**Secure Management of Patient Medical Records using Blockchain Technology**

.

ABSTRACT

|  |
| --- |
| Blockchain technology has transformed the way information is stored and secure. It provides a transparent and tamper-proof ledger system for transactions in optimized time frame hence serving as the foundation for cryptocurrencies such as bitcoin, but its applications have now extended to healthcare data privacy. The mining process is an essential part of blockchain technology, which ensures validity and immutability of data. The present paper deals with mining of blocks which are stored in a blockchain in a secure manner and related to records of store patients. The study implemented a simulation that allows users or medical professionals to mine the patient medical history in a secure form, preventing from unauthorized access or data breach. Users may have a better understanding of the fundamentals process by mining blocks. The study uses Python programming language and a popular API development tool like Postman, to mine the patient data on blockchain. Postman allows users to send transactions that are subsequently included to the next block for mining. The article not only gives a theoretical view of mining but also includes hands-on experience, making the concepts more practical and interesting for the users. |

*Keywords: Blockchain Technology, Data Mining,* HealthCare System, *Security, Transaction Processing*

1. INTRODUCTION

Blockchain technology has changed the digital environment through its decentralized nature and tamper-proof ledger system. It is based on the concept of distributed database used to maintain data integrity, consistency, and transparency over the network [1]. At its core, blockchain technology was initially developed for the digital cryptocurrency bitcoin. However, it is not limited to bitcoin but also used in various domains such as Internet of Things (IoT) security, banking sectors, healthcare, supply chain management, and many more due to its secure, transparent, and immutable nature [2].

Moreover, one of the crucial aspects of blockchain technology is the process of mining of blocks. Mining is the process of validating and adding the information to the blockchain ledger system. It is not only used for adding new blocks to the chain but also ensures the security of the entire system and verifies the legitimacy of transactions [3]. Mining of blocks is a multi-step process that needs the involvement of specialized nodes called miners. The participating miners execute complex mathematical computations to solve cryptographic puzzle. The miners who successfully solve the puzzle may be able to add a new block to the blockchain and get a reward as a cryptocurrency. The steps of mining of a block start by collecting unconfirmed transactions from the mem-pool, which is an interim repository for awaiting transactions. After collecting a transaction, the miners start the mining process by selecting a block header [4] which contains crucial details like the hash value of the block, the previous block address, a timestamp, and nonce.

Consequently, the miners integrate the block header with the chosen transactions and then employ a hashing technique, such as SHA-256, to create the block hash value. The main goal of miner is to find a hash value that meets a certain difficulty target defined by the blockchain network [5]. The difficulty target is a fixed number that indicates that the hash value of a block should be below from the target. When miners find a hash value that satisfies the goal difficulty, then disseminate the solution to the network. Other miners on the network confirm the solution by independently validating the computations [6]. The miner block gets added to the blockchain if the solution is accepted as valid and the miner gets rewarded for the work. The complete mining procedure of blockchain is explained in the figure 1.

**Fig. 1. Data Mining Process through Blockchain Technology**

Therefore, on the basis of above, the present article provides an in-depth analysis of the mining process through practical implementation and simulate the procedure for users to mine the blocks. The study evaluates the blockchain mining process, focusing on a secure method of maintaining health data. The presented method involves creating a health record ledger that securely stores patient health record and registration numbers on the blockchain. This guarantees that only authorized individuals have access to the records.

Users or medical professional mines the patient health record into the blockchain. Once a record is entered into the blockchain, it becomes immutable and tamper-proof. Additionally, the approach also ensures data integrity and transparency of the data.

1. **Related Work**

From the literature, it is observed that there are some studies conducted, that discuss the concept of mining, but there has been limited progress in discovering the detailed workings of the mining process. Chen et al. [7] have discussed the issues of centralization in mining power in the context of a Proof of Work (PoW) blockchain system. Additionally, it developed Endex, a decentralized index that measures the degree of decentralization Cong et al. [8], have designed a mining pool that highlights the risk sharing as a natural centralized factor and described how a blockchain system may continue to be decentralised over time and provide actual data from the bitcoin mining sector to back up our hypothesis. Todorović et al. [9], have proposed Combinatorial Optimization Consensus Protocol (COCP) which is a Proof-of-Useful-Work (PoUW) consensus protocol that substitutes typical cryptographic puzzles with real-life examples of Combinatorial Optimization (CO) issues.

Further in the year of 2023 Vaigandla et al. [10] have presented a review of security issues in IoT devices and investigated the usage of blockchain method to improve security and privacy in IoT applications. It emphasizes IoT network difficulties due to decentralized structure and limited resources. Chen et al. have presented a review on blockchain technology and explained all the key features, benefits and consensus protocols of the blockchain. A block withholding attack avoidance technique is based on blockchain mining behaviors which has been presented in [12]. The goal is to identify malicious miners, reduce the income, and enhance the income of legitimate miners. Albshri, et al. [13], have focused on modelling the financial incentives of blockchain mining in PoW protocols, with a special emphasis on cryptocurrency mining such as bitcoin. The study proposed a profit function and an equilibrium model for analyzing hashing power demand in terms of income, mining expenses, and the number of miners.

In blockchain technology, mining is a crucial procedure which guarantees the security and integrity of the distributed ledger. It is a process of adding new blocks to the blockchain using computing resources and consensus procedures [14]. As per figure 1, the overview of mining process is discussed below:

1. **Transaction Pool (Mempool)**

Mempool is the area where all the unconfirmed transactions exist. The transactions indicate cryptocurrency like bitcoin or data transfer on the blockchain. Every transaction comprises information such as the sender, receiver, and amount (in cryptocurrency), or the exact data being transferred as discussed by Allam et al. [15]. Initially, every bitcoin transaction is store into a Mempool. Thereafter, the miners retrieve transactions from the Mempool and organize them into blocks.

1. **Block Creation**

Miners gather all of the transactions and then combine into a block, which includes the three components containing the transaction list, the block header, and the merkle tree root [16]. Transaction list serves as an inventory of approved transactions that will be added in the block. Block header contains essential information about the block, like the timestamp of the block, a previous block hash, and other essential information used in the mining process. Further, Merkle tree root, which also referred to as a binary hash tree, is generated by hashing the transactions and it also ensures the data integrity.

1. **Transaction Validation**

Before a block is mined, all transactions go through with verification process to ensure block authenticity and integrity [17]. Firstly, each transaction is checked to confirm that the sender has enough funds and then the transaction is properly organized. Next, a signature checked is performed, where the sender cryptographically signs transactions, which are subsequently verified to guarantee the legitimacy of block. Finally, a double-spending check is performed to ensures that the same funds are not used multiple times, which prevent from fraud transaction in blockchain network.

1. **Proof of Work (PoW)**

It is a consensus mechanism as well as a primary mining process used in blockchain. It is like a tournament where miners race to solve cryptographic puzzles as discussed by Choudhary and Saxena [18]. The process involves determining nonce, it is a 32-bit random number used to generate a hash value. When the block header is combined with this nonce, it generates a hash with a particular number of leading zeroes. The nonce range start from$0 to 2^{32}-1$ $≅0 to $4\*$10^{9}$, while the total number of valid hashes$10^{77}.$ The SHA-256 hash algorithm is widely used to compute the hash value. Miners repeatedly calculate the hash of the block with various nonce values until a valid hash is discovered. Furthermore, obtaining a hash less than a specific target is measured by the difficulty target. Once miners discover a nonce that generates a valid hash and meet the difficulty threshold, the solution is broadcast to the network for validation.

1. **Block Validation and Addition**

When a miner discovers a valid solution, the proposed block distributes all over the network. Other nodes in the network then performs the several checks [19]. First, the verification of block header hash is accurate and satisfies the difficulty target. Next, to reverify the transaction within the block to ensure that no tampering has occurred. Finally, if the block is deemed legitimate then node appends the block to blockchain. This process ensure consensus, as the majority of the network collectively determine the blockchain's current state.

1. **Reward and Incentive**

A certain amount of new digital currencies is granted to miners, as a reward, who successfully mines the block [20]. After that, the process is then restarted and miners compete to create the subsequent block and add it to the blockchain.

1. **Propagation and Synchronization**

The new block is transmitted all over the network, ensuring that all nodes have the most recent version of the blockchain.

1. **Methodology**

The present work proposes a blockchain architecture which includes block generation, mining, and verification. Each block contains essential information, including the patient's name, ID, registration number, proof, hash value, previous hash, and timestamp. The methodology is outlined below.

* 1. **System Design**

The system design covers building a blockchain in which each block contains the following attributes:

* **Patient name and ID:** The patient ID, or unique identifying number, is obtained from the patient's medical report and is linked to the patient's name on the record.
* **Registration number (Reg\_no):** The registration number from the medical report is appended into the block to verify its authenticity.
* **Proof:** The result of the proof-of-work algorithm is a nonce value that meets the specified criteria of the difficulty target to validate the block.
* **Previous Hash:** The hash value of the preceding block, ensuring the continuity of the chain.
* **Timestamp:** Each block's creation time is recorded. Because timestamps change every second, the hash result likewise varies over time, adding an extra level of protection. The range of nonce is 4\*$10^{9}$ and the total valid hash is $10^{77}.$ Therefore, 4\*$10^{9}$ the entire nonce range is exhausted in 40 seconds because of $10^{8} $hashes generate in 1 second and (4\*$10^{9}$) / $(10^{8})$ = 40 seconds. So, there is a problem that all hashes are generated within the nonce range; that’s why “Timestamp” comes into the picture. Consequently, every 1-second timestamp will change; if the timestamp changes, then the hash also changes. So, nonce is not completely utilized. Due to the timestamp, the nonce generates a large number of hashes.

* **Hash:** The cryptographic SHA-256 hash of the current block.
	1. **Implementation**

The blockchain system is implemented with Python and Flask, a lightweight web framework for Python that allows developers to construct web applications. Furthermore, the Postman is used to test the blockchain, which is an Application Programming Interface (API) development tool that helps build, test, and modify API’s. It makes various types of HTTP requests (GET, POST, PUT, PATCH). The implementation consists of the following main functions and the complete procedure of mining of patient medical record is represented in algorithm 1.

* **Block Creation:** Creating new blocks with the appropriate properties, such as create\_block(patient\_name, patient\_ID, Reg\_no, proof, previous\_hash)
* **Proof of Work:**  The function proof\_of\_work(previous\_proof) implements the proof-of-work methods to verify a blockchain by finding a nonce that generates a hash value.
* **Hash Calculation:** Determine the hash of each block with the help of hash(block). Further, convert and encode the block dictionary into a JSON string. Return the SHA-256 hash of the encoded block.
* **Chain validation:** It is the process of ensuring the blockchain integrity with the method is\_chain\_valid(chain). It is verifying that each block's 'previous\_hash' matches the hash previous block.

|  |
| --- |
| **Chart 1:** Patient Medical Record Mining in the Blockchain |
| *Input: patient\_name, patient\_ID, Reg\_no**Output: Updated blockchain with mined patient record**Begin**If blockchain is empty then* *Create genesis block with default data* *Calculate hash of genesis block* *Append genesis block to chain**EndIf**previous\_block ← get last block in chain**previous\_proof ← previous\_block.proof**new\_proof ← 1**While True do* *hash\_val ← SHA256(new\_proof^2 - previous\_proof^2)**If hash\_val starts with '0000' then* *Break* *Else* *new\_proof ← new\_proof + 1**EndIf**EndWhile**previous\_hash ← hash(previous\_block without its hash field)**Create new block with:**patient\_name, patient\_ID, Reg\_no**index ← length of chain + 1**timestamp ← current time**proof ← new\_proof**previous\_hash ← previous\_hash**block\_hash ← hash(new block without its hash field)**Add block\_hash to new block**Append new block to chain**Return "Patient record securely added to blockchain ledger"**End* |

* 1. **Testing and validation**

The system is tested by mining several patient records and retrieving the blockchain to ensure each block is mined successfully with the correct hash. Hence, the step-by-step procedure is described as follows:

*Step-1 Define a route* ***/get\_chain****: It returns the whole blockchain with all patient records and ensures that each block has the right hash value;*

*Step-2 Define a route* ***/mine\_block****: It is used for mining a new block with the patient name, patient ID and registration number;*

*Step-3 Define a route* ***/is\_valid****: It ensures the blockchain integrity and verifies whether the blockchain is valid.*

1. **Results and Discussion**

The present work represents code snippets and details about the implementation. It demonstrates Postman interacts with a simulated network. It also includes a sample scenario in which users submit details and mine blocks, showing the validity blocks to the blockchain.

* The JSON output below indicates the successful establishment and validation of the blockchain. Therefore, figure 2 describes the code, that generates the HTTP request as shown in the box.



**Fig. 2. Code of Blockchain**

* The HTTP request is produced, as seen in the figure 2. The HTTP call is executed in the Postman workspace to get a chain using the **/get\_chain** function. Furthermore, after hitting the GET request, we will get the first block (Genesis block) as shown in Figure 3.



Fig. 3. Genesis Block Generation

* Now to mine a new block in this chain, the mine function like **/mine\_block** is executed as shown in figure 4. After hitting the POST request, the new block is mine. The patient’s name of the second block is “Alice”.

 **Fig. 4. Mining of the Second Block**

* After mine the second block, the researcher wants to retrieve the chain. As a result, the authors again perform the **/get\_chain** function to obtain the chain, as shown in figure 5.

****

 **Fig. 5. Second Block Generation**

* Further, to verify the blockchain validity, the function such as **/is\_valid** is executed. Figure 6 represents the validation of blocks and the results show that the chain is valid. In this way, the miner may mine new block one after the other.

 **Fig. 6. Verification of the blockchain.**

The said findings show that the mining process is critical to the security and integrity of blockchains. By making it, miners solve complicated mathematical problems, the method assures that changing any block in the chain requires re-mining of all the blocks. It offers significant security against tampering and double-spending attack. Furthermore, the effective deployment of PoW and hashing techniques demonstrate the feasibility of blockchain. The study gives the fundamental concept of block mining and users or medical professional may experience the real time mining process by mined the patient medical record.

# Conclusion and Future Scope

The mining process in blockchain technology is a complex but necessary mechanism that protects the blockchain’s privacy, integrity, and decentralization. Miners use computing effort and cryptographic techniques to authenticate transactions, solve cryptographic puzzle, and add new blocks to the chain, ensuring the trust and stability of the whole blockchain ecosystem. Therefore, the study describes a technique for simulating blockchain mining with Python, flask, and Postman. Additionally, it also gives useful insights into the fundamental functions of blockchain technology. Future work may expand the simulation to include a multi-user environment with block rewards and network synchronization features. Furthermore, investigating alternate consensus methods such as Proof of Stake (PoS) may provide comparable security advantages while using less energy.

References

[1] Sultan, A., Mushtaq, M. A., & Abubakar, M. (2019, March). IOT security issues via blockchain: a review paper. In *Proceedings of the 2019 international conference on blockchain technology* (pp. 60-65) doi: [10.1145/3320154.3320163](http://dx.doi.org/10.1145/3320154.3320163).

[2] Klinkmüller, C., Ponomarev, A., Tran, A. B., Weber, I., & van der Aalst, W. (2019, August). Mining blockchain processes: Extracting process mining data from blockchain applications. In *International conference on business process management* (pp. 71-86). Cham: Springer International Publishing. <https://doi.org/10.1007/978-3-030-30429-4_6>.

[3] Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), 147-156.<https://doi.org/10.1016/j.dcan.2019.01.005>.

[4] Feng, J., Zhao, X., Chen, K., Zhao, F., & Zhang, G. (2020). Towards random-honest miners selection and multi-blocks creation: Proof-of-negotiation consensus mechanism in blockchain networks. *Future Generation Computer Systems*, *105*, 248-258.<https://doi.org/10.1016/j.future.2019.11.026>.

[5] Hamza, N. M., Ouf, S., & El-Henawy, I. M. (2020, March). A Proposed Technique for Enhancing the Mining Process in Blockchain Architecture. In *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 7-12). IEEE.DOI:[10.1109/ICCMC48092.2020.ICCMC-0002](https://doi.org/10.1109/ICCMC48092.2020.ICCMC-0002)

[6] Ding, X., Guo, J., Li, D., & Wu, W. (2020). Attract More Miners to Join in Blochchain Construction for Internet of Things. *arXiv preprint arXiv:2003.10560*.[10.48550/arXiv.2003.10560](https://ui.adsabs.harvard.edu/link_gateway/2020arXiv200310560D/doi%3A10.48550/arXiv.2003.10560)

[7] Chen, R., Tu, I. P., Chuang, K. E., Lin, Q. X., Liao, S. W., & Liao, W. (2020). Endex: Degree of mining power decentralization for proof-of-work based blockchain systems. *IEEE Network*, *34*(6), 266-271.[10.1109/MNET.011.2000178](https://doi.org/10.1109/MNET.011.2000178)

[8] Cong, L. W., He, Z., & Li, J. (2021). Decentralized mining in centralized pools. *The Review of Financial Studies*, *34*(3), 1191-1235.<https://doi.org/10.1093/rfs/hhaa040>

[9] Todorović, M., Matijević, L., Ramljak, D., Davidović, T., Urošević, D., Jakšić Krüger, T., & Jovanović, Đ. (2022). Proof-of-useful-work: Blockchain mining by solving real-life optimization problems. *Symmetry*, *14*(9), 1831.[**https://doi.org/10.3390/sym14091831**](https://doi.org/10.3390/sym14091831)

[10] Vaigandla, K. K., Karne, R., Siluveru, M., & Kesoju, M. (2023). Review on blockchain technology: architecture, characteristics, benefits, algorithms, challenges and applications. *Mesopotamian journal of Cybersecurity*, *2023*, 73-84.DOI: [10.58496/MJCS/2023/012](http://dx.doi.org/10.58496/MJCS/2023/012)

[11] Chen, H., Chen, Y., Xiong, Z., Han, M., He, Z., Liu, B., ... & Ma, Z. (2023). Prevention method of block withholding attack based on miners’ mining behavior in blockchain. *Applied Intelligence*, *53*(9), 9878-9896.<https://doi.org/10.1007/s10489-022-03889-3>.

[12] Soria, J., Moya, J., & Mohazab, A. (2023). Optimal mining in proof-of-work blockchain protocols. *Finance research letters*, *53*, 103610..<https://doi.org/10.1016/j.frl.2022.103610>

[13] Albshri, A., Alzubaidi, A., Alharby, M., Awaji, B., Mitra, K., & Solaiman, E. (2023). A conceptual architecture for simulating blockchain-based IoT ecosystems. *Journal of Cloud Computing*, *12*(1), 103.<https://doi.org/10.1186/s13677-023-00481-z>.

[14] Tiwari, M. G. D., & Kumar, K. A. (2023). Decentralization System Using Smart Blockchain with Secure Hash. *SN Computer Science*, *4*(5), 620.<https://doi.org/10.1007/s42979-023-02026-2>.

[15] Allam, A. H., Gomaa, I., Zayed, H. H., & Taha, M. (2024). IoT-based eHealth using blockchain technology: a survey. *Cluster Computing*, *27*(6), 7083-7110.<https://doi.org/10.1007/s10586-024-04357-y>.

[16] Priyanka, K., Vipin, S., & Shalini, C. (2025). Prediction of Type-II Diabetic through Blockchain Technology. *Indian Journal of Science and Technology*, *18*(15), 1177-1188.[10.17485/IJST/v18i15.3423](https://doi.org/10.17485/IJST/v18i15.3423)

[17] Chanal, P. M., & Kakkasageri, M. S. (2024). Blockchain-based data integrity framework for Internet of Things. *International Journal of Information Security*, *23*(1), 519-532.. <https://doi.org/10.1007/s10207-023-00719->

[18] Choudhary, B., & Saxena, V. (2023). Blockchain Implementation for Faster Accessing of Database of Banking Industry. *International Journal on Recent and Innovation Trends in Computing and Communication*, *7*, 504-512.Available from: <https://www.researchgate.net/publication/379986243_Blockchain_Implementation_for_Faster_Accessing_of_Database_of_Banking_Industry>

[19] Saxena, V., Verma, V., Verma, V., & Singh, K. V. (2023, October). Data Cube Technology for Accessing of Large Database. In *International Conference on Computer & Communication Technologies* (pp. 39-48). Singapore: Springer Nature Singapore. <https://doi.org/10.1007/978-981-99-9704-6_4>.

[20] Verma, V., Kumar, H., Saxena, V., Singh, K.V. and Verma, V. (2025) Blockchain Technology: A Comprehensive Review, Grenze International Journal of Engineering and Technology, January Issue, 2445-2458, Grenze Scientific Society, Grenze ID: 01.GIJET.11.1.8