



Paper Type: Original Article

## Leveraging Blockchain and IoT for Secure and Scalable Healthcare Innovations

Sedigheh Kaveh<sup>1</sup>, Fatemeh Ebrahimzadeh<sup>1</sup>, Ramin Safa<sup>1,\*</sup> 

<sup>1</sup>Department of Computer Engineering, Ayandehgan Institute of Higher Education, Tonekabon, Iran; s.kaveh@aihe.ac.ir; f.ebrahimzadeh@aihe.ac.ir; safa@aihe.ac.ir.

### Citation:

Received: 15 July 2024

Revised: 10 October 2024

Accepted: 25 January 2025

Kaveh, S., Ebrahimzadeh, F., & Safa, R. (2025). Leveraging blockchain and IoT for secure and scalable healthcare innovations. *Annals of healthcare systems engineering*, 2(1), 16-27.

### Abstract


Blockchain is a distributed technology with the potential to revolutionize various industries. Since its introduction in 2008, it has found applications in financial transactions, online trading, smart contracts, supply chain management, and identity verification. Blockchain consists of interconnected blocks containing cryptographic data, the previous block's hash, a timestamp, and transaction data. This structure ensures system security and prevents cyberattacks such as 51% and Distributed Denial of Service (DDoS) attacks. Despite the widespread adoption of the Internet of Things (IoT), developing a secure and privacy-compliant model remains a challenge. Integrating blockchain with IoT enhances security, scalability, energy efficiency, and data management. In recent years, electronic Health (eHealth) has gained significant attention. Healthcare applications include hospital networks, pharmaceutical supply chains, blood banks, and insurance systems. However, challenges such as patient privacy, large medical data management, and collaboration issues highlight blockchain's importance in healthcare. Blockchain can improve security in IoT and eHealth by preventing unauthorized data manipulation. Its applications in remote medical monitoring, pharmaceutical supply chains, counterfeit drug prevention, and patient consent processes are expanding. However, challenges such as high energy consumption in Proof of Work (PoW), lack of international standards, and reluctance to share medical data hinder its adoption in healthcare. This paper reviews blockchain and IoT concepts, assessing their feasibility in healthcare. It analyzes scalability, security, and adoption challenges while proposing solutions to overcome these barriers.

**Keywords:** Blockchain, Security, Internet of Things, Healthcare, Patient privacy, Medical data management.

## 1 | Introduction

With advancements in digital technologies, blockchain and the Internet of Things (IoT) have emerged as two key fields that can drive significant transformations across various industries [1]. One of the most critical sectors that can benefit from these technologies is healthcare [2]. In recent years, the rapid growth of medical

 Corresponding Author: safa@aihe.ac.ir

 <https://doi.org/10.22105/ahse.v2i1.27>



Licensee System Analytics. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

data and the increasing need for security, privacy, data integrity, and quick access to patient records have posed serious challenges to traditional healthcare data storage and management systems [3].

Blockchain is a decentralized and immutable ledger technology that ensures the security and transparency of medical data [3]. By leveraging blockchain, patient records can be stored in a decentralized manner, reducing dependency on central servers while preventing data tampering and deletion [4]. IoT also plays a vital role in enhancing medical services by enabling the collection of real-time health data through smart sensors and wearable medical devices, facilitating remote patient monitoring [5].

One of the key advantages of integrating blockchain and IoT in healthcare is the enhanced security of medical data, prevention of record forgery, and implementation of access control through smart authorization mechanisms [4]. Additionally, these technologies can optimize pharmaceutical supply chains and improve drug distribution management, helping to prevent counterfeit medications from entering the market [4]. However, challenges such as scalability, high energy consumption in consensus mechanisms like Proof of Work (PoW), lack of standardization, and resistance from healthcare organizations in adopting these technologies remain major obstacles to the widespread implementation of blockchain in healthcare systems [6].

This paper first explores the fundamental concepts of blockchain and IoT and introduces their applications in healthcare. Then, the technical and operational challenges of these technologies in medical systems are discussed, and potential solutions to overcome these barriers are presented [7]. Blockchain has the ability to overcome security and privacy challenges in the IoT [8]. IoT encompasses a wide range of applications, including smart grids, smart cities, healthcare management, and more. However, the increasing invisibility, pervasiveness, and widespread collection, processing, and exchange of information have raised serious security and privacy concerns [9].

Blockchain can enhance the security framework of this technology by integrating IoT tools and encrypting information. One of its key features is decentralization and the distribution of information among users [1].

Moreover, the type and volume of stored data are crucial factors; it is essential to determine what kind of data is stored, in what quantity, and with what level of access. Fortunately, this challenge can be addressed with advanced technologies. For these reasons, blockchain was introduced as a system that stores information in a decentralized and distributed manner among users.

## 2 | Understanding Blockchain Technology

Blockchain is a new technology that has recently emerged in the market. It is a distributed, collaborative, and collective electronic ledger used for recording payments across multiple devices, ensuring that the database cannot be arbitrarily altered without modifying all associated frames and platforms. Additionally, it enables secure transactions without the need for intermediaries [3].

Blockchain acts as a time-stamped ledger used for storing and sharing data in a decentralized manner. The stored data may include payment records, such as Bitcoin transactions, contracts, or even personal information [9]. Blockchain is a peer-to-peer distributed ledger that determines, through an algorithm, which nodes contain valid information and can integrate with other devices, such as smart contracts.

Blockchain functions as a digital contract that allows a legal or natural person to engage in direct (Peer-to-peer) transactions with another party [4]. Moreover, smart contracts are a key component of blockchain, automatically executing agreements based on predefined conditions. There are various types of blockchain networks, such as Bitcoin and Hyperledger [1].

Moreover, the type and volume of stored data are crucial factors; it is essential to determine what kind of data is stored, in what quantity, and with what level of access. Fortunately, this challenge can be addressed with advanced technologies. For these reasons, blockchain was introduced as a system that stores information in a decentralized and distributed manner among users.

## 2.1 | Functionality

When a provider and a customer agree to enter into a transaction, they define its details by specifying the sender, recipient, transaction amount, and other relevant variables. Then, all information related to the individual transaction, along with additional details, is combined to create a new block of data.

Each transaction is encrypted and distributed across a large number of computers in the network. Each of these computers stores the data locally and verifies its accuracy. This process allows the network to automatically validate the recorded transactions.

The stored data in each block is verified using cryptographic algorithms and assigned unique hashes. If a transaction's information is altered due to tampering or transmission errors, the algorithms running on that block will also change, preventing the creation of a valid hash. In this case, the system will report an error, identifying the transaction as fraudulent. Because of this mechanism, the chain of interconnected data blocks is called a "Blockchain" or "Block chain" [10].

The basic structure of blockchain consists of three layers:

- I. Peer-to-peer layer: Enables communication between geographically dispersed devices [5].
- II. Distributed ledger layer: Stores transaction data within blocks.
- III. Application layer: Provides an interface for executing smart contracts and other applications.

In this structure, each block is linked to the previous block through the hash of its header. To validate new blocks, a consensus mechanism such as PoW is used.

## 2.2 | Security Features

Blockchain is highly secure due to its decentralized structure and complex combination of cryptographically encoded numbers and letters. The information stored on the blockchain is immutable, meaning that any attempt to alter it would require modifying the entire network of blocks. This would demand an immense amount of computational power and cost, making such an attack economically unfeasible, even for someone with the necessary technical knowledge.

The continuous validation process of blocks, known as mining, is carried out by network participants. Miners receive rewards based on the computing power they contribute to the network. This process ensures that all network members can add new transactions to the blockchain, but once recorded, they cannot be altered or edited. This characteristic eliminates the need for third-party intermediaries to verify transactions [10].

## 2.3 | Algorithms

Using one of the well-known mathematical models, the possibility of changing and tampering with any block in the blockchain is nearly zero. This means that even if 51% of network users decide to alter or forge a block, the consensus algorithms eliminate this possibility. The two main algorithms that ensure this security are PoW and Proof of Stake (PoS).

### 2.3.1 | Proof of work

The PoW algorithm requires solving complex computational problems, which results in high energy consumption. In this method, any node with sufficient processing power can participate in the creation of new blocks. The algorithm works as follows:

A hash is generated from the block's header. A random number (Nonce) is appended to the generated hash. The new value is hashed again. If the resulting hash is lower than the network's difficulty target (Difficulty target), the block is considered valid. Otherwise, the random number must be changed, and the steps above are repeated. Once a valid nonce is found, the successful node sends the nonce, final hash, and new block to the network. Other nodes verify the block's validity, and if confirmed, the block is added to the blockchain.

In this algorithm, miners use their hardware's processing power to solve cryptographic equations and validate transactions. The mining reward is given to the miner who is the first to solve the equation and publish the new block.

### 2.3.2 | Proof of stake

In contrast to PoW, the PoS algorithm works without requiring the solving of complex computational problems. In this method, transactions are validated based on the amount of stake each participant holds in the network. These participants are known as validators.

The process works as follows:

- I. Validators lock a portion of their assets as collateral (Stake) instead of using computational power.
- II. The network randomly selects a validator to create the new block, but the selection probability is based on the amount of stake the individual has in the network.
- III. The greater the stake, the higher the chance of being selected to create the new block.
- IV. After the block is published, other validators check its validity.
- V. If confirmed, the block is added to the blockchain, and the selected validator receives a reward.

In this method, the reward for validating a block is proportional to the amount of capital the validator has locked in the network. Users with more stake receive higher rewards, as a higher stake represents a greater commitment to the network's security.

## 3 | Blockchain in the Internet of Things

Blockchain and the IoT are two crucial technologies expected to significantly impact all industries in the coming years. The healthcare industry will not be exempt from these changes. Blockchain has the potential to address the security and privacy challenges of IoT. The IoT refers to a network of physical objects embedded with technologies to communicate and sense or interact with their internal states or the external environment [9]. However, the recent expansion of IoT and its vast data volume have created several challenges.

According to recent Gartner reports, approximately one million new IoT devices are sold every hour. By providing suitable and cost-effective cloud computing resources, a large amount of IoT data can be transmitted over the internet. Secure, scalable, and efficient resource management is one of the primary goals for future IoT networks. By using blockchain technology, applications can operate in a distributed manner, without the need for intermediaries. Recent reports predict that by 2027, around 10% of the global GDP will be stored using blockchain technology [11].

Some researchers argued that smart homes are vulnerable to attacks carried out by smartphones [12]. In another paper, a method with three different modules for protecting user privacy in smart homes was proposed [6]. Regarding blockchain-based security and privacy, authors suggested a host identity protocol for IoT security. In this proposed protocol, the header size is reduced from 40 bytes to a maximum of 25 bytes, thereby reducing network overhead by eliminating unnecessary headers. In another paper, the authors proposed a new method for authentication and access control to prevent unauthorized access to IoT [13].

The integration of blockchain and IoT enables the sharing of services and resources among devices and allows the automation of multiple tasks simultaneously. Researchers highlighted some specific issues that need to be addressed before deploying a blockchain network in an IoT environment. Their conclusion is that combining blockchain and IoT could lead to major transformations across various industries, paving the way for new business models and innovative applications [7].

Several studies have focused on the integration of blockchain and IoT networks in next-generation healthcare systems to ensure privacy and security. One paper proposed the idea of assessing the use of virtual resources

combined with a permissioned blockchain to provide IoT services on edge hosts. The authors believe that moving IoT components from the cloud to edge hosts could help reduce overall network traffic and, in turn, minimize latency. However, providing IoT services on IoT edge devices introduces new challenges related to system design and maintenance. One proposed approach is to use software-defined IoT components as virtual resources. This, in turn, allows the device layer and IoT service layer to be divided into a set of microservices across a wide range of hosts [14]. In another paper, the same authors discussed the idea of using blockchain as a service for IoT and evaluated the cloud and edge host performance [15]. *Table 1* compares consensus algorithms in blockchain.

**Table 1. Comparison of consensus algorithms in blockchain.**

Feature	PoW	PoS	Delegated Proof of Stake (DPoS)	Proof of Authority (PoA)
Validator selection basis	Computational power and solving mathematical puzzles.	Amount of stake in the network.	Voting by stakeholders.	Verified identity of nodes.
Transaction speed	Low (Slow due to complex computations)	Medium	High	Very high
Energy consumption	Very high	Low	Very low	Very low
Decentralization	High (But may become centralized over time)	Medium (Whales may concentrate power)	Lower than PoS (Power lies with delegates)	Low (More centralized)
Network security	Very high	High	High, but dependent on delegates.	High, but requires trust in validators.
51% attack risk	High (Expensive but possible)	Possible, requires substantial capital	Low, as voting plays a key role	Low (Relies on designated validators)
Blockchain examples	Bitcoin, Ethereum 1.0, Litecoin	Ethereum 2.0, Cardano, Polkadot	Steem, EOS, Tron	VeChain, Ripple, some private networks.

The IoT is a model used for efficient computing that helps us improve performance in various aspects of daily life. In IoT, the mutual connection of different devices allows them to interact with each other effectively and at any time. These systems make tasks more accurate and with minimal human intervention [3].

In IoT, various devices are used. The most common of these devices include mobile phones, smart sensors, and household devices. However, the large volume of data and high speed in these systems increase their complexity. In IoT systems, the network infrastructure is used for integration so that remotely controlled physical devices and computer-based systems can effectively communicate with each other.

The IoT technology enables devices to operate with greater efficiency and accuracy. It also requires minimal human intervention and has the capability to collect data from various sensors. Many organizations are interested in IoT technology because the use of sensors and actuators in this technology is less costly [3].

Wireless Sensor Networks (WSNs) are one of the early developments in the IoT field. These networks connect sensors and various actuator hubs to a framework, and this framework is then transformed into an aggregated structure through the internet [3].

## 4 | Blockchain and Healthcare

Electronic medical records (EMRs) contain important and sensitive information about healthcare, making their protection highly critical. Health systems require a more efficient and secure method for managing medical records and other data. Blockchain provides a shared, immutable, and transparent history, allowing applications to create trust, transparency, and auditability [9].

The features of blockchain, such as its decentralized, transparent, and permissionless nature, may offer a unique solution for healthcare. The broader application of this technology paves the way for its use in various healthcare aspects, including wearable devices and advancements in medical research [6].

The healthcare sector has an increasing demand for blockchain developments, and a recent survey by Deloitte shows that the traditional industry is actively seeking new ways to use blockchain to address its critical needs. Blockchain's immutability is a key feature for healthcare data. This technology can secure health records, clinical test results, and ensure compliance with regulations. The use of smart contracts demonstrates how blockchain can support real-time monitoring of patients and medical interventions [13].

These systems ensure the security of records while providing access to patients and medical professionals in accordance with the Health Insurance Portability and Accountability Act (HIPAA).

### **Accurate and comprehensive medical records**

Longitudinal medical records, including images, disease databases, medical tests, medications, and other information, can be managed through blockchain. Specifically, hospitalization details, walking status, and wearable information enable providers to learn better methods of distributing treatment.

### **Complete patient list**

Records are regularly updated when managing the intersection or copy of necessary pharmaceutical data.

A broader application of blockchain concerns the pharmaceutical supply chain and the development of countermeasures against counterfeit drugs. While the development of new drugs incurs significant costs for trials to assess the safety and efficacy of the drug, the use of smart contracts facilitates the process of obtaining informed consent and improves identity and data quality management [6].

Providing patients with access to manage their own identity also enables the integration of the informed consent process and ensures the privacy of individual health data.

The storage of patient medical data in healthcare is extremely important. These data are highly sensitive and, therefore, a primary target for cyber-attacks. Therefore, the security of sensitive data is crucial [7].

Blockchain provides a comprehensive medical history of each patient in multiple small pieces, which include information from the patient, doctors, regulators, hospitals, insurers, and others, offering a secure mechanism for recording and maintaining each patient's complete medical history [16].

### **Distributed denial of service attacks**

Distributed Denial of Service (DDoS) attacks are typically aimed at disrupting access to services by sending a massive volume of requests. These attacks can flood systems with unexpected traffic, causing service disruptions. The proposed remedy is based on a decentralized system that uses IPFS and blockchain, which can neutralize DDoS attacks [17].

Another aspect is control over data, which ideally should be managed by the patient. Therefore, sharing and accessing patient health data is a use case that can benefit from modern and advanced technologies. Blockchain technology is highly resistant to attacks and failures and provides various methods for controlling access. Thus, blockchain provides a suitable framework for health data.

For personal medical data, the most suitable type of blockchain would be a private blockchain. According to the Würst and Gervais decision model, blockchain can be used in scenarios where multiple parties who do

not trust each other need to interact and exchange shared data, but do not want a Trusted Third Party (TTP) involved [6].

Their model provides several factors that need to be considered when analyzing whether a specific scenario requires blockchain. In relation to storage, several factors (Questions) need to be examined:

- I. Is there a need to store the data (Based on the authors of a specific situation)?
- II. Is there a need for multiple write access?
- III. Is a TTP available, and can the always-online TTP be used?

First, the need to store data must be determined (In a typical scenario, this is a database). Then, it must be determined whether multiple parties need write access. If there is only one writer, blockchain is unnecessary, and alternative solutions (e.g., a database) can be considered. It should be noted that traditional databases perform better than blockchain. If a TTP is available, always online, and fully trustworthy, blockchain is not required. The Würst and Gervais decision model also helps determine which type of blockchain should be used (e.g., permissionless public, permissioned public, or private).

If the writers are unknown, the only clear option is permissionless public blockchain. If the TTP is offline, it can act similarly to a certificate authority, and the parties involved may not trust each other, so permissioned blockchain can be used. However, if all parties trust each other, a shared access database can be used instead of blockchain. On the other hand, if the writers are known and trustworthy, the choice is between permissioned public blockchain and private blockchain. The first is for cases requiring public verification, and the second is when this is not necessary.

Current medical data infrastructure is mostly reliant on trusted third parties. In many cases, these third parties cannot be fully trusted. Blockchain, relying on consensus and not requiring a central authority, is a possible solution to this problem [6]

### Supply chain control

Blockchain-based contracts allow organizations to control medical services for tracking supply and demand across their entire lifecycle. For example, how a transaction occurs or whether a transaction is effective can be monitored [7].

### Delay

In blockchain systems, due to decentralized processing, there may be some delays [7].

**Table 2. Types of Attacks in a smart home and how to counter them [9].**

Probability	Attack Resistance	Defense	Definition	Attack
Unlikely	Beyond high	An OBM can detect a fake block before confirmation.	The attacker creates a fake block.	Appending attack
Unlikely	High	OBMs send transactions to their members.	The attacker floods a node with a high volume of transactions.	DoS
Unlikely	Beyond high	Various cryptographic methods are used in a smart home.	A distributed version of a DOS attack where multiple smart home devices are compromised by an attacker.	DDoS
Possible	Medium	OBM creates a shared key requiring the homeowner's approval.	The attacker introduces fake devices to the smart home to gain access to internal data.	Device injection attack

Table 2. Continued.

Probability	Attack Resistance	Defense	Definition	Attack
Unlikely	High	OBM's can correlate cluster members if they detect unprocessed transactions.	The attack removes transactions from cluster members or isolates them.	Drooping attack
Unlikely	Beyond high	Each transaction contains stored data as evidence of its timestamp, but the data is not recoverable	Malicious cloud storage modifies or deletes stored data.	Modification attack
Possible	Medium	OBM's detect false inflation during transaction confirmation.	Attackers increase their transaction production to boost their own ratings.	False reputation attack
Unlikely	Beyond high	The consensus algorithm limits the number of blocks an OBM can generate in a given time. This prevents attackers from creating a long fraudulent ledger.	The attacker announces fake blocks and writes them as the longest ledger, misleading all nodes.	Public BC modification
Unlikely	Beyond high	Other OBM's detect this as they receive more than the allowed number of blocks during a consensus period, reducing trust and isolating the attacker	The OBM generates more than one block per consensus period.	Breaking the time interval
Unlikely	High	A request is considered valid only if at least half of the OBM's sign it, making this attack highly unlikely.	Attackers (Visitors) send false requests to update the consensus period.	Consensus period attack
Unlikely	Beyond high	The attack can be detected during block confirmation through consensus algorithms with other OBM's.	The attacker gains control of more than 51% of the network and compromises consensus by generating fake or excessive blocks	51% attack

## 4.1 | Practical Applications

Ensuring data security and maintaining patient privacy when collecting medical data is a very important goal. By using blockchain technology, the process of collecting patient data for research purposes becomes easier. Managing medical history, access control, medical prescriptions, insurance definitions, and payments are inevitable and often time-consuming and inconvenient. Managing the storage and transfer of data may delay an important treatment.

Table 3. Healthcare and blockchain network use cases.

Network	Description
Hospital network	Hospitals can connect to different hospitals through a distributed ledger network, with information and data stored in different blocks. Each transaction is uniquely identified and stored as a block. Patients can share their identity.
Blood bank network	Blood banks will be connected through a network of distributed ledgers to various blood banks. Information and data are stored in different blocks. Excess blood can easily be transferred to the nearest blood bank that lacks supplies. The blood bank can manage donors and blood recipients.



Table 3. Continued.

Network	Description
Laboratory network	A laboratory can be connected to blockchain technology via a distributed ledger. Laboratory records are stored in an individual handbook, and laboratory history will be kept in distributed ledgers as blocks. Users can view reports using their unique identification number (User ID).
Pharmaceutical network	Pharmacists and chemists can communicate using blockchain technology where each transaction between manufacturers, wholesalers, pharmacists, and patients is stored in a distributed ledger. This ensures drug traceability.
Insurance partner network	Insurance organizations can connect to the blockchain network, eliminating fraud related to health insurance.

As shown in Fig. 1, the proposed Internet of Medical Things (IoMT) architecture for patient healthcare monitoring integrates wearable sensors, communication technologies, and cloud-based analytics to facilitate real-time health data collection, analysis, and remote medical intervention [14].

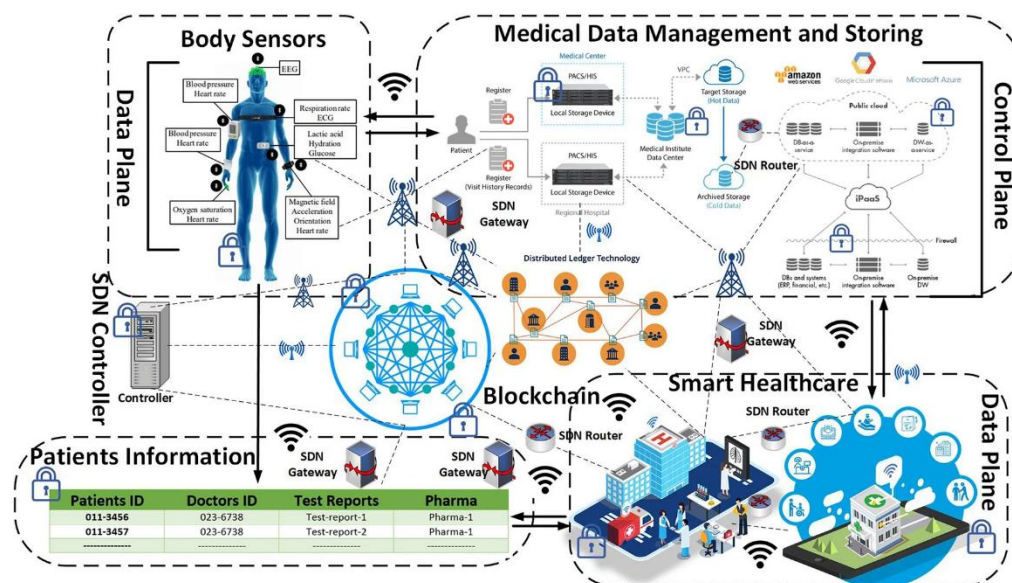
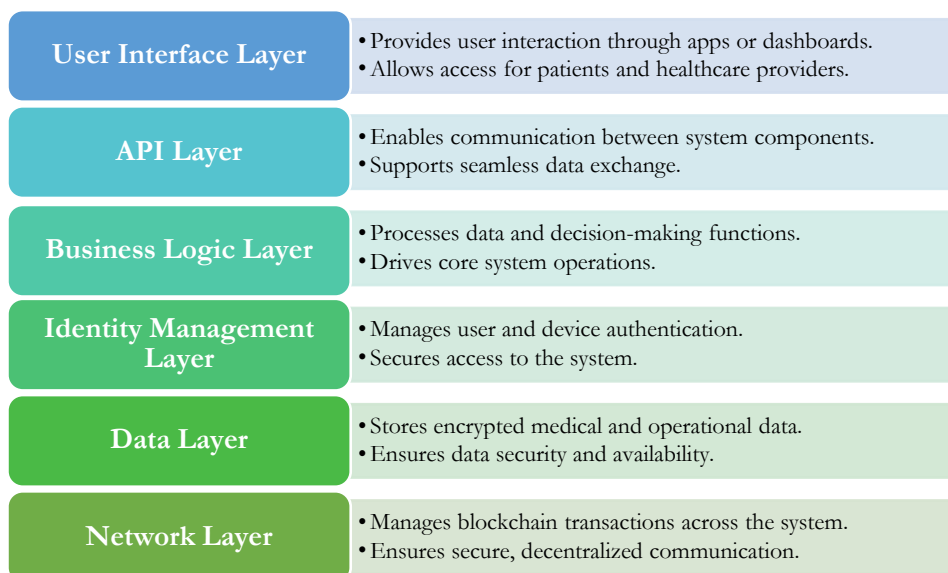


Fig. 1. Internet of medical things-based architecture for real-time patient healthcare monitoring [18].

## 4.2 | Healthcare Network Architecture

The proposed healthcare network architecture is structured into six distinct layers: 1) the user interface layer, 2) API layer, 3) business logic layer, 4) identity management layer, 5) data layer, and 6) network layer. Each layer plays a critical role in ensuring the secure, scalable, and seamless operation of healthcare services. As illustrated in Fig. 2, these layers are interconnected through a blockchain-enabled framework that facilitates secure data exchange and system interoperability. The architecture is designed to be adaptable and compatible with various blockchain platforms, ensuring flexibility and extensibility. It supports integration with diverse data stores and ensures that all participating users and devices undergo robust identity verification. The blockchain network is orchestrated through external APIs, which manage its operations and ensure trusted execution of network events. The system's intelligent design allows it to respond dynamically to a variety of real-time events across the network.



**Fig. 2. Blockchain-based layered architecture for secure and scalable healthcare network.**

### 4.3 | Challenges

Blockchain technology in the healthcare and medical fields faces numerous challenges, with some of the most significant being scalability, security and privacy, energy consumption, inter-organizational collaboration, and technology adoption. One of the main challenges is transparency and reliability. In a blockchain network, all information is transparent, which can reduce user trust. This issue is particularly critical in healthcare applications because patient data (Protected health information and personally identifiable information) is highly sensitive. In Healthcare systems, privacy mechanisms allow users to choose who can view their sensitive information, but in blockchain, a user can have multiple addresses, and the information is visible to everyone. Blockchain cannot fully guarantee the privacy of transactions because the amounts of all transactions and the balances of each public key are publicly visible.

Another challenge is scalability and transaction speed. Depending on the protocol used and technical limitations, transaction processing times may become very long, which could disrupt healthcare system performance. For example, using PoW, only 7 transactions per second are processed, while networks like Visa can process over 4,000 transactions per second. This issue is especially important for real-time applications such as managing medical records and emergency services. Moreover, the need for storing large volumes of medical data, such as scan images, lab reports, and longitudinal patient records, is another challenge for blockchain scalability [19].

Another significant challenge is high energy consumption. Blockchain consumes a lot of energy due to the use of consensus algorithms like PoW. For example, the PoW algorithm requires more energy than PoS, which can increase computational costs and affect the stability of healthcare systems. On the other hand, many medical organizations, hospitals, and insurance companies are reluctant to share their data due to the lack of common standards. In many cases, hospitals withhold financial and insurance information due to economic competition and concerns about treatment costs.

Furthermore, the adoption of blockchain technology in healthcare systems still faces challenges. Many medical professionals and hospital staff are accustomed to traditional systems, and transitioning to new technologies like blockchain-based electronic records can be difficult for them. For example, doctors may face limitations when entering data into digital systems, as some digital fields are mandatory and must be completed, unlike paper forms. Additionally, trust in technologies such as blockchain and IoT for remote monitoring remains a significant challenge, requiring education and awareness-building among healthcare professionals.

Another security challenge is 51% attacks. In blockchain, if more than 51% of the nodes in a network are compromised, the entire system can be attacked, which poses a serious threat to patient data security. Moreover, data ownership and accountability remain important issues. Questions such as who owns the health data of patients, who will authorize the sharing of private data, and which entity is responsible for protecting this data, remain unanswered and require clear legal frameworks.

Given these challenges, to integrate blockchain into healthcare systems, solutions must be developed to improve scalability, optimize energy consumption, create common standards, increase collaboration between hospitals and insurance companies, and educate medical professionals to adopt new technologies. Furthermore, the development of advanced security mechanisms to prevent cyberattacks and 51% threats is essential for the successful implementation of blockchain in the healthcare sector [1].

## 5 | Conclusion

With the advancement of technology, blockchain and the IoT have emerged as two key areas that can address many challenges in healthcare systems. Blockchain, as a distributed ledger, offers capabilities such as ensuring data security, guaranteeing the integrity of medical information, better managing the pharmaceutical supply chain, preventing drug counterfeiting, and improving the performance of smart contracts in insurance interactions. Alongside these capabilities, the IoT can enable monitoring of patient health status, gathering more accurate data, and optimizing medical processes, potentially leading to a significant transformation in the management of electronic Health (eHealth).

This paper examined the role of blockchain in enhancing the security and scalability of medical data and demonstrated how the combination of this technology with IoT can create numerous benefits in the healthcare sector. The results of this study show that the major challenges facing this technology include scalability, high energy consumption in consensus algorithms like PoW, lack of standardization in medical systems, and resistance from some healthcare organizations to adopting this technology. However, the development of new solutions such as low-energy consensus algorithms (e.g., PoS and BFT), enhanced security standards, and increased awareness among healthcare professionals can accelerate the adoption of this technology.

It is also recommended that more precise legal frameworks be developed for the successful implementation of blockchain in healthcare to protect patient privacy and facilitate collaboration between hospitals, insurance companies, and other relevant entities. Additionally, considering the large volume of medical data, utilizing innovative methods such as hybrid storage (On-Chain and Off-Chain) could help reduce storage costs and improve processing speed. Finally, the results of this research suggest that, with further development and optimization, blockchain can become a key technology for improving digital health services and enhancing the security of medical data.

## Funding

This research was conducted without external funding.

## Conflicts of Interest

The authors declare no conflicts of interest regarding this study.

## Declaration

The authors declare they have used AI language models to provide editorial assistance with language clarity in preparing this manuscript.

## References

- [1] Sharma, P. K., Chen, M. Y., & Park, J. H. (2018). A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE access*, 6, 115–124. <https://doi.org/10.1109/ACCESS.2017.2757955>
- [2] Li, G., Dong, M., Yang, L. T., Ota, K., Wu, J., & Li, J. (2020). Preserving edge knowledge sharing among IoT services: A blockchain-based approach. *IEEE transactions on emerging topics in computational intelligence*, 4(5), 653–665. <https://doi.org/10.1109/TETCI.2019.2952587>
- [3] Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. *Bitcoin*, 4(2), 15. <https://bitcoin.org/bitcoin.pdf>
- [4] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014), 1–32. <https://B2n.ir/yx9330>
- [5] Notra, S., Siddiqi, M., Habibi Gharakheili, H., Sivaraman, V., & Boreli, R. (2014). An experimental study of security and privacy risks with emerging household appliances. *2014 IEEE conference on communications and network security* (pp. 79–84). IEEE. <https://doi.org/10.1109/CNS.2014.6997469>
- [6] Sivaraman, V., Chan, D., Earl, D., & Boreli, R. (2016). Smart-phones attacking smart-homes. *Proceedings of the 9th ACM conference on security & privacy in wireless and mobile networks* (pp. 195–200). New York, NY, USA: Association for Computing Machinery. <https://doi.org/10.1145/2939918.2939925>
- [7] Chakravorty, A., Wlodarczyk, T., & Rong, C. (2013). Privacy preserving data analytics for smart homes. *2013 IEEE security and privacy workshops* (pp. 23–27). IEEE. <https://doi.org/10.1109/SPW.2013.22>
- [8] Li, G., Dong, M., Yang, L. T., Ota, K., Wu, J., & Li, J. (2020). Preserving edge knowledge sharing among IoT services: A blockchain-based approach privacy and security in computational intelligence. *IEEE transactions on emerging topics in computational intelligence (TETCI)*, 4(5), 653 - 665. <https://doi.org/10.1109/TETCI.2019.2952587>
- [9] Roshan, N. P., & Pavithra, N. (2020). A bird eye view on Lsb (Lightweight scalable blockchain) in the platform of internet of things. *International research journal of engineering and technology (IRJET)*, 7(9), 2819–2825. <https://B2n.ir/np6846>
- [10] Dwivedi, A. D., Malina, L., Dzurenda, P., & Srivastava, G. (2019). Optimized blockchain model for internet of things based healthcare applications. *2019 42nd international conference on telecommunications and signal processing (TSP)* (pp. 135–139). IEEE. <https://doi.org/10.1109/TSP.2019.8769060>
- [11] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized blockchain for IoT. *Proceedings of the second international conference on internet-of-things design and implementation* (pp. 173–178). New York, NY, USA: Association for Computing Machinery. <https://doi.org/10.1145/3054977.3055003>
- [12] Liu, J., Xiao, Y., & Chen, C. L. P. (2012). Authentication and access control in the internet of things. *2012 32nd international conference on distributed computing systems workshops* (pp. 588–592). IEEE. <https://doi.org/10.1109/ICDCSW.2012.23>
- [13] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE access*, 4, 2292–2303. <https://doi.org/10.1109/ACCESS.2016.2566339>
- [14] Wu, Y., Hu, Y., Chen, M., Yesha, Y., & Debbah, M. (2024). Blockchains for internet of things: Fundamentals, applications, and challenges. *IEEE network*, 38(6), 443–450. <https://doi.org/10.1109/MNET.2024.3410640>
- [15] Yang, W., Aghasian, E., Garg, S., Herbert, D., Disiuta, L., & Kang, B. (2019). A survey on blockchain-based internet service architecture: Requirements, challenges, trends, and future. *IEEE access*, 7, 75845–75872. <https://doi.org/10.1109/ACCESS.2019.2917562>
- [16] Mahmood, M. S., & Al Dabagh, N. B. (2023). Blockchain technology and internet of things: review, challenge and security concern. *International journal of electrical and computer engineering*, 13(1), 718. <https://doi.org/10.11591/ijece.v13i1.pp718-735>
- [17] Hannan, S. A. (2023). A blockchain technology and internet of things to secure in healthcare system. *Journal of advance research in computer science & engineering issn*, 2456, 3552. <https://www.researchgate.net/publication/370034212>
- [18] Rahman, A., Wadud, M. A. H., Islam, M. J., Kundu, D., Bhuiyan, T. M. A. U. H., Muhammad, G., & Ali, Z. (2024). Internet of medical things and blockchain-enabled patient-centric agent through SDN for remote patient monitoring in 5G network. *Scientific reports*, 14(1), 5297. <https://doi.org/10.1038/s41598-024-55662-w>
- [19] Bak, O., Braganza, A., & Chen, W. (2025). Exploring blockchain implementation challenges in the context of healthcare supply chain (HCSC). *International journal of production research*, 63(2), 687–702. <https://doi.org/10.1080/00207543.2023.2286491>