

# Optimizing blockchain for healthcare IoT: a practical guide to navigating scalability, privacy, and efficiency trade-offs

Mwaffaq Abu Alhija<sup>1</sup>, Osama Al-Baik<sup>1</sup>, Abdelrahman Hussein<sup>1</sup>, Hikmat Abdeljaber<sup>2</sup>

<sup>1</sup>Al-Ahliyya Amman University, Amman, Jordan

<sup>2</sup>Applied Science Private University, Amman, Jordan

## Article Info

### Article history:

Received Feb 28, 2024

Revised Apr 29, 2024

Accepted May 27, 2024

### Keywords:

Blockchain

Cryptographic techniques

Healthcare

Internet of things

Trade-off quantification

Use case mapping

## ABSTRACT

The adoption of blockchain technology provides significant disruptive benefits to internet-of-things (IoT) applications in healthcare in vital aspects like security, integrity, transparency, and efficiency. Nevertheless, in order to fully realize the potential of blockchain-driven solutions, healthcare organizations have to address intricate compromises between essential factors including scalability, privacy and resource utilization considering that the data sensitivity alongside strict regulatory compliance requirements characterize this sector. This research discusses the fundamental aspects of these trade-offs, including the range of consensus protocols (e.g. proof-of-work, proof-of-stake) and cryptographic techniques (e.g. zero-knowledge proofs, homomorphic encryption). A systematic choice matrix is created, which relates specific use cases of the healthcare IoT to the optimal tailored blockchain structures on such critical metrics as transaction volume, frequency, privacy level and resource restrictions. The suggested framework provides solid, actionable recommendations to healthcare organizations in order to help them benefit from the enormous promise of the blockchain for connected IoT healthcare by finding a balance between decentralization advantages and performance, security and compliance requirements.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Mwaffaq Abu Alhija

Al-Ahliyya Amman University

Amman, Jordan

Email: m.abualhija@ammanu.edu.jo

## 1. INTRODUCTION

Wearable sensors and internet of things (IoT) devices have proliferated at a rapid rate in the medical sector with applications including patient monitoring, remote diagnostics, and even fitness services [1], [2]. The number of health data products has skyrocketed due to the spread of devices; this information must be interpreted and transmitted safely between multiple systems for various stakeholder groups' benefit [3], [4]. However, centralized databases and health information systems imply a number of major disadvantages: the possibility of single point failures, vulnerability to data breaches, secretive operation without transparency, poor performance in working patterns and issues associated with interoperability [5], [6].

These issues have spurred the development of blockchain technology as a decentralized system to improve security, confidentiality, quality, and efficiency regarding healthcare data [1], [2]. Blockchain is a distributed ledger technology where transactions are entered in a chronological and public order across a peer-to-peer network by cryptographic validation and consensus mechanisms [3], [4]. Figure 1 shows the basic blocks of blockchain. The inherent characteristics of blockchain, such as decentralization, cryptographic security, immutability, and smart contracts, bring several benefits to healthcare, including secure data storage, integrity, auditability, and controlled access to medical records [5]-[7].

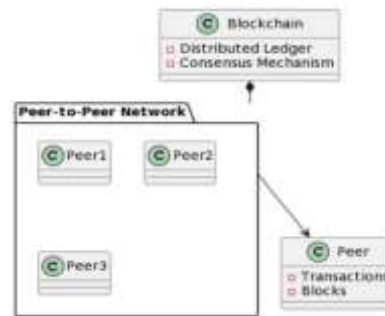


Figure 1. Basic blocks of blockchain

Rolling out blockchain-backed systems into healthcare, however, has its own implications. The specific healthcare applications should be evaluated with respect to the trade-offs encountered between scalability, privacy preservation, and resource performance [4], [8], [9]. For example, an IoT system for continuous patient monitoring which uses data from multiple IoT devices will demand a very high transaction rate with extremely low latency. In contrast, wearables living in the real world with heavy resource constraints might have to have protocols that are very efficient and quick. This implies that the sharing of health data between private parties requires a highly specialized level of control and anonymity in order to guarantee patient privacy. The activities transparency together with the anonymity of patients should be provided relative to the pharmaceutical supply chains [3], [10]

The focus of this paper is on the systematization and analytical basis for the use of blockchain architectures by healthcare stakeholders to guide their selection according to their particular demands and limitations. The evaluation of trade-offs between transaction throughput, network scalability, privacy preservation, computational complexity and energy efficiency is measured for diverse blockchain consensus mechanisms and cryptographic primitives. This is then linked to the specific requirements of heterogeneous healthcare use cases driven by IoT systems for uninterrupted monitoring, medical records sharing, pharmaceutical supply chains and so on. A decision matrix is proposed to match healthcare applications to optimal blockchain protocols considering both technical factors and compliance with healthcare regulations such as HIPAA [11]. The overarching goal is to enable informed choices in implementing customized blockchain-based solutions for secure and efficient healthcare data management.

## 2. LITERATURE REVIEW

Living healthy goes beyond avoiding illness and encompasses physical well-being, mental tranquility, and meaningful social interaction (World Health Organization, 2005). Ensuring quality healthcare for everyone, particularly as lifespans lengthen, becomes increasingly vital. Over the last twenty years, average life expectancy has increased from 73.7 to 78.6 years [12]. This development installs health care as the core part that is interrelated with the whole human life. Modern healthcare and wellness include not only social and mental health but also innovative technologies [13]. Our dream is to advocate “health for all” by using technology, interpreting the obtained data and developing new models of cooperative healthcare between patients and carers. This allows us to achieve a more profound understanding of our health and to personalize treatment plans [14], [15], thus leading us to the future of global health and resilience.

Health informatics goes beyond just computerization of healthcare. It covers handling the whole data life cycle, from capturing patient data to maximizing its use [16]. It is like a huge system of people, communities, diseases, treatments, and complex devices—all closely linked and interrelated [17]. Before the advent of computers, medical records were simply paper trails that are labyrinthine in nature, with each note filed in distinct folders that are only accessible at certain locations [18], [19]. Nonetheless, the 1960s and 1970s saw the advent of electronic health records (EHRs) driven by emerging technologies [19], [20]. These digital wonders made information retrieval and data analysis of treatment outcomes easy and also promoted patient compliance with checkups and medications [19], [20]. EHRs changed the entire concept of medical records into the easy to access, understandable and portable files. However, this digital convenience carries a shadow: increased worries about data security and privacy [21], [22].

Health-care systems should be designed to make information security the focus so that there is no unauthorized access or records altered by an unwanted process. Among needs to be addressed are ensuring the security of information and eliminating control by a single center; blockchain technology, which marks an

innovative breakthrough as compared with how things were done previously, does that successfully [23], [24]. Instead of traditional central servers, which are vulnerable to a single point failure and attacks [21], the whole blockchain network secures different sections of data in an unbroken chain making alteration or removal virtually impossible [25]. This non- mutability ensures data integrity, thereby protecting the information from internal and external threats. With its implementation, blockchain innovation comes to revolutionize healthcare by changing the most critical aspects of data security and authenticity [2]. This specific physical integrity offers a sequential nature that is supported by strong cryptographic codes, further contributing to the impossibility of tampering with records. This paradigm shift, from centralized vulnerability to decentralized resilience, empowers transformative healthcare practices and bolsters patient data protection.

**2.1. Overview of blockchain**

In healthcare, information would not be merely passed around but safely passed on and protected from tampering or disruption. This is the role of blockchain technology, a unique way for data communication and storage [23]. In the center of blockchain lies a decentralized network computers that eliminates the necessity for an intermediary authority creating unprecedented transparency and trust [26]. Figure 2 depicts the high-level blockchain architecture.

Origins: the seeds of blockchain were sown in the late 2000s with concepts that included, digital currencies like bitcoin. In 2008, an anonymous man by the name Satoshi Nakamoto released a white paper entitled “A peer-to-peer electronic cash system” that described his new model of financial transactions which were secure but at the same time decentralized and confidential. This revolutionary concept dubbed blockchain eliminated the role of banks as intermediaries to validate transactions and created new ways for trustless cooperation [27].

Core principles: i) decentralization: unlike those systems that use one server blockchain stores data across a network of computers which makes it nearly impossible to hijack the entire system [28]. ii) Immutable ledger: the blocks of information are connected, such that every one is cryptographically secured to the predecessor. Once a block is added, modifying its contents becomes virtually impossible, ensuring data integrity and permanence [25]; and iii) consensus mechanisms: transaction validation and network synchronization are ensured by protocols like proof-of-work or proof-of-stack.

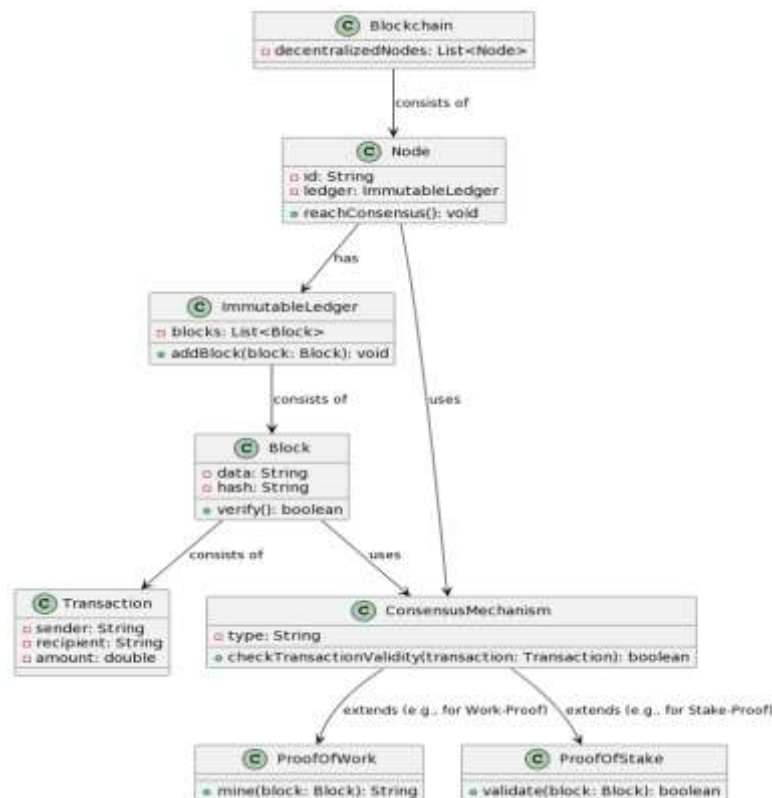


Figure 2. High-level blockchain architecture

Challenges and future: it is full of importance while blockchain technology faces challenges including scalability limitations, high energy consumption and variable regulative conditions [8]. However, these problems are better addressed by today's research and development. It is a revolutionary pre-coded all round scalable safe blockchain technology across virtually every industry [24].

## 2.2. Blockchain in healthcare

The potential to revolutionize the healthcare industry is high with blockchain technology. Blockchain's unique features, such as decentralization, transparency, and security, can help address several problems in healthcare information management. Here are some key aspects of how blockchain can benefit the healthcare sector:

- i) **Security and data integrity:** first, in terms of security issues related to the storage and administration of confidential health information on dematerialized blockchain systems, this research solutions showed that cryptographic algorithms used by those blockchains provide a high level of data protection [8]. Second, among well-implemented authentication mechanisms such as those of process-based access control procedures, robust ones ensure that they also contribute significantly to creating a very secure environment in which healthcare-related records should be stored [2]. Therefore, historical health records stored on the blockchain become almost invulnerable to any unauthorized changes or manipulations and offer one of the most influential attributes for both data integrity and security that are essential when seeking trustworthiness in healthcare information [4].
- ii) **Interoperability in healthcare:** blockchain technology serves as a single and standardized infrastructure in which healthcare-related data can be easily transmitted [25], [29]. This ensures secure collaboration between various healthcare providers and different systems as well as IoT devices. Blockchain makes it easier and more secure to obtain information about patients [24]; therefore, data can be easily communicated different entities in the healthcare ecosystem [3], [30]. Activities of healthcare providers become more coordinated and largely devoid of inefficient actions. Additionally, blockchain provides interoperability that improves communication and collaboration to deliver a fully integrated healthcare system centered around the patients.
- iii) **Data ownership and consent:** blockchain technology, which employs smart contracts, can successfully enable patients to define "who" may have access as well as the manner in which they should receive their sensitive health information [31]; this gives individuals an easy method of exercising more control over their personal medical data. These smart contracts enable patients to give out or refuse a right of access and ensure that no such data is given away to anybody who has not been authorized. This potential goes beyond the aspect of patient confidentiality to refer also in terms of informed consent [5], [31], getting a safe and transparent philosophy on health-related information management.
- iv) **Streamlined processes:** another promising feature of a blockchain is its potential for simplifying healthcare processes by becoming the only and single source of truth that all observers understand [7]. This reduces the number of mediators and intermediaries who were the causes of mistakes and needless delays in different administrative processes [23]. First and foremost, blockchain technology increases efficiency in billing processes, insurance claims, and supply chain management within the healthcare industry [1], [10]. The preferred technological solution for managing administrative functions in healthcare's ecosystem is the untrusted and transparent nature of blockchain. In the above-discussed ecosystem, this would provide all stakeholders with reliable access to information about accurate records because reliability fosters activities that occur efficiently when demonstrating desired levels.
- v) **Drug traceability:** in this respect, blockchain technology presents a vital solution for improving drug traceability [32] by offering an obvious and protected system across the pharmaceutical supply chain. The application of the blockchain ensures that drugs can be traced to their origin's authenticity is now confined, thereby reducing fakes or counterfeit perceptions surrounding medicines [33]. This increased traceability not only ensures the integrity of pharmaceuticals, but also safeguards patients as such a move fastens identification concerning their authenticity and movement. Blockchain technology stimulates confidence in the pharma supply chain [34]; therefore, it is a tool for confirming that medicines are authentic and of high quality by using decentralized immutable ledger.
- vi) **Clinical trials and research:** as reported by Trillium Health Partners (2017), blockchain technology may improve the transparency and efficiency of clinical trials and research. It increases the validity of study results because there is a reduced incidence of fraud as data cannot be illicitly altered in storage during trials [17], [35]. This platform is distributed and immutable in nature, thus providing a legal way for researchers to access information from trials [5], thus eliminating the chances of manipulation or misbehavior with reference to research. Overall, the inclusion of blockchains into clinical trials leads to increased transparency and accountability in research practice, which enhances the credibility of the results [6].

vii) Immutable audit trail: the first important point to note is that blockchain technology imparts an irreversible audit trail with logging and time stamping for every transaction or modification of the record. Therefore, it ensures an open and objective history [34]. Second, such an example provides the functionality for creating a non-modifiable audit trail, and this feature becomes a crucial part of organizations' efforts to fulfill their regulatory needs [33], along with boosting audits within many sectors, including health care. It offers an auditable trail that leaves a trace for various transactions, and it does not allow fraud issues since the officials are answerable. Hence, blockchain technology is ideal because it can be used as an effective tool to have the best performing record-keeping instruments.

Despite the advantages of blockchain technologies for healthcare, such challenges as scalability, privacy, resource efficiency, and regulatory implications or requirements must be considered [36]-[38]. However, using large ledgers may be cumbersome when applied at scale due to a vast number of transactions that require significant resources being available if all parties are expected to use it regularly enough [32]. Continual research and development in this area are bound to play a crucial role in conquering these challenges as well utilizing those benefits that blockchain technology can offer for healthcare. This has underlined and motivated this study. Below, we briefly overview the challenges and limitations of implementing blockchain in healthcare.

### 3. PROBLEM STATEMENT AND MOTIVATION

The discussion of blockchain protocols and their trade-offs in the arena of health IoT deployments is important because it helps to highlight some of the security issues as well as opportunities that can be embedded within sensitive healthcare data. The main considerations to the trade-offs between scalability, privacy, and resource efficiency in the realm of secure healthcare IoT using blockchain are as follows:

**Scalability:** one of the main issues to overcome by blockchain protocols is scalability, especially regarding effective processing of a high number of transactions [8]. Scalability is critical for smooth operation in the healthcare IoT context where a tremendous number of devices keep generating huge amount of data over the clock. The selected blockchain protocol should be scalable in the sense of being able to handle an increasing volume of data without affecting its performance [25], or with minimal impact. Solving the issue of scalability is critical to enabling successful adoption of blockchain technology across IoT devices used in healthcare.

**Privacy:** in healthcare, privacy is crucial to the success of the medical services provider; however, blockchain's transparent nature poses challenges in ensuring confidentiality between physicians and patients [31], [39]. Some blockchain protocols include privacy features such as zero-knowledge proofs or homomorphic encryption which add an additional layer of security for an individual's sensitive health data [40]. Nevertheless, there might be trade-offs while trying to implement these privacy-enhancing features [6], whereby scalability and efficiency may become compromised. It is necessary to find a middle ground between system performance and privacy to create a successful healthcare blockchain secure program.

**Resource efficiency:** especially in IoT devices with limited resources, blockchain transactions require computational resources [1], and therefore energy issues become critical for an IoT environment where computation ability is low and there are restrictions about the number of resources that can be used [4]. To address this, lightweight consensus protocols and optimized protocols must be the first. These measures are beneficial in protecting the IoT devices against being loaded by their resource requirement for the blockchain transaction, thereby responsible and efficient development of blockchain technology assimilation under these settings.

**Regulatory compliance:** the larger challenges emanate from the integration of blockchain solutions in healthcare because implementation needs to follow a framework that introduces other levels of complexity under health law, such as HIPAA-7819, which aims at protecting patient health data [5]. Healthcare information management should follow-up regulations, such as HIPAA, which are necessary for protecting patient privacy and to maintain the integrity and morality of healthcare settings [41]. Thus, when dealing with blockchain technologies as applied in healthcare settings, the compromise that one has to accept is scalability vs. privacy and resource-efficiency within the framework of applicable law, with solutions that should not only be based on advantages arising from the introduction of blockchain but also be well enough in relation to preceding regulatory contexts determining the health sector [42].

#### 3.1. Research objectives

With the growth of more connected IoT objects in healthcare, such as smartphones and wearable devices, healthcare needs to adapt to this growing amount of data, keep private health details secure, and work well even if their IoT objects are limited in resources. Selecting the best blockchain build for every job needs to deal with this tricky balance. The research has been classified into two main categories:

**Technical efficiency analysis:** we will examine how different mechanisms of agreeing (consensus methods), protecting information secretly (cryptography), and setting network connections affect growth,

keeping private details safe, and using resources in dominant blockchain systems. To conduct this analysis, we impose the following research question:

RQ1: how does the choice of consensus mechanisms in prominent blockchain protocols affect transaction throughput, network size limitations, and privacy-preserving capabilities for resource-constrained healthcare IoT environments?

Compliance use case mapping: we will develop a matrix to classify health apps that use IoT devices based on how important their data are, how often they perform transactions, and what resources are limited. We match these with proper blockchain architectures in terms of security measures. To conduct this analysis, we ask the following research questions:

RQ2: How can we create a framework to help healthcare stakeholders (institutions and developers) choose and implement blockchain solutions for IoT deployment, considering factors beyond technical efficiency, i.e., regulatory compliance?

### 3.2. Research scope

The scope of this research project is to explore how to leverage blockchain technology for secure and efficient data management in the booming healthcare IoT landscape. It highlights two key areas of focus:

- i) Trade-off quantification: develop a clear and straightforward framework to test the dominant blockchain systems (such as Hyperledger Fabric, Ethereum, Quorum) in terms of scalability, privacy preservation, and resource efficiency. This will ultimately help in developing a matrix for blockchain protocol selection. This framework will consider the following: a) scalability metrics: transaction throughput, latency, and network size limitations; b) privacy metrics: information leakage, attack resistance, and cryptographic strength of privacy-preserving features; and c) resource efficiency metrics: storage requirements, computational complexity, and energy consumption.
- ii) Use case mapping: apply the quantified trade-offs to specific healthcare IoT applications (e.g., continuous patient monitoring, secure medical record sharing, medication supply chain management) to a) identify optimal blockchain architectures for each use case based on its data sensitivity, frequency of transactions, and resource constraints; and b) develop a decision-making matrix to guide healthcare institutions and developers in selecting the most suitable blockchain solution for their specific needs.

### 3.3. Research questions

This study aims to demystify the complex trade-offs between scalability, privacy, and resource efficiency within blockchain protocols, empowering healthcare institutions and developers to optimize their IoT deployments. By providing a quantitative framework and decision-making tool, this research will pave the way for secure and trustworthy data management in healthcare, ultimately contributing to improved patient care and unlocking the full potential of connected devices in this critical domain. The research questions have been further decomposed as follows:

RQ 1.1: can a standardized classification system be developed for healthcare IoT applications on the basis of their trade-off requirements for scalability, privacy, and resource efficiency to facilitate targeted blockchain solution selection?

RQ 1.2: how can the decision-making framework be seamlessly integrated into existing healthcare IT planning processes and methodologies to ensure efficient adoption and enable adaptation to accommodate future advancements and innovations in blockchain protocols and healthcare IoT technologies?

## 4. METHOD

This study utilizes a mixed methods approach that combines qualitative and quantitative data. A systematic literature review was conducted to identify and analyze existing research on blockchain architectures and healthcare applications. The following databases were searched in November 2023: IEEE Xplore, PubMed, ACM Digital Library, and ScienceDirect. The search strategy included terms related to "blockchain", "healthcare", "internet of things", and "security". The following inclusion criteria were applied during screening: i) peer-reviewed articles, ii) published between 2016-2023, iii) written in English, and iv) relevance to blockchain protocols and/or healthcare applications.

Articles were excluded if they did not meet these criteria. Full text review was performed for articles that met the inclusion criteria after title/abstract screening. A standardized data extraction form was used to compile relevant findings from the included studies. The following data fields were extracted: blockchain architecture, performance metrics, healthcare use case, privacy and security evaluation, and compliance considerations. Two independent reviewers performed screening and data extraction, with any disagreements resolved through discussion. In total, 32 articles met the inclusion criteria and were included in the literature review.

To determine consistency between the reviewers in study selection, interrater reliability was evaluated using Cohen's kappa statistic. The two reviewers independently screened titles, abstracts, and full texts from the initial search results against the inclusion and exclusion criteria. Cohen's kappa assesses the level of agreement between raters beyond what would be expected by chance alone. A kappa value of 0.61-0.80 indicates substantial agreement, while 0.81-1.00 represents almost perfect agreement.

After independent screening of titles and abstracts, the interrater agreement between the two reviewers was found to be kappa=0.82, indicating near perfect agreement in deciding which articles should proceed to full text review. For full text review, Cohen's kappa was calculated to be 0.69, reflecting substantial agreement between the two reviewers on final article selection for inclusion in the systematic literature review. The high degree of interrater agreement at both screening stages demonstrates consistency in applying the predefined inclusion/exclusion criteria.

## 5. RESULTS

### 5.1. Consensus mechanism

The selection of consensus mechanisms in blockchain protocols can profoundly influence the system in terms of transaction throughput, network size limitations, and important options such as preserving privacy. For a summary of the most well-known consensus mechanisms reported in the literature, see Table 1.

- Proof-of-work (PoW): this is the original consensus algorithm employed in Bitcoin. Miners engage in difficult mathematical calculations to certify purchases and add new blocks. It is highly computational and energy intensive.
- Proof-of-stake (PoS): validators are selected to create a new block by the number of cryptocurrencies they own or that will be staked as collateral in PoS. It is more energy saving than PoW.
- Delegated proof-of-stake (DPoS): DPoS is a form of PoS in which a few delegates are voted as members by people in the community to attest transactions and produce blocks. It enhances the scalability and speed of transactions.
- Practical byzantine fault tolerance (PBFT): PBFT is a type of consensus algorithm that makes it possible for nodes within the network to come together and agree on the state despite the presence of faulty or malicious actors. It is commonly employed in permissioned blockchain networks.
- HoneyBadgerBFT: this is another BFT algorithm used to gain consensus in networks whose nodes are malicious or fail arbitrarily. BFT is characterized by asynchrony and high throughput.
- Proof-of-authority (PoA): in PoA, consensus is reached by a handful of authorized bodies (authorities) rather than through an open contest or stake-based serving. It is typically employed in a private or consortium blockchain.
- Proof-of-burn (PoB): in PoB, people send cryptocurrencies to an address that cannot be spent by anyone, thus burning them. Burning coins is believed to be a sign of dedication. Participants can either mine or validate transactions and be rewarded for their efforts.
- Proof-of-space (PoSpace) and proof-of-capacity (PoC): participants' available disk space is a resource that can be used as part of these consensus mechanisms. The larger the free space a participant has, the greater his or her chance to create a block.
- Proof-of-elapsed-time (PoET): PoET was created by Intel as a consensus mechanism in which participants are required to wait their turn for randomly determined intervals before developing blocks. It seeks to be energy efficient and secure.
- Proof-of-weight (PoWeight): this is a mechanism of consensus in which nodes with greater "weights" (which could be based on parameters such as reputation or stake) are more likely to have been chosen for making new blocks.

A suitable consensus mechanism is critical to the selection in resource-impaired IoT settings [40]. For example, PoS, in general, supports higher transaction throughput than PoW because it has a lower computational load. BFT consensus algorithms can offer high transaction throughput and low latency; however, they might have some issues scaling more extensive networks. Consensus mechanism selection is one of the factors used to decide how transactions should be validated and added to a blockchain.

Relatively, PoS may be more scalable than PoW, although the scope still exists on the count of available validity in efficient participation within the consensus process. As such, BFT algorithms are designed for a known and fixed set of nodes, which makes them inappropriate when it comes to big and dynamic networks. More specifically, PoS has no strong inherent privacy features, though such can be implemented through additional cryptographic mechanisms or dedicated privacy layers. Often, BFT algorithms concentrate on establishing consensus in an environment that is byzantine-faulty, but they usually do not directly consider issues such as privacy. Struggles with privacy are present across healthcare IoT environments despite the number of consensus mechanisms utilized in the most popular blockchain protocols.

Table 1. Consensus mechanism metrics

Consensus mechanism	Transaction throughput	Network size limitations	Privacy-preserving capabilities
Proof-of-work (PoW)	Moderate to high	Scalability challenges due to competition	Generally, lower because of transparent transactions.
Proof-of-stake (PoS)	High	Scales well with stake; wealth concentration may limit	May offer some privacy, but additional measures are needed.
Delegated proof-of-stake (DPoS)	High	Scalable; improved scalability over PoW	Similar to PoS; may require additional measures.
Practical byzantine fault tolerance (PBFT)	Very high	Suitable for permissioned networks	Focuses on consensus; additional measures needed.
HoneyBadgerBFT	High, asynchronous	Designed to scale gracefully	Focuses on consensus; additional measures needed.
Proof-of-authority (PoA)	High	Suited for private and consortium lockchains	Limited; relies on the trustworthiness of the authorities.
Proof-of-burn (PoB)	Depends on consensus (PoW/PoS)	Similar to the underlying consensus mechanism	Limited; burning addresses are public.
Proof of space and proof of capacity	Moderate	Scalable based on the available storage space	Limited; similar to PoW in terms of transparency.
Proof-of-elapsed-time (PoET)	Moderate to high	Scalable: fairness in timeout selection	Limited; primarily focuses on fairness in block creation.
Proof-of-weight (PoWeight)	Depends on the weighting criteria	Scalability depends on the weighting factors	Variations; additional measures may be needed.

## 5.2. Cryptographic techniques

The use of cryptographic techniques is essential for improving privacy protection on specific healthcare blockchain networks. These methods aid in the protection of patient data, maintain confidentiality, and ensure that health-related records are preserved. These techniques are often combined to create comprehensive privacy-preserving solutions tailored to the specific needs and regulatory requirements of the healthcare industry. The goal is to strike a balance between data utility and individual privacy, ensuring secure handling and sharing of healthcare information. Table 2 shows these common techniques and how they are recommended for use in healthcare.

Table 2. Cryptographic techniques in their uses in healthcare

Cryptographic technique	Brief description	Use in healthcare
Encryption	Involves transforming plaintext data into ciphertext using cryptographic algorithms and keys. Decryption reverses this process.	Used to protect data at rest (stored data) and data in transit (during transmission), ensuring that only authorized entities can access the information.
Zero-knowledge proofs	ZKPs allow one party to prove knowledge of a statement without revealing the actual information. This ensures that the verifier gains confidence in the truth of the statement without learning the details.	Employed for authentication, access control, and verifiable computation without exposing the underlying health information.
Homomorphic encryption	Enables computations on encrypted data without decrypting it. This allows data to remain confidential while being processed.	Enables secure computation of sensitive health data without compromising privacy, facilitating secure data analysis and sharing.
Secure multi-party computation (SMPC)	Allows parties to jointly compute a function over their inputs while keeping those inputs private. No party learns the inputs of others.	Facilitates collaborative data analysis and computations across multiple entities without revealing individual patient data.
Attribute-based encryption (ABE)	Allows access to data based on specific attributes, such as role, age, or medical condition, without revealing unnecessary details.	Supports fine-grained access control, ensuring that only authorized individuals with specific attributes can access relevant health data.
Differential privacy	Ensures that the inclusion or exclusion of a single record does not significantly impact the results of a data analysis, thus providing privacy guarantees.	Applied to statistical databases and health research to protect individual privacy while allowing aggregate data analysis.
Secure hash functions	Generate a fixed-size hash value from a variable-size input, and they are designed to be irreversible.	Employed to create hash values for data integrity verification, password storage, and anonymization.
Digital signatures	Use cryptographic algorithms to provide proof of the origin, identity, and status of an electronic document, transaction, or message.	Applied to electronic health records (EHRs) and communication to verify the authenticity and integrity of medical information.
Tokenization	Replaces sensitive data with unique tokens, ensuring that the original information is not exposed.	Applied to protect credit card information, patient identifiers, and other sensitive data in healthcare transactions.

Nevertheless, the implementation of these methods may influence the trade-offs between transaction latency, resource utilization, and the possibility of information leakage. A comparison of the most well-known techniques in terms of these trade-offs is presented in Table 3. In conclusion, the use of cryptographic techniques in healthcare-specific blockchain networks has proven to significantly improve privacy. It requires deliberate



consideration of the application under consideration, the desired level of privacy, and the type of computational resources available to the network members. The evolution of new cryptographic protocols stems from research, thereby ensuring that increased efficiency and generally reduced resource consumption are achieved over time. With any security strategy, an end-to-end approach that combines efficacy and applicability is a must when it comes to a successful implementation of the described cryptographic techniques within healthcare blockchain networks. Concerning the blockchain architectures designed for different healthcare systems that would offer optimal performance and meet some of the common healthcare standards such as HIPAA, proper consideration should be given to significant metrics and thresholds. With the help of these metrics, it is possible to perform an evaluation based on efficiency, stability, and regulatory compliance variables for a particular blockchain architecture. Table 4 provides a summary of key metrics and thresholds to consider.

Table 3. Cryptographic techniques comparison of trade-offs

Cryptographic technique	Transaction latency	Resource consumption	Information leakage
Encryption	Moderate to high	Moderate to high	Minimized with proper implementation
Zero-knowledge proofs	Moderate to high	Moderate to high	Minimized using proper ZKP protocols
Homomorphic encryption	Moderate to high	High	Minimized with proper implementation
SMPC	Moderate to high	High	Minimized using proper SMPC protocols
ABE	Low to moderate	Low to moderate	Minimized with proper ABE implementation
Differential privacy	Low to moderate	Low to moderate	Minimized with proper implementation
Secure hash functions	Low	Low	Minimal, designed to be irreversible
Digital signatures	Moderate to high	Moderate to high	Minimized with proper key management
Tokenization	Low	Low to moderate	Reduced, but secure tokenization is crucial

Table 4. Cryptographic metrics key items and description

Metric	Key item	Description
Data privacy metrics	Encryption strength	Evaluate the effectiveness of the encryption algorithms used to protect vulnerable medical data. Be sure that the company adheres to industry standards and regulations.
	Privacy-preserving techniques	Evaluate the use of cryptographic techniques that preserve privacy, such as zero-knowledge proofs, homomorphic encryption, and differential privacy.
	Data anonymization	Assess the effectiveness of anonymization techniques in preserving patient identities while achieving data utility
Transaction frequency metrics	Transactions per second (TPS)	Assess whether the system can handle a particular number of transactions every second. Also ensure that the number of transactions per second in the healthcare use case is aligned with what it expects.
	Scalability	To what extent has the scalability of blockchain architecture to handle larger transaction volumes without compromising performance been evaluated?
	Latency	Assess the transaction finalization time span and determine how quickly a deal is confirmed and integrated into the block drive. Latency may be critical for healthcare systems in real time.
Resource utilization metrics	Computational resources	Calculate the requirements for consensus protocols, cryptographic functions, and smart contract processing power. Ensure that it is friendly with the resources at our disposal.
	Storage requirements	Assess the requirements of storage space for the persistence of the blockchain ledger. Factors to be considered include the data growth rate and storage capacities.
	Network bandwidth	Evaluate the network requirements for communicating transaction data among nodes. Ensure that there is sufficient bandwidth to support communication.
Compliance metrics	HIPAA compliance	Assess HIPAA compliance frequently. The architecture of the blockchain must have the necessary provisions for privacy, security, and auditability.
	Audit trail	Evaluate whether the blockchain guarantees access to an authentic and unmodifiable ledger of all transactions along with any accessibility point set health data.
	Data ownership and consent management	Ensure that the blockchain architecture is equipped with tools for handling patient consent and information ownership issues according to healthcare standards.
	Regular audits	Put in place a program of periodic audits to ensure that healthcare stipulations are adhered to.
Security metrics	Node authenticity	Validate the participating nodes using secure authentication techniques.
	Smart contract	Assess smart contracts for weaknesses and possible attacks.
	Consensus mechanism security	Quantify the resistance of the chosen consensus mechanism to attacks and bad behaviors.
Interoperability metrics	Integration with existing systems	Assess the compatibility between the blockchain architecture and health information systems.
	Data interoperability	Assess the capability of blockchain to support standardized and fungible information exchanges among different health care actors.
Continuous development metrics	User experience (usability)	Evaluate the general overview of user experience by health professionals with regard to blockchain. Make it user-friendly for healthcare providers and compatible with their normal workflow.
	Continuous monitoring	Start off a culture of a never-ending monitoring system to reveal and treat inconsistencies with many needed norms.

The selection or design of a blockchain architecture based on those metrics, considering decision-specific thresholds (i.e. determining whether data is indeed confidential) that dials the optimal trade-off between usability and protecting patient confidentiality. Continual regular assessments and adaptations need to be made in relation to the dynamics of people's needs, demand patterns, and government regulations. Table 5 shows the decision matrix. This quantifiable decision matrix matches specific healthcare applications to optimal blockchain architectures based on technical factors such as transaction volume, privacy needs, and device constraints, along with healthcare regulatory compliance considerations. The guidelines help select customized blockchain solutions that are tailored to application requirements.

Table 5. Decision matrix of healthcare applications for optimal blockchain protocol

Healthcare application	Data sensitivity	Transaction frequency	Resource constraints	Recommended blockchain protocol
Continuous patient monitoring using IoT devices	High	High	Moderate	Permitted blockchain with BFT consensus (e.g., Hyperledger Fabric)
Remote patient diagnostics and telehealth	High	Moderate	Low	Public permissionless blockchain with PoW consensus (e.g. Ethereum)
Supply chain management for pharmaceuticals	High	Low	Low	Hybrid blockchain with PoA consensus (e.g., Xayn Chain)
Medical research and clinical trials	High	Low	Moderate	Private permissioned blockchain with PBFT consensus (e.g. Hyperledger Sawtooth)
Health data exchange between providers	High	Moderate	Moderate	Consortium blockchain with PoET consensus (e.g., Intel Sawtooth)
Fitness and lifestyle data tracking	Low	High	Low	Public permissionless blockchain with PoS consensus (e.g. Cardano)

## 6. DISCUSSION

Integrating a decision-making framework for adopting blockchain protocols and healthcare IoT technologies into existing healthcare IT planning processes requires a thoughtful and systematic approach. This approach should underscore the need for a strategic and careful methodology when introducing new technologies such as blockchain protocols and healthcare IoT solutions into the healthcare information technology (IT) landscape. We propose the following approach to seamlessly integrate the decision-making framework and ensure adaptability to future advancements:

- Understanding existing processes: first, it should be understood and analyzed what is currently happening with healthcare IT planning processes. Isolate the relevant stakeholders, decision makers, and currently used acceptance criteria for technologies.
- Strategic alignment: place the decision-making framework within the larger context of organizational goals and strategic objectives held by the healthcare facility. Ensure that the adoption of technology conforms to the mission and vision.
- Stakeholder involvement: identify the necessity to address various stakeholders in decision making. This may involve IT specialists, clinicians, administrators, compliance officers, among others.
- Defining decision criteria: define the decision criteria for selecting blockchain protocols and healthcare IoT technologies. Data security, regulatory compliance (HIPAA), interoperability, scalability, and adaptiveness
- Educating stakeholders: train and create awareness programs for stakeholders affected by the decision-making process. Ensure that all stakeholders are aware of the potential and challenges involved in implementing these technologies.
- Governance integration: aligning with governance by embedding the decision-making framework in the current IT governance architecture. Ensure that the framework is aligned with governance principles, compliance requirements, and risk management practices.
- Scalability and flexibility: evaluate the scalability and flexibility of the selected technologies. Opt for solutions that can adapt to changing healthcare IT infrastructure and allow integration of future innovations in blockchain protocols and IoT technologies.
- Testing feasibility: by conducting pilot projects for the evaluation of selected technologies in a confined setting. This offers organizations the opportunity to collect field data before large-scale deployment.
- Transparent communication: create a clear communication strategy to inform stakeholders about the deliberation process. Generate feedback mechanisms to help respond in time and subsequently make productive decisions.

- Documentation and knowledge transfer: recording: on a regular basis, note down decisions which are made using the framework. Besides enumerating reasons, circumstances and consequences, we will be able to use them to my advantage in the future. Knowledge transfer: publicize to new team members or stakeholders for the reason of not losing consistency.
- Vendor collaboration: join hands with technology vendors and solution providers in creating partnerships. Make sure you stay abreast with the recent advancements and the new developments in the blockchain protocols and the health care IoT technologies by regular dialog.
- Continuous improvement: an iterative approach is used to undertake the decision-making. Review and update the decision-making system on a regular basis by adding in new technologies as they come out and adjusting to the changing needs of the organization.
- Compliance integration: encompass the parts pertinent to following regulations, especially in the field of healthcare where the observance of rules like HIPAA is mandatory. Ensure that the chosen technologies must be in compliance with the authority regulations.
- Risk assessment: the bottom line is to make sure that a risk management structure is integrated into the decision-making process. Assess the possible dangers of network using blockchain protocols and IoT technology, and develop mitigation strategies.

Finally, the employment of blockchain technologies in combination with the framework of healthcare IoT solutions for decision-making is a holistic approach that integrates the organizational goals, the stakeholders' involvement, governance tokens, scalability, and continuous improvement. The institutions can overcome the problems of technology adoption and, at the same time, stay successful in the planning and compliance with the regulations. Figure 3 depicts the relational network between the different metrics, trade-offs, and decisions components.

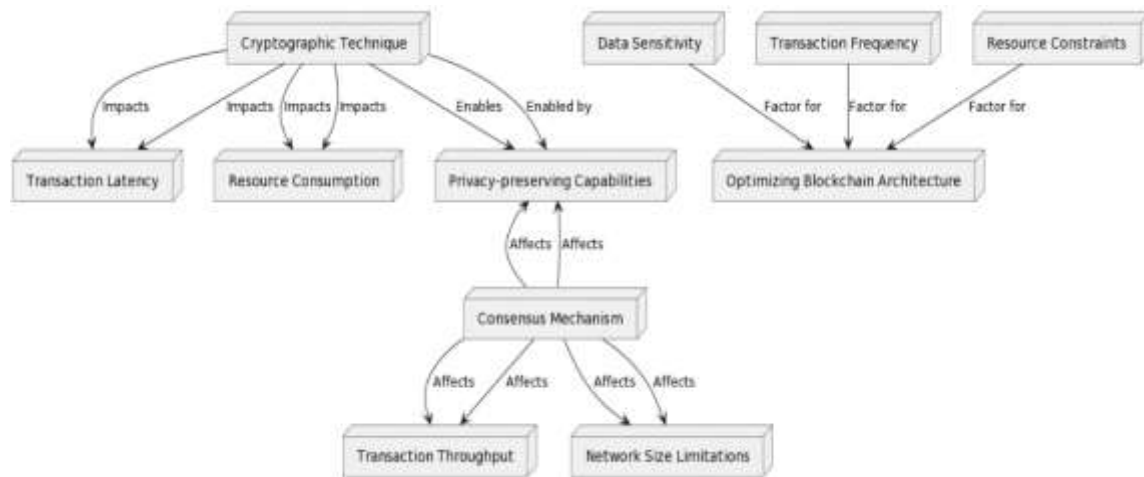


Figure 3. Relational network of blockchain protocol selection metrics

## 7. CONCLUSION

In this paper, we offer a systematic framework for assessing blockchain protocols and determining the best constructions among healthcare IoT deployments. We quantified the trade-offs between scalability, privacy and resource efficiency for different consensus mechanisms as well as cryptographic techniques. This study, however, revealed that transaction throughput; network limitations computational complexity and information leakage change considerably based on the design of blockchain. However, matching protocol capabilities to application requirements is critical.

A decision matrix was proposed to link healthcare use cases involving data sensitivity, transaction frequency, and device constraints to the most appropriate blockchain solutions. This provides concrete guidelines for stakeholders seeking to harness the advantages of blockchain while meeting industry regulations. As the healthcare IoT landscape continues to evolve, this research equips institutions with the knowledge to securely share data and drive efficiency gains through customized blockchain implementations. Further studies can build on these foundations to incorporate new technologies and refine architecture choices for the next generation of connected care.





## REFERENCES

- [1] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/IJWGS.2018.095647.
- [2] A. Azaria, A. Ekblaw, and A. Lippman, "MedRec: trustworthy and efficient health record management using blockchain," 2016.
- [3] S. Singh, S. K. Sharma, P. Mehrotra, P. Bhatt, and M. Kaurav, "Blockchain technology for efficient data management in healthcare system: opportunity, challenges and future perspectives," *Materials Today: Proceedings*, vol. 62, pp. 5042–5046, 2022, doi: 10.1016/j.matpr.2022.04.998.
- [4] K. Christidis and G. Devetzis, "Blockchain: A distributed ledger technology with applications beyond cryptocurrency," *Future Generation Computer Systems*, vol. 78, pp. 394–401, 2016.
- [5] R. Dabholkar, N. Banait, and R. S. Gunti, "Blockchain technology in healthcare: securing medical records through distributed ledger technology," *Journal of Electronic Commerce in Research and Applications*, vol. 17, no. 4, pp. 229–242, 2018.
- [6] X. Yue, H. Wang, W. Jin, and X. Yu, "A secure and trustworthy medical information exchange scheme based on blockchain technology," *International Journal of Medical Informatics*, vol. 97, pp. 123–134, 2016.
- [7] A. Azaria and S. R. Mudumbai, "Secure and transparent provenance chain for healthcare blockchain," *IEEE Journal of Biomedical and Health Informatics*, vol. 21, no. 4, pp. 1262–1271, 2016.
- [8] M. P. McBee and C. Wilcox, "Blockchain technology: principles and applications in medical imaging," *Journal of Digital Imaging*, vol. 33, no. 3, pp. 726–734, 2020, doi: 10.1007/s10278-019-00310-3.
- [9] M. H. Miraz and M. Ali, "Applications of blockchain technology beyond cryptocurrency," *Annals of Emerging Technologies in Computing*, vol. 2, no. 1, pp. 1–6, Jan. 2018, doi: 10.33166/AETiC.2018.01.001.
- [10] N. H. Truong, Y. Lee, and D. Park, "IoT applications in supply chain management: a comprehensive overview," *Journal of King Saud University - Computer and Information Sciences*, vol. 32, no. 4, pp. 428–448, 2020.
- [11] R. S. Evans, "Electronic health records: then, now, and in the future," *Yearbook of medical informatics*, vol. 25, no. S 01, pp. S48–S61, 2016, doi: 10.15265/IYS-2016-s006.
- [12] E. Yu, Q. He, J. Wu, and F. Wang, "Medical big data mining and analytics: challenges and opportunities for healthcare systems," *Journal of Medical Systems*, vol. 41, no. 12, 2017.
- [13] S. V. Zanjali and G. R. Talmale, "Medicine reminder and monitoring system for secure health using IoT," *Procedia Computer Science*, vol. 78, pp. 471–476, 2016, doi: 10.1016/j.procs.2016.02.090.
- [14] L. Y. Mano *et al.*, "Exploiting IoT technologies for enhancing health smart homes through patient identification and emotion recognition," *Computer Communications*, vol. 89–90, pp. 178–190, Sep. 2016, doi: 10.1016/j.comcom.2016.03.010.
- [15] W. Zhao, K. Lun, and C. Gordon, "IoT-enabled real-time patient flow management for smart hospitals," *IEEE Access*, vol. 7, pp. 127775–127785, 2019.
- [16] R. L. Blum and N. M. Lorenzi, "Health informatics: looking back and moving forward," *Yearbook of medical informatics*, vol. 21, no. 01, pp. 1–6, 2011.
- [17] J. Kang *et al.*, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, 2019, doi: 10.1109/JIOT.2018.2875542.
- [18] G. Harvey and A. Kitson, *Implementing evidence-based practice in healthcare*. Taylor & Francis, 2015.
- [19] E. Coiera, "Learning from the history of electronic medical records," *Journal of the American Medical Informatics Association*, vol. 4, no. 6, pp. 589–596, 1997.
- [20] R. S. Dick, E. B. Steen, and F. E. Carr, "The ONC data standards for meaningful use: a framework for improving health information exchange," *Health Affairs*, vol. 24, no. 3, pp. 485–495, 2005.
- [21] D. V. N. Car, "Health information security and privacy: an overview," *Journal of medical Internet research*, vol. 17, no. 5, 2015.
- [22] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017, doi: 10.1109/JIOT.2017.2694844.
- [23] D. Tapscott and A. Tapscott, "Blockchain revolution: how the technology behind Bitcoin is transforming business, government, and our lives." 2016.
- [24] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *Journal of Medical Systems*, vol. 43, no. 1, p. 5, 2018, doi: 10.1007/s10916-018-1121-4.
- [25] M. Swan, *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc., 2015.
- [26] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," pp. 1–9, 2013, [Online]. Available: <https://bitcoin.org/bitcoin.pdf>.
- [27] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *arXiv preprint*, 2019.
- [28] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
- [29] A. Mazayev, J. A. Martins, and N. Correia, "Interoperability in IoT through the semantic profiling of objects," *IEEE Access*, vol. 6, pp. 19379–19385, 2018, doi: 10.1109/ACCESS.2017.2763425.
- [30] M. H. Miraz and M. Ali, "Blockchain enabled enhanced IoT ecosystem security," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 200, 2018, pp. 38–46.
- [31] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of Medical Systems*, vol. 40, no. 10, 2016, doi: 10.1007/s10916-016-0574-6.
- [32] M. K. Chen, Y. Ma, Y. Liu, and Y. Cheng, "Smart wearable healthcare systems: opportunities and challenges," *IEEE Communications Magazine*, vol. 57, no. 10, pp. 30–35, 2019.
- [33] T. J. Oh and N. Jung, "Big data analysis in healthcare systems for medical doctors: a comprehensive review," *Journal of Healthcare Engineering*, vol. 9, no. 4, pp. 369–383, 2019.
- [34] S. Jha, R. Kumar, J. M. Chatterjee, and M. Khari, "Secured blockchain based e-health record management system," *International Journal of Advanced Science and Technology*, vol. 29, no. 7s, pp. 454–460, 2019.
- [35] D. Verma *et al.*, "Internet of things (IoT) in nano-integrated wearable biosensor devices for healthcare applications," *Biosensors and Bioelectronics: X*, vol. 11, p. 100153, Sep. 2022, doi: 10.1016/j.biosx.2022.100153.
- [36] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.
- [37] A. R. H. Hussein, "Internet of things (IOT): research challenges and future applications," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 6, pp. 77–82, 2019, doi: 10.14569/ijacsa.2019.0100611.
- [38] Z. Alansari *et al.*, "Challenges of internet of things and big data integration," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 200, 2018, pp. 47–55.





- [39] Z. Alansari *et al.*, "Internet of things: infrastructure, architecture, security and privacy," in *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, Aug. 2018, pp. 150–155, doi: 10.1109/iCCECOME.2018.8658516.
- [40] M. Andoni, A. Raychowdhury, and D. Zheng, "Zero-knowledge proofs for blockchain privacy: Foundations, state of the art, and future directions," in *2018 IEEE International Conference on Blockchain (Blockchain)*, 2018, pp. 202–214.
- [41] J. W. Creswell and V. L. P. Clark, *Designing and conducting mixed methods research*. Sage publications, 2017.
- [42] R. Krueger and M. Casey, *Focus groups: a practical guide for applied research*. Sage publications, 1989.

## BIOGRAPHIES OF AUTHORS







**Mwaffaq Abu Alhija**     is an Associate Professor at the Department of Computer Science at Al-Ahliyya Amman University, Jordan. His main research interests lie in the areas of operating system design, distributed computing systems, multimedia communication and networking, mobile and wireless networks, data and network security, wireless sensor networks, Cybersecurity, and parallel computing. He can be contacted at email: m.abualhija@ammanu.edu.jo.







**Osama Al-Baik**     is currently an assistant professor in the Software Engineering Department at Al-Ahliyya Amman University, his research interests have been in AI and machine learning, software and systems engineering, lean software development, software process improvements (SPI), and software project management. He has over 18 years of experience and technical expertise in a diverse range of technologies within multiple industry settings. He has demonstrated accumulative success in various footprints including SDLC implementation, process improvements and reengineering, IT governance, IT operations, and implementing international IT quality standards. He has been working in software development and project management for multinational companies, where he has held senior positions. He has a Bachelor's degree in Computer Information Systems from Amman University, Jordan, a Master's degree in Software Engineering from DePaul University, USA, and a Doctor of Philosophy in Software Engineering and Intelligent Systems from the University of Alberta, Canada. He is a Project Management Professional (PMP) by PMI, a Certified Project Manager (CPM) by IAPPM, and an AI Maturity Assessor (AIMA) by IAIDL. He can be contacted at email: o.albaik@ammanu.edu.jo.



**Abdelrahman Hussein**     is an Associate Professor at the Department of Computer Science at Al-Ahliyya Amman University, Jordan. He received his first degree in Computer Science from Jordan University of Science and Technology, Jordan, in July 2000, master degree in Computer Science from Jordan University, Jordan in July 2003, and Ph.D. from the Anglia Ruskin University ARU, UK in 2010. His main research interests lie in the areas of VoIP, mobile Ad-Hoc networking, and E-learning. He can be contacted at email: a.husein@ammanu.edu.jo.



**Hikmat Abdeljaber**     received the Ph.D. degree in Information Sciences and Technology in 2010 from the Universiti Kebangsaan Malaysia, UKM, Malaysia. He currently holds a University Assistant position at the Applied Science Private University in Jordan, Faculty of Information Technology. He lectured in the fields of computer science and information systems for both undergraduate and graduate levels. He has published papers in the area of information retrieval and artificial intelligence. His research interests include information retrieval, semantic web technology, natural language processing and machine learning. He can be contacted at email: h\_abdeljaber@asu.edu.jo.