Blockchain-Enabled Secure and Efficient Integration of IoT Devices: A Novel Approach for the Internet of Medical Things(IoMT)

Publisher: IEEE

Kamalika Bhowal All Authors

Abstract:
The research highlights the necessity of innovative blockchain solutions for improving scalability, energy efficiency, security, and speed in IoMT applications. Solana and Polygon, employing advanced consensus mechanisms like Proof of His-tory (PoH) and Delayed Proof of Stake (DPoS), offer superior transaction processing capabilities, reducing network congestion and energy consumption while ensuring data security. The study underscores how these platforms enhance real-time data processing and decision-making in healthcare, providing a more secure and efficient infrastructure for patient care. By comparing traditional blockchain solutions with newer technologies, the research presents a compelling case for adopting Solana and Polygon in IoMT systems. This adoption is poised to revolutionize the IoMT landscape, offering unparalleled scalability, security, and cost-effectiveness, ultimately improving patient care and healthcare outcomes. The findings suggest significant potential for future development in blockchain-enabled IoMT applications.

Published in: 2024 4th International Conference on Computer, Communication, Control & Information Technology (C3IT)

Date of Conference: 28-29 September 2024

DOI: 10.1109/C3IT60531.2024.10829426

Date Added to IEEE *Xplore*: 13 January 2025

Publisher: IEEE

ISBN Information:

Conference Location: Hooghly, India

SECTION I.
Introduction

In the modern era, there is a high demand for Internet of Things(IoT) and blockchain technologies in various aspects of everyday life. The IoT typically refers to a collection of decentralized services and the performance and functionality of these services depend on the efficiency of the servers. Therefore, it is crucial to enhance the performance of IoT devices to ensure smooth connectivity and collaboration with computing resources. Blockchain technology offers a solution to these challenges by providing decentralization, reliability, and security. Consequently, implementing blockchain in IoT systems can effectively enhance security and create a robust infrastructure. [1] In the landscape of technological advancements, healthcare devices have surged in popularity for their pivotal role in enabling constant patient-physician communication and seamless health monitoring within daily routines [2]. Leveraging IoT technologies, these devices have given rise to intricate networks of varying sizes, which aim to process patient data, yielding essential insights for well- informed healthcare decisions. Characterized by their intelligence, IoT networks interconnect a diverse array of digi-tally communicating objects, effectively facilitating information exchange and standardized device integration. Spanning functions from localization to tracking, monitoring, and object management, the encompassing term 'IoT' encompasses diverse applications [3]. Within the healthcare sector, IoT ap-plications harness sophisticated communication technologies, forging connections between healthcare providers and patients, and delivering value-added services. Among these, remote patient health monitoring and data analysis applications, powered by sensor data, offer indispensable support for both medical professionals and patients alike [4]. As a result, IoT takes on a transformative role in shaping the landscape of medical and healthcare information, even influencing processes such as transcription. In the realm of IoMT devices [5], [6], conventional blockchain solutions have emerged as stalwarts for securing and managing the extensive volumes of sensitive healthcare data generated by interconnected medical devices. Esteemed blockchains like Bitcoin and Ethereum have seamlessly integrated themselves into IoMT applications, capitalizing on their well-established infrastructure and robust security features. These blockchain implementations, commonly relying on PoW(Proof of Work) [7] or Proof of Stake and File (PoSF) algorithms,

bolster transaction validation and data integrity. Yet, the escalating presence of IoMT devices and the substan-tial real-time patient data they generate spotlight the demand for blockchain solutions that are not only efficient but also scalable. This need has prompted the evolution of newer blockchain algorithms, specifically tailored to surmount the unique challenges within the realm of IoMT, addressing con-cerns such as high energy consumption, transaction throughput limitations, and latency issues [8]. One promising alternative is the utilization of DAG technology, which offers a more scalable and lightweight approach compared to traditional blockchains. DAG-based blockchains, exemplified by IOTA's Tangle, have garnered attention in the IoMT sector. These blockchains employ a distinct consensus mechanism that elim-inates the dependence on miners or validators, resulting in swifter and feeless transactions. This proves advantageous for IoMT applications [9], [6]necessitating real-time data processing, microtransactions, and seamless device interoperability. Furthermore, DAG technology strengthens data protection compliance, enhancing privacy, security, and streamlined data exchange within the IoMT ecosystem. Additionally, newer blockchain algorithms like Proof of Authority (PoA) and DPoS have gained traction in IoMT applications due to their efficiency and reduced energy consumption. These algorithms rely on a trusted set of validators or block producers, reducing the need for resource intensive mining and facilitating faster transaction speeds. This is particularly beneficial for IoMT deployments that rely on real-time monitoring, data analy-sis, and timely decisionmaking for optimal patient care [10]. Solana is a high-performance blockchain platform designed for rapid transaction processing and scalability, making it an ideal choice for real-time data processing and high-throughput applications like the IoMT. This platform is well-suited for IoMT devices as it enables seamless real-time data exchange among interconnected medical devices, facilitating continuous monitoring. Its scalability ensures the ability to accommodate the increasing number of IoMT devices without sacrificing performance, thereby establishing a robust healthcare infras-tructure. In contrast, Polygon (formerly Matic Network) functions as a Layer 2 scaling solution built on top of Ethereum, addressing Ethereum's scalability challenges [11]. Particularly advantageous for IoMT, Polygon's Layer 2 approach enables IoMT devices to interact with Ethereum's ecosystem, bene-fiting from accelerated transaction speeds and reduced fees. This integration streamlines IoMT data into healthcare systems and Ethereum's smart contracts, promoting smooth data analysis, patient monitoring, and secure health data management. Both Solana and Polygon offer advanced security features for IoMT applications, leveraging blockchain's immutability and decentralized nature to ensure the security and tamper-proof nature of medical data generated by IoMT devices [12]. The transparent and auditable characteristics of blockchain technology also contribute to maintaining a reliable record of patient health data, enhancing data provenance, and aiding compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) [13]. Moreover, the developer-friendly nature of Solana and Polygon facilitates the creation of custom smart contracts and decentralized applications (Dapps) [14], [15] tailored to IoMT needs. This opens up possibilities for innovative solutions in healthcare, including patient-centric health data management platforms, decentral-ized telemedicine applications, and interoperable healthcare ecosystems[16]. The Introduction Section 1. Briefly introduces the concept of using Blockchain in IoMT whereas the Problem Statement Section 3, Highlights challenges in existing medical tech infrastructure, emphasizing secure data transmission in IoT. Introduces blockchain as a solution, but notes limitations like energy consumption, scalability, and consensus. So In the Methodology, Section 6 we have proposed a detailed research design and setup, involving IoT and gateway devices, along with blockchain platforms like Solana and Polygon. It Outlines the experiment workflow and theoretical frameworks. Result Analysis, Section 9. Discusses findings, comparing traditional blockchain with newer alternatives like Proof of History, DAG, and Delayed Proof of Stake. Considers factors like scalability, energy efficiency, security, speed, and cost. Finally in the Conclusion Section 10, Outlines future research and Development avenues, including refining blockchain algorithms, enhancing interoperability, integrating AI, and prioritizing user experience for maximum potential in healthcare.

SECTION II.
Problem Statement

Current medical technology infrastructures face significant challenges in ensuring secure, large-scale data transmission, particularly given the rising frequency of cybersecurity breaches. While Blockchain technology has emerged as a promising solution for secure data communication, it still grapples with issues such as energy management, limited computational power, and consensus inefficiencies. Traditional mechanisms like Proof of Work (PoW) in Bitcoin demand substantial energy and specialized hardware, limiting scalability. A novel approach, such as Proof of History (PoH), offers a solution by using cryptographically secure and verifiable timestamps to order transactions and blocks, making it both energy-efficient and secure. PoH is employed in platforms like Solana and Polygon, providing enhanced scalability and lower energy consumption compared to PoW and PoS. To improve IoMT integration, the following strategies are proposed: enhancing data security, optimizing blockchain for IoT devices, leveraging recent blockchain advancements for IoMT protection, and overcoming current adoption limitations. The proposed work focuses on analyzing infrastructure vulnerabil-ities, exploring blockchain's potential for IoMT, developing a secure decentralized framework, and assessing the frame-work's impact on security and efficiency.

SECTION III.
Literature Review

In this section, we delve into the recent advancements in the integration of blockchain technology with IoMT devices. The following table summarizes key studies highlighting the potential of blockchain in enhancing the security and privacy aspects of IoMT applications.

SECTION IV.
Theoritical Framework

The evolution of blockchain technology has been a fas-cinating journey, marked by key milestones, innovations, and shifts in focus. The development started with development of a cryptographically secured chain of blocks to timestamp digital documents, ensuring their immutability and authenticity. From the early conceptual foundations in the 1980s and 1990s, proposed by researchers like Stuart Haber and W. Scott Stornetta for cryptographically securing digital documents, to the water-shed moment with the introduction of Bitcoin in 2008–2009 by the pseudonymous Satoshi Nakamoto, blockchain technology has undergone a remarkable evolution. The 2010s saw the proliferation of alternative cryptocurrencies or “altcoins” like Litecoin, Ripple, and Ethereum[14], [17], each experimenting with different consensus mechanisms and introducing the concept of programmable blockchain through smart contracts. As the technology garnered attention, businesses began exploring its potential beyond cryptocurrencies, leading to the emer-gence of “Blockchain 2.0” platforms in 2015–2017, aiming to provide scalability, interoperability, and support for complex business processes. The Initial Coin Offering (ICO) boom in 2017 brought both funding potential and concerns about project legitimacy, while also highlighting scalability issues, particularly with Ethereum. Subsequently, the focus shifted towards private or permissioned blockchains for enterprises to address specific industry needs, exemplified by platforms like Hyperledger, Corda, and Quorum. The 2020s witnessed explosive growth in the decentralized finance (DeFi) sector and the rise of Non-Fungible Tokens (NFTs), revolutionizing traditional financial services and enabling the ownership and trading of unique digital assets. Ongoing developments include Ethereum's ambitious upgrade to Ethereum 2.0, which aims to transition to a more environmentally friendly con-sensus mechanism, as well as the pursuit of interoperability and cross-chain solutions by projects like Polkadot, Cosmos, and Avalanche to facilitate communication between different blockchains, envisioning a multi-chain future. The evolution of blockchain technology is ongoing, with ongoing efforts to address scalability, interoperability, sustainability, and the integration of emerging technologies like IoT and AI. As the technology continues to evolve, its impact on industries, finance, supply chain, healthcare, and more is likely to become even more profound[19]. A comparative analysis of traditional and recent technology based on Solana/Polygon is presented in the Table 2 based on important parameters such as scalability, energy consumption etc.

Table I Literature survey of blockchain technology with iomt devices.

Year	Authors	Title	Key Findings
2022	R.K. Garg, S.K. Singh, S.K. Rathore, S.K. Sharma	Blockchain Enabled Biometric Security in IoMT Devices	Proposed a secure blockchain-based architecture for IoMT-based healthcare applications that can provide decentralized and secure communication while taking into account the constraints listed above.
2022	S.K. Rathore, S.K. Sharma, R.K. Garg, S.K. Singh	Enabling Blockchain with IoMT Devices for Healthcare	Proposed a blockchain-based architecture for IoMT devices that can provide decentralized and secure storage of medical data.
2021	M. Boukhebouze, A. Yahiaoui, A. Ait-Mokhtar	Blockchain Solutions for IoMT Devices	Explored the capacity of blockchain technology to tackle the security and privacy issues associated with IoMT devices.
2021	A.K. Shukla, A.K. Singh	Blockchain Enabled IoMT and Security	Identified the security and privacy challenges of IoMT devices and discussed how blockchain technology can be used to address these challenges.
2017	Anatoly Yakovenko, Greg Fitzgerald, et al.	Solana: Introducing a Novel Design for a High-Performance Blockchain	Solana uses a unique combination of Proof-of-History and delegated Proof-of-Stake algorithms to achieve high throughput and low latency.
2019	Suman Jana, Soumyajit Chakraborty, et al.	S2HS- A blockchain-based approach for smart healthcare system	S2HS proposes a blockchain-based system for smart healthcare that provides data security, privacy, and traceability. It uses a two-level blockchain architecture with a private blockchain for internal entities and a public blockchain for external entities. S2HS also uses smart contracts to manage access to data and to automate workflows.
2020	Amirhosein Adavoudi Jolfaei, Farhad Aghili, et al.	A Survey on Blockchain-based IoMT Systems: Towards Scalability	The survey discusses the challenges and opportunities of blockchain-based IoMT systems and how to improve scalability. It recommends hybrid architecture, permissioned blockchain, and on-chain/off-chain storage.
2018	Ankit Kumar, Anju Sethi, et al.	Blockchain-based smart contracts for the IoMT in e-healthcare	The paper proposes a blockchain-based smart contract architecture for e-healthcare that can be used to automate workflows, track medical records, and manage payments and evaluates the performance of the proposed architecture and shows that it can achieve high throughput and low latency.
2021	Egala Bhaskara Santhosh, Ashok Kumar Pradhan, et al.	Fortified-Chain: A Blockchain Based Framework for Security and Privacy Assured IoMT With Effective Access Control	The framework uses a hybrid computing paradigm with a blockchain-based distributed data storage system (DDSS) to overcome the drawbacks of cloud-centric IoMT healthcare systems. The framework also introduces a decentralized selective ring-based access control (SRAC) mechanism to improve the security of the system and evaluates the performance of the proposed framework and shows that it can achieve high throughput and low latency.
2021	Bassam A. Y. Alqaralleh, Thavavel Vaiyapuri, Velmurugan Subbiah Parvathy et al.	Blockchain Assisted Secure Image Transmission and Diagnosis Model on the IoMT Environment	The model uses a combination of ECC encryption, NIS-BWT hash function, and DBN for image encryption and classification. The model is evaluated on a medical dataset and shows that it can achieve high accuracy and security.
2020	Ali Hassan Sodhro, Sandeep Pirbhulal, et al.	Towards Blockchain-Enabled Security Technique for Industrial Internet of Things Based Decentralized Applications	The paper proposes a blockchain-based security technique for IIoT-based decentralized applications. The technique uses a combination of random initial and master key generation, blockchain, and AHP for secure data delivery. The technique is evaluated on a simulation platform and shows that it can achieve high security and efficiency.

Table II Comparison between traditional blockchain technologies and solana/polygon

Parameters	Traditional Blockchain Technologies	Current Blockchain Technologies (Solana/Polygon)
Scalability	Limited scalability due to network congestion	High scalability with layer 2 scaling solutions
Energy Consumption	High energy consumption with PoW	Energy-efficient with PoS, PoH, DAG, and DPoS
Security	Transparent and secure, potential vulnerabilities	Enhanced security with advanced consensus mechanisms
Speed and Efficiency	Longer confirmation times	Fast transaction speeds enabling real-time processing
Cost Efficiency	Higher transaction fees	Cost-efficient with optimized consensus mechanisms

SECTION V.
Methodology

In this section, the research methods, approaches, and procedures employed to investigate and analyze the integration of blockchain with IoMT is researched [1]. Additionally, we will conduct a comparative analysis of Proof of History (PoH) and Proof of Work (PoW) consensus mechanisms to evaluate their suitability for IoMT applications.

A. Research Design

The amalgamation of blockchain technology with IoMT holds the promise of effectively addressing concerns related to security and privacy. We refer to this integration as “blockchain-enabled IoMT.” Figure 1 illustrates the architec-tural framework of blockchain-enabled IoMT, comprising four tiers:

1) The device layer,

2) The edge computing layer,

3) The blockchain network layer, and

4) The data analytics layer.

At the foundational tier of this multilayered structure, a vari-ety of IoMT devices, such as heat sensors, thermal cameras, wristband sensors, thermometers, and RFID tags, populate the device layer. Moving upwards, the edge computing layer materializes as a fusion of communication networks and edge computing infrastructure. This level encompasses edge computing nodes positioned at base stations, WiFi access points (APs), and IoT gateways, which handle the collection and initial processing of IoMT data. Additionally, the blockchain network layer plays a pivotal role as an intermediary, ensuring reliable management of diverse resources spanning the underlying layers.

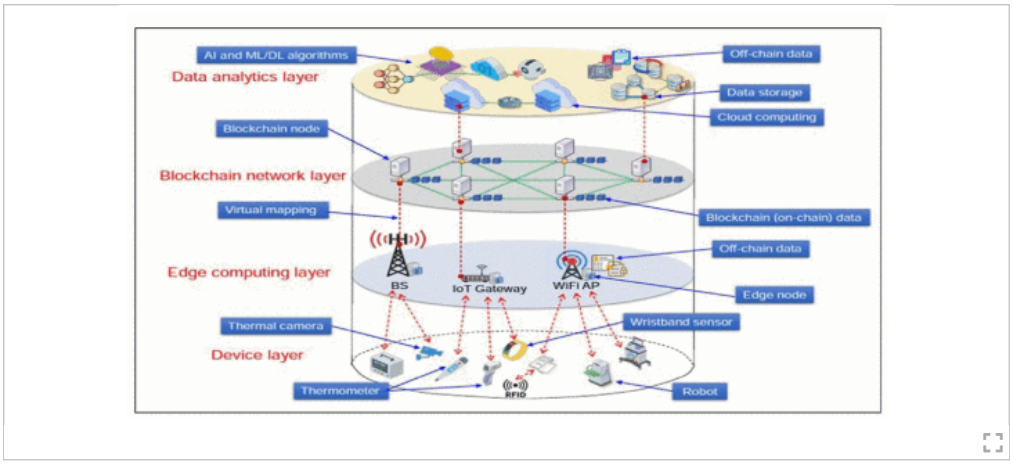

Fig. 1.
Architecture of blockchain-enabled IoMT consisting of device layer, edge computing layer, blockchain network layer and data analytics layer [2].

Initially, the data analytics layer encompasses several components: cloud computing resources, data storage servers, as well as artificial intelligence (AI), machine learning (ML), or deep learning (DL) algorithms. It's important to highlight that both the edge computing facilities within the edge computing layer and the entities within the data analytics layer are strate-gically aligned with nodes in the blockchain network layer. This strategic alignment serves a vital purpose in enabling a robust establishment of authentication and access control mechanisms across both the edge computing and blockchain network layers in a blockchain-enabled IoMT framework.

Transitioning to the topic of consensus mechanisms used in blockchain networks, it's essential to distinguish between Proof of History (PoH) and Proof of Work (PoW) based on specific parameters. These mechanisms, although part of blockchain networks, fulfill different roles and exhibit unique characteristics. To provide clarity, let's delve into a comparative analysis of PoH and PoW, elucidating how they differentiate from each other across various aspects is highlighted in Table 3.

Table III Comparative analysis of poh and pow

Parameters	PoH	PoW	Better
Consensus	Time-based consensus algorithm	Computational puzzle-based consensus algorithm	PoH
Scalability	Highly scalable, can handle high transaction rates	Scalability limitations as transaction rates increase	PoH
Energy Consumption	Low energy consumption	High energy consumption	PoH
Security	Provides strong security guarantees	Relies on computational power for security	PoH
Accessibility	More accessible to a wider range of devices	Requires specialized hardware (mining rigs)	PoH
Centralization	More decentralized and resistant to centralization	Centralized due to mining concentration	PoH
Speed	Fast confirmation times	Longer confirmation times	PoH
Cost Efficiency	More cost-effective	Expensive due to high computational requirements	PoH
Environment	Environmentally friendly	High carbon footprint due to energy consumption	PoH
Trust	Builds trust through verifiable timestamps	Trust based on computational proof of work	PoH

B. Experimental Setup

This experiment aims to validate the proposed method for securely and efficiently integrating IoT devices with blockchain technology within the context of the IoMT. The experimental setup involves both hardware and software components to facilitate the integration of Internet of Medical Things (IoMT) devices with a blockchain platform for secure data management and processing.

The Hardware Components used are:

IoMT Devices: Device 1: Medtronic Continuous Glucose Monitor (Model: Guardian Connect) with real-time glucose monitoring and Bluetooth 4.0 connectivity. Device 2: Philips Wearable Heart Rate Monitor (Model: Health Watch) equipped with an optical heart rate sensor and Bluetooth 4.1. Processing Units: CPU: ARM Cortex-A53, 1.2 GHz, Quad-core, 64-bit architecture for efficient processing of IoMT data. Memory: 4GB LPDDR4 RAM operating at 1600 MHz for smooth multitasking and data handling. Storage: 256GB NVMe SSD with PCIe Gen 3.0 interface for high-speed data storage. Network Interfaces: Ethernet: Intel 1219-V Gigabit Ethernet Controller providing 1 Gbps wired connectivity. Wi-Fi Mod-ule: Qualcomm Atheros QCA9377 supporting dual-band 2.4/5 GHz, 802.11ac wireless communication. Blockchain Nodes: Server: Intel Xeon E5-2620 v4 processor, with 32GB DDR4 RAM, a 1TB SSD, and a 10 Gbps Ethernet Interface for hosting blockchain nodes.

Software Components used are:

Operating System: Ubuntu 20.04 LTS with Kernel Version 5.4.0 for a stable and secure environment. Blockchain Plat-form: Hyperledger Fabric v2.2 utilizing the Practical Byzan-tine Fault Tolerance (PBFT) consensus mechanism for secure and reliable transaction processing. Programming Languages: Python 3.8.5 for scripting and automation. JavaScript (Node.js) 14.17.0 for backend development and blockchain integration. Development Tools: IDE: Visual Studio Code 1.58 for code editing and debugging. Build Tools: Docker 20.10.7 for containerization and Maven 3.6.3 for project management and build automation. Simulation Tools: MATLAB R2021a for algorithm development and data analysis. NS-3.29 for network simulation and testing. Security Libraries: OpenSSL 1.1.1k for implementing encryption protocols. Bouncy Castle 1.68 for additional cryptographic functions. Network Configuration:

Topology: A hybrid network consisting of both wired and wireless connections. Protocols: Utilization of HTTP/2 and MQTT for IoMT device communication, with TLS 1.2 employed for encryption to ensure secure data transmission. Data Management:

Database System: MongoDB 4.4, a NoSQL distributed database system, is used for storing and managing data. Data Handling: Collection Method: Real-time sensor data is collected via Bluetooth and Wi-Fi. Storage Mechanism: A hybrid approach is employed, with local SSD storage for real-time processing and AWS S3 for archival storage.

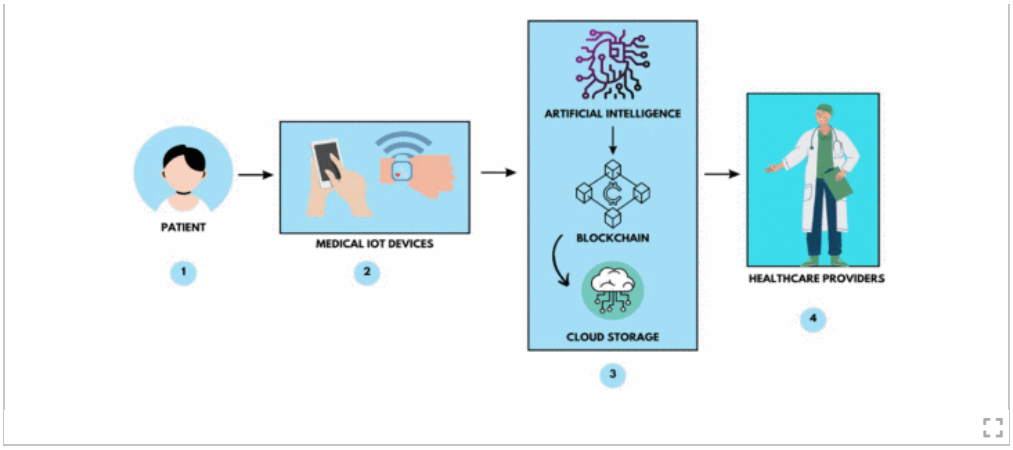

Fig. 2.
Proposed Implementation Setup of IoMT Devices in Blockchain

1) Medical Iot Devices
For the experimental purpose the IoMT devices are used, as depicted in Figure 2

1) **Wearable Health Trackers**: The devices shown in the Figure 2, are typically worn by individuals and collect data related to health and fitness. Examples include smartwatches, fitness bands, and heart rate monitors. These devices can track parameters such as heart rate, sleep patterns, steps taken, and calories burned.

2) **Medical Sensors**: Medical sensors are used to monitor vital signs and collect specific health-related data. Ex-amples include blood pressure monitors, glucose meters, pulse oximeters, and temperature sensors. These sensors can provide real-time data on blood pressure, blood sugar levels, oxygen saturation, and body temperature.

3) **Smart Medical Devices**: These are advanced medi-cal devices that can connect to a network and provide additional functionality. Examples include smart pill dispensers, smart inhalers, and connected medical equipment. These devices can help with medication management, asthma treatment, and remote monitoring of medical equipment.

4) **Implantable Medical Devices**: These devices are surgi-cally implanted inside the body and can wirelessly trans-mit data to external systems. Examples include pace-makers, implantable cardioverter-defibrillators (ICDs), and neurostimulators. These devices monitor and reg-ulate specific physiological functions and can transmit data such as heart rate, rhythm, and device performance.

2) Gateway Device
The gateway device (shown in Figure 2) serves as a pivotal component in this experiment, playing the role of an intermediary or bridge between IoT devices and the blockchain network. It facilitates seamless communication, data transfer, and transaction handling between the IoT devices and the blockchain. [3]

1) **Purpose**: The gateway device acts as an intermediary or bridge between the IoT devices and the blockchain network. It facilitates communication, data transfer, and transaction handling between the IoT devices and the blockchain.

2) **Hardware**: The gateway device can be a dedicated hardware device or a software-based solution running on a server or a computing device. It should have the necessary processing power, memory, and connectivity capabilities to handle the communication requirements of the IoT devices and the blockchain network [4].

3) **Communication Protocols**: The gateway device should support the relevant communication protocols used by the IoT devices, such as Wi-Fi, Bluetooth, Zigbee, or cellular connectivity. It should be able to receive data from the IoT devices, process it, and transmit it securely to the blockchain network.

4) **Data Encryption and Security**: The gateway device should implement robust security measures to ensure the confidentiality, integrity, and authenticity of the data transmitted between the IoT devices and the blockchain network. This may involve implementing encryption protocols, digital signatures, and secure communication channels.

5) **Data Pre-processing**: In some cases, the gateway device may perform data preprocessing tasks before transmitting the data to the blockchain network. This could involve data filtering, aggregation, or

anonymization, depending on the requirements and privacy concerns [5].

6) **Blockchain Integration**: The gateway device should be capable of interacting with the blockchain network. It should have the necessary software components or libraries to connect to the blockchain nodes, submit transactions, and retrieve data from the blockchain [6].

7) **Transaction Handling**: The gateway device plays a role in facilitating the creation and submission of transactions to the blockchain network on behalf of the IoT devices. It may include packaging the data received from the IoT devices into transactions, adding necessary metadata, and handling the transaction submission process [7].

8) **Monitoring and Management**: The gateway device should have monitoring and management capabilities to track the status and health of the connected IoT devices. This includes monitoring device connectivity, data transmission, and any errors or anomalies that may occur.

9) **Scalability**: Depending on the size and complexity of the IoMT network, the gateway device should be scalable to handle a large number of IoT devices and their data. This may involve load balancing, efficient data processing, and network optimization techniques.

Overall, the gateway device acts as a critical component in the secure and efficient integration of IoT devices with the blockchain network. It facilitates the seamless flow of data between the IoT devices and the blockchain, ensuring the reliability, security, and integrity of the IoMT system [8].

SECTION VI.
Software Setup

The figure 3 titled “Implementation of PoS in IoMT De-vices” offers a visual representation of the seamless integration of PoS blockchain technology within the realm of IoMT for healthcare applications. It portrays a system that harnesses the power of IoMT devices, including wearable health trackers and medical sensors, to remotely monitor patients' vital signs in real-time. This continuous data generation is meticulously observed, enabling the collection of real-time health statistics [7]. These valuable insights are securely transmitted and stored on a PoS-enabled blockchain network, known for its energy-efficient consensus mechanism. In this ecosystem, medical practitioners, denoted as “doctors,” have access to the real-time health data, allowing them to monitor patients and provide timely advice and interventions. Moreover, the figure underscores the significance of data integrity by illustrating medical practitioners uploading reports and essential patient information onto the blockchain network. This holistic approach enhances healthcare delivery, fosters remote patient care, and ensures the secure, tamper-proof management of critical health data [9].

Blockchain is composed of a series of blocks, as illustrated in Figure 4. Within this structure, all blocks, except the initial one (known as the genesis block), establish a direct connection with the preceding block through a retroactive reference, which takes the form of the hash value originating from the previous block. To elaborate, the hash value of block i is incorporated into block i + 1. Alongside this linkage, each block encompasses various additional data fields [3]. These fields encompass a timestamp, a cryptographic nonce (a unique random number utilized exclusively once), a root hash of all conducted transactions, and a root hash of all incorporated contracts. The unchanging root hash values allocated to transactions and contracts maintain a high degree of immutability. This robustness to alteration is due to the fact that even the slightest modification of a single bit could yield an entirely distinct hash value [10].

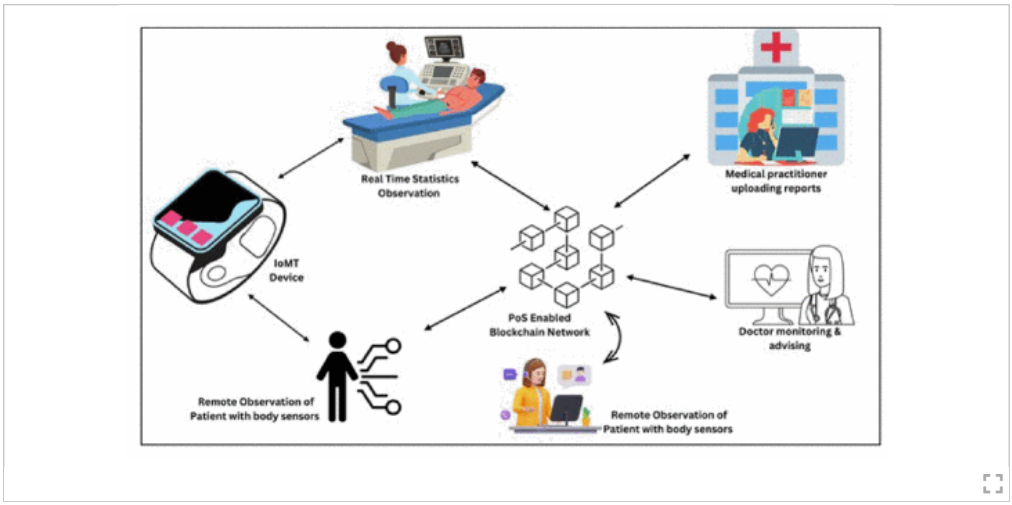

Fig. 3.
Implementation of PoS in IoMT Devices

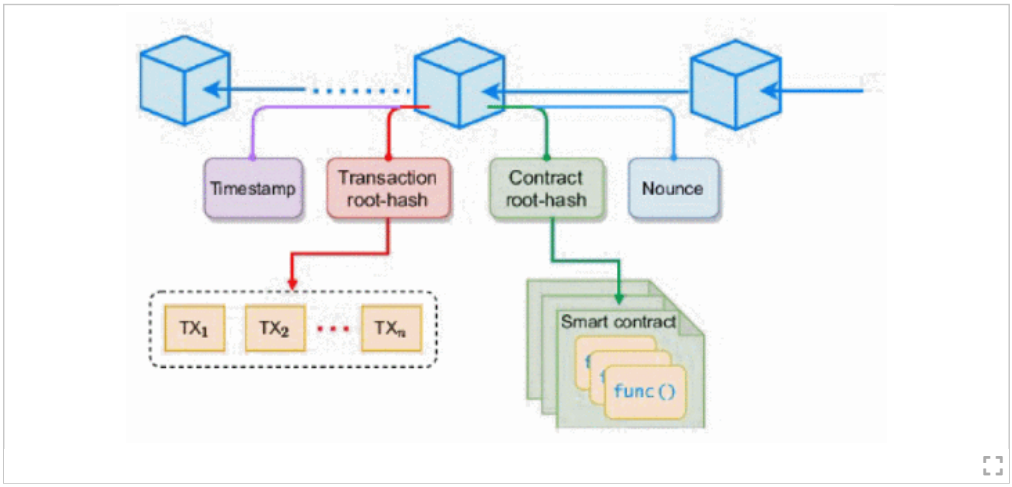

Figure 4:
Blockchain consisting of a number of blocks

SECTION VII.
Experiment Workflow

In this section, we outline the key components and objectives of our experimental workflow. The workflow serves as the foundation of our study, allowing us to systematically investigate the integration of blockchain technology with IoMT devices. Our approach aims to address crucial aspects of security, data management, and efficiency within the IoMT ecosystem [11]. In the evolving landscape of IoMT devices, the choice of underlying blockchain architectures plays a pivotal role in shaping the functionality and capabilities of these devices. Three notable architectures, Directed Acyclic Graph (DAG), Proof of History (PoH), and Delayed Proof of History (DPoH), have emerged as influential paradigms in the context of IoMT [7].

A. Dag Articheture

The study encompassed both categories of workloads, in-cluding workflows and fine-grained tasks, within the simulation configuration file. As depicted in Figure 5, the system in-terfaces are presented alongside the outcomes of the workflow directed acyclic graph (DAG) task graph during its execution within the system [12].

All tasks within this context are classified as workflows, with some tasks holding original data while others share their data for processing purposes. These tasks are all subject to limitations imposed by their preceding and succeeding tasks within the system.

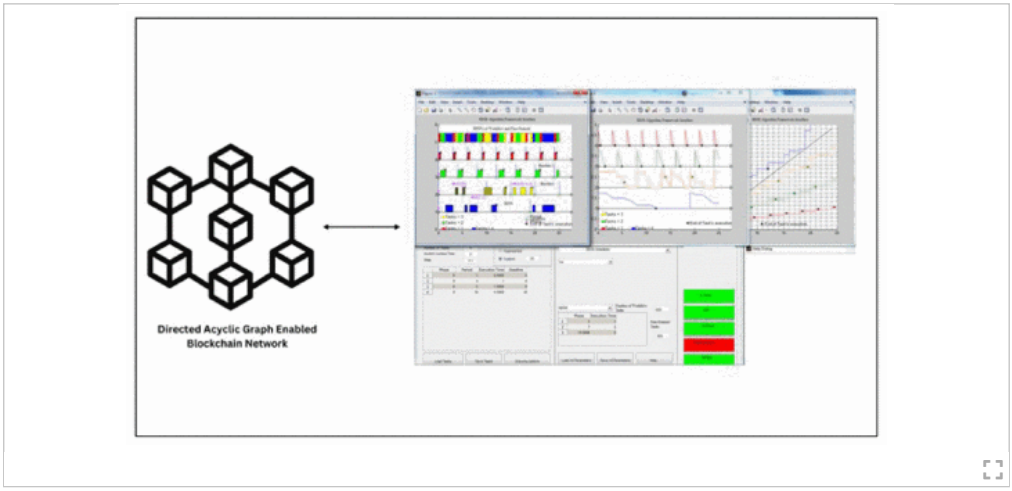

Fig. 5.
Directed Acyclic Graph architecture in IoMT Devices [13]

The work authored by Abdullah Lakhan, Qurat-ul-ain Mastoi, Mazhar Ali Dootio, Fehaid Alqahtani, Ibrahim **R**. Alzahrani, Fatmah Baothman, Syed Yaseen Shah, Syed Aziz Shah, Nadeem Anjum, and Muhammad Saddam Khokhar focuses on three distinct task types. [14] The initial phase involved the comprehensive analysis of all applications using DAG graphics, considering diverse task types. The primary application centered on annotating notations, exemplifying various task types annotated during the design phase. Subsequently, the IoMT workflow was transformed into a DAG graph. Within this representation, security tasks are denoted by blue nodes (e.g., local tasks), edge tasks are depicted by light yellow nodes, and remote tasks are symbolized by red nodes. Each task includes its respective execution time and communication time (measured in milliseconds and kilobytes) attributed to the precedence constraints in place [9].

B. Poh Architecture

As depicted in Figure 6, at any given instance, a system node assumes the role of the Leader, responsible for generating a Proof of History (PoH) sequence. This sequence not only establishes global read consistency across the network but also offers a verifiable measure of the passage of time.

The Leader's main role involves organizing user messages in a structured manner to facilitate efficient processing by other nodes in the system. This sequencing is crucial for maintaining the network's integrity. Additionally, the Leader is responsible for executing transactions on the current state stored in RAM memory. Afterwards, it shares both the transactions and a signature of the final state with the replication nodes, referred to as Verifiers.

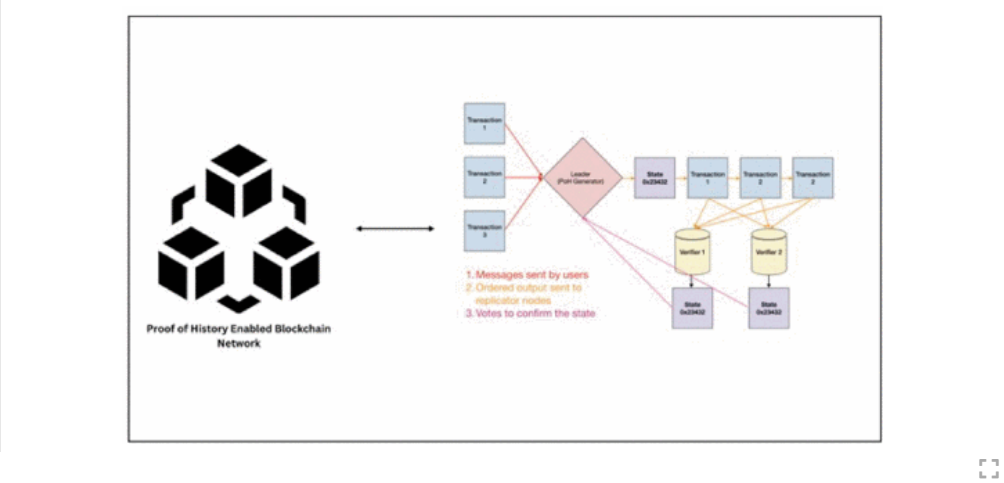

Fig. 6.
Proof of History architecture in IoMT Devices [15]

Verifiers have a significant role in implementing the same transactions on their local copies of the state. They then publicly release their computed signatures of the state as confirmations. These published confirmations serve as votes in the consensus algorithm, specifically in the PoS consensus mechanism iteration. This PoS mechanism not only facilitates the voting process but also aids in selecting the next PoH generator. It also serves as a deterrent against any validators engaging in malicious activities.

In the case of a failure experienced by a PoH generator, the process is activated to elect a new generator. The validator with the highest voting power is designated as the new PoH generator through this process.

The Proof of History mechanism empowers network Ver-ifiers to observe past events with a certain level of temporal certainty. As the PoH generator consistently produces a stream of messages, Verifiers are required to submit their state signatures within a specified time frame, typically 500 milliseconds, which can be further reduced based on network conditions. This comprehensive system architecture enables the infrastructure to achieve transaction rates of up to 710,000 transactions per second, leveraging modern hardware capabil-ities effectively.

SECTION VIII.
Result Analysis of the Proposed Work

Analyzing the diverse set of results obtained from our research endeavors, it becomes evident that alternative consensus mechanisms such as PoH, DAG structures, or DPoS present promising advantages over traditional technologies commonly employed in IoMT ecosystems, such as the conventional PoS mechanism.

Our investigation has shed light on the multifaceted aspects of these blockchain solutions, taking into account various factors that are paramount in the context of IoMT applications. These factors encompass scalability, energy consumption, se-curity, accessibility, transaction speed, and cost efficiency.

In conclusion, our research underscores the potential of PoH, DAG, and DPoS mechanisms, along with blockchain platforms like Solana and Polygon, to elevate the security and efficiency of IoMT applications. As we embark on this journey of discovery, it is clear that the fusion of blockchain technology with IoMT is poised to revolutionize healthcare, ushering in an era of enhanced data integrity, accessibility, and patient care. The road ahead is illuminated with opportunities for innovation, and we eagerly anticipate the transformative impact of blockchain on the IoMT landscape in the years to come.

SECTION IX.
Conclusion

In conclusion, Solana and Polygon represent a significant advancement for the Internet of Medical Things (IoMT), effectively addressing traditional limitations through innovative blockchain technologies. By utilizing consensus mechanisms like Proof of Stake (PoS), Proof of History (PoH), and Dele-gated Proof of Stake (DPoS), these platforms enhance energy efficiency, crucial for preserving IoMT device battery life and supporting sustainability goals. They also bolster security with advanced encryption, consensus models, and governance, ensuring the confidentiality and integrity of sensitive medical data. Despite these innovations, further research is needed to fully realize the potential of blockchain in IoMT. Key areas for exploration include optimizing scalability to support a growing network of devices, refining energy efficiency in resource-constrained environments, and advancing cryptographic techniques for data security. Additionally, improving accessibility and interoperability with existing healthcare systems, developing real-time IoMT applications, and identifying cost-effective strategies for widespread adoption are vital. The continued evolution of Solana and Polygon in these areas promises to revolutionize IoMT, offering unparalleled scalability, security, and efficiency in healthcare.

Authors
Figures
References
Keywords
Metrics