IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Blockchain-Based Approach To Health Care Privacy

[1]Prof.Mandar S. Joshi, [2]Miss.Divya Verekar, [3]Miss.Sejal Sawant, [4]Miss.Riya Rane, [5]Miss.Riddhi Manjarekar

[1]Assistant Professor, [2]Student, [3]Student, [4]Student, [5]Student
[1]Department Of Information Technology,
[1]Finolex Academy of Management and Technology, Ratnagiri, India

Abstract: The rapid digitization of healthcare systems has brought unprecedented convenience and efficiency to medical data management. However, it has also exposed critical vulnerabilities in maintaining patient privacy and safeguarding sensitive health records from unauthorized access and breaches. This paper proposes a blockchain-based framework to address these challenges by leveraging the inherent characteristics of blockchain technology, including decentralization, immutability, and cryptographic security. The proposed system ensures secure, transparent, and patient-centric management of healthcare data, enabling controlled data sharing through smart contracts while maintaining data integrity and access control. By integrating blockchain with existing healthcare infrastructure, this approach enhances privacy, provides a tamper-proof audit trail, and ensures interoperability across diverse healthcare systems. Experimental analysis demonstrates the effectiveness of the proposed model in reducing data breaches and unauthorized access while maintaining operational efficiency. This paper highlights the potential of blockchain to revolutionize healthcare privacy, ensuring trust and security in digital health ecosystems.

***Index Terms* -** Blockchain, Smart contracts, PHR (Personal Health Records), healthcare, access control.

I. Introduction

The central outline of the proposed algorithm is the implementation of healthcare data storage using blockchain. The system creates trustworthy communication between multiple parties without using any third-party interface. We use the Hash generation algorithm and the Hash will be generated for the given string. Before executing any transaction, we use peer to peer verification to validate the data**.** Blockchain, the digital ledger technology that can securely maintain continuously growing lists of data records and transactions, has the power to potentially transform health care, according to industry experts. By simplifying and expediting the way the healthcare industry processes data in such areas as revenue cycle management, health data inter permeability, and supply chain validation, blockchain has the power to dramatically reduce back-office data input and maintenance costs and improve data accuracy and security.

II.Literature survey

According to [1] a novel blockchain technology that secures health data in the cloud, aids in authentication, and ensures the integrity of medical records. Here, blockchain with optimal encryption is deployed via an improved Blowfish model that also guarantees authentication features. Further, the optimal key generation is carried out using a new approach termed "Elephant Herding Optimization with Opposition-Based Learning" (EHO-OBL). Thus, the developed approach maintains data integrity, and ultimately, various measures prove the supremacy of the presented approach.

According to [2] a blockchain-based system designed to secure Internet-of-Things (IoT) healthcare devices. In addition to data encryption, we propose to use blockchain technology to enhance security and privacy in healthcare systems. The system is intended to allow remote patient monitoring, particularly for chronic diseases that necessitate regular monitoring. Three important characteristics were taken into account: security, scalability, and processing time. We ensure security by encrypting data and controlling access to it using the re-encryption proxy in conjunction with blockchain. We store data in an Inter Planetary File System (IPFS) off-chain database to ensure blockchain scalability. We use an Ethereum blockchain based on proof of authority (PoA) to speed up the data storage.

According to [3] a thorough analysis of current blockchain-based IoHT systems is carried out to find out if it is possible to protect privacy by combining blockchain and IoHT. In addition, various types of privacy challenges in IoHT are identified by examining the General Data Protection Regulation (GDPR). More importantly, an associated study of cutting-edge privacy-preserving techniques for the identified IoHT privacy challenges is presented. Lastly, some problems are listed in four interesting areas of research for blockchain-based IoHT systems. This is done to encourage researchers working in these areas to come up with possible solutions.

According to [4] an end-to-end blockchain-based and privacy-preserving framework called SmartMedChain for data sharing in a healthcare environment. (e) Blockchain is built on hyper ledger Fabric and stores encrypted health data by using the Inter Planetary File System (IPFS), a distributed data storage solution with high resiliency and scalability. Indeed, compared to other propositions and based on the concept of smart contracts, our solution combines both data access control and data usage auditing measures for both medical IoT data and electronic health records (EHRs) generated by healthcare services. Also, people involved in healthcare can be held responsible by putting in place a new Privacy Agreement Management system that checks that the service is carried out according to patient preferences and privacy laws.

An [5] architecture to ensure the privacy of health-related data, which is stored and shared within a blockchain network in a decentralized manner through the use of encryption with the RSA, ECC, and AES algorithms. We conducted evaluation tests to confirm how cryptography affects the proposed architecture's computational effort, memory usage, and execution time.

In [6] regarding the safety and privacy needs for sharing medical data using blockchain. It gives a thorough examination of the safety and privacy risks and needs, along with technical solution methods and plans. First, we discuss the security, privacy, and attributes required for electronic medical data sharing by deploying the healthcare blockchain. Second, we divide current efforts into three reference blockchain usage scenarios for sharing electronic medical data. We then talk about the technologies that can be used to make these security and privacy features work in these three healthcare blockchain usage scenarios. These technologies include anonymous signatures, attribute-based encryption, zero-knowledge proofs, and verification techniques for smart contract security. Finally, we discuss other potential blockchain application scenarios in the healthcare sector.

According to [7] the application of blockchain in smart grids, energy trading, and big data management emphasizes its ability to enable secure peer-to-peer energy trading, enhance data integrity, and streamline energy transactions. Despite its advantages, blockchain implementation faces several security issues, including data privacy, scalability, and cyber threats. Additionally, regulatory and interoperability challenges pose significant hurdles to its adoption. This study provides an in-depth analysis of these issues and offers actionable recommendations to enhance blockchain's effectiveness in the energy domain.

In [8] a comprehensive review of the intersection of blockchain technology and the Internet of Things (IoT), highlights the role of blockchain in enhancing the security, scalability, and trustworthiness of IoT ecosystems. The study begins with a taxonomy of blockchain-based IoT applications, categorized by domains such as smart homes, healthcare, supply chain management, energy systems, and transportation. It also examines popular blockchain platforms, including Ethereum, Hyperledger, and IOTA, and their suitability for IoT integration.

In [9] the study focuses on the transformative impact of blockchain technology on manufacturing supply chains and logistics, emphasizing its potential to enhance transparency, traceability, and efficiency. Blockchain, with its decentralized and immutable ledger, addresses critical challenges in these sectors, such as fraud, counterfeit goods, and lack of real-time visibility. By enabling secure data sharing among stakeholders, blockchain facilitates seamless tracking of goods, efficient inventory management, and faster dispute resolution.

According to [10] the healthcare industry has designed a blockchain-based healthcare data management system to tackle critical security, privacy, and interoperability issues. The decentralized nature of blockchain is used by the system to protect the privacy and integrity of patient data. This lowers the risks that come with centralized healthcare data storage systems, like data breaches and unauthorized access.

III.PROPOSED SYSTEM DESIGN

In the proposed research works to design and implement a system for healthcare data, where users can store all information in a single blockchain without any Trusted Third Party (TTP) in a fog computing environment. The system also carried out data integrity, and confidentiality as well as eliminates the inconsistency for end users. The system highlights the implementation of healthcare data storage using blockchain. In the system if the patient changes the city and then refers to the doctor of the other city then through fog networks the new doctor can get the complete history of that patient and for maintaining the secure data, we use blockchain technology. In this data is processed in multiple servers so the transactions are processed in a sequencing fog network. This illuminates the quality-of-service issue and time limits. This is a middleware system in which the processing environment in which the load will be balanced using threads. The request generated will be parallels saved on all nodes in a Blockchain manner. Hash generation algorithm and the Hash will be generated for the given string. Before executing any transaction, we use peer to peer verification to validate the data. If any chain is invalid then it will recover or update the current server blockchain. This will validate till all the nodes are verified and commit the query. A mining algorithm is used to check the hash generated for the query till the valid hash is generated.

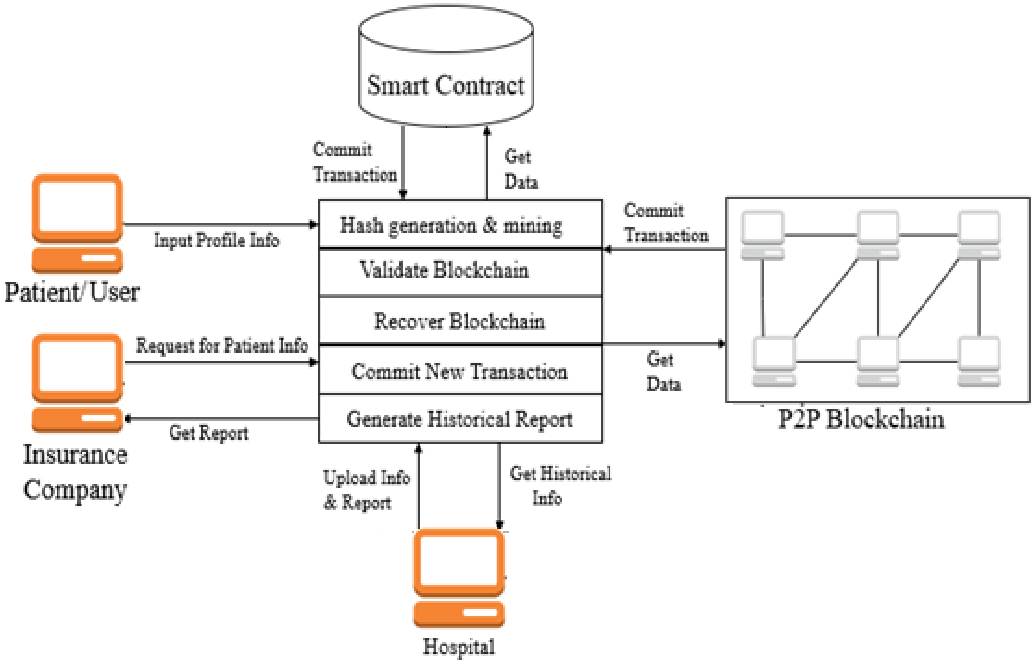


Fig.1: System Design

Methodology
The system contains the following modules:
Patient/User:
The patient enters their profile information into the system.
This information is processed, generating a transaction that is hashed and mined before being added to the blockchain.

Smart Contract:

Acts as the governing mechanism that enforces rules for data sharing and access control. It retrieves data from the blockchain and ensures transactions comply with predefined conditions.

P2P Blockchain Network:

The distributed ledger is where all validated transactions are stored. Ensures data immutability, transparency, and security through a consensus mechanism.

Insurance Company:

Can request specific patient information (e.g., medical history or reports). The smart contract validates the request and retrieves the required data securely.

Hospital:

Uploads patient-related data, such as reports or medical history, to the blockchain. Can retrieve historical information for further medical or operational purposes.

Verification Transaction is detected -

Majority Voting: A decision-making process known as majority voting selects the option that receives more than half of the votes. In the context of blockchain consensus, each node independently verifies a proposed block's validity and casts a vote—typically 1 for valid and 0 for invalid. The network then aggregates these votes, and if the number of approving votes exceeds a predefined threshold (usually over 50%), the block is accepted. In weighted majority voting, the influence of a node's vote depends on factors like stake, reputation, or computational power, ensuring that more trusted or resourceful participants have a greater impact on the final decision.

Recovery Data: Blockchain data recovery generally pertains to the restoration of lost or damaged blockchain data resulting from node failures, inadvertent deletions, or cyberattacks. The recovery method is contingent upon the blockchain architecture. In the majority of blockchains, each full node retains a whole copy of the blockchain. If a node loses data, the network may resynchronise with it to recover the missing blocks. In the event of a node failure, it may recover data from the valid block rather than resynchronize with the genesis block. In consortium or private blockchains, consensus procedures like majority voting facilitate the recovery of lost transactions.

Custom Blockchain Workflow Overview:

A block in a blockchain is a container data structure that stores a list of transactions. Below is the process to create a new block.

Collect Transaction

- Gather transactions that need to be added to the blockchain.
- Validate each transaction to ensure it follows the rules of the network (e.g., verifying digital signatures, and checking balances).

Create a Merkle Tree:

Organize the transactions into a Merkle tree structure. Compute the Merkle Root, which will be included in the block header.

Assemble the Block:

- Create the block header with the required fields (version, previous block hash, Merkle root, timestamp, etc.).
- Add the transactions to the block body.
- Calculate the block hash based on the header.

Proof of Work

- If using a proof-of-work consensus mechanism, miners must find a nonce that produces a block hash below a certain difficulty target.
- Once found, the block is broadcasted to the network for validation.

Entity description for the application.

- Block
- Transaction
- Wallet
- Node
- Smart Contract
- Consensus Mechanism
- Ledger
- User

Description

- A User owns a Wallet.
- A Block contains multiple Transactions.
- A Transaction is initiated by a User through their Wallet.
- A Node validates and stores Blocks and Transactions.
- A Smart Contract is created by a User and executed on the blockchain.
- The Ledger is maintained by all Nodes and is composed of a series of Blocks.

Smart contract details in-depth-

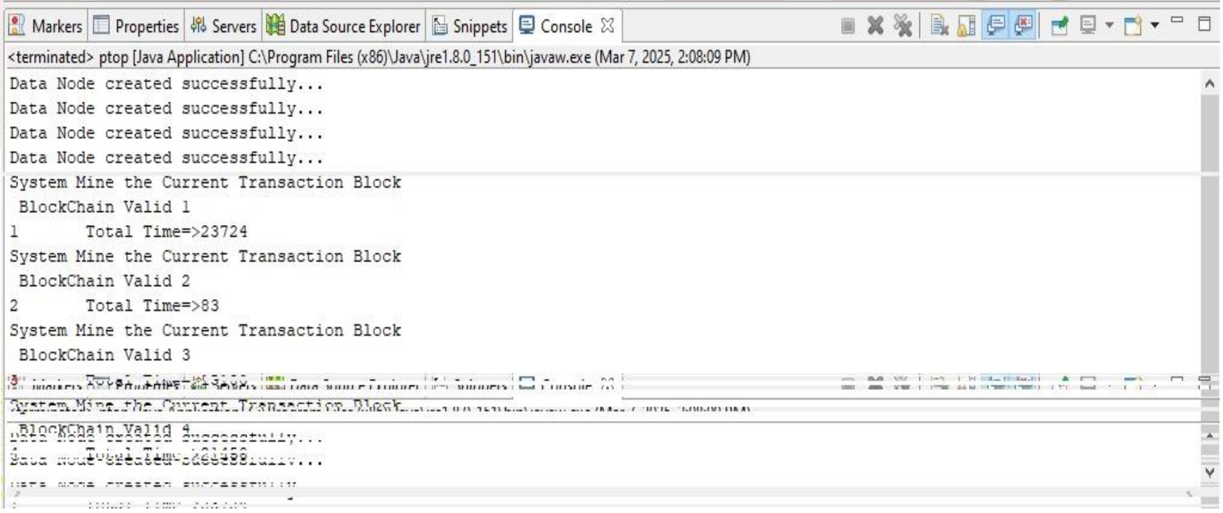
- A smart contract is defined as a digital agreement that is signed and stored on a blockchain network, which executes automatically when the contract's terms and conditions (T&C) are met. The T&C is written in blockchain-specific programming languages such as Solidity.
- Smart contracts form the foundation of most blockchain use cases, from non-fungible tokens (NFTs) to decentralized apps and the metaverse.
- Here we explain how smart contracts work and detail their various types. These are the steps needed for the functioning of smart contracts.

Agreement: The parties wanting to conduct business or exchange products or services must concur on the arrangement's terms and conditions. Furthermore, they must determine how a smart contract will operate, including the criteria that must be fulfilled for the agreement to be fulfilled.

Contract creation: Participants in a transaction may create a smart contract in many ways, including building it themselves or collaborating with a smart contract provider. The provisions of the contract are coded in a programming language. During this stage, verifying the contract's security thoroughly is critical.

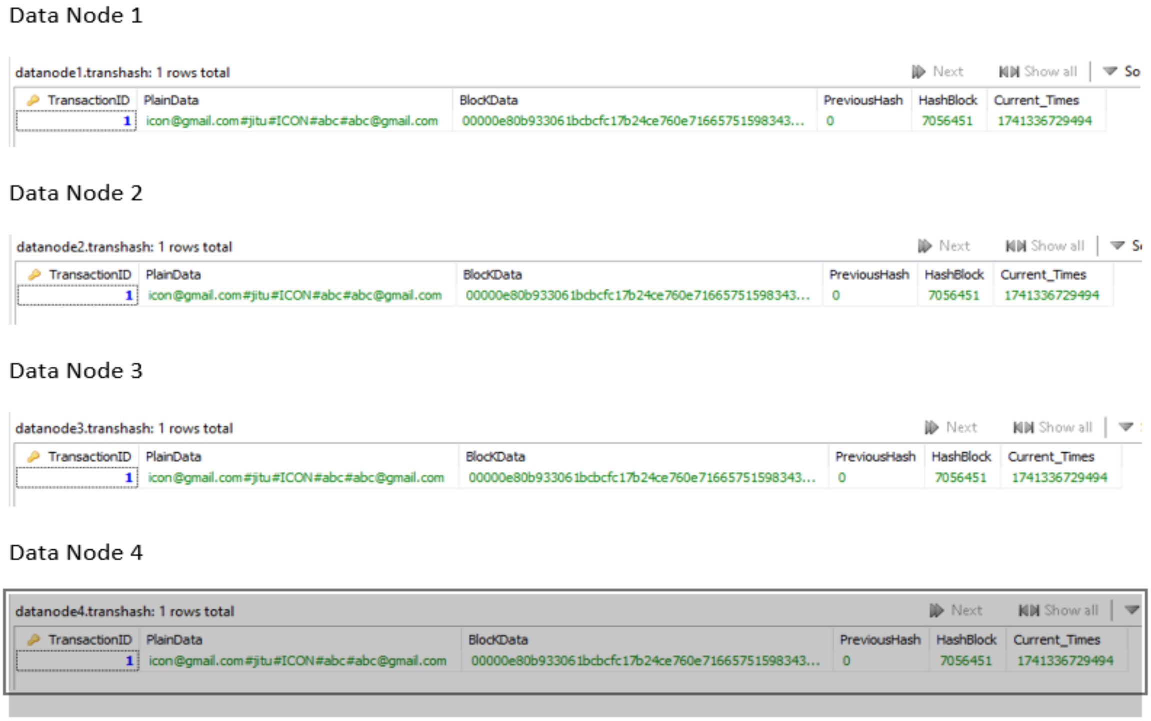
Deployment: When the contract has been finalized, it must be published on the blockchain. The smart contract is uploaded to the blockchain in the same way as regular crypto transactions, with the code inserted into the data field of the exchange. Once the transaction has been verified, it's deemed active on the blockchain and cannot be reversed or amended.

Monitoring conditions: A smart contract runs by tracking the blockchain or a different reliable source for predetermined conditions or prompts. These triggers can be just about anything that can be digitally verified, like a date attained, a payment made, etc.



```
<terminated> ptop [Java Application] C:\Program Files (x86)\Java\jre1.8.0_151\bin\javaw.exe (Mar 7, 2025, 2:08:09 PM)
Data Node created successfully...
Data Node created successfully...
Data Node created successfully...
Data Node created successfully...
System Mine the Current Transaction Block
 BlockChain Valid 1
1       Total Time=>23724
System Mine the Current Transaction Block
 BlockChain Valid 2
2       Total Time=>83
System Mine the Current Transaction Block
 BlockChain Valid 3
3       Total Time=>[illegible]
System Mine the Current Transaction Block
 BlockChain Valid 4
4       Total Time=>21456
```

Fig2. shows the execution of a blockchain-based program within the Eclipse IDE



Data Node 1

datanode1.transhash: 1 rows total

TransactionID	PlainData	BlocKData	PreviousHash	HashBlock	Current_Times
1	icon@gmail.com#jitu#ICON#abc#abc@gmail.com	00000e80b933061bcbcfc17b24ce760e71665751598343...	0	7056451	1741336729494

Data Node 2

datanode2.transhash: 1 rows total

TransactionID	PlainData	BlocKData	PreviousHash	HashBlock	Current_Times
1	icon@gmail.com#jitu#ICON#abc#abc@gmail.com	00000e80b933061bcbcfc17b24ce760e71665751598343...	0	7056451	1741336729494

Data Node 3

datanode3.transhash: 1 rows total

TransactionID	PlainData	BlocKData	PreviousHash	HashBlock	Current_Times
1	icon@gmail.com#jitu#ICON#abc#abc@gmail.com	00000e80b933061bcbcfc17b24ce760e71665751598343...	0	7056451	1741336729494

Data Node 4

datanode4.transhash: 1 rows total

TransactionID	PlainData	BlocKData	PreviousHash	HashBlock	Current_Times
1	icon@gmail.com#jitu#ICON#abc#abc@gmail.com	00000e80b933061bcbcfc17b24ce760e71665751598343...	0	7056451	1741336729494

Fig 3: - Demonstrating the integrity and replication of blockchain data across all data nodes.

Execution: When the trigger parameters are met, the smart contract is activated as per the "if/when…then…" statement. This may implement only one or multiple actions, like passing funds to a vendor or registering the buyer's possession of an asset.

Recording: Contract execution results are promptly published on the blockchain. The blockchain system verifies the actions taken, logs their completion as an exchange, and stores the concluded agreement on the blockchain. This document is available at all times.

Proposed Blockchain-Based Claim Settlement Methodology for Patients, Hospitals, and Insurance Companies

By integrating customized blockchain technology into claim settlement, the healthcare industry can overcome inefficiencies, fraud, and administrative burdens associated with traditional systems. The use of smart contracts, real-time validation, and secure data storage ensures a seamless, transparent, and faster claim processing mechanism.

The use of blockchain technology in healthcare claim settlements introduces a revolutionary approach that enhances efficiency, transparency, and security. By leveraging a decentralized ledger, this system ensures seamless interaction among patients, hospitals, and insurance companies, reducing fraud and expediting the claim process.

Step 1: Patient Treatment and Data Recording

When a patient visits a hospital for treatment, all relevant medical records, prescriptions, diagnostic reports, and billing details are securely recorded on a customized blockchain platform. This data is encrypted and stored in a decentralized manner, ensuring that it is immutable and protected from unauthorized alterations.

Unlike traditional systems where paperwork and manual entry introduce delays and errors, blockchain automates record-keeping, ensuring accuracy and preventing data loss. Every transaction is time-stamped and accessible only to authorized stakeholders, such as the hospital, insurance provider, and patient.

Step 2: Smart Contract-Driven Claim Processing

Smart contracts play a crucial role in automating the claim verification and approval process. These self-executing contracts contain predefined conditions based on insurance policies, hospital charges, and treatment procedures.

Once a patient's treatment details are recorded on the blockchain, the smart contract checks if the treatment is covered under the patient's insurance policy. If all conditions match, the claim request is automatically triggered and sent to the insurance company for further validation.
This automation reduces human intervention, eliminates paperwork, and minimizes administrative costs, ensuring a faster and more accurate claim settlement process.

Step 3: Claim Submission and Insurance Verification
After the claim is initiated, the hospital submits the request to the insurance company through the blockchain platform. The insurance provider's system uses AI-driven algorithms and blockchain-based validation to cross-check claim details against the patient's policy terms.
If the claim is valid and meets the eligibility criteria, the system automatically processes it. However, in cases where discrepancies arise—such as missing documents or mismatched billing details—the blockchain system sends instant notifications to the concerned parties for prompt resolution.
This real-time validation mechanism reduces disputes and unnecessary delays, ensuring smoother communication between hospitals and insurance companies.

Step 4: Secure Data Encryption and Compliance
A major concern in healthcare data management is privacy and compliance with regulations such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation). Blockchain addresses this issue through advanced cryptographic encryption, ensuring that sensitive patient information remains confidential and accessible only to authorized entities.

Since blockchain records are immutable, the risk of fraud, unauthorized alterations, or data breaches is significantly reduced. Additionally, every transaction in the claim process is logged, creating a transparent and auditable system that insurers, hospitals, and regulators can review when needed.
This methodology enhances trust among patients, hospitals, and insurance companies, ultimately leading to improved service delivery, reduced costs, and a more efficient healthcare ecosystem. As blockchain technology continues to evolve, its adoption in healthcare insurance settlements will pave the way for a more secure and reliable future.

IV.RESULTS

The time required for the consensus algorithm to validate the blockchain in four nodes is shown in Figure 2. The X-axis depicts the size of the blockchain, while the Y-axis depicts the time needed in milliseconds for each of the four nodes.

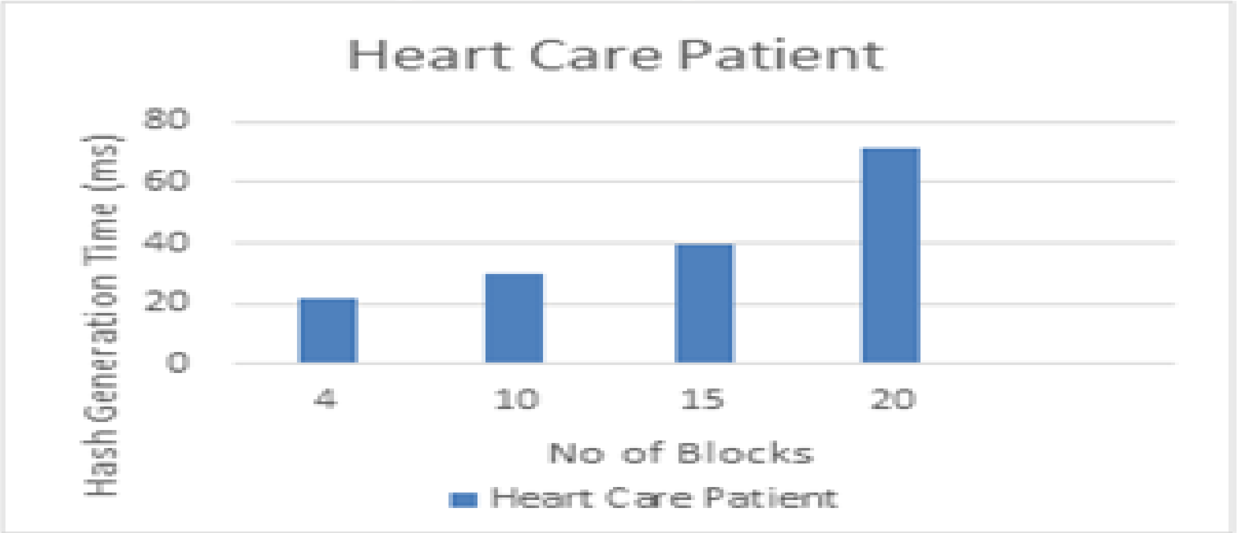


Fig. 4. Comparative Analysis of Blockchain hash generation time and number of blocks

In the second experiment, we evaluate the proposed system with smart contract validation by consensus algorithm in a different number of peer to peer nodes.

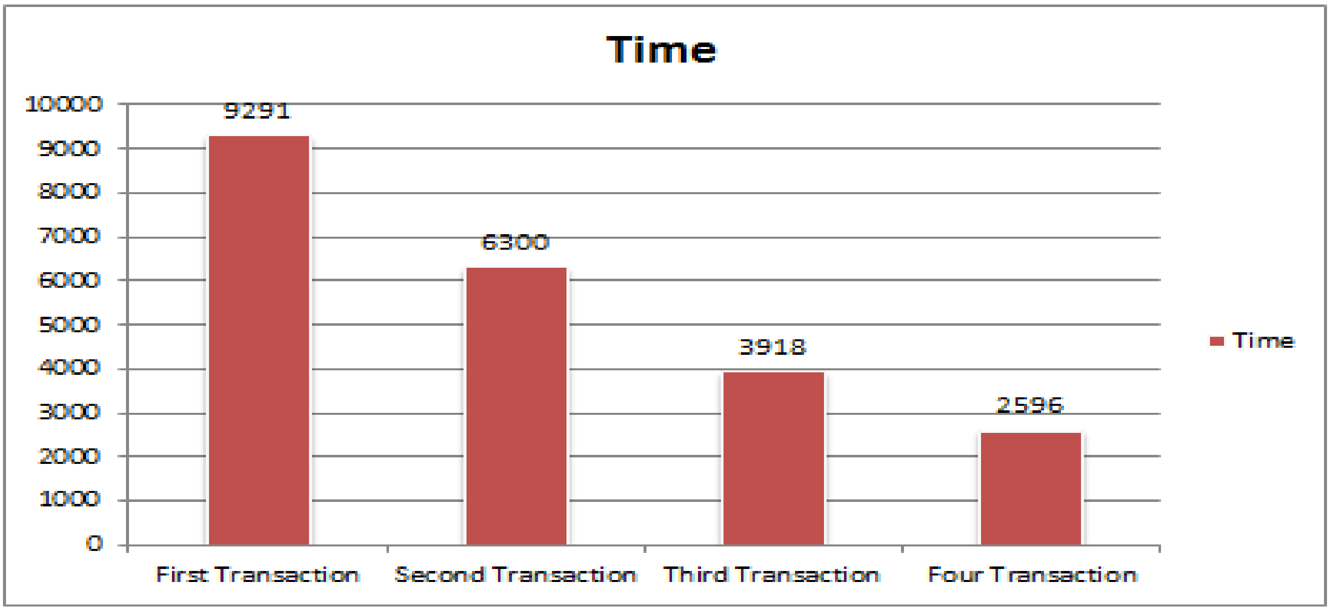


Fig.5: Time required for smart contract validation with different no. of P2P network in the blockchain.

V.CONCLUSION

The integration of blockchain technology into healthcare systems offers a transformative approach to addressing the critical challenge of preserving patient privacy and securing sensitive medical data. By leveraging the decentralized, immutable, and cryptographically secure nature of blockchain, this paper presents a robust framework that ensures data integrity, enhances access control, and fosters trust among stakeholders. The use of smart contracts enables automated, transparent, and patient-centric data sharing, empowering individuals with greater control over their health information.

VI.REFERENCES

[1] Verma, Garima. "Blockchain-based privacy preservation framework for healthcare data in a cloud environment." Journal of Experimental & Theoretical Artificial Intelligence 36.1 (2024): 147-160.

[2] Azbeg, Kebira, Ouail Ouchetto, and Said Jai Andaloussi. "Access control and privacy-preserving blockchain-based system for diseases management." IEEE Transactions on Computational Social Systems 10.4 (2022): 1515-1527.

[3] Qi, Minfeng, et al. "Privacy protection for blockchain-based healthcare IoT systems: A survey." IEEE/CAA Journal of Automatica Sinica (2022).

[4] Healthcare Engineering, Journal of. "Retracted: SmartMedChain: A Blockchain-Based Privacy-Preserving Smart Healthcare Framework." (2023): 9791481.

[5] de Moraes Rossetto, Anubis Graciela, Christofer Sega, and Valderi Reis Quietinho Leithardt. "An architecture for managing data privacy in healthcare with blockchain." Sensors 22.21 (2022): 8292.

[6] Zhang, Rui, Rui Xue, and Ling Liu. "Security and privacy for healthcare blockchains." IEEE Transactions on Services Computing 15.6 (2021): 3668-3686.

[7] Hasan, Mohammad Kamrul, et al. "Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations." Wireless Communications and Mobile Computing 2022.1 (2022): 9065768.

[8] Abdelmaboud, Abdelzahir, et al. "Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges, and future research directions." Electronics 11.4 (2022): 630.

[9] Raja Santhi, Abirami, and Padmakumar Muthuswamy. "Influence of blockchain technology in manufacturing supply chain and logistics." Logistics 6.1 (2022): 15.

[10] Zaabar, Bessem, et al. "HealthBlock: A secure blockchain-based healthcare data management system." Computer Networks 200 (2021): 108500**.**