International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
IJISAE
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Novel Consensus Algorithm for Blockchain IoT Prototype in Health Care System

Mr. Muneshwara M. S. [1*] **, Dr. Pushpa S. K.** [2]

Submitted: 16/09/2023 **Revised**: 17/11/2023 **Accepted**: 29/11/2023

Abstract: Blockchain is a decentralized, tamper-resistant digital ledger technology that securely and transparently records transactions. It provides healthcare systems with a stable and immutable platform for storing patient data, maintaining data integrity, and increasing stakeholder trust. Because blockchain is decentralized, no single entity has influence over the network. This makes blockchain resistant to tampering and restricts the ability to change a block, which requires network consensus. Over the past few years, blockchain consensus algorithms have been applied to the healthcare sector to provide electronic health data linked to patient safety. Consensus algorithms provide agreement and confidence among network participants, which is essential for blockchain based IoT healthcare systems. In the healthcare system, consensus algorithms offer secure, dependable data sharing, immutability, and decentralized decision-making. Particularly when used with healthcare data systems, current Proof of Stake (PoS) algorithm frequently encounter issues with consensus time, transaction throughput and energy efficiency. The primary goals of this research paper were to improve the Proof of Stake (PoS) consensus algorithm by optimizing the consensus time, transaction throughput and energy efficiency for the Blockchain Internet of Things (BIoT) prototype designed for the healthcare industry. Better performance is guaranteed by the novel consensus technique known as the Enhanced Proof of Stake (ePoS) consensus algorithm.

Keywords: *Blockchain, Consensus, Consensus Time, Internet of Things, Enhanced Proof-of-Stake, Ganache, Node, Proof-of-Stake, Throughput, Transaction.*

1. Introduction

Blockchain technology, known for its decentralized and secure characteristics, has transcended its initial use in cryptocurrencies and is currently under exploration and application across a wide range of industries. It possesses the capacity to bring about transformative changes in sectors including finance, supply chain management, healthcare, voting systems, and many others. Blockchain technology has the potential to effectively manage electronic patient data and facilitate its secure sharing, which is crucial for promptly updating clinical information and enabling swift follow-up. In the context of data exchange and sharing among patients, blockchain technology allows for remote identification and referral to the appropriate physicians. It leverages consensus algorithms to ensure data sharing is both secure and reliable, while also ensuring data immutability and decentralized decision-making within the healthcare ecosystem. The healthcare industry faces a constant struggle with issues like data breaches, interoperability, and data silos. Blockchain technology offers a promising solution by providing a tamper-resistant, decentralized ledger to securely store and share patient health data [1]. Blockchain enhances data security and integrity, streamlines access for authorized parties, and ensures the privacy of sensitive patient information. Here are three common types:

i. Public Blockchain: Public blockchains are open and decentralized networks that allow participation from anyone. These networks are upheld by a distributed array of nodes and are commonly employed in the realm of cryptocurrencies such as Bitcoin and Ethereum. In the context of the Internet of Things (IoT), public blockchains offer the potential to deliver transparency and immutability to IoT device data. This, in turn, fosters secure and reliable interactions between IoT devices.

ii. Private Blockchain: Private blockchains are networks with restricted access, known as permissioned networks, where only a specific group of participants, typically recognized entities like organizations or consortiums, are allowed to join. Unlike public blockchains, private blockchains offer enhanced control over network access and scalability. In the context of IoT applications, private blockchains are instrumental in building trust among devices within a particular network or organization.

iii. Consortium Blockchain: Consortium blockchains represent a hybrid concept that merges features from both public and private blockchains. These networks are overseen by a consortium, a collaborative body of organizations responsible for collectively upkeeping the

[1] Research Scholar, Department of Information Science and Engineering, BMS Institute of Technology and Management Yelahanka, Bengaluru, Visvesvaraya Technological University, 590018, Karnataka India.
Email: muneshwarams@bmsit.in, ORCID ID: 0000-0003-4714-4100
[2] Research Supervisor, Professor, Department of Information Science and Engineering BMS Institute of Technology and Management Yelahanka, Bengaluru, Visvesvaraya Technological University, Karnataka India. Email: pushpask@bmsit.in , ORCID ID : 0000-0001-6927-5684
** Corresponding Author Email: muneshwarams@bmsit.in*

blockchain infrastructure. Consortium blockchains strike a balance between decentralization and control, rendering them well-suited for IoT implementations that involve multiple stakeholders. They facilitate secure data sharing and collaboration among their members, all the while preserving a high degree of trust.

IoT prototype leverages the ESP32 microcontroller to create a versatile and connected ecosystem for healthcare data. This prototype incorporates SpO2 and ECG sensors for real-time health monitoring, enabling healthcare providers to receive vital patient information promptly [2]. However, the challenge lies in transmitting this sensitive data securely and efficiently to healthcare systems for analysis and storage.

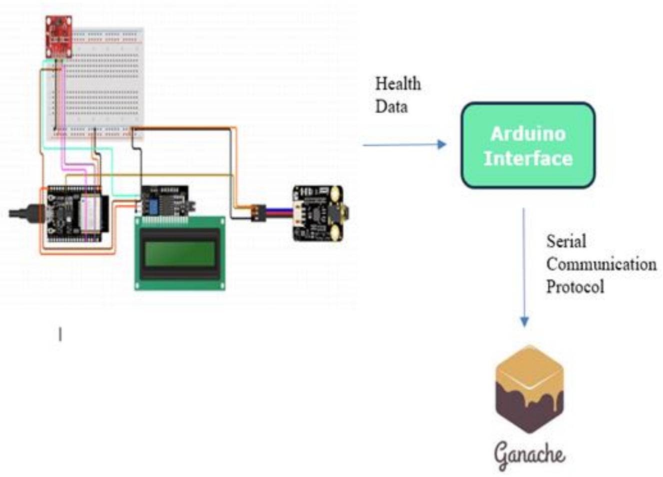


Fig 1. Blockchain IoT prototype with Ganache

The Fig 1 shows a blockchain IoT prototype which offers essential features such as heart rate monitoring, blood oxygen level (SPO2) measurement, electrocardiogram (ECG) recording analysis. The fusion of IoT, blockchain and healthcare presents a pivotal opportunity to heighten data security and optimize patient care. Development of a PoS consensus driven IoT prototype, focusing on healthcare data collection and secure transmission. By harnessing ESP32, serial communication, and Ganache blockchain emulation, the prototype ensures robust and decentralized data management. With a steadfast commitment to patient data integrity, the system exemplifies efficient device-to-blockchain communication, accompanying in an era of enhanced security and patient-centred healthcare practices. However, integrating IoT devices with healthcare systems poses several challenges, especially concerning data transfer and security. Existing data transfer protocols like UART (Universal Asynchronous Receiver-Transmitter) have limitations in terms of scalability and security in the context of healthcare data. Hence Serial communication protocol is used for transmitting and receiving data between electronic devices. It serves as a key enabler for secure and efficient data transfer between IoT devices and healthcare systems.

Ganache is a popular development tool for Ethereum that provides a local blockchain environment for testing and development purposes. While Ganache is valuable for various Ethereum development scenarios, including healthcare applications in a controlled and efficient environment. Ganache is Ease of Use for Development, Speed and Efficiency, Integration with Development Tools rather than Truffle and Remix etc. In healthcare IoT applications, blockchain events like smart contract, transaction confirmations are crucial for data communication. Ganache allows you to simulate these events, enabling applications to respond to real-time updates from the blockchain.

Consensus algorithms continue to evolve and improve, leading to research and innovation in the field. The exploration to enhance consensus mechanisms specific to IoT healthcare systems can drive advancements in scalability, energy efficiency, latency, and other performance factors [3]. Due to this Proof of Stake (PoS) algorithm is used in the overall functionality and effectiveness of the systems. PoS is a blockchain consensus algorithm that relies on validators who "stake" cryptocurrency where validators are chosen based on the number of coins they hold and are willing to "stake" as collateral.to confirm transactions and create new blocks. It offers a energy-efficient and scalable solution, making it an ideal choice for sustainable healthcare blockchain systems [[4],[5]].

The following steps shows about the PoS algorithm [6]:

```
1. Start
2. for each transaction
3.     add into transaction set
4. end for
5. All nodes participate in the selection of validator
6. Randomly selection of validator
7. for transactions in block
8.     if all transactions valid
9.         add to ledger
10.        end if
11.        else
12.            discard
13.        end else
14.    end for
15.    Publish block to blockchain network
16.    End
```

Smart contracts are essentially software programs residing within a blockchain, designed to execute when specific predefined conditions are satisfied. Their primary function is to automate the fulfilment of an agreement, ensuring that all involved parties can instantly ascertain the outcome without the need for intermediaries or unnecessary delays. Additionally, smart contracts have the capability to automate workflow processes by triggering subsequent actions once the specified conditions are met. Solidity, an object-oriented programming language purpose-built by the Ethereum Network team, is employed for the creation and design of smart contracts on blockchain platforms. This language is utilized to develop smart contracts that embody business logic and generate a series of transaction records within the blockchain system.

2. Literature Survey

Md Julhas et al. [7] highlighted the utilization of Pulse sensor technology as a pivotal component in IoT-based healthcare monitoring system. This system embodies the convergence of cutting-edge technology and healthcare, contributing to the rapidly expanding field of health related IoT devices. The Pulse sensor's role in this context underscores its importance in tracking vital health metrics non-invasively. Furthermore, the research likely delved into the intricacies of designing such IoT devices tailored for healthcare applications. IoT devices can be vulnerable to data breaches. Protecting sensitive healthcare data is critical, and any compromise in security could lead to privacy violations and misuse of personal health information.

Caixiang et al. [8], underscores the growing interest in utilizing blockchain technology in healthcare due to its decentralization, immutability, and traceability features. While offering numerous benefits, blockchain in healthcare also presents challenges, including scalability issues, interoperability hurdles, the need for technical expertise, security concerns, and authorization complexities. This research highlights the importance of distinguishing between different blockchain design types (public, private, and hybrid) in healthcare settings. It emphasizes the need for future studies to provide guidance for healthcare organizations in selecting the most suitable blockchain design based on their specific needs, which can help optimize data management and enhance patient care. The work does not offer immediate solutions to the challenges associated with blockchain in healthcare. It serves as a call to action for future research without providing concrete recommendations or strategies for addressing the risks mentioned. A more comprehensive analysis could have offered practical insights into mitigating these challenges.

Hoai Luan et al. [9] introduced the innovative concept of blockchain technology's application within the medical and healthcare sector. Their research emphasizes blockchain's pivotal role in revolutionizing and improving the overall performance of medical and healthcare fields. Furthermore, the researchers propose the utilization of the Ethereum protocol to bolster IoT within healthcare systems, especially for small-scale applications through centralized storage. The advantage of this approach lies in its potential to enhance data security, integrity, and accessibility. However, the weakness of centralization may introduce a single point of failure, necessitating robust security measures to safeguard sensitive healthcare information effectively.

Partha et al. [10], the focus is on the integration of IoT with centralized systems, highlighting the potential drawbacks, including the vulnerability to a single point of failure and concerns about data trustworthiness. To address these issues, they propose the implementation of blockchain technology to introduce decentralization, along with the innovative IOB-Health framework, aiming to combine IoT, blockchain, and healthcare into a cohesive system. While blockchain offers enhanced security and data trust, the primary concern raised is the computational intensity of hash operations in existing blockchain networks, which may not be essential for non-critical systems like IoT. The study investigates various consensus mechanisms and measures to determine the most suitable for such applications. One advantage is improved data integrity and resilience, but the drawback lies in potential scalability challenges and increased complexity in managing the decentralized system.

K. Christidis et al. [11], the highlight is on the implementation of automation through smart contracts. The synergy between blockchain and IoT is explored for facilitating the seamless sharing of services among devices in a cryptographically verifiable and time-efficient manner. The core concept involves the use of computerized transaction protocols to execute contractual terms. These protocols translate contract clauses into code, which is then embedded in hardware, all without human intervention. This approach reduces the reliance on trusted intermediaries and mitigates the risk of malicious exceptions. This system includes increased efficiency, reduced operational costs, enhanced transparency, and minimized human errors. However, potential weaknesses may arise from the complexity of smart contract code, which requires rigorous validation, and the need for robust security measures to prevent unauthorized access and exploitation of vulnerabilities in the IoT devices.

Sorin et al. [12], the study delves into the intricacies of distributed systems, highlighting the complexity of achieving consensus while considering the limited resources of nodes. Emphasis is placed on maintaining the effectiveness of consensus mechanisms while keeping network load to a minimum to conserve power. The paper identifies gaps in existing systems, such as the lack of comprehensive surveys addressing the quality requirements of e-healthcare and the unexplored potential of IoT-Blockchain platforms. Notably, it introduces a focus on the performance of consensus in IoT-Blockchain systems, including reducing the time required for consensus, managing the number of participating nodes, and optimizing the time to achieve consensus. Advantages of this approach encompass enhanced efficiency, quicker decision-making, and resource conservation in IoT-Blockchain applications. However, potential weaknesses may stem from the complexity of implementing and fine-tuning consensus algorithms to achieve these performance goals, as well as the necessity for robust security measures to safeguard the network against potential threats.

Vishal et al. [13], the central focus is on consensus mechanisms, which serve as the bedrock for establishing trust among nodes within a distributed ledger. The authors explore both public and private blockchain variants, recognizing the unique challenges each presents. Key issues addressed include the prevention of double spending, wherein the same coins are used in two transactions simultaneously. This challenge is mitigated by verifying transactions across all participating nodes, ensuring agreement and trust. Byzantine problems, where consensus is crucial to avoid system failure, are also discussed. This research encompasses a deeper understanding of the intricate workings of consensus mechanisms in blockchain systems, enabling better security and trust establishment. However, challenges arise in permissioned blockchains where increased throughput may compromise decentralization, and in permissionless blockchains, the non-deterministic nature of transactions may result in unpredictability, making it challenging to manage and scale.

Moamin et al. [14], the study primarily emphasizes on elucidating well-established blockchain consensus algorithms. The paper offers an in-depth exploration of the implementation, advantages, and limitations of four prominent consensus mechanisms: Proof of Work (POW), Proof of Stake (POS), Delegated Proof of Stake (DPOS), and Practical Byzantine Fault Tolerance (PBFT). Notably, the research centers on the emerging POW-POS hybrid consensus mechanism, representing a focal point of current investigation. Another innovative aspect is the utilization of smart contracts to enhance transparency in defining consensus rules. The strength of this research is its comprehensive coverage of diverse consensus algorithms, providing a valuable resource for decision-makers in blockchain technology adoption. Additionally, the exploration of a POW-POS hybrid and smart contract integration offers the potential for improved scalability, efficiency, and customization. However, the weaknesses may include the complexity of hybrid mechanisms and potential security vulnerabilities in smart contract-based consensus rules, which require rigorous scrutiny and testing to ensure robustness and reliability.

Wai Yan Maung et al. [15], the authors focus on the importance of formal analysis and verification in blockchain consensus algorithms. They specifically examine the proof-of-stake consensus algorithm, finding that it is deadlock-free and effective when at least 2/3 of the network agrees. However, they highlight a significant weakness - that a minority of nodes comprising more than 1/3 of the network can censor the majority, hindering consensus and availability. While potential mitigation strategies are suggested, such as ignoring disconnected nodes or implementing a time lock consensus protocol, these solutions have limitations. The advantage is the rigorous analysis, emphasizing the need for thorough assessments, while the weakness lies in the identified censorship vulnerability and limited mitigation options.

Paul Schaaf et al. [16], this study explores the rapidly evolving field of blockchain technology, particularly focusing on Proof of Stake (PoS) consensus mechanisms, which offer an alternative to the energy-intensive Proof of Work used in Bitcoin. The primary objective is to assess these PoS mechanisms' capabilities in addressing the Scalability, which involves achieving decentralization, security, and scalability simultaneously. Advantage lies in providing a comparative analysis of different PoS flavors, shedding light on their strengths and weaknesses. It identifies Unbonded PoS as the most decentralized but with unclear security assumptions, Bonded PoS as more secure but less decentralized, and Delegated PoS as achieving scalability but sacrificing decentralization and security. It underscores the challenge of finding a single mechanism that satisfies all three aspects of the Scalability. A weakness of the paper is its potential oversimplification of the comparisons, as different blockchains within each PoS flavor may vary significantly. Furthermore, the analysis doesn't consider how these mechanisms interact with other technologies in practice. A more comprehensive analysis should involve real-world applications and broader innovations beyond the protocol level to provide a deeper understanding of the evolving blockchain landscape.

Iddo Bentov et al. [17], The work reveals pure Proof of Stake (PoS) systems, prominent challenge emerge was network fragility when nodes act rationally rather than altruistically. This analysis focuses on the latter issue in existing pure PoS systems. It introduces the CoA and Dense-CoA PoS systems as novel solutions to mitigate network fragility without relying on the depletion of physical scarce resources. The paper offers a potential improvement in the security of pure PoS protocols compared to existing systems, addressing a fundamental concern in the field of decentralized systems. The proposed systems may introduce added complexity to the network. Their practical implementation and real-world effectiveness would require thorough testing and validation. Additionally, the paper acknowledges that further analysis and extension of the study to encompass a wider range of strategic considerations are needed, indicating the complexity and ongoing nature of the challenge.

Aggelos et al. [18], The "Ouroboros" blockchain is introduced, offering rigorous security guarantees and comparable security properties to Bitcoin. It operates on a "proof of stake" basis, providing efficiency advantages over "proof of work" systems. The paper also presents a novel reward mechanism that incentivizes honest behavior, neutralizing attacks such as selfish mining. Real-world practicality is demonstrated through an experimental implementation in Haskell and Rust-based Parity Ethereum, showcasing transaction confirmation and processing. Ouroboros offers improved efficiency by using a "proof of stake" mechanism, reducing the energy-intensive computational work required in "proof of work" systems like Bitcoin. The detailed cryptographic and technical implementation described may be complex and require advanced expertise. Ensuring the security and reliability of such a system would require thorough testing and scrutiny.

Y. Gao et al. [19], This work reveals into the challenge of scalability in blockchain technology, particularly concerning healthcare, which can only process a limited number of transactions per second. To tackle this issue, the authors propose a novel consensus protocol that combines sharding and proof of stake. Their approach is anticipated to result in linear scalability with network size, offering a promising solution. The paper claims to be the first to integrate sharding and proof of stake in a blockchain protocol. The proposed protocol provides a potential solution to one of the most pressing issues in blockchain technology - scalability. Linear scalability with network size could significantly enhance the capacity of blockchain networks to handle more transactions. While the paper outlines the proposed protocol, it indicates the need for experiments in an emulated network. This implies that the solution is theoretical and untested, raising questions about its real-world feasibility and security.

DENIS et al. [20], the study focuses on consolidating, identifying, and discussing parameters that pertain to the performance and security of consensus mechanisms within blockchain technology. The research systematically analyzes and compares various consensus algorithms, evaluating their performance and security against these parameters. Notably, the paper highlights research gaps, emphasizing the need for designing more efficient consensus algorithms and evaluating the existing ones comprehensively. This work lies in its comprehensive approach to understanding the critical factors influencing consensus mechanisms, paving the way for more informed decision-making in blockchain technology adoption. However, the research may face challenges related to the rapidly evolving nature of blockchain technology, necessitating ongoing updates and adaptation to remain relevant in the dynamic field of blockchain consensus.

Cleverence et al. [21], the primary focus is on the evaluation of a framework for performance monitoring in distributed systems. The key performance metrics examined include memory consumption, disk read/write operations, network data utilization and CPU usage. Notably, the study reveals that consortium-based platforms excel in handling a larger volume of transactions and resources. The strength of this research lies in shedding light on the efficiency and resource management capabilities of consortium-based platforms. These platforms often offer enhanced scalability and performance for specific use cases. However, the weakness lies in the complex nature of consensus mechanisms within distributed systems. Achieving consensus is challenging, requiring robust resistance to node failures, network partitioning, message delays, and the presence of corrupted or malicious nodes. This complexity necessitates careful design and security measures to ensure system integrity and trustworthiness.

Based on a review of the literature**,** current Proof of Stake (PoS) commonly encounter issues concerning consensus time, throughput, and Resource utilization. In this paper chosen the Proof of Stake (PoS) consensus algorithm to enhance among the others consensus algorithm because it is better suited for IoT devices

3. Proposed System Architecture

In this research endeavour, presenting a proposed system aimed at creating an ePoS consensus-based Blockchain IoT prototype for the healthcare sector. This prototype's primary function is to collect physiological data (SpO2, heart rate, ECG) using sensors and ESP32 devices. Data is then transferred to local storage via USB connections, and subsequently integrated into the blockchain framework. The system architecture of the proposed model is depicted in Figure 2.

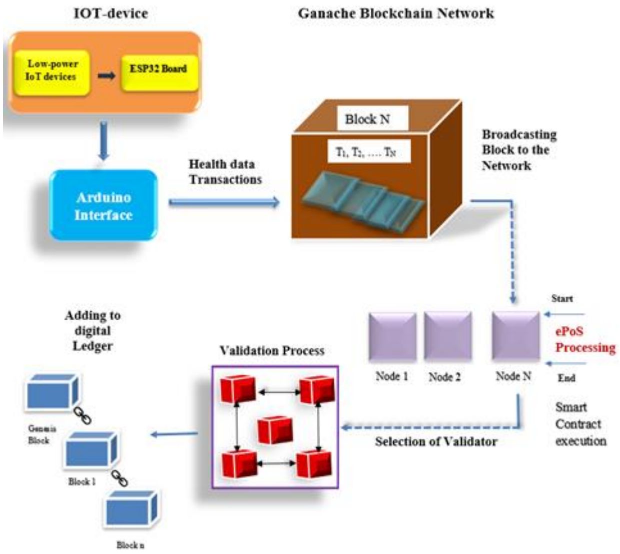


Fig 2. Proposed System architecture

The proposed system section could be structured as follows:

3.1. IoT Device

In a healthcare system, an IoT device equipped with SpO2 (blood oxygen saturation) and ECG (electrocardiogram) sensors measures vital signs, enabling real-time patient monitoring. This data is transmitted securely over the internet, facilitating remote patient management and timely medical interventions when necessary.

The ESP32 is a versatile microcontroller that can be used in IoT-blockchain healthcare systems to collect and process data from sensors like SpO2 and ECG, offering a reliable platform for real-time health monitoring. Its low power consumption, Wi-Fi and Bluetooth connectivity, and compatibility with blockchain technology make ESP32 a suitable choice for securely transmitting vital health data to blockchain networks, ensuring data integrity and patient privacy in healthcare applications [22].

The Arduino interface between an ESP32 and Ganache local storage in blockchain IoT applications enables devices to interact with blockchain networks. Arduino serves as a critical component in the data collection process for IoT applications interfacing with blockchain networks. It bridges the physical world of sensors with the digital realm of blockchain by collecting, processing, formatting, and transmitting data, thus enabling secure and transparent data recording on the blockchain network. Serial communication via USB links ESP32 and the central unit, transmitting binary data. The central unit assembles and processes these bits, storing them temporarily for data integrity [23].

3.2. Ganache Blockchain networks

Ganache serves as a private blockchain development tool for smart contract creation and testing. This blockchain operates on an enhanced Proof of Stake (ePoS) mechanism outlined in a study. It receives healthcare data from IoT prototypes, generating blocks using smart contracts for sensed data, encompassing numerous transactions. These transaction blocks are disseminated throughout the network for validation.

Within the Ganache blockchain network, nodes play crucial roles as distinct entities. In this private blockchain ecosystem, nodes can assume either mining or non-mining roles. The network's primary mission involves facilitating data dissemination, achieving consensus, and ensuring synchronization among participating nodes. Communication predominantly entails nodes exchanging transaction and block data, and they actively propagate newly created transactions and blocks across the network.

Smart contracts specify how a node in the network is chosen at random to act as a validator in the ePoS method. It is the responsibility of these chosen nodes to validate transactions before adding them to the digital ledger. One notable feature of the Enhanced Proof of Stake (ePoS) consensus mechanism is its energy-efficient method of verifying and safeguarding transactions including patient data. The use of ePoS consensus in real-world applications—whether on a public or private Ethereum blockchain network—proves beneficial for safely handling patient data in a production setting. To ensure an unchangeable record and secure maintenance of each patient's health data, this arrangement makes use of smart contracts and blockchain transactions.

4. System Methodology

The methodology section serves as a blueprint for the study, The methodology section functions as a roadmap for the study, outlining its purpose and objectives. In this research, the primary goal is to enhance the PoS consensus-based system and apply it in the form of an improved ePoS to a healthcare Internet of Things (IoT) prototype integrated with a blockchain system. This prototype is designed to collect essential vital signs data, such as SpO2, heart rate, and ECG, using ESP32 technology. The objectives involve several key steps, including the prototype's design, the implementation of an ePoS consensus mechanism, and the integration of Ganache to ensure secure data transmission. This section presents a detailed and systematic approach to achieving these objectives, providing readers with a clear and comprehensive roadmap to understand the study's methodology and anticipated outcomes.

The utilization of an ePoS consensus mechanism is in accordance with the demand for energy-efficient and decentralized data management. By steering clear of resource-intensive mining, ePoS effectively curtails energy consumption. The decentralization aspect contributes to enhanced data security, eliminating the concentration of power within a single entity [24]. This strategy not only optimizes network sustainability but also fosters a more environmentally friendly and secure approach to data handling, especially in the realms of IoT and healthcare applications.

The outlined steps delineate the methodology employed to integrate an IoT prototype, blockchain technology, and ePoS, ensuring the secure and decentralized management of patient data for healthcare professionals. This methodology aims to enhance data integrity and elevate patient care standards through ePoS.

4.1. Selection and Setup

Hardware: For the IoT device, the ESP32 microcontroller is paired with SpO2, heart rate, and ECG sensors. This choice is in accordance with healthcare standards for vital sign monitoring. The ESP32's compatibility and availability of analog pins facilitate smooth integration of sensors, addressing various data requirements.

Software Architecture: The software architecture integrates ESP32 firmware for data collection, Ganache for PoS blockchain simulation, and web3.js for interaction. Smart contracts are employed to validate data, ensuring secure and real-time storage, thereby maintaining the integrity of healthcare data.

Data Serialization and Transmission: Data from IoT sensors is serialized, transmitted via USB to a central unit. Serialized data is processed, temporarily stored, and then transferred to the blockchain, ensuring secure and efficient healthcare data management.

Data Collection and Sensor Integration: ESP32 interfaces with sensors (SpO2, heart rate, ECG) via analog/digital pins, converting readings to digital values. It processes and prepares data for transfer and analysis using appropriate libraries and programming. ESP32 to local storage at 100 KB/s, Ganache ePoS consensus under 5 seconds per transaction, and 300 ms query response time. Confirms real-time data processing, secure storage, and timely access for healthcare.

Data Encoding and Local Storage: Collected data is encoded for structured transmission. ESP32 includes local storage as a buffer, preventing data loss during network disruptions and enhancing reliability and data integrity during transfer

4.2. Integration with Ganache and Blockchain:

A blockchain powered by Ethereum's Proof of Stake (PoS) mechanism is chosen due to its energy efficiency and privacy features. Smart contracts coded in Solidity oversee the reception of IoT data, guaranteeing its authenticity and proper formatting. Once the data is validated, it's securely stored in blockchain blocks, ensuring immutability through hashing. Ganache comes into play by creating a simulated blockchain environment that enables secure data transfer, thorough testing, and validation procedures before the seamless integration of the system into the live blockchain.

The following Flow chart shows Smart contract for reading and storing data pseudocode for integration

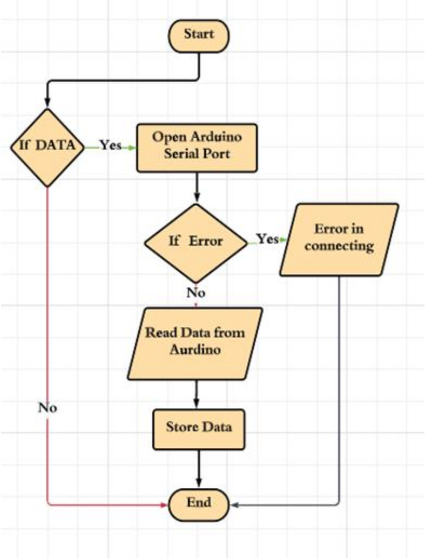


Fig 3. Pseudocode code for reading data

The process in Fig 3 begins by initiating communication with an IoT device through the Serial Port. It checks for the presence of incoming data and, if data is detected, proceeds with next stage. In the event of an error during the connection process, indicates a failure to establish communication. In the case of successful data reception then proceeds to read the data from the IoT device. Subsequently, the obtained data is stored for Adding into the blockchain. However, if there is an error during the data reading process, an error message is generated, alerting the user or system administrator about the connection or data retrieval issue. This encapsulates a basic data communication and retrieval sequence with an IoT device. It incorporates conditional branches to handle successful communication, errors in connection, and errors during data retrieval.

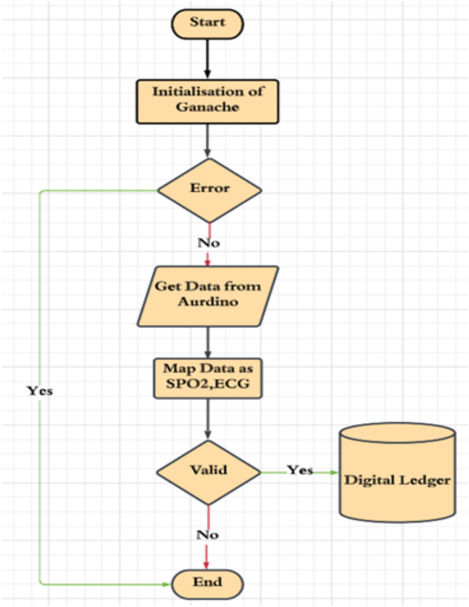


Fig 4. Smart contract for storing data

The smart contract in Fig 4 with the critical step of initializing Ganache, a local blockchain network commonly used for Ethereum development. This initialization process is pivotal for creating a reliable blockchain environment. If an error occurs during this initialization, the algorithm makes signaling a failure in setting up Ganache. Once Ganache is successfully initialized, the contract proceeds to acquire data from an IoT device. The obtained data is then intelligently mapped, associating specific parameters such as SPO2 (blood oxygen saturation) and ECG (electrocardiogram). Subsequently, a validation check is performed, determining the integrity and accuracy of the acquired data. In the affirmative validation scenario, where the validated data is securely recorded in a digital ledger. This ledger serves as an immutable and transparent repository, leveraging the principles of blockchain technology to ensure data integrity and traceability. With its integration of Ganache, IoT data acquisition, intelligent mapping, validation, and blockchain-based digital ledger, represents a robust foundation for secure and verifiable data management.

4.3 Designing of Enhanced Proof of Stake (ePoS)

The Enhanced Proof of Stake (ePoS) was integrated into the blockchain platform to secure and validate transactions. EPoS relies on participants' ownership of tokens to validate transactions, minimizing energy consumption while maintaining decentralization. The smart contract was modified to accommodate ePoS principles. Validators, holding tokens, were selected through a deterministic process. These validators were responsible for verifying transactions and adding blocks. This ensured that only participants with a vested interest in the network's integrity could contribute, bolstering security.

Steps in ePoS Algorithm

```
1. Start.
2. Nodes make transactions.
3. for each transaction from network participants do
4.     Add to the transaction set.
5. end for
6. All the nodes compete to become validators for the next block raising a stake.
7. Random node selection for validation.
8. if  all the transactions verified by validator then
9.     Publish the block.
10.     end if
11.     The stake still remains locked.
12.     if  nodes on the network confirm the new block then
13.         The validator gets the stake and the reward also block is accepted.
14.     else
15.         Validator losses stake and block is discarded.
16.     end if
17.     Update the ledger.
18.     The process again starts from step 2 to produce the new blocks.
19.     End
```

The above algorithm is implemented in solidity smart contract offers a foundational blockchain model, it introduces essential components such as transactions and blocks, along with a competitive validator selection process based on stake amounts. Users can submit transactions to the current block, and the validator's role is assigned to the participant with the highest stake. Following transaction validation, the validator publishes the block, receiving rewards upon success and losing the stake in case of failure. The smart contract provides a fundamental framework for proposed blockchain network.

The algorithm introduced in the research represents an improved iteration of the fundamental PoS algorithm. The primary distinction lies in the selection of validators. Unlike the standard PoS algorithm, which randomly designates validators without considering their stake, the proposed algorithm only permits nodes that have invested in the system to become validators. This adjustment enhances the algorithm's security by deterring nodes from engaging in dishonest conduct. Any node that acts unscrupulously faces the risk of losing their stake.

The following table 1 highlights the distinctions between the PoS and ePoS consensus algorithm.

Table 1. Comparison of PoS and ePoS

Algorithm / Points	**PoS**	**ePoS**
Authority of validation	All nodes in the network	Nodes that have maximum stake
Validator selection criteria	Randomly	Only nodes that have raised a stake
Transaction per second	Less	More

If a validator behaves dishonestly	The validator is not penalized	The validator loses their stake.

5. Result and Discussion

This research work evaluated the performance of blockchain ePoS consensus algorithm in the healthcare domain via simulation using Python with system INTEL i-5 processor and 8GB RAM. One hundred healthcare blockchain nodes were simulated in the proposed Ganache. The performance was evaluated in terms of the consensus time, throughput, and resource utilization.

5.1. Consensus time

Consensus time refers to the time it takes for a distributed network of nodes to agree on a single valid version of the blockchain. In a blockchain network, multiple nodes participate in validating and adding new blocks of transactions to the chain. Consensus mechanisms are protocols or algorithms that ensure all nodes in the network reach an agreement on the state of the blockchain [25]. The consensus time can vary depending on the consensus mechanism used in the blockchain network.

The following equation is used for calculating the consensus time

$$\boldsymbol{C(t) = \int (Tc(t) - Ti(t))dt}$$ ------- **Equation 1**

In this integral equation,

***C*(*t*)** represents the Consensus Time as a function of time.

Integrating the difference between the Time of Confirmation ***Tc*(*t*))** and the Time of Initiation ***Ti*(*t*))** with respect to time.

This equation essentially calculates the total Consensus Time over a given time interval by summing the difference between Time of Confirmation and Time of Initiation for all time points within that interval

The depicted graph illustrates the consensus time results, providing evidence that the ePoS algorithm required less time when compared to Xinyu Li's PoS [6] in the Local System across a range of nodes from 20 to 100.

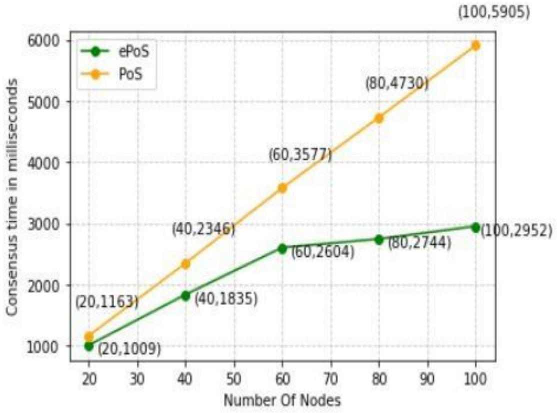


Fig 5. Comparison of Consensus time for PoS and ePoS

Table 2 and the associated graph display the consensus time results, demonstrating that the ePoS algorithm required approximately 2952ms for 100 nodes. This timeframe is notably shorter when contrasted with the PoS algorithms in Local System as presented in the works of Lina Ge[27] and Xinyu Li [6].

Table 2. ePoS Consensus Time comparison

	Lina Ge [27](2022) PoS	**Xinyu Li[6](2020) PoS**	**ePoS** **(Present research)**
Consensus Time **(milliSecs)** **for 100 nodes**	6400	5905	2952

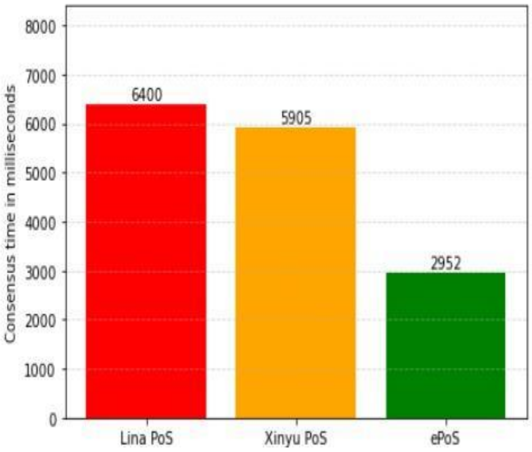


Fig 6. ePoS Consensus Time compared with others PoS work

In the investigation, the Xinyu Proof-of-Stake (PoS) consensus algorithm demonstrated a 5% reduction in consensus time compared to the Lina PoS protocol. Additionally, this analysis revealed a remarkable 50%

decrease in consensus time for Xinyu when tested with 100 nodes, surpassing Lina PoS. This significant improvement underscores the effectiveness of the modifications made to ePoS, positioning it as a more efficient consensus mechanism.

5.2 Throughput

Throughput in the context of blockchain refers to the number of transactions that a blockchain network can process within a given time frame. It's a measure of the network's capacity to handle a certain volume of transactions per second (TPS) or transactions per minute (TPM).

The Throughput is calculated using the following equation.

$$T\frac{x}{s} = \boldsymbol{Blocksize}/(\boldsymbol{T\ xsize} \times \boldsymbol{Blocktime}) \qquad \text{------}$$

Equation 2

T x/s - This to represent a rate or throughput, possibly transactions per second (Tx/s).

Block size - This be the size of a data block.

T xsize - This is the size of a single transaction.

Block time - The time it takes for a new block to be added to a blockchain.

Throughput plays a pivotal role in the design and assessment of blockchain networks, particularly in scenarios where efficiently processing a substantial volume of transactions is crucial [26]. Upon incrementing the number of nodes from 20 to 40, 60, 80, and 100, the analysis revealed throughputs of 141, 151, 169, 221, and 270 transactions per second, respectively. The accompanying graph illustrates that the proposed ePoS consensus algorithm attained a superior throughput due to its shorter consensus time when compared to Xinyu Li's PoS [6].

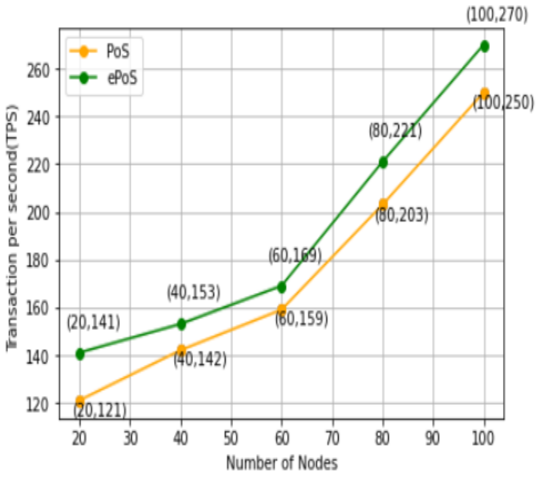


Fig 7. Comparison of Average throughput for PoS and ePoS.

Table 3 and the accompanying graph illustrate the Transaction Per Second (TPS) results, establishing that the ePoS algorithm achieved 270 transactions for 100 nodes. This figure surpasses the transaction rates of Cong T 28 PoS and Xinyu Li[6] PoS in Local System.

Table 3. ePoS Throughput comparison

	Cong T [28] -2019 **PoS**	Xinyu Li[6] -2020 **PoS**	**ePoS** **(Present research)**
Transaction per second (TPS) for 100 nodes	257	250	270

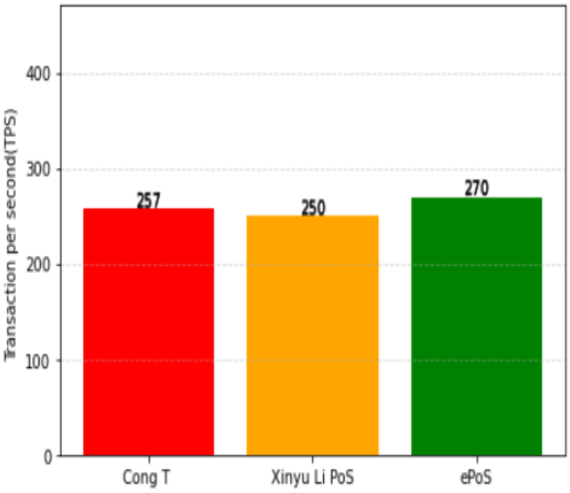


Fig 8. ePoS Throughput Compared with others PoS work.

During the examination, the proposed enhanced Proof-of-Stake (ePoS) consensus algorithm demonstrated significant enhancements, revealing an approximate 5% surge in throughput when contrasted with alternative PoS algorithms. Furthermore, in comparative analyses, the proposed ePoS consistently surpassed other algorithms, affirming its superior ability to achieve heightened throughput. These findings offer valuable insights into the comparative efficiency of consensus algorithms.

5.2. Resource utilization

Resource utilization in an IoT blockchain healthcare system depends on sensor data volume, network traffic, and computational needs. Efficient PoS consensus minimizes energy use, while Ganache's local testing reduces resource demand during development. Resource consumption in a blockchain network, particularly in terms of CPU and memory, plays a crucial role in determining the network's performance and efficiency. Efficient resource usage is essential to ensure that the network can handle a high volume of transactions while maintaining decentralization.

This work considers the CPU and Memory utilization.

5.3.1. CPU (Central Processing Unit) Utilization:

CPU utilization refers to the percentage of the CPU's processing power that is being actively used at any given time for blockchain nodes. In a blockchain network that supports smart contracts, CPU usage increases when executing complex code within smart contracts.

This can vary based on the complexity of the contracts being executed. Different consensus mechanisms have varying CPU requirements. The work demonstrated that CPU usage was very low for each node in the blockchain network.

The following equation is used to compute the CPU Utilization.

$$\boldsymbol{U(t) = T1 \times 100 \times \int 0T(A(t) - I(t))dt}$$ **-- Equation 3**

In this equation:

U(t) represents the CPU Utilization as a percentage at time t.

T is the total time interval over which you want to calculate the CPU utilization.

A(t) is the Total Active Time at time (t).

I(t) is the Idle Time at time (t).

The depicted graph illustrates that the CPU usage was 6, 9, 15, 7, and 10 percentage (%) respectively when the number of nodes increased from 20 to 40, 60, 80, and 100. In comparison to Xinyu Li's PoS [6] (2020), the proposed ePoS consensus method demonstrated lower consumption of CPU resources.

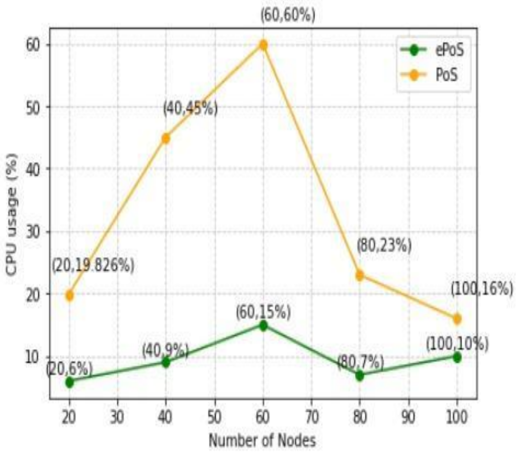


Fig 9. Comparison of CPU usage of blockchain nodes in PoS and ePoS

In the graph above, the number of nodes and CPU usage are displayed surrounding each point in parenthesis.

Table 4 and the accompanying graph present the results of CPU utilization, providing evidence that the ePoS algorithm exhibits lower CPU usage compared to Xinyu Li 6 PoS in the Local System across a range of nodes from 20 to 100.

Table 4. ePoS CPU utilization comparison

	Xinyu Li[6](2020) **PoS**	**ePoS** **(Present research)**
CPU utilization for 100 nodes (%)	16	10

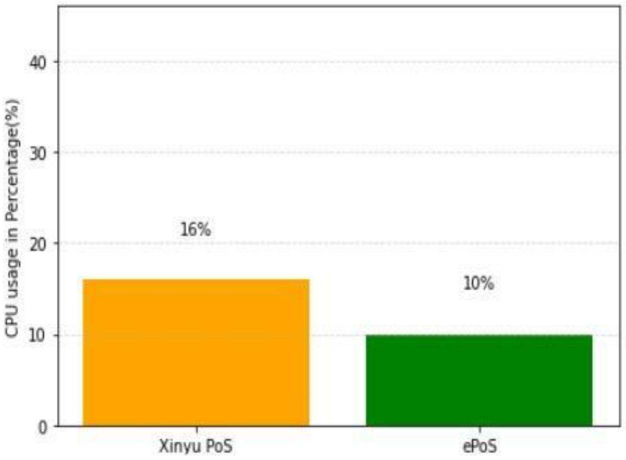


Fig 10. ePoS CPU Utilization compared with others PoS work

5.3.2. Memory Utilization

Memory utilization in an IoT healthcare blockchain system depends on data processing, encryption, and consensus algorithm. PoS and Ganache in development minimize CPU load, while production memory usage varies with network complexity and sensor data volume.

Memory utilization refers to memory used by each node during the consensus mechanism. Mining nodes may need extra memory for mining activities. During mining or transaction validation, temporary data structures are often used, contributing to memory usage.

Smart contracts and their associated data also reside in memory while being executed. Complex contracts with large amounts of data can consume significant memory.

The equation below is used to compute the memory utilization

$$\boldsymbol{M(t) = \int (T(t) - F(t))dt} \text{ -- \textbf{Equation 4}}$$

In this equation:

***M*(*t*)** represents Memory Utilization in kilobytes (KB) as a function of time *t*.

***T*(*t*)** represents Total Available Memory in kilobytes (KB) at time *t*.

***F*(*t*)** represents Free Memory in kilobytes (KB) at time *t*.

This integral equation calculates Memory Utilization as the cumulative difference between Total Available Memory and Free Memory over a given time interval, resulting in the total Memory Utilization over that interval.

The proposed system employed 259, 268, 279, 289, and 331 kilobytes of memory for 20, 40, 60, 80, and 100 nodes, respectively. It is noteworthy that the ePoS algorithm demonstrates reduced memory usage when compared to Xinyu Li's PoS [6] in the Local System across a spectrum of nodes from 20 to 100. The number of nodes and memory use are shown in parenthesis around each point in the graph below.

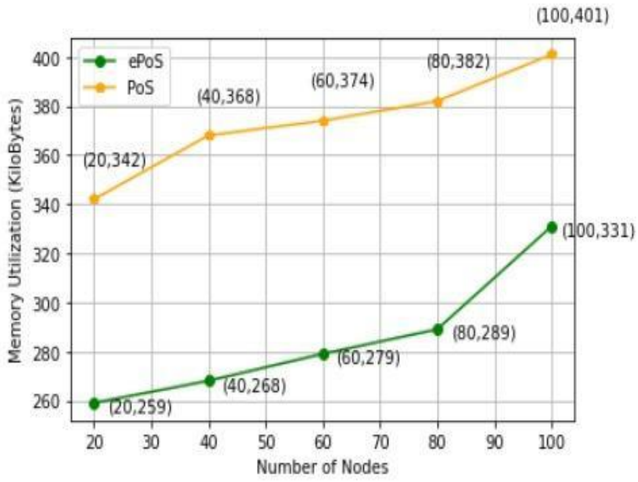


Fig 11. Comparison of Memory usage of blockchain nodes in PoS and ePoS

The outcomes of Memory usage presented in Table 5 and the corresponding graph below demonstrate that the ePoS algorithm utilized 331KB of memory for 100 nodes. This usage is notably lower than that observed in Xinyu Li's PoS [6] in the Local System.

Table 5. ePoS Memory utilization Comparison

	Xinyu Li[6](2020) **PoS**	**ePoS** **(Present research)**
Memory utilization (kb) for 100 nodes	401	331

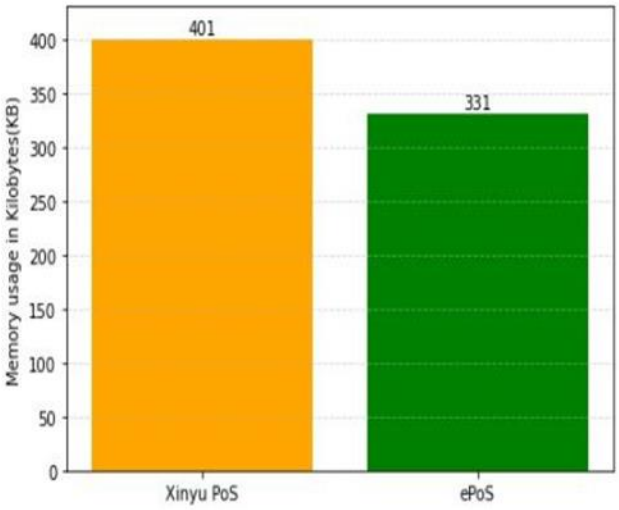
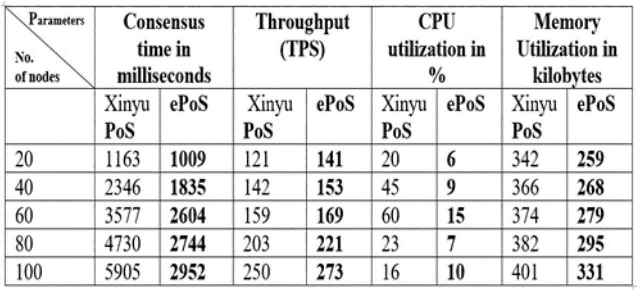


Fig 12. ePoS Memory Utilization with other PoS work

The investigation revealed a noteworthy accomplishment, highlighting an approximate 7% decline in network utilization when compared to Xinyu PoS. This reduction underscores the effectiveness of the proposed ePoS. Moreover, the comparative analyses consistently showcased the superior performance of the proposed method over Xinyu PoS concerning network utilization. These results provide valuable insights into the heightened efficiency achieved by the proposed consensus algorithm.

The presented table.6 offers a comprehensive evaluation aimed at demonstrating the superior performance of ePoS consensus algorithms in comparison to the established PoS consensus algorithm. This research focuses on enhancing the PoS consensus algorithm for the BIoT healthcare system and ultimately concludes that the ePoS consensus algorithm stands out as a more effective and innovative solution.

Table 6. Evaluation table



Parameters / No. of nodes	Consensus time in milliseconds		Throughput (TPS)		CPU utilization in %		Memory Utilization in kilobytes	
	Xinyu PoS	ePoS	Xinyu PoS	ePoS	Xinyu PoS	ePoS	Xinyu PoS	ePoS
20	1163	**1009**	121	**141**	20	**6**	342	**259**
40	2346	**1835**	142	**153**	45	**9**	366	**268**
60	3577	**2604**	159	**169**	60	**15**	374	**279**
80	4730	**2744**	203	**221**	23	**7**	382	**295**
100	5905	**2952**	250	**273**	16	**10**	401	**331**

6. Conclusion and Future Enhancements

The integration of the Enhanced Proof of Stake (ePoS) consensus algorithm into the Blockchain IoT Prototype represents a significant milestone in healthcare data management. By accelerating consensus mechanisms, optimizing resource utilization, and enhancing transaction throughput, ePoS opens up new frontiers for secure and efficient blockchain applications in the healthcare sector. This pioneering consensus algorithm not only addresses the challenges of traditional PoS but also sets the stage for a transformative era where blockchain technology can fully realize its potential in revolutionizing healthcare systems. The adoption of ePoS marks a crucial step toward fostering trust, ensuring data integrity, and unlocking innovative possibilities for the secure management of healthcare data on the blockchain. In the ever-evolving landscape of healthcare technology, the incorporation of the ePoS consensus algorithm signifies not just an advancement but a paradigm shift. Its ability to expedite consensus and optimize resource allocation not only addresses existing challenges but propels healthcare systems into a realm of heightened efficiency and security. The adoption of ePoS emerges as a beacon of progress, offering a robust foundation for the secure and streamlined management of healthcare data on the blockchain. This transformative leap not only meets the immediate needs of the industry but also lays the groundwork for a future where blockchain technology plays a pivotal role in shaping the future of healthcare.

Utilizing machine learning and AI algorithms in the suggested blockchain network can advance predictive analytics, automate the identification of diseases, and offer personalized treatment recommendations, ultimately enhancing patient care. The creation of smart contracts has the potential to automate and streamline various processes, including insurance claims, patient consent management, and the tracking of the supply chain.

Acknowledgment

I am extremely grateful to my research supervisor **Dr. Pushpa S.K** Professor, ISE, BMSIT&M for her continuous guidance in conducting the research work and in completing the paper writing.

I would like to thank my well-wishers and doctoral committee members during my work, **Dr. Manjunath T.N,** (Domain Expert-2-Internal) , Professor Dept. of ISE , BMSIT&M, Yelahanka Bengaluru-560064.and **Dr. Raghavendra S** , (Domain Expert-1-External) , (Assistant Professor) , Dept, of Information and Communication Technology, Manipal Institute of Technology, MAHE, MANIPAL. for their valuable and timely guidance in the smooth preparation of the paper.

I also thank the **Head of the department of CSE**, Fellow colleagues, Friends, Family members, students, and non-teaching staff for their moral support of BMS Institute of Technology and Management, Yelahanka, Bengaluru-560064

I express my gratitude to the **Head of the ISE Research Center**, the **Management, Principal, and Vice Principal** of BMS Institute of Technology and Management, Yelahanka, Bengaluru-560064

References

[1] Abid Haleem, Mohd Javaid, Ravi Pratap Singh, Rajiv Suman, Shanay Rab, “Blockchain technology applications in healthcare: An overview”,International Journal of Intelligent Networks Volume 2, 2021, Pages 130-139.

[2] Mostafa Haghi Kashani , Mona Madanipour , Mohammad Nikravan , Parvaneh Asghari , Ebrahim Mahdipour ,“A systematic review of IoT in healthcare: Applications, techniques, and trends”, Journal of Network and Computer Applications , Volume 192, 15 October 2021, 103164.

[3] Natalia Chaudhry,Muhammad Murtaza Yousaf, “Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities”,12th International Conference on Open Source Systems and Technologies (ICOSST),19-21 December 2018

[4] Xiaohong Deng, Kangting Li, Zhiqiang Wang, Juan Li, Zhiqiong Luo, “A Survey of Blockchain Consensus Algorithms”,International Conference on Blockchain Technology and Information Security (ICBCTIS), 11 August 2022.

[5] Sivleen Kaur, Sheetal Chaturvedi, Aabha Sharma, Jayaprakash Kar,“A Research Survey on Applications of Consensus Protocols in Blockchain”,Security and Communication Networks Volume 2021, Article ID 6693731, 22 pages.

[6] Xinyu Li; Jing Xu; Xiong Fan; Yuchen Wang; Zhenfeng Zhang, “Puncturable Signatures and Applications in Proof-of-Stake Blockchain Protocols”, IEEE Transactions on Information Forensics and Security, 11 June 2020.

[7] Md Julhas Hossain; Md. Amdadul Bari; Mohammad Monirujjaman Khan, “Development of an IoT Based Health Monitoring System for e-Health”, IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 26-29 January 2022.

[8] Caixiang Fan,Sara Ghaemi,Hamzeh Khazaei,Petr Musilek,“Performance Evaluation of Blockchain Systems: A Systematic Survey”,IEEE Access (Volume: 8),30 June 2020.

[9] Hoai Luan Pham, Thi Hong Tran, Yasuhiko Nakashima,“A Secure Remote Healthcare System for Hospital Using Blockchain Smart Contract”, IEEE Globecom Workshops (GC Wkshps),February 2019**.**

[10] Partha Pratim Ray, Dinesh Dash, Debashis De, Khaled Salah, Neeraj Kumar,**“**Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases”, IEEE Systems Journal · January 2020.

[11] K. Christidis, M. Devetsikiotis: “Blockchains and Smart Contracts for the IoT” , IEEE Systems Journal i VOLUME 4, 2016.

[12] Sorin Zoican,Marius Vochin,Roxana Zoican, “ Blockchain and Consensus Algorithms in Internet of Things”,IEEE Systems Journal, November 2018.

[13] Vishal Sharma , Niranjan Lal , “A NOVEL COMPARISON OF CONSENSUS ALGORITHMS IN BLOCKCHAIN”,Advances and Applications in Mathematical Sciences Volume 20, Issue 1, November 2020, Pages 1-13.

[14] Moamin A. Mahmoud 1,Mathuri Gurunathan 2,Ramona Ramli 1,Kazeem Alasinrin Babatunde 3 and Faisal Hadi Faisal,”Review and Development of a Scalable Lightweight Blockchain Integrated Model (LightBlock) for IoT Applications” ,https://doi.org/10.3390/electronics12041025, *Electronics* 2023, *12*(4), 1025.

[15] Wai Yan Maung Maung Thin; Naipeng Dong; Guangdong Bai; Jin Song Dong ,“Formal Analysis of a Proof-of-Stake Blockchain”, 2018 23rd International Conference on Engineering of Complex Computer Systems 30 December 2018

[16] Paul Schaaf, Filip Rezabek∗ , Holger Kinkelin∗,“Analysis of Proof of Stake flavors with regards to The Scalability Trilemma”, Network Architectures and Services, November 2021

[17] Iddo Bentov, Ariel Gabizon, Alex Mizrahi, “Cryptocurrencies without Proof of Work”, International Conference on Financial Cryptography and Data Security, Jan 2017

[18] Aggelos Kiayias ,Alexander Russell†, Bernardo David, Roman Oliynykov,“Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol”, Annual International Cryptology Conference, 29 July 2017

[19] Y. Gao and H. Nobuhara ,“A Proof of Stake Sharding Protocol for Scalable Blockchains”, APAN – Research Workshop 2017, June 24th, 2017

[20] DENIS STEFANESCU , LETICIA MONTALVILLO, PATXI GALÁN-GARCÍA , JUANJO UNZILLA , AND AITOR URBIETA ,”A Systematic Literature Review of Lightweight Blockchain for IoT”,IEEE Access,VOLUME 10, 2022.

[21] Cleverence Kombe, Mussa Dida, Anael Sam,”A review on IOT healthcare information systems and consensus protocol in blockchain”,International Journal of Advanced Technology and Engineering Exploration · December 2018.

[22] V Tamilselvi; Sri balaji; P Vigneshwaran; P Vinu; J. GeethaRamani, “IoT Based Health Monitoring System”, 6th International Conference on Advanced Computing and Communication Systems (ICACCS) ,06-07 March 2020.

[23] Niclas Kullig, Philipp Lämmel, Nikolay Tcholtcheva,”Prototype Implementation and Evaluation of a Blockchain Component on IoT Devices”,Procedia Computer Science Volume 175, 2020, Pages 379-386.

[24] Shivani Wadhwa; Gagandeep,”Lightweight Modified Consensus Approach in IoT Blockchain”,International Conference on Emerging Smart Computing and Informatics (ESCI),22 April 2022.

[25] Y. Supreet, P. Vasudev H., Pavitra,Mouna Naravani,D.G. Narayan,”Performance Evaluation of Consensus Algorithms in Private Blockchain Networks”,International Conference on Advances in Computing, Communication & Materials (ICACCM), 21-22 August 2020.

[26] Faiza Hashim; Khaled Shuaib; Farag Sallabi,”Performance Evaluation of Blockchain Consensus Algorithms for Electronic Health Record Sharing”, Global Congress on Electrical Engineering (GC-ElecEng),07 June 2022

[27] Lina Ge , Jie Wang, Guifen Zhang ,” Survey of Consensus Algorithms for Proof of Stake in Blockchain”, Security and Communication Networks May 2022

[28] CONG T. NGUYEN, DINH THAI HOANG, DIEP N. NGUYEN, DUSIT NIYATO, HUYNH TUONG, NGUYEN, AND ERYK DUTKIEWICZ, “Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities”, IEEE Systems Journal 2019.