*Egypt. J. Chem.* Vol. 67, SI: M. R. Mahran, pp. **1891 - 1900** (2024)

**Egyptian Journal of Chemistry**

**http://ejchem.journals.ekb.eg/**

# Integration of IoT and Blockchain for Medical Records and Health Information-An Updated Review For The Diagnosis of Chronic Diseases: Diabetes as a Case

**Shahd Alhusain Mohammed Mussiry, Hanan Ibrahim Omar Baydhi, Rehan Othman Ibrahim Jaber, Ghada Salem Khamis Alyusuf, Yasmine Yahya Ahmed Barakat, Yasir Ali Jaber Ageeli, Zahra Aalwi Taha Alsafi, Awatif Mudhaya Hussain Mahbu, Muaddiyah Ahmed Yahya Jarba, Hanan Abdo Ahmad Breik, Rehab Abdo Ahmad Breik, Salah Khlief Almotairi, Fahad Mushabbab Alqahtani**

*Ministry of Health, Saudi Arabia*

**Abstract**

**Background**: The integration of the Internet of Things (IoT) and Blockchain (BC) in healthcare has been transformative, particularly for managing Electronic Health Records (EHRs). IoT devices, including wearable sensors, generate vast amounts of personal health data, while BC ensures secure, immutable, and efficient data management. However, security, privacy, and interoperability challenges continue to hinder their widespread adoption.

**Aim**: This paper aims to provide an updated review on integrating IoT and BC for medical records, with a focus on addressing security concerns, improving interoperability, and developing efficient frameworks for healthcare applications. The present study aims to evaluate the role of blockchain technology in the diagnosis and monitoring chronic diseases. Diabetes was evaluated using biochemical Markers.

**Methods**: A systematic review of existing literature on IoT, BC, and EHR systems was conducted. The study analyzed the security risks of IoT integration into healthcare, reviewed the potential of BC in mitigating these risks, and proposed a novel BC-based IoT-EHR framework.

**Results**: The review found that while IoT devices enhance patient monitoring and data collection, they introduce significant privacy and security vulnerabilities. BC's tamper-proof and decentralized structure offers an ideal solution for securing EHRs generated by IoT devices. However, the computational constraints of IoT devices and the complexity of BC consensus mechanisms present challenges. The paper proposes a BC-based IoT-EHR framework that addresses these limitations while ensuring secure data storage, transaction integrity, and compliance with regulations like HIPAA and GDPR. Blockchain technologies have a great role in chronic diseases diagnosis and management.

**Conclusion**: The integration of IoT and BC holds promise for transforming healthcare data management. Despite challenges related to computational power and interoperability, BC can significantly enhance the security and privacy of IoT-enabled EHR systems, ensuring safe and efficient healthcare delivery.

**Key Words**: Internet of Things (IoT), Blockchain (BC), Electronic Health Records (EHR), Security, Diagnosis, Privacy, Healthcare, Interoperability, Consensus Mechanisms, and Framework.

.

## 1. Introduction

The Internet of Things (IoT) is a concept that promotes the interconnection of various devices to the internet. It encompasses the use of software, sensors, actuators, and connectors that enable the connection, data collection, and data transmission among vehicles, home appliances, and other devices embedded with electronic systems [1]. In parallel, blockchain (BC) technology focuses on ensuring infrastructure reliability, immutability, and trustworthiness. BC operates as a distributed database characterized by its encrypted ledger, comprising a chain of blocks that record validated transactions. Each block is cryptographically linked to its predecessor, contains transaction data, and is assigned a consolidated hash code. Upon the completion of a transaction, a new block is appended to the chain, thereby continuously expanding the BC [2].

The healthcare sector, particularly electronic health records (EHRs), has also been significantly influenced by IoT and BC technologies. Managing and utilizing the vast amounts of personal health data generated through routine healthcare operations remains a challenge. Wearable devices and other monitoring tools produce extensive health-related data, much of which is inaccessible, non-standardized, and difficult to exchange or interpret across systems. The integration of IoT and BC technologies has propelled exponential growth within healthcare, enabling advancements in data handling and operational efficiency. However, the increasing use of IoT devices introduces heightened security and privacy concerns, and research uniting these technologies remains limited [3][4]. Security risks in the healthcare industry, particularly with IoT integration, require targeted attention. For instance, a study [5] reviewed IoT-based healthcare systems and application areas, emphasizing the heterogeneity of IoT sensors and suggesting cloud architecture as a solution to interoperability issues. It also highlighted privacy vulnerabilities inherent to IoT and cloud systems. Further analysis [6] explored IoT applications in healthcare, revealing significant privacy and

*Corresponding author e-mail: shahdmussiry@hotmail.com (**Shahd Alhusain Mohammed Mussiry**)
Receive Date: 19 December 2024, Revise Date: 28 December 2024, Accept Date: 31 December 2024
DOI: 10.21608/ejchem.2024.345798.11013

security concerns. Cryptographic mechanisms for securing IoT systems were also evaluated, but challenges due to device heterogeneity were noted. Centralized cloud structures exacerbate these issues, as they are susceptible to various attacks [7]. Additional research [8] reviewed security standards such as the Health Insurance Portability and Accountability Act (HIPAA) and demonstrated the role of BC in addressing security and EHR standardization.

Several studies have analyzed architectures for IoT-based healthcare, including cloud- and fog-based systems, highlighting challenges such as latency, fault tolerance, energy efficiency, security, and interoperability [9]. Resource constraints in IoT nodes limit the applicability of traditional cryptographic techniques, prompting a shift toward cloud-based structures for processing tasks. Nevertheless, the centralized nature of cloud systems introduces vulnerabilities to cyberattacks. Regulations like HIPAA and the General Data Protection Regulation (GDPR) demand robust compliance mechanisms, as non-adherence incurs significant penalties [10][11]. Managing identity and granting user control over data within conventional centralized frameworks remains a challenge [12]. Blockchain technology offers transformative potential in healthcare by providing a peer-to-peer system with global consensus, ensuring that validated transactions remain immutable. BC's intrinsic properties—such as tamper-proofing, traceability, security, and anonymity—make it a robust solution for healthcare applications. However, its computationally intensive operations pose limitations when applied to resource-constrained IoT devices [13][14]. Studies suggest that BC encryption can enhance healthcare communication networks, connecting various stakeholders while ensuring data accuracy and immutability. Yet, the computational demands of BC consensus mechanisms remain a challenge for IoT integration [15][16].

Recent research highlights BC's capacity to address security challenges in IoT-EHR frameworks, emphasizing the need for tailored solutions to meet healthcare's unique demands. The primary contribution of this paper is the proposal of a BC-based IoT-EHR framework designed to provide secure and interoperable health record storage. This framework supports efficient data transactions and storage while addressing IoT-specific limitations, such as energy and computational constraints. By reviewing existing BC consensus mechanisms and their suitability for IoT-EHR systems, this study identifies optimal approaches for enhancing security and functionality in healthcare [17][18][19]. A systematic review of related works underscores the gaps in current research, particularly concerning consensus mechanisms for IoT-EHR systems. While several studies have explored BC's healthcare applications, they often fall short of addressing resource constraints in IoT environments or proposing comprehensive frameworks. This paper bridges this gap by analyzing prominent consensus mechanisms and introducing a novel BC-based IoT-EHR framework to advance secure and reliable healthcare data management.

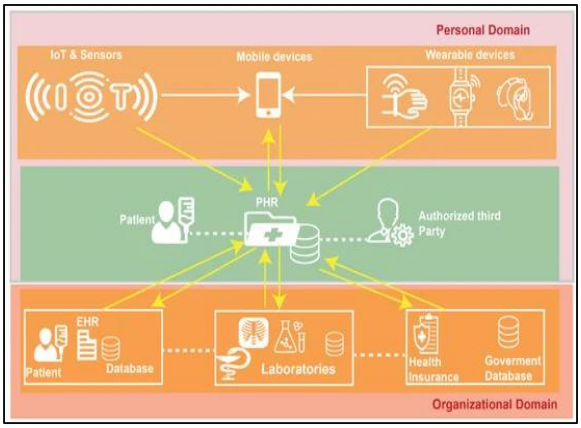


**Figure 1:** Structure of IoT-EHR system.

**Summary of Related Works**

Existing studies have explored various facets of BC and IoT applications in healthcare. For example, research [5] reviewed IoT healthcare systems, focusing on EHR and sensor integration challenges. Another study highlighted IoT's security and privacy concerns, proposing cryptographic solutions despite device heterogeneity limitations. Similarly, [8] examined security standards like HIPAA and the implications for healthcare data management. However, none comprehensively reviewed BC consensus mechanisms for IoT-EHR integration, which is the core focus of this study. This paper distinguishes itself by presenting a tailored BC-based IoT-EHR framework that overcomes interoperability and resource constraints while ensuring secure, reliable, and compliant data management. It evaluates consensus mechanisms based on adaptability, energy efficiency, and e-health support, addressing critical gaps in existing literature and paving the way for future research in this domain.

**Electronic Health Record (EHR) System**

The Electronic Health Record (EHR) system serves as a repository of patients' electronic health information. A subset of this information, stored within the Personal Health Record (PHR), encompasses healthcare-related data managed by patients themselves. This data is often obtained from wearable devices operated by patients, who may subsequently share it with healthcare providers. The fundamental goal of the EHR system is to enhance the security, privacy, and accessibility of stored data. It ensures that information is exchanged exclusively between authorized users, such as medical professionals, who are permitted access to facilitate accurate diagnoses [31,32]. EHR systems are invaluable for machine learning and data analysis due to their ability to store vast amounts of data, making them integral to research efforts aimed at predicting diseases like COVID-19. The integration of Internet of Things (IoT) devices and wearables significantly contributes to these systems by collecting and uploading essential data into EHR and PHR platforms. This integration supports the delivery of personalized healthcare services and continuous health monitoring, thereby improving overall healthcare outcomes [33].

**Internet of Things (IoT)**

The healthcare sector has encountered numerous challenges in recent decades, primarily due to escalating healthcare costs, population growth, and a shortage of caregivers. These challenges were exacerbated during the global spread of COVID-19, which highlighted issues related to the exchange and management of medical data. A

healthcare system involves a complex network of hospital collaborations, advancements in medical diagnostics, coordination across medical institutions, and the collection of patient information, either directly or via interconnected devices and sensors. The Internet of Things (IoT) refers to a network of physical devices, objects, or individuals equipped with unique system identifiers (UIDs), enabling them to communicate and exchange data. IoT systems operate similarly to humans and computers on the internet, with devices being assigned internet protocol addresses to facilitate data transmission. The technology finds application across domains requiring data collection and sensing from diverse sources, demonstrating its versatility and transformative potential [8].

**Security Challenges Related to IoT in EHR**

IoT devices face significant security challenges, particularly concerning end-to-end data protection across various domains. As IoT-enabled networking among appliances and devices is relatively novel, security measures are often absent from the initial design of these products. A notable vulnerability arises from the use of default or hardcoded passwords, which, despite periodic updates, remain susceptible to infiltration [34,35]. Additionally, IoT devices are constrained by limited computing capabilities, impeding the implementation of robust security protocols. Many IoT devices, such as temperature and humidity sensors, lack advanced encryption settings or other sophisticated security mechanisms. These devices typically do not receive security updates or patches throughout their operational lifecycle. From a manufacturer's perspective, integrating advanced security features can increase production costs, delay development, and affect device functionality [36]. Most IoT devices currently utilize a server-client model, where authenticated devices connect to centralized cloud servers with extensive processing and storage capacities. This setup allows devices to communicate over the internet, regardless of proximity, but necessitates the establishment of numerous communication linkages and extensive device networking. These requirements significantly inflate costs for large-scale IoT networks. Furthermore, the reliance on centralized cloud servers introduces a vulnerability to single-point failures, highlighting the need for robust security measures to protect IoT nodes against physical tampering and data breaches. While various techniques exist to safeguard IoT devices, many are overly complex and incompatible with resource-constrained devices with limited computational power [37,38].

**Blockchain (BC)**

Blockchain (BC) represents an immutable digital ledger that records data in a decentralized manner, eliminating the need for a trusted central authority. By enabling secure engagement among entities, BC maintains an ever-expanding set of interconnected data blocks. These blocks, accepted through cryptographic protocols, are linked to previous and subsequent blocks, forming a continuous chain. Participating entities can read, write, and protect these data blocks from tampering using consensus mechanisms [39]. This structure supports decentralized data management and transactions [40,41]. BC also facilitates self-executing smart contracts, reducing reliance on centralized authorities. Among the platforms leveraging BC for smart contracts, Ethereum stands out as the most prominent [32]. In the context of EHR applications, BC requires specific features, which are crucial for ensuring security and functionality [42].

**Types of Blockchain**

Blockchain is categorized into three main types based on its consensus mechanisms:

- **Public BC**: This type allows unrestricted participation in the BC network. Participants can freely join or leave, function as miners, or operate as standard BC nodes without requiring authorization. All participants enjoy equal access, and incentives are provided to encourage active engagement.
- **Consortium BC**: This form restricts governance and consensus mechanisms to a select group of nodes, offering controlled participation.
- **Private BC**: Managed and administered by a specific entity, private BCs require users to obtain authorization from relevant authorities to participate. Transactions are confidential and are not disclosed to the public. Furthermore, private BCs typically have faster block generation rates and can process more transactions compared to public or consortium BCs.

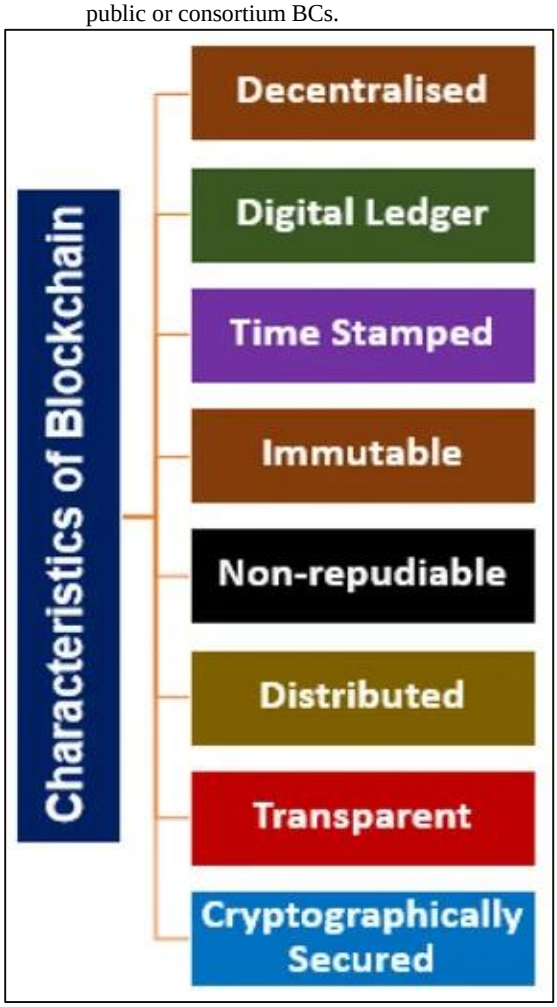


**Figure 2:** Characteristics of Blockchain.

**Blockchain and IoT in EHR**

The Internet of Things (IoT) enables seamless connectivity among devices using the internet. Through integrated electronics, hardware inputs, and internet connectivity, IoT devices can interact, allowing remote monitoring and control [44]. BC complements IoT by providing a secure and reliable framework for the stringent requirements of IoT networks in the following ways:

1. **Secure Communication**: BC offers a robust platform for secure communication between all connected devices.
2. **Network Security**: It ensures the protection of data stored within IoT systems against potential cyber threats.

**Benefits of BC and IoT Integration in EHR**

The integration of BC and IoT within EHR systems delivers multiple advantages, outlined as follows:

- **Privacy and Anonymity**: BC utilizes public-key cryptography to maintain anonymity. Digital identities specific to transactions conceal the actual identities involved in IoT applications that manage sensitive data [44].
- **Smart Contracts**: These self-executing contracts are automatically triggered once predefined conditions are met. For instance, Ethereum-based BC can facilitate payments upon the delivery of specific products or services [45].
- **Auditability**: BC ensures comprehensive audit logs, recording who accessed what information, through which system, and for what purpose. Time-stamping all operations across the data lifecycle further strengthens security and accountability [46,47].
- **Trustworthiness**: By enabling data sharing across IoT infrastructures under multiple organizations, BC enhances trust, thereby improving the quality of services provided by these organizations [48,49].

**Security Features**

- **Privacy**: BC limits access to authenticated members only, ensuring confidentiality. Combining BC with other cryptographic mechanisms further enhances privacy [50].
- **Integrity**: Data recorded on BC cannot be altered by unauthorized entities, guaranteeing its accuracy during transmission.
- **Availability**: Information access is restricted to legitimate users, ensuring consistent availability while preventing unwarranted denial of resources.
- **Accountability**: All entities involved are monitored, audited, and held accountable for their actions.

**DDoS Mitigation**

BC, in conjunction with smart contracts, can create collaborative frameworks to detect and mitigate Distributed Denial of Service (DDoS) attacks. Transactions powered by BC make it nearly impossible for attackers to launch malware or use IoT devices as botnets for DDoS attacks. Additionally, stringent monitoring of outgoing traffic prevents DDoS messages from propagating through IoT networks [42].

**Blockchain Application in IoT-Based EHR**

Blockchain (BC) has been effectively integrated into Internet of Things (IoT)-enabled Electronic Health Records (EHR) systems to ensure secure communication and storage of health records generated by IoT sensors. Numerous researchers have proposed BC frameworks for IoT-based EHR systems, with key contributions summarized below. These frameworks provide solutions for patient safety, data management, and secure data sharing. For instance, a BC-based storage system for data generated by IoT healthcare devices was introduced by [51], incorporating a virtual patient agent (PA) to outline BC capabilities.

In [51], a consortium BC framework was suggested, wherein data blocks are verified by a group head before being added to the chain. Data are stored off-chain in cloud storage, enabling efficient management and analysis of Internet of Medical Things (IoMT) data. A private BC framework was proposed by [52], focusing on secure on-chain storage within hospitals. This approach utilizes advanced hashing technologies to encrypt confidential patient information during transactions, ensuring data security and reliability. The use of Ethereum-based BC frameworks is notable in several studies. In [53], a private Ethereum-based BC platform was developed for IoMT data management, storing health records off-chain on external servers. Smart contracts control data access for participants such as patients, clinics, and research institutions. Similarly, [54] proposed a public Ethereum BC system that integrates InterPlanetary File System (IPFS) for off-chain data storage, facilitating secure communication between patients and healthcare providers. In [55], a private Ethereum BC was employed with a proof-of-medical-stake consensus mechanism, using IPFS to manage access control for IoMT applications. Further advancements include a Hyperledger Fabric BC system proposed by [56], designed for remote health monitoring. This private BC system employs on-chain storage and validates transactions through smart contracts supporting Byzantine Fault Tolerance. In contrast, [57] introduced MedChain, a consortium-based BC platform addressing challenges in securely recording medical device-generated data blocks. MedChain ensures immutable storage of time-series medical data and supports efficient data sharing.

In [58], a custom private BC platform for IoMT data analysis and remote patient monitoring was introduced. This system replaces traditional consensus mechanisms like proof-of-work with a cluster-head-based verification approach, ensuring efficient connectivity and data transmission. Similarly, [59] designed a cloud-based IoMT framework to monitor neurological disorders, integrating Ethereum BC to securely share and transfer data between healthcare providers and patients. The overarching benefits of these frameworks include enhanced privacy, reliable data sharing, and secure storage of critical medical information. For example, the integration of smart contracts in [54] and [55] ensures confidentiality and precise access control, while IPFS enables scalable storage solutions. Moreover, the adoption of private and consortium BC systems as seen in [53], [57], and [58] highlights the importance of tailored blockchain architectures in addressing specific IoMT and EHR requirements. Collectively, these studies underscore the potential of blockchain technology to revolutionize IoT-based healthcare systems by ensuring data security, fostering interoperability, and facilitating seamless management of EHRs.

**Comparative Analysis of Blockchain Consensus Mechanisms for IoT-Based EHR**

A consensus mechanism is a fundamental element in evaluating the efficiency of any blockchain (BC)-based system. Although numerous consensus mechanisms exist, their applicability to IoT-based Electronic Health Records (IoT-EHR) systems varies significantly due to differing resource requirements. This

section provides a comprehensive overview of key consensus algorithms suitable for IoT-EHR applications, highlighting their unique characteristics, adaptability, and relevance to e-healthcare services. Proof of Work (PoW) is a consensus algorithm that relies on solving computationally intensive cryptographic puzzles, making verification straightforward despite the complexity of solving the problem. Although PoW is widely adopted across platforms, its high resource requirements render it less practical for healthcare systems involving IoT devices [61]. Leased Proof of Stake (LPoS) addresses centralization issues in PoS by enabling low-balance nodes to lease contracts and share benefits, thereby improving e-health service quality [62]. Delegated Proof of Stake (DPoS), an evolution of PoS, allows network participants to elect delegates for block verification, making it highly applicable to electronic health scenarios requiring efficient verification processes [63].

Proof of Importance (PoI) extends PoS by incorporating node balance and credibility metrics, enhancing network efficiency. In healthcare, this mechanism can leverage healthcare professionals' credibility for informed patient decision-making [64]. Practical Byzantine Fault Tolerance (PBFT) involves collaboration among nodes to reach consensus, requiring two-thirds of nodes to agree. While its tolerance for malicious nodes is limited, it is suitable for healthcare applications due to its reliability in secure environments [65]. Proof of Activity (PoA) combines PoW and PoS, where transactions are verified through a dual-phase process. However, its lengthy delay makes it unsuitable for IoT and e-healthcare systems [66]. Delegated Byzantine Fault Tolerance (dBFT) refines PBFT by selecting representative nodes for consensus. Despite its potential, its application in IoT-based BC healthcare frameworks remains underexplored [67]. Proof of Capacity (PoC), an upgraded version of PoW, supports large data set recording but is inadequate for IoT due to its resource-intensive nature, though it may be applied to other health-specific programs [68].

Proof of Stake (PoS) is a widely adopted mechanism that randomly selects nodes for mining without relying on coin production rewards. Miners are compensated through transaction fees, making PoS a reliable and adaptable choice for healthcare systems [69]. Conversely, Proof of Burn (PoB) involves sending coins to irreversible addresses, making it more suitable for cryptocurrency systems. Its economic model and coin-burning mechanism make it inappropriate for IoT and e-healthcare applications [70]. Proof of Trust (PoT) offers equal participation opportunities in crowdsourcing activities, utilizing subjective logic algorithms, time stamps, and digital signatures to enhance block node unpredictability. PoT ensures validity, fairness, and security, making it a promising candidate for IoT-EHR systems [61,71]. Finally, Proof of Luck (PoL) executes real-time protocols for Gateway Agreement, providing data tolerance and encryption digests for input validation. PoL employs SHA-256 to generate replicated data digests, which are particularly useful for IoT-based healthcare systems [63,72]. In summary, the selection of an appropriate consensus mechanism for IoT-EHR systems depends on factors such as adaptability, accessibility, and energy efficiency. While mechanisms like PoS, PoI, and PoT show significant promise for e-healthcare applications, others like PoA and PoB remain less practical due to resource-intensive or economic constraints. Each mechanism must be evaluated within the context of specific healthcare requirements to ensure secure and efficient integration.

**Blockchain-Framework:**

The Blockchain-Based Framework for IoT-EHR is an innovative approach integrating blockchain technology with the Internet of Things (IoT) to enhance the electronic health record (EHR) system. This framework offers several advantages over traditional healthcare systems. It ensures the privacy and traceability of IoT-based patient EHRs, safeguarding against data tampering or corruption. It enhances the security of EHR data and enables patients to grant or revoke permissions for data access. Moreover, the framework facilitates collaboration among healthcare organizations and pharmaceutical companies for clinical trials and drug development through a publicly accessible ledger database. Additionally, it reduces operational costs while improving interoperability, universal accessibility, and reliability.

**Framework Overview**

The proposed blockchain-based IoT-EHR framework integrates IoT devices into the EHR ecosystem. It can also be extended to unify other healthcare facilities requiring seamless integration of personal health records and patient monitoring. The framework comprises three main layers:

1. **EHR Layer:** This layer serves as the healthcare provider interface, allowing various healthcare organizations to collaborate and share specific healthcare records irrespective of their storage types.
2. **Blockchain (BC) Layer:** Acting as an intermediary, the BC layer translates records into a unified format using an interface. It incorporates components like smart contracts, storage policies, an EHR manager, a consensus mechanism, and IPFS storage. These elements facilitate processing and secure storage of records while ensuring interoperability. The PoT consensus mechanism validates new records before storing them on the blockchain, and smart contracts enable automated execution for transaction processing.
3. **IoT-Based Patient Monitoring Layer:** Sensors monitor patient data, such as blood pressure, EMG, ECG, and glucose levels. This data is processed via the BC layer for storage.

**User Interface Layer:** Users interact with the system through an interface that allows them to enter or view records in a standardized format, regardless of storage formats.

**Operational Workflow**

The system follows a structured process:

- Healthcare providers maintain EHRs in heterogeneous formats, processed by the BC layer for interoperability and security.
- The BC layer authenticates and verifies records before storage in EHR systems, ensuring no direct user access to EHRs.
- IoT sensors collect patient data, which is transferred to the BC layer via an IoT server. This data is processed using smart contracts and stored securely.
- Newly sensed data undergoes validation through a consensus mechanism and is stored in IPFS

storage. Older records are hashed and stored for immutability.

- An identical EHR copy is stored in IPFS storage and EHR systems to enhance record interoperability.

**Algorithms for System Operations**

Three algorithms exemplify system functionality:

1. **Algorithm 1: Oxygen Saturation Analysis:** This algorithm monitors oxygen saturation levels, triggering alerts if levels fall below 94%.
2. **Algorithm 2: Adding New EHRs:** The algorithm outlines a mechanism for securely adding new EHR records to the blockchain using a suitable consensus mechanism like PoT.
3. **Algorithm 3: Viewing EHR Data:** Depending on user roles (e.g., doctor or general user), this algorithm defines access levels for viewing patient EHRs. Doctors can access all attributes, whereas other users have restricted access.

**Security Analysis**

The framework leverages blockchain's inherent security features, addressing key aspects such as:

1. **Privacy:** Blockchain's decentralized nature and elliptic curve cryptography (ECC) protect against privacy breaches and man-in-the-middle attacks. Digital signatures and session keys ensure data confidentiality and patient identity verification.
2. **Data Integrity:** Record integrity is maintained through hashing and validation via the consensus algorithm. Access control mechanisms verify user eligibility before granting record access.
3. **Availability and Defense Against DDoS Attacks:** The framework mitigates DDoS attacks through node authentication and two-factor authentication mechanisms. Blockchain-based identity frameworks provide additional safeguards.
4. **Authentication and Access Control:** Smart contracts ensure role-based access control. Re-encryption keys linked to user credentials allow authorized entities to decrypt specific EHR data, maintaining robust access security.

This blockchain-based IoT-EHR framework represents a transformative step in enhancing data privacy, security, and interoperability in healthcare systems, ensuring efficient and reliable management of electronic health records.

**Future Directions**

The implementation of blockchain (BC) technology in Internet of Things (IoT)-based electronic health records (EHRs) presents a range of challenges that warrant further exploration and research.

- **Resource Constraints:** IoT systems often operate with limited memory and processing capabilities, posing significant challenges for blockchain integration. The computational demands associated with BC, especially for tasks like mining blocks, exceed the capacity of resource-constrained IoT devices. Addressing this disparity is critical for enabling effective deployment.
- **Bandwidth Limitations:** Blockchain's decentralized architecture relies on collaboration among network nodes to verify transactions. However, the constrained bandwidth typical of IoT devices at the end-device layer can impede the functionality of BC-based applications. To ensure seamless operation, edge devices must be equipped to manage the heightened bandwidth demands of blockchain technology.
- **Connectivity Challenges:** In blockchain ecosystems, all nodes must remain interconnected and adhere to predefined communication protocols. While this characteristic facilitates integration with IoT devices, it also introduces heightened vulnerability to security threats. Strengthening connectivity protocols is imperative to mitigate such risks.
- **Memory Limitations:** The public blockchain technologies commonly employed involve transaction fees, which serve as incentives for peers engaged in block mining. However, the unique requirements of healthcare data—characterized by regular analysis and storage—introduce significant memory management challenges. The accumulation and storage of extensive health data across numerous patients could exacerbate memory constraints, necessitating innovative solutions.
- **Compliance with GDPR:** The General Data Protection Regulation (GDPR) emphasizes the transparent acquisition, processing, and storage of personal data, enabling individuals to reclaim control over their information. Compliance with GDPR simplifies data protection measures and reduces costs for organizations. In healthcare, adherence to GDPR and the Health Insurance Portability and Accountability Act (HIPAA) is essential for minimizing privacy risks associated with patient data [73].

Continued research in these areas is crucial for overcoming the barriers to integrating blockchain into IoT-based EHRs while maintaining compliance with regulatory frameworks.

**IoT, Blockchain, and Chronic Diseases:**

Remote patient monitoring has emerged as one of the most prevalent uses of IoT devices in healthcare. These devices enable the automatic collection of health data such as heart rate, blood pressure, and body temperature from patients who are not physically present at healthcare facilities. This eliminates the need for patients to visit medical providers or manually measure and record their health metrics. Once collected, the data is transmitted to software platforms that both patients and healthcare professionals can access. Algorithms can analyze this data to generate alerts or recommend treatments. For instance, if an IoT sensor detects an abnormally low heart rate, it can trigger an alert to prompt timely intervention by healthcare providers. However, the major concern surrounding remote monitoring devices is safeguarding the sensitive data they collect, ensuring both their security and privacy.

For individuals with diabetes, monitoring glucose levels has historically been a cumbersome process. Manual testing is not only inconvenient but also fails to capture continuous fluctuations in glucose levels, as it provides results at a single point in time. IoT-enabled glucose monitoring devices offer a solution by automatically tracking glucose levels continuously. This removes the need for manual record-keeping and helps detect abnormal glucose levels promptly. Alerts can be sent to patients, notifying them of critical changes, which ensures timely

intervention and better management of the condition. Monitoring heart rates, especially for patients with cardiac issues, has its own challenges. Traditional periodic checks are insufficient for detecting rapid or unexpected heart rate changes, and continuous monitoring in healthcare settings often requires patients to remain tethered to wired machines, limiting mobility. Modern IoT devices address these limitations by offering portable and wireless heart rate monitoring solutions that allow patients to move freely while being continuously observed. Although achieving perfect accuracy remains a challenge, most current devices provide highly reliable results, typically exceeding 90% accuracy.

For patients with respiratory conditions like asthma or chronic obstructive pulmonary disease (COPD), sudden attacks can occur without warning. IoT-connected inhalers are designed to mitigate these risks by tracking the frequency of attacks and analyzing environmental data to identify potential triggers. These devices can also notify patients if they leave their inhalers behind, reducing the risk of experiencing an attack without access to necessary medication. Additionally, connected inhalers help ensure correct usage, alerting users if they administer the medication improperly. Continuous tracking of mood and depression symptoms has traditionally been challenging due to its subjective nature. While healthcare providers can inquire about a patient's emotional state during visits, this method relies heavily on self-reporting, which may not always be accurate. IoT devices equipped with mood-monitoring capabilities address this issue by analyzing physiological data such as heart rate and blood pressure to infer mental states. Advanced devices can even monitor eye movements for further insight. While these tools do not guarantee absolute accuracy in detecting mood changes or depression symptoms, they offer a valuable supplement to traditional mental health assessments. The integration of IoT in surgical procedures has paved the way for robotic-assisted surgeries, which involve deploying small, internet-connected robotic devices inside the human body. These robots enable surgeons to perform intricate and precise operations that might otherwise be challenging or impossible using only human hands. By enhancing surgical accuracy and control, IoT-driven robotic surgery represents a significant advancement in modern healthcare.

**Blockchain in the Diagnosis of Diabetes Using Biochemical Aspects**

Blockchain technology is revolutionizing healthcare systems, particularly in securely managing data for chronic diseases like diabetes. The diagnosis and monitoring of diabetes largely depend on critical biochemical markers such as blood glucose levels, glycated hemoglobin (HbA1c), insulin levels, and lipid profiles. These biochemical indicators are collected through advanced diagnostic tools, laboratories, and continuous glucose monitoring (CGM) devices. Blockchain plays a pivotal role in ensuring that these highly sensitive data points are securely stored, managed, and shared between patients, healthcare providers, and diagnostic centers.

One of the primary benefits of blockchain technology in diabetes diagnosis is its ability to provide secure and tamper-proof storage for biochemical data. As IoT devices and diagnostic tools collect glucose and HbA1c measurements, blockchain can encrypt and store this data in decentralized ledgers. This ensures the integrity of the data, preventing unauthorized access or alterations. Healthcare providers can trust that the biochemical test results reflect accurate and unmodified information, which is essential for reliable diabetes diagnosis and monitoring. Blockchain also enables decentralized and transparent sharing of biochemical data. Traditionally, fragmented healthcare systems can hinder efficient communication between laboratories, clinics, and patients. Blockchain addresses this challenge by providing a unified platform where biochemical data, including glucose and insulin levels, can be shared securely in real time. Healthcare providers can access the patient's biochemical history when authorized, leading to faster diagnosis and timely interventions. Patients also benefit from this system as they retain control over their health data, authorizing access only when necessary, which enhances privacy and trust.

Smart contracts further enhance the role of blockchain in diabetes diagnosis by automating specific processes based on predefined conditions. For example, if a patient's glucose or HbA1c levels surpass a particular threshold, the blockchain system can automatically notify healthcare providers or recommend follow-up tests. This eliminates manual errors and ensures that patients receive timely care. Additionally, smart contracts can link laboratory results to treatment plans, creating a seamless process for managing diabetes. Moreover, blockchain technology supports the longitudinal monitoring of biochemical data. Diabetes is a progressive condition that requires continuous monitoring to detect changes over time. By securely storing historical biochemical data, blockchain allows healthcare providers to track trends in glucose levels, HbA1c readings, and lipid profiles. This long-term visibility enables clinicians to identify early warning signs of diabetes or monitor the effectiveness of treatment strategies, improving patient outcomes.

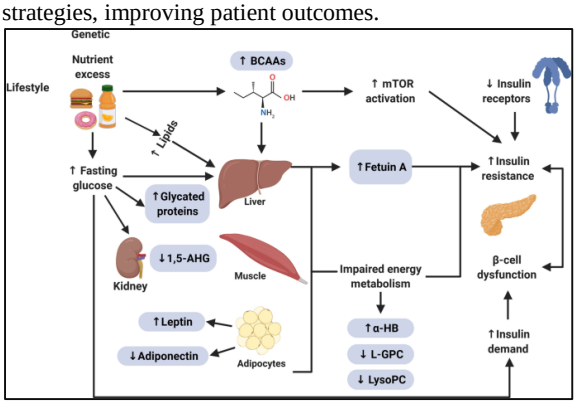


**Figure 3**: Diagnostic Biochemical Markers of Diabetes Mellitus.

Beyond diagnosis and monitoring, blockchain facilitates research and predictive analytics in diabetes care. Aggregated biochemical data stored on blockchain networks can be anonymized and used for large-scale studies, helping researchers identify patterns and correlations between biochemical markers and diabetes risk. Machine learning models integrated with blockchain systems can analyze this data to predict diabetes onset or progression, enabling more proactive care. In conclusion, blockchain technology offers a secure, efficient, and transparent framework for managing biochemical data in diabetes diagnosis and care. By addressing challenges such as data privacy, interoperability, and accuracy, blockchain ensures that healthcare providers can make informed decisions based on reliable biochemical data. This integration not only improves the diagnosis and monitoring of diabetes but also empowers patients to take control of

their health information while contributing to advancements in diabetes research and predictive care.

**Conclusion:**

The integration of the Internet of Things (IoT) and Blockchain (BC) technologies in healthcare has introduced a paradigm shift in the way medical records and health information are managed. IoT-enabled devices such as wearable sensors play a pivotal role in capturing real-time health data, which can be used for continuous monitoring and personalized care. However, the exponential growth of these devices has created substantial challenges in terms of data security, privacy, and interoperability. These challenges are amplified by the heterogeneity of IoT devices, which are often resource-constrained and incapable of supporting traditional cryptographic mechanisms. Blockchain technology, with its decentralized and immutable nature, has emerged as a promising solution to address these challenges. By ensuring that medical records are tamper-proof and auditable, BC not only improves the security and privacy of health data but also enhances trust among various stakeholders, including patients, healthcare providers, and insurers. The use of BC's consensus mechanisms provides a means to verify data integrity and ensures that all parties have access to accurate, up-to-date information. The proposed BC-based IoT-EHR framework introduced in this study addresses the inherent limitations of both IoT and BC technologies. By optimizing the consensus mechanisms for energy efficiency and computational feasibility, this framework enhances the security of medical records while reducing the operational burden on IoT devices. Additionally, the framework supports compliance with regulatory standards like HIPAA and GDPR, ensuring that data management practices adhere to legal requirements.

Despite the promising potential of this integration, several challenges remain. The computational demands of BC consensus mechanisms, particularly in resource-constrained IoT environments, require further optimization. Moreover, the interoperability between various IoT devices and BC platforms remains a critical issue, as seamless data exchange is essential for effective healthcare delivery. Further research is necessary to develop lightweight consensus protocols that are more suitable for IoT devices without compromising security or efficiency. In conclusion, the combination of IoT and Blockchain in healthcare systems offers significant benefits, especially in securing medical records and facilitating real-time data exchange. As technology continues to evolve, the integration of these technologies will undoubtedly play a pivotal role in shaping the future of healthcare by improving patient care, enhancing data privacy, and streamlining healthcare operations. However, continued efforts are needed to address the computational and interoperability challenges to unlock their full potential.

**References:**


1. Rahmani, M.K.I.; Shuaib, M.; Alam, S.; Siddiqui, S.T.; Ahmad, S.; Bhatia, S.; Mashat, A. Blockchain-Based Trust Management Framework for Cloud Computing-Based Internet of Medical Things (IoMT): A Systematic Review. *Comput. Intell. Neurosci.* **2022**, *2022*, 9766844.
2. Alam, S.; Shuaib, M.; Khan, W.Z.; Garg, S.; Kaddoum, G.; Hossain, M.S.; Zikria, Y. Bin Blockchain-Based Initiatives: Current State and Challenges. *Comput. Netw.* **2021**, *198*, 108395.
3. Khubrani, M.M.; Alam, S. A Detailed Review of Blockchain-Based Applications for Protection against Pandemic like COVID-19. *Telecommun. Comput. Electron. Control* **2021**, *19*, 1185–1196.
4. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On Blockchain and Its Integration with IoT. Challenges and Opportunities. *Futur. Gener. Comput. Syst.* **2018**, *88*, 173–190.
5. Selvaraj, S.; Sundaravaradhan, S. Challenges and Opportunities in IoT Healthcare Systems: A Systematic Review. *SN Appl. Sci.* **2020**, *2*, 139.
6. Nazir, S.; Ali, Y.; Ullah, N.; García-Magariño, I. Internet of Things for Healthcare Using Effects of Mobile Computing: A Systematic Literature Review. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 1–20.
7. Pradhan, B.; Bhattacharyya, S.; Pal, K. IoT-Based Applications in Healthcare Devices. *J. Healthc. Eng.* **2021**, *2021*, 6632599.
8. Ratta, P.; Kaur, A.; Sharma, S.; Shabaz, M.; Dhiman, G. Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives. *J. Food Qual.* **2021**, *2021*, 7608296.
9. Naresh, V.S.; Pericherla, S.S.; Murty, P.S.R.; Sivaranjani, R. Internet of Things in Healthcare: Architecture, Applications, Challenges, and Solutions. *Comput. Syst. Sci. Eng.* **2020**, *35*, 411–421.
10. Awotunde, J.B.; Jimoh, R.G.; Folorunso, S.O.; Adeniyi, E.A.; Abiodun, K.M.; Banjo, O.O. Privacy and Security Concerns in IoT-Based Healthcare Systems. In *The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 105–134.
11. Mustafa, M.; Alshare, M.; Bhargava, D.; Neware, R.; Singh, B.; Ngulube, P. Perceived Security Risk Based on Moderating Factors for Blockchain Technology Applications in Cloud Storage to Achieve Secure Healthcare Systems. *Comput. Math. Methods Med.* **2022**, *2022*, 6112815.
12. Reegu, F.A.; Abas, H.; Hakami, Z.; Tiwari, S.; Akmam, R.; Muda, I.; Almashqbeh, H.A.; Jain, R. Systematic Assessment of the Interoperability Requirements and Challenges of Secure Blockchain-Based Electronic Health Records. *Secur. Commun. Netw.* **2022**, *2022*, 1953723.
13. Zulkifl, Z.; Khan, F.; Tahir, S.; Afzal, M.; Iqbal, W.; Rehman, A.; Saeed, S.; Almuhaideb, A.M. FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs. *IEEE Access* **2022**, *10*, 15644–15656.
14. Bigini, G.; Freschi, V.; Lattanzi, E. A Review on Blockchain for the Internet of Medical Things: Definitions, Challenges, Applications, and Vision. *Futur. Internet* **2020**, *12*, 208.
15. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of Things Security: A Top-down Survey. *Comput. Netw.* **2018**, *141*, 199–221.
16. Butpheng, C.; Yeh, K.-H.; Xiong, H. Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review. *Symmetry* **2020**, *12*, 1191.
17. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for Healthcare Data Management: Opportunities, Challenges, and Future

Recommendations. *Neural Comput. Appl.* **2021**, *34*, 11475–11490.
18. Khezr, S.; Moniruzzaman, M.; Yassine, A.; Benlamri, R. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. *Appl. Sci.* **2019**, *9*, 1736.
19. Zhao, S.; Li, S.; Yao, Y. Blockchain Enabled Industrial Internet of Things Technology. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1442–1453.
20. Saha, A.; Amin, R.; Kunal, S.; Vollala, S.; Dwivedi, S.K. Review on "Blockchain Technology Based Medical Healthcare System with Privacy Issues". *Secur. Priv.* **2019**, *2*, e83.
21. Kassab, M.H.; DeFranco, J.; Malas, T.; Laplante, P.; Destefanis, G.; Graciano Neto, V.V. Exploring Research in Blockchain for Healthcare and a Roadmap for the Future. *IEEE Trans. Emerg. Top. Comput.* **2019**, *9*, 1835–1852.
22. Hussien, H.M.; Yasin, S.M.; Udzir, S.N.I.; Zaidan, A.A.; Zaidan, B.B. A Systematic Review for Enabling of Develop a Blockchain Technology in Healthcare Application: Taxonomy, Substantially Analysis, Motivations, Challenges, Recommendations and Future Direction. *J. Med. Syst.* **2019**, *43*, 320.
23. Agbo, C.; Mahmoud, Q.; Eklund, J. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* **2019**, *7*, 56.
24. De Aguiar, E.J.; Faiçal, B.S.; Krishnamachari, B.; Ueyama, J. A Survey of Blockchain-Based Strategies for Healthcare. *ACM Comput. Surv.* **2020**, *53*, 1–27.
25. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on Blockchain for Internet of Things. *Comput. Commun.* **2019**, *136*, 10–29.
26. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R. A Systematic Literature Review of Blockchain Cyber Security. *Digit. Commun. Netw.* **2020**, *6*, 147–156.
27. Houtan, B.; Hafid, A.S.; Makrakis, D. A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare. *IEEE Access* **2020**, *8*, 90478–90494.
28. Jaiswal, K.; Anand, V. A Survey on IoT-Based Healthcare System: Potential Applications, Issues, and Challenges. In *Advances in Biomedical Engineering and Technology*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 459–471.
29. Soltanisehat, L.; Alizadeh, R.; Hao, H.; Choo, K.-K.R. Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review. *IEEE Trans. Eng. Manag.* **2020**, *70*, 353–368.
30. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions. *Blockchain Res. Appl.* **2021**, *2*, 100006.
31. Chukwu, E.; Garg, L. A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations. *Ieee Access* **2020**, *8*, 21196–21214.
32. Hasselgren, A.; Kralevska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in Healthcare and Health Sciences—A Scoping Review. *Int. J. Med. Inform.* **2020**, *134*, 104040.
33. Shi, S.; He, D.; Li, L.; Kumar, N.; Khan, M.K.; Choo, K.-K.R. Applications of Blockchain in Ensuring the Security and Privacy of Electronic Health Record Systems: A Survey. *Comput. Secur.* **2020**, *97*, 101966.
34. Srivastava, G.; Parizi, R.M.; Dehghantanha, A. The Future of Blockchain Technology in Healthcare Internet of Things Security. *Blockchain Cybersecur. Trust Priv.* **2020**, *79*, 161–184.
35. Marques, G.; Pitarma, R.; Garcia, N.M.; Pombo, N. Internet of Things Architectures, Technologies, Applications, Challenges, and Future Directions for Enhanced Living Environments and Healthcare Systems: A Review. *Electronics* **2019**, *8*, 1081.
36. Somasundaram, R.; Thirugnanam, M. Review of Security Challenges in Healthcare Internet of Things. *Wirel. Netw.* **2021**, *27*, 5503–5509.
37. HaddadPajouh, H.; Dehghantanha, A.; Parizi, R.M.; Aledhari, M.; Karimipour, H. A Survey on Internet of Things Security: Requirements, Challenges, and Solutions. *Internet Things* **2021**, *14*, 100129.
38. Aceto, G.; Persico, V.; Pescapé, A. Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0. *J. Ind. Inf. Integr.* **2020**, *18*, 100129.
39. Raikwar, M.; Gligoroski, D.; Kralevska, K. SoK of Used Cryptography in Blockchain. *IEEE Access* **2019**, *7*, 148550–148575. ]
40. Reegu, F.; Daud, S.M.; Alam, S. Interoperability Challenges in Healthcare Blockchain System-A Systematic Review. *Ann. Rom. Soc. Cell Biol.* **2021**, *25*, 15487–15499.
41. Alam, S. A Blockchain-Based Framework for Secure Educational Credentials. *Turk. J. Comput. Math. Educ.* **2021**, *12*, 5157–5167.
42. Zaman, U.; Imran; Mehmood, F.; Iqbal, N.; Kim, J.; Ibrahim, M. Towards Secure and Intelligent Internet of Health Things: A Survey of Enabling Technologies and Applications. *Electronics* **2022**, *11*, 1893.
43. Dimitrov, D. V Blockchain Applications for Healthcare Data Management. *Healthc. Inform. Res.* **2019**, *25*, 51–56.
44. Ray, P.P.; Dash, D.; Salah, K.; Kumar, N. Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. *IEEE Syst. J.* **2020**, *15*, 85–94.
45. Shuaib, M.; Daud, S.M.; Alam, S.; Khan, W.Z. Blockchain-Based Framework for Secure and Reliable Land Registry System. *TELKOMNIKA (Telecommun. Comput. Electron. Control)* **2020**, *18*, 2560–2571.
46. Shuaib, M.; Alam, S.; Ahmed, R.; Qamar, S.; Nasir, M.S.; Alam, M.S. Current Status, Requirements, and Challenges of Blockchain Application in Land Registry. *Int. J. Inf. Retr. Res.* **2022**, *12*, 20.
47. Shuaib, M.; Hassan, N.H.; Usman, S.; Alam, S.; Bhatia, S.; Agarwal, P.; Idrees, S.M. Land Registry Framework Based on Self-Sovereign Identity (SSI) for Environmental Sustainability. *Sustainability* **2022**, *14*, 5400.
48. Odeh, A.; Keshta, I.; Al-Haija, Q.A. Analysis of Blockchain in the Healthcare Sector: Application and Issues. *Symmetry* **2022**, *14*, 1760.
49. Aslam, T.; Maqbool, A.; Akhtar, M.; Mirza, A.; Khan, M.A.; Khan, W.Z.; Alam, S. Blockchain Based Enhanced ERP Transaction Integrity Architecture and PoET Consensus. *Comput. Mater. Contin.* **2022**, *70*, 1089–1109.
50. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A Survey on Privacy Protection in Blockchain System. *J. Netw. Comput. Appl.* **2019**, *126*, 45–58.

51. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. Blockchain Leveraged Decentralized IoT EHealth Framework. *Internet Things* **2020**, *9*, 100159.
52. Bhalaji, N.; Abilashkumar, P.C.; Aboorva, S. A Blockchain Based Approach for Privacy Preservation in Healthcare Iot. In *Proceedings of the ICICCT 2019–System Reliability, Quality Control, Safety, Maintenance and Management: Applications to Electrical, Electronics and Computer Science and Engineering*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 465–473.
53. Khatoon, A. A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics* **2020**, *9*, 94.
54. Gupta, S.; Malhotra, V.; Singh, S.N. Securing IoT-Driven Remote Healthcare Data through Blockchain. In Proceedings of the Advances in Data and Information Sciences: Proceedings of ICDIS 2019; Springer: Berlin/Heidelberg, Germany, 2020; pp. 47–56.
55. Ellouze, F.; Fersi, G.; Jmaiel, M. Blockchain for Internet of Medical Things: A Technical Review. In Proceedings of the The Impact of Digital Technologies on Public Health in Developed and Developing Countries: 18th International Conference, ICOST 2020, Hammamet, Tunisia, 24–26 June 2020; pp. 259–267.
56. Attia, O.; Khoufi, I.; Laouiti, A.; Adjih, C. An IoT-Blockchain Architecture Based on Hyperledger Framework for Health Care Monitoring Application. In Proceedings of the NTMS 2019-10th IFIP International Conference on New Technologies, Mobility and Security, Canary Islands, Spain, 24–26 June 2019; IEEE Computer Society: Washington, DC, USA, 2019; pp. 1–5.
57. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient Healthcare Data Sharing via Blockchain. *Appl. Sci.* **2019**, *9*, 1207.
58. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* **2019**, *19*, 326.
59. Nguyen, D.C.; Nguyen, K.D.; Pathirana, P.N. A Mobile Cloud Based Iomt Framework for Automated Health Assessment and Management. In Proceedings of the 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Berlin, Germany, 23–27 July 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 6517–6520.
60. Salimitari, M.; Chatterjee, M.; Fallah, Y.P. A Survey on Consensus Methods in Blockchain for Resource-Constrained IoT Networks. *Internet Things* **2020**, *11*, 100212.
61. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: **https://assets.pubpub.org/d8wct41f/31611263538139.pdf** (accessed on 2023).
62. Indhuja, E.; Venkatesulu, M. A Survey of Blockchain Technology Applications and Consensus Algorithm. In *Sustainable Communication Networks and Application. Lecture Notes on Data Engineering and Communications Technologies*; Karuppusamy, P., Perikos, I., Shi, F., Nguyen, T.N., Eds.; Springer: Singapore, 2021; Volume 55, pp. 173–187.
63. Bachani, V.; Bhattacharjya, A. Preferential Delegated Proof of Stake (PDPoS)—Modified DPoS with Two Layers towards Scalability and Higher TPS. *Symmetry* **2022**, *15*, 4.
64. Aggarwal, S.; Kumar, N. Cryptographic Consensus Mechanisms. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2021; Volume 121, pp. 211–226. ISBN 0065-2458.
65. Kotla, R.; Alvisi, L.; Dahlin, M.; Clement, A.; Wong, E. Zyzzyva: Speculative Byzantine Fault Tolerance. *ACM Trans. Comput. Syst.* **2009**, *27*, 45–58.
66. Barinov, I.; Baranov, V.; Khahulin, P. POA Network Whitepaper. 2018. Available online: **https://github.com/poanetwork/wiki/wiki/POANetwork-Whitepaper** (accessed 2023).
67. Bodkhe, U.; Mehta, D.; Tanwar, S.; Bhattacharya, P.; Singh, P.K.; Hong, W.C. A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems. *IEEE Access* **2020**, *8*, 54371–54401.
68. Dziembowski, S.; Faust, S.; Kolmogorov, V.; Pietrzak, K. Proofs of Space. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9216, pp. 585–605. ISBN 9783662479995.
69. Larimer, D. Transactions as Proof-of-Stake. 2013, pp. 1–8. Available online: **https://cryptochainuni.com/wp-content/uploads/Invictus-Innovations-Transactions-As-Proof-Of-Stake.pdf** (accessed 2023).
70. Ghosh, M.; Richardson, M.; Ford, B.; Jansen, R. *A TorPath to TorCoin: Proof-of-Bandwidth Altcoins for Compensating Relays*; Naval Research Lab: Washington, DC, USA, 2014.
71. Zou, J.; Ye, B.; Qu, L.; Wang, Y.; Orgun, M.A.; Li, L. A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services. *IEEE Trans. Serv. Comput.* **2019**, *12*, 429–445.
72. Milutinovic, M.; He, W.; Wu, H.; Kanwal, M. Proof of Luck. In Proceedings of the 1st Workshop on System Software for Trusted Execution, Trento, Italy, 12 December 2016; ACM: New York, NY, USA, 2016; pp. 1–6.
73. Rahman, M.S.; Islam, M.A.; Uddin, M.A.; Stea, G. A Survey of Blockchain-Based IoT EHealthcare: Applications, Research Issues, and Challenges. *Internet Things* **2022**, *19*, 100551
74. Saad ZM, Al-Chaabawi NJ, Hassan SA. A novel adaptive noise cancellation method based on minimization of error entropy for electrocardiogram denoising. Indonesian Journal of Electrical Engineering and Computer Science. 2023 Oct;32(1):185-96.
75. Falih IQ, Alobeady MA, Banoon SR, Saleh MY. Role of Oxidized Low-density Lipoprotein in Human Diseases: A Review. Journal of Chemical Health Risks. 2021 Sep 2;11.
76. Lawi ZK, Merza FA, Banoon SR, Jabber Al-Saady MA, Al-Abboodi A. Mechanisms of Antioxidant Actions and their Role in many Human Diseases: A Review. Journal of Chemical Health Risks. 2021 Sep 2;11