 32-bit constant value based on its position in the sequence.
6. Message Schedule Calculation: A 64-entry message schedule is generated from the 64-word message block and the round constant.
7. Working Variables Update: The working variables, comprising 8 32-bit words storing intermediate values in the hashing process, are updated based on the message schedule and a set of logical operations.
8. Hash Value Calculation: Upon completion of all 64 rounds, the final values of the working variables are combined to produce the 256-bit hash value.
9. The output of the SHA-256 hash algorithm is a 256-bit final hash value, serving as a digital fingerprint for the input data.

In summary, this blockchain implementation not only serves as a secure repository for digital information but also allows users to interact with the system through a publicly available website, utilizing proof of work as a consensus algorithm and the SHA256 cryptographic algorithm to ensure the integrity and confidentiality of the stored data.

1. **Proof-of-Work ALGORITHM:**

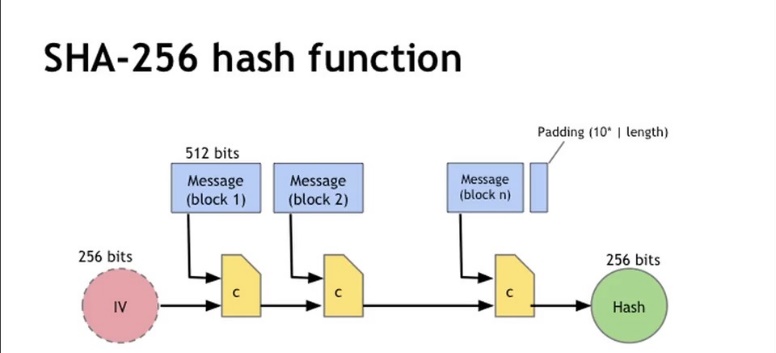
Blockchain-based applications commonly operate as peer-to-peer networks, emphasizing a high degree of decentralization. In order to bolster this decentralization, all network peers should possess the capability to introduce new blocks. Proof of work algorithms emulate the concept of each peer having the ability to add a new block, aiming to solve cryptographic puzzles. Peers that solve these puzzles more swiftly gain the privilege to append a new block to the blockchain.

Our blockchain implementation incorporates two distinct proof of work algorithms, both striving to solve the same cryptographic puzzle but employing different approaches. According to these algorithms, the peer who discovers a hash value for their block containing a specified number of leading zeros is eligible to announce it to the chain. For instance, our blockchain mandates that miners can only add a block if the hash value starts with three zeros, denoting a difficulty level of 3. The term "miner" refers to peers actively seeking to add blocks to the blockchain.

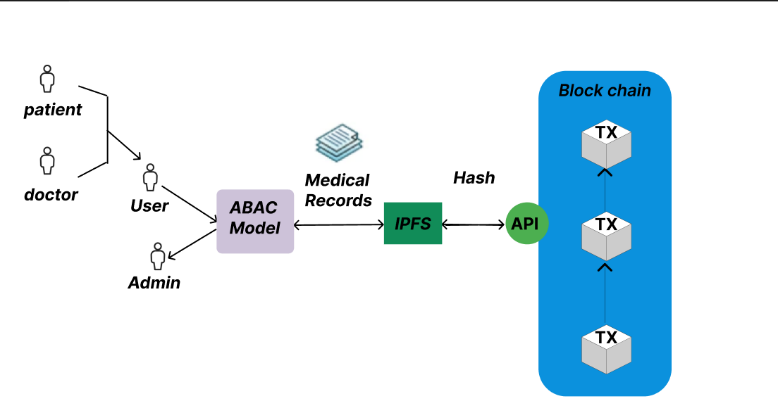
Drawing from this concept, we have instituted two algorithms, each employing a distinct approach to calculate the nonce. One algorithm generates the nonce randomly in each iteration, while the other increments the nonce by one in each iteration. The runtime and behaviour of both algorithms have been scrutinized and documented in the file named "POW\_Comparison.py." Based on the file's output, we have derived conclusive results for both methods.

**IV. SYSTEM ARCHITECTURE**

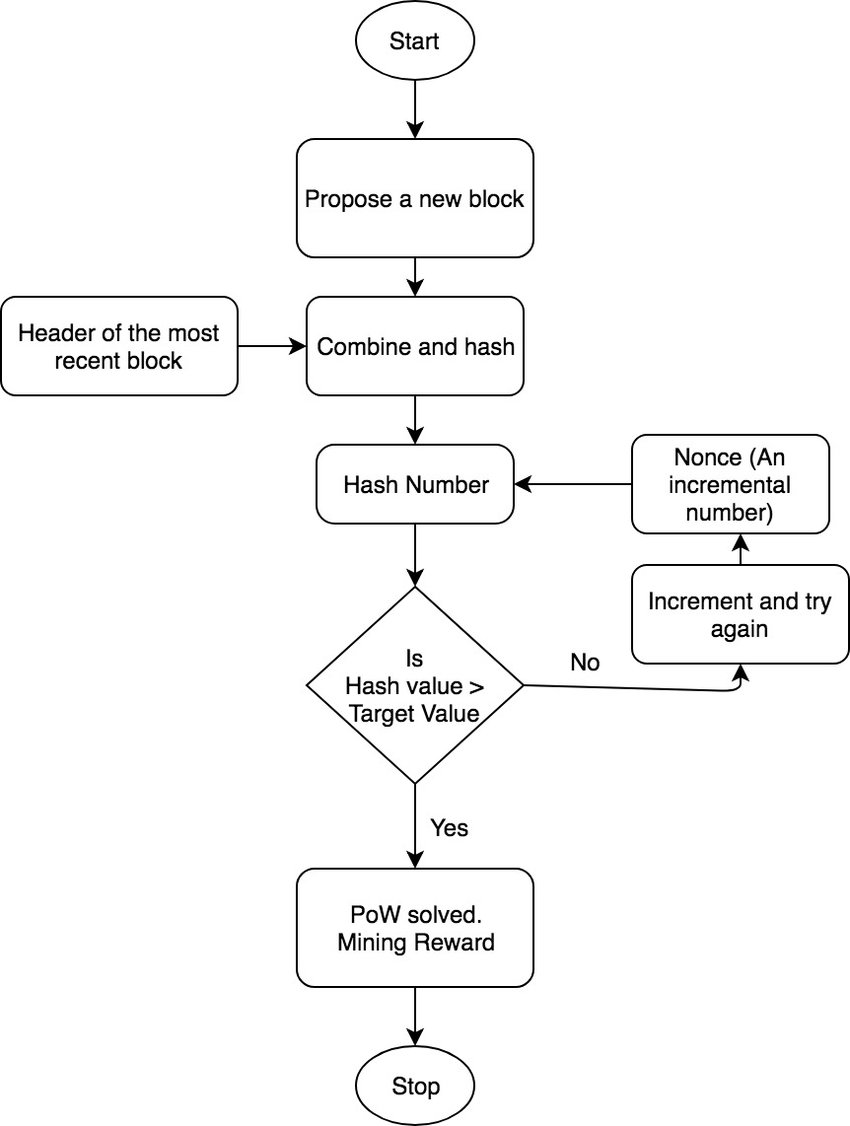
**figure 1: SHA-256**



**figure 2: Architecture diagram**

****

**figure 3: Proof-of-Work**

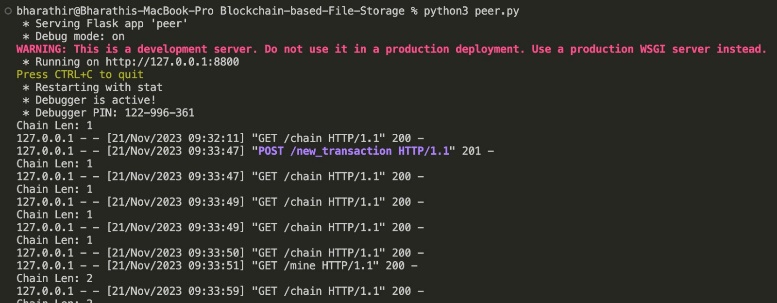


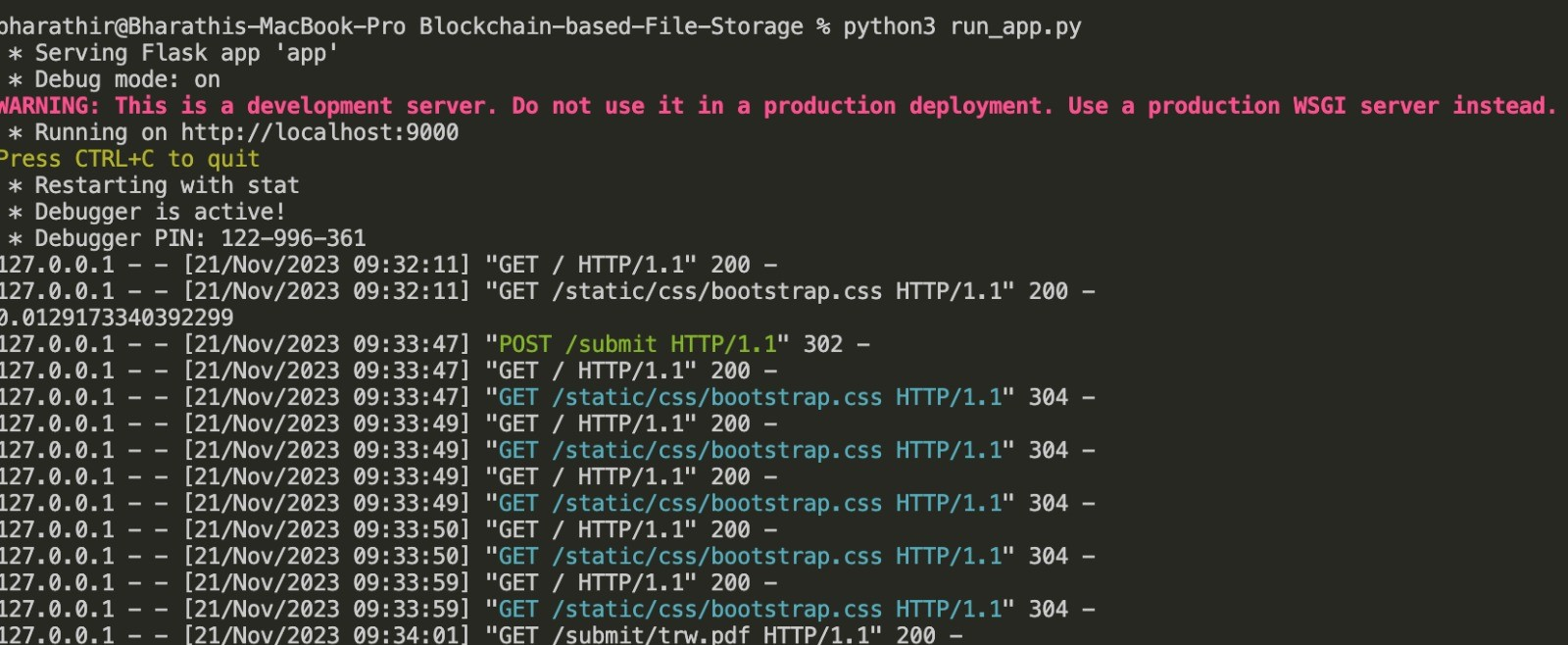
**V. PROBLEMS DEFINED**

The problem addressed in this project centres on the creation of a web-based application designed for decentralized file storage using blockchain technology. The application allows users to upload files of any type and size, one at a time. All users, including the uploader and other peers in the network, can download and access these files. To ensure security and immutability, the system employs a blockchain structure. When a user uploads a file, its details, including username, filesize, and file data, are stored in a block. These blocks are then appended to the existing blockchain, making it virtually impossible to edit or delete the files or blocks. The implementation incorporates a proof of work concept with randomly generated nonces to achieve a specified difficulty level, enhancing the security of the file storage process. The underlying motivation for using blockchain is to leverage its ability to safeguard files against unauthorized modification or deletion. For a detailed explanation and demonstration, the project provides a demo link for users to explore further.

**VI. RESULTS**

To run the application:

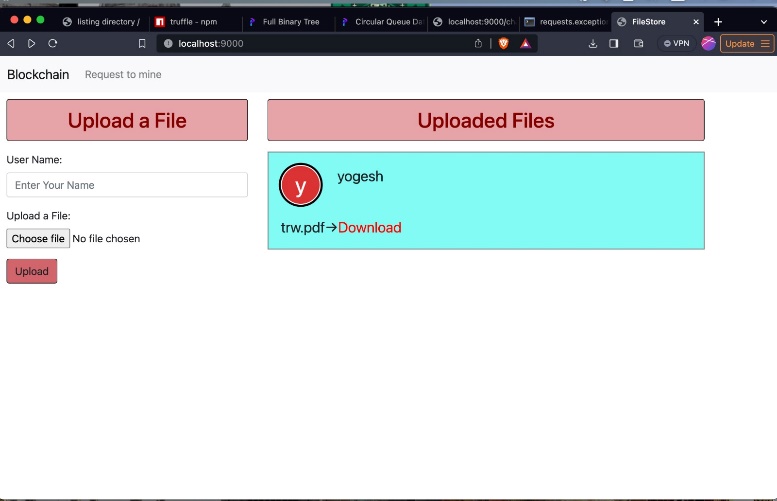
1. Open one terminal and start server/peer: python peer.py
2. Open another terminal and start a client: python run\_app.py



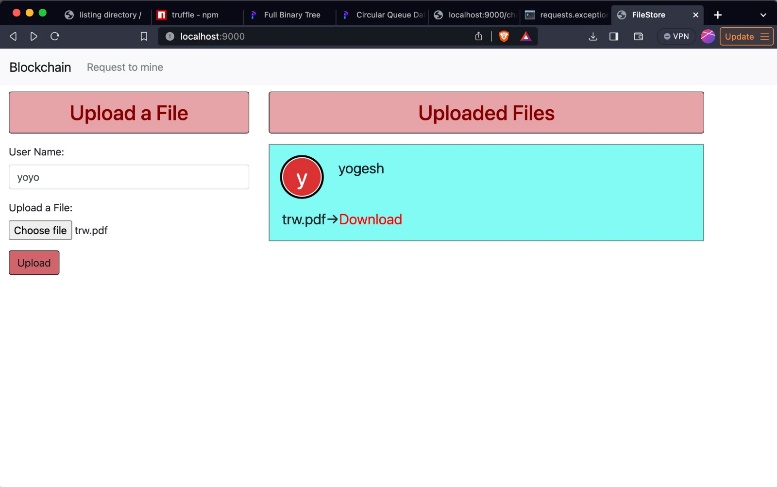
1. Copy the link from the client terminal and paste it in any browser.

After opening the link:

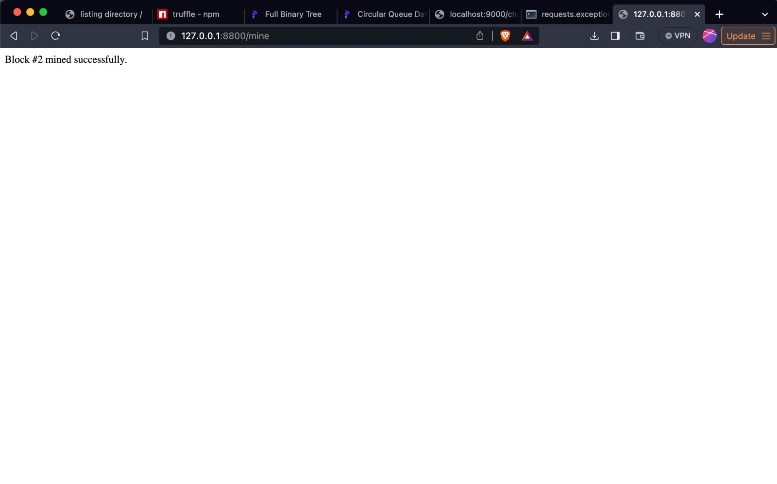
**Initial page**



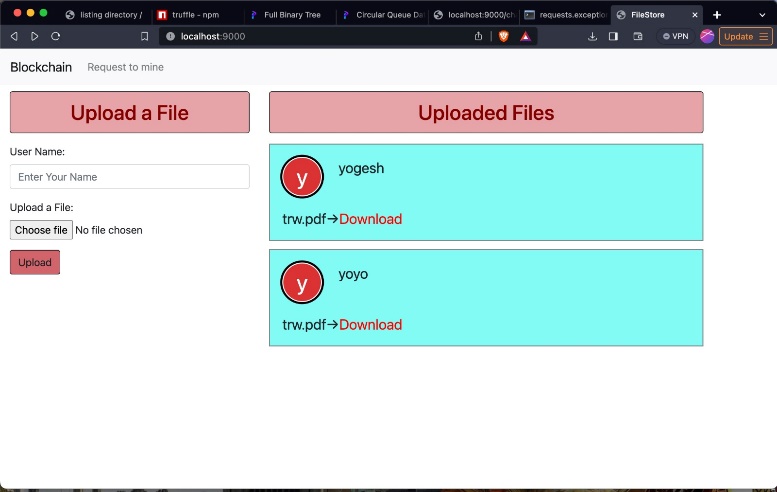
**Uploading file**

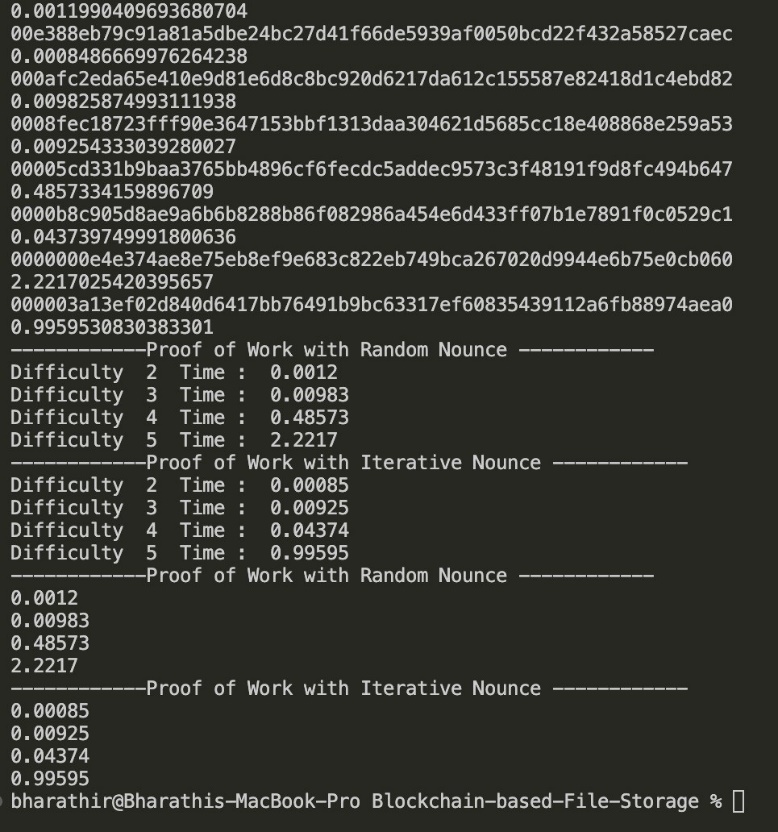


**Acknowledgement for uploading**



**File uploaded and is ready to download**



To run our experiment of different Proof of Work concepts: python POW\_Comparison.py

* focus is only to interconnect wireless sensor networks and
* actuator networks to the Internet as a web service. Similarly,
* the EPC global IoT architecture has mainly focused on the
* RFID network and smart logistics system [12]. There is no
* suitable uniﬁed architecture till date that is appropriate for a
* global IoT infrastructure. The existing architectural proposals
* are deﬁned for a particular type of application. From a security
* perspective, these proposals list requirements for each type of
* application (e.g. identiﬁcation and usage control), but do not
* propose or adopt speciﬁc security frameworks
* Castellani et al., have proposed an
* architecture for a smart ofﬁce application [11]. Their main
* focus is only to interconnect wireless sensor networks and
* actuator networks to the Internet as a web service. Similarly,
* the EPC global IoT architecture has mainly focused on the
* RFID network and smart logistics system [12]. There is no
* suitable uniﬁed architecture till date that is appropriate for a
* global IoT infrastructure. The existing architectural proposals
* are deﬁned for a particular type of application. From a security
* perspective, these proposals list requirements for each type of
* application (e.g. identiﬁcation and usage control), but do not
* propose or adopt speciﬁc security frameworks
* Castellani et al., have proposed an
* architecture for a smart ofﬁce application [11]. Their main
* focus is only to interconnect wireless sensor networks and
* actuator networks to the Internet as a web service. Similarly,
* the EPC global IoT architecture has mainly focused on the
* RFID network and smart logistics system [12]. There is no
* suitable uniﬁed architecture till date that is appropriate for a
* global IoT infrastructure. The existing architectural proposals
* are deﬁned for a particular type of application. From a security
* perspective, these proposals list requirements for each type of
* application (e.g. identiﬁcation and usage control), but do not
* propose or adopt speciﬁc security frameworks
* Castellani et al., have proposed an
* architecture for a smart ofﬁce application [11]. Their main
* focus is only to interconnect wireless sensor networks and
* actuator networks to the Internet as a web service. Similarly,
* the EPC global IoT architecture has mainly focused on the
* RFID network and smart logistics system [12]. There is no
* suitable uniﬁed architecture till date that is appropriate for a
* global IoT infrastructure. The existing architectural proposals
* are deﬁned for a particular type of application. From a security
* perspective, these proposals list requirements for each type of
* application (e.g. identiﬁcation and usage control), but do not
* propose or adopt speciﬁc security frameworks
* Castellani et al., have proposed an
* architecture for a smart ofﬁce application [11]. Their main
* focus is only to interconnect wireless sensor networks and
* actuator networks to the Internet as a web service. Similarly,
* the EPC global IoT architecture has mainly focused on the
* RFID network and smart logistics system [12]. There is no
* suitable uniﬁed architecture till date that is appropriate for a
* global IoT infrastructure. The existing architectural proposals
* are deﬁned for a particular type of application. From a security
* perspective, these proposals list requirements for each type of
* application (e.g. identiﬁcation and usage control), but do not
* propose or adopt speciﬁc security frameworks
* Castellani et al., have proposed an
* architecture for a smart ofﬁce application [11]. Their main
* focus is only to interconnect wireless sensor networks and
* actuator networks to the Internet as a web service. Similarly,
* the EPC global IoT architecture has mainly focused on the
* RFID network and smart logistics system [12]. There is no
* suitable uniﬁed architecture till date that is appropriate for a
* global IoT infrastructure. The existing architectural proposals
* are deﬁned for a particular type of application. From a security
* perspective, these proposals list requirements for each type of
* application (e.g. identiﬁcation and usage control), but do not
* propose or adopt speciﬁc security frameworks
* Castellani et al., have proposed an
* architecture for a smart ofﬁce application [11]. Their main
* focus is only to interconnect wireless sensor networks and
* actuator networks to the Internet as a web service. Similarly,
* the EPC global IoT architecture has mainly focused on the
* RFID network and smart logistics system [12]. There is no
* suitable uniﬁed architecture till date that is appropriate for a
* global IoT infrastructure. The existing architectural proposals
* are deﬁned for a particular type of application. From a security
* perspective, these proposals list requirements for each type of
* application (e.g. identiﬁcation and usage control), but do not
* propose or adopt speciﬁc security frameworks
* Castellani et al., have proposed an
* architecture for a smart ofﬁce application [11]. Their main
* focus is only to interconnect wireless sensor networks and
* actuator networks to the Internet as a web service. Similarly,
* the EPC global IoT architecture has mainly focused on the
* RFID network and smart logistics system [12]. There is no
* suitable uniﬁed architecture till date that is appropriate for a
* global IoT infrastructure. The existing architectural proposals
* are deﬁned for a particular type of application. From a security
* perspective, these proposals list requirements for each type of
* application (e.g. identiﬁcation and usage control), but do not
* propose or adopt speciﬁc secur i

**VII. C****ONCLUSION**

**Probability of Valid Output & Running Time:**

Analyzing the results from the POW\_Comparison.py file, it is evident that at lower difficulty levels, the running time exhibits minimal variation. However, as difficulty levels increase, the first algorithm, employing randomly generated nonces, demonstrates potential for faster performance. This can be attributed to the concurrent addition of transactions while the Proof of Work (POW) process is ongoing. In the second algorithm, where the nonce is incremented systematically, there is a lower probability of revisiting previously tested nonces, though the possibility remains. The introduction of new transactions during POW execution alters the hash generation equation, influencing the nonce value sought by the algorithm. This dynamic behavior may impact runtime, potentially resulting in scenarios where no solution is found or the probability of finding a solution decreases significantly.

For example, let's assume POW is in progress, and the nonce has reached 99978. The probability of finding a solution in the range of 0-99977 becomes negligible. However, if a new transaction is added, the equation changes, and while the earlier values won't be retested, the subsequent nonce values may have reduced probabilities of being a solution. Such circumstances can lead to extended running times or even failure to solve the puzzle.

In contrast, the first algorithm, employing random nonce selection, ensures that each nonce has an equal probability of being selected at any given time. This randomness increases the likelihood of the algorithm producing output in less time, especially at higher difficulty levels.

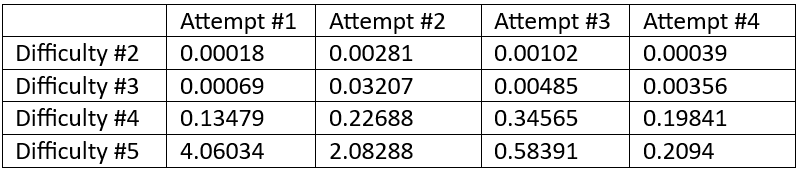


Table 1: Running time of first algorithm

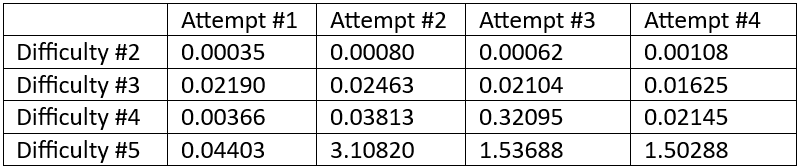


Table 2: Running time of second algorithm

**Security:**

Additionally, the second algorithm raises security concerns as the nonce value can be estimated based on the algorithm's running time. For instance, if the nonce value is assumed to be between 0 and 10000, a shorter running time implies a smaller nonce (0-1000), while a longer running time suggests a nonce closer to 10000. The significance of nonce security becomes apparent when considering that if someone gains information about one block and can deduce its nonce, they could compromise the entire blockchain system, given the interconnected nature of blocks through their hash values.

**VIII. REFERENCES**

1.B. Bhandari, P. R. Vairagade, H. Trivedi, H. Thakre, G. Indurkar and A. Yadav, "Decentralized Medical Healthcare Record Management System Using Blockchain," 2023 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP), Nagpur, India, 2023, pp. 1-5, doi: 10.1109/ICETET-SIP58143.2023.10151658.

2.A. Martínez, C. Molina and D. Subauste, "Electronic Medical Records Management in Health Organizations using a Technology Architecture based on Blockchain," 2020 IEEE ANDESCON, Quito, Ecuador, 2020, pp. 1-6, doi: 10.1109/ANDESCON50619.2020.927199

3.Y. Zhang, S. Lin and J. Zhao, "SV-DEMR: An Electronic Medical Record Data Sharing Scheme Based on Searchable and Verifiable Encryption via Consortium Blockchain," 2022 International Conference on Blockchain Technology and Information Security (ICBCTIS), Huaihua City, China, 2022, pp. 123-126, doi: 10.1109/ICBCTIS55569.2022.00038.

4.N. Nautiyal, P. Agarwal and S. Sharma, "Rechain: A Secured Blockchain-Based Digital Medical Health Record Management System," 2023 4th International Conference on Innovative Trends in Information Technology (ICITIIT), Kottayam, India, 2023, pp. 1-6, doi: 10.1109/ICITIIT57246.2023.10068707.

5.V. B, S. N. Dass, S. R and R. Chinnaiyan, "A Blockchain based Electronic Medical Health Records Framework using Smart Contracts," 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2021, pp. 1-4, doi: 10.1109/ICCCI50826.2021.9402689.

6.R. Widhawati, Royani, A. Khoirunisa, N. P. L. Santoso and D. Apriliasari, "Secure System Medical Record with Blockchain System: Recchain Framework," 2022 International Conference on Science and Technology (ICOSTECH), Batam City, Indonesia, 2022, pp. 1-8, doi: 10.1109/ICOSTECH54296.2022.9828811.

7.[A. S. Koushik, B. Jain, N. Menon, D. Lohia, S. Chaudhari and V. K. B.P, "Performance Analysis of BlockChain-based Medical Records Management System," 2019 4th International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), Bangalore, India, 2019, pp. 985-989, doi: 10.1109/RTEICT46194.2019.9016812.

8.T. Jaya, S. E. Nugraha, G. R. Davinsi, J. V. Moniaga and B. A. Jabar, "Implementation of Blockchain Technology Using Hash Method in Java for Medical Record Application Development," 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA), Yogyakarta, Indonesia, 2022, pp. 1-6, doi: 10.1109/ICITDA55840.2022.9971286.

9.A. Vernekar, A. Sakhare, P. Bhapkar, S. Jadhav and R. B. Adhao, "Blockchain Based Record Management System in Hospitals," 2023 4th International Conference on Innovative Trends in Information Technology (ICITIIT), Kottayam, India, 2023, pp. 1-4,

doi: 10.1109/ICITIIT57246.2023.10068685.

10.Y. Hu, J. Shen, S. He, G. Xu and H. Yang, "Research on Secure Data Sharing Technology of Block Chain," 2022 6th Asian Conference on Artificial Intelligence Technology (ACAIT), Changzhou, China, 2022, pp. 1-10, doi: 10.1109/ACAIT56212.2022.10137979.

11. S. Bhattacharyya and K. Chandrasekaran, "Towards a Secure Electronic Health Record System Using Blockchain Technology," 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2021, pp. 1-8, doi: 10.1109/ICCCNT51525.2021.9579571.

12. S. Ismail and H. Reza, "Security Challenges of Blockchain-Based Supply Chain Systems," 2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, NY, USA, 2022, pp. 1-6, doi: 10.1109/UEMCON54665.2022.9965682.

13. M. A. Hussen Wadud, A. Rahman, M. J. Islam, T. M. Amir-Ul-Haque Bhuiyan, M. J. Hossain and R. Hossen, "A Decentralized Secure Blockchain-based Privacy-Preserving Healthcare Clouds and Applications," 2023 International Conference on Electrical, Computer and Communication Engineering (ECCE), Chittagong, Bangladesh, 2023, pp. 1-6, doi: 10.1109/ECCE57851.2023.10101540.

14. C. Mulligan, J. Z. Scott, S. Warren, and J. Rangaswami, “Blockchain Beyond the Hype A Practical Framework for Business Leaders,” World Econ. Forum, no. April, pp. 1–7, 2018.

15. M. A. Fauzi, N. Paiman, and Z. Othman, “Bitcoin and cryptocurrency: Challenges, opportunities and future works,” J. Asian Financ. Econ. Bus., vol. 7, no. 8, pp. 695–704, 2020, doi: 10.13106/JAFEB.2020.VOL7.NO8.695.

16. D. B. Rawat, V. Chaudhary, and R. Doku, “Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems,” J. Cybersecurity Priv., vol. 1, no. 1, pp. 4–18, 2020, doi: 10.3390/jcp1010002.

17. A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, “Blockchain in healthcare and health sciences—A scoping review,” Int. J. Med. Inform., vol. 134, no. December 2019, p. 104040, 2020, doi: 10.1016/j.ijmedinf.2019.104040.

18. S. Zhai, Y. Yang, J. Li, C. Qiu, and J. Zhao, “Research on the Application of Cryptography on the Blockchain,” J. Phys. Conf. Ser., vol. 1168, no. 3, 2019, doi: 10.1088/1742-6596/1168/3/032077.

19. R. Johari, V. Kumar, K. Gupta, and D. P. Vidyarthi, “BLOSOM: BLOckchain technology for Security Of Medical records,” ICT Express, vol. 8, no. 1, pp. 56–60, 2022, doi: 10.1016/j.icte.2021.06.002.

20. O. Pal, B. Alam, V. Thakur, and S. Singh, “Key management for blockchain technology,” ICT Express, vol. 7, no. 1, 2021, doi: 10.1016/j.icte.2019.08.002.

21. A. A. Monrat, O. Schelén, and K. Andersson, “A survey of blockchain from the perspectives of applications, challenges, and opportunities,” IEEE Access, vol. 7, pp. 117134–117151, 2019.

22. O. Dzobo, B. Malila, and L. Sithole, “Proposed framework for blockchain technology in a decentralised energy network,” Prot. Control Mod. Power Syst., vol. 6, no. 1, 2021, doi: 10.1186/s41601-021-00209-8.

23. T. Rama Reddy, P. V. G. D. Prasad Reddy, R. Srinivas, C. V. Raghavendran, R. V. S. Lalitha, and B. Annapurna, “Proposing a reliable method of securing and verifying the credentials of graduates through blockchain,” Eurasip J. Inf. Secur., vol. 2021, no. 1, 2021, doi: 10.1186/s13635-021-00122-5.

24. I. Surjandari, H. Yusuf, E. Laoh, and R. Maulida, “Designing a Permissioned Blockchain Network for the Halal Industry using Hyperledger Fabric with multiple channels and the raft consensus mechanism,” J. Big Data, vol. 8, no. 1, 2021, doi: 10.1186/s40537-020-00405-7.

25. D. Shah, D. Patel, J. Adesara, P. Hingu, and M. Shah, “Integrating machine learning and blockchain to develop a system to veto the forgeries and provide efficient results in education sector,” Vis. Comput. Ind. Biomed. Art, vol. 4, no. 1, 2021, doi: 10.1186/s42492-021-00084-y.

26. J. Park, “Promises and challenges of Blockchain in education,” Smart Learn. Environ., vol. 8, no. 1, 2021, doi: 10.1186/s40561-021-00179- 2.

27. G. Chen, B. Xu, M. Lu, and N.-S. Chen, “Exploring blockchain technology and its potential applications for education,” Smart Learn. Environ., vol. 5, no. 1, pp. 1–10, 2018, doi: 10.1186/s40561-017-0050-x.

28. G. Wood, `Ethereum: A Secure Decentralised generalized transaction ledger. EIP-150 revision,'' Tech. Rep., IEEE Aug. 2017, p. 33.

29. S. Gupta and M. Sadoghi, ``Blockchain transaction processing,'' in Encyclopedia of Big Data Technologies. IEEE 2019, pp. 366\_376.

30. Xiaoming Liu; Yueping Hong; Jintao Sun, Blockchain-based Medical Data Storage and Sharing System,2022 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA)