ACHSM Asia-Pacific Journal of Health Management

RESEARCH ARTICLE

INVESTIGATING BLOCKCHAIN UTILIZATION CHALLENGES IN THE HEALTHCARE SYSTEM IN JORDAN

Ahmad AL dalabeeh[1], *Ahmad Nabot*[*2]

1. Software Engineering Department, University of Petra, Jordan
2. Software Engineering Department, Al-zaytoonah University of Jordan

Correspondence: a.nabot@zuj.edu.jo

ABSTRACT

Blockchain technology has emerged as a transformative innovation across multiple sectors, including finance, healthcare, agriculture, and real estate. Despite its widespread adoption, the healthcare system in Jordan has not yet leveraged blockchain for patient information storage, facing significant implementation challenges.

This study aims to investigate blockchain utilization challenges in Jordanian hospitals, clinics, and medical labs as doctors face challenges in verifying patient diagnostic conditions and accessing medical histories in the current off-chain systems. The study employed a mixed methodology to collect the required data from the study participants using a questionnaire survey and to confirm the study hypotheses with published studies. Data is collected from 100 participants, such as doctors, managers, nurses, consultants, and software developers. The collected data was analyzed using SPSS to investigate the challenges of utilizing blockchain in the healthcare industry.

The study findings revealed that security, privacy, reliability, and integrity help improve the healthcare industry in Jordan by storing and retrieving patients' histories for better treatment. In addition, these challenges are the main concerns of such technology in the healthcare industry in Jordan. Therefore, the study recommends utilizing such technologies in healthcare institutions for better diagnostics. Finally, the findings provide insights into the healthcare industry by examining the benefits of such technology in addressing such challenges.

KEYWORDS

blockchain, smart contract, healthcare, EHR, Jordan

INTRODUCTION

Today, blockchain technology is used in many applications including data management, financial services, cybersecurity, the Internet of Things, and the healthcare industry. Blockchain applications are attracting much attention to offer secure healthcare data and uphold patient privacy. Through the safe exchange of patient data and the encryption of such data using blockchain technology, the blockchain transforms conventional healthcare into a more dependable and accurate diagnosis and treatment. Additionally, blockchain utilization facilitates the doctors' understanding and storage of patient information [1]. Healthcare is a significant worldwide industry that contains personal and sensitive information that must be stored appropriately. This information should be accessible and utilized by authorized personnel for medical purposes.

Moreover, blockchain technology has gained significant traction across various industries, including healthcare, due to its potential to enhance security, privacy, and interoperability [71 - 74]. Many countries have explored blockchain applications in healthcare to secure electronic health records (EHR), streamline data sharing, and improve regulatory compliance. However, there has been limited research on blockchain adoption in Jordan's healthcare sector. Therefore, this study aims to bridge this gap by investigating the feasibility and challenges of implementing blockchain in Jordan's healthcare system.

Despite global advancements, Jordan presents a unique case for blockchain adoption in healthcare. The country's healthcare system is highly fragmented, comprising various government and private hospitals, each maintaining separate data management systems [3]. Unlike centralized models in some countries, this fragmentation poses significant challenges to implementing a unified blockchain-based system. Furthermore, awareness and understanding of blockchain technology among Jordanian healthcare professionals remain limited, creating additional adoption barriers. This study seeks to analyze the current landscape of blockchain in healthcare in Jordan, assess its potential benefits, and address the challenges specific to its implementation. By leveraging insights from international studies and contextualizing them within Jordan's unique healthcare infrastructure, this research aims to provide a comprehensive evaluation of blockchain's role in enhancing data security, reliability, and interoperability in Jordan's healthcare sector.

Blockchain deploys various techniques that help improve information storage, retrieval, protection, and safety. These techniques include electronic health records (EHR), decentralized networks, cryptographic techniques, smart contracts, and consensus mechanisms [2]. Furthermore, blockchain increases the healthcare industry's efficiency, reliability, and trust for all parties. This is because of the techniques used, such as distributed ledger technology (DLT) of transactions and a decentralized, immutable database that makes tracking assets and transaction data in a corporate network easier. A property may be physical [3] or mental [4]. Most users participating in the blockchain network must agree and provide their consent for a transaction to be recorded in the ledger [5].

The next section discusses the relevant studies of blockchain technology and the healthcare industry. Section 3 describes the research method. Section 4 presents the results, while Section 5 discusses the study results. Finally, section 6 outlines the study conclusion including limitations and future work.

BACKGROUND

BLOCKCHAIN TECHNOLOGY

A blockchain is a decentralized network of records or public ledger for all transactions that have taken place or digital events that have been exchanged between the involved parties in the blockchain. Most system users verify each transaction in the general ledger, and data cannot be deleted once entered. To make a simple and direct comparison, each transaction made is contained in a private, verifiable record on the blockchain. Instead of stealing files from a prominent site stored in a secure area, it is simpler to do so than to do it in a place where hundreds of people could witness your actions [6]. The word blockchain is derived from the "chain" of a group of "blocks" that contains information, where the block represents a network transaction and the "chain" refers to a group of" blocks". Each new" block" is added to a distributed ledger and verified by a group of network participants known as miners. the new transaction is attached to the end of the chain [7]. Blockchain is a distributed ledger technology (DLT) of transactions and a decentralized, immutable database that makes tracking assets and transaction data in a corporate network easier. A ledger consists of a chain of blocks, which allocates a block to a set of transactions. Each block includes a date and a hash function of the previous block to tie the blocks together. Block data integrity and non-denial are verified using the hash function [8]. Finally, blockchain is a database that only permits adding and changing its contents and maintains a comprehensive record of each addition and update. These operations are called" Transactions," and are applied to the database in batches called clusters. The blocks are connected because each block carries a hash of all the transactions from the preceding block [9].

HOW DOES BLOCKCHAIN WORK?

In buy and sell transactions, the seller records the sale as a credit, while the buyer debits their ledger. Both parties maintain ledgers to track activities. The buyer initiates the exchange by creating a blockchain block containing transaction details. This allows verification of funds transfer. Blocks form a chronological chain, serving as a permanent, accessible ledger. Blockchain is encrypted for integrity and extends beyond cryptocurrencies to various applications like copyright management, voting, and supply chain oversight. [10]. Eliminating the need for third-party validation and payment processing, blockchain technology reduces transaction costs and processing times. Additionally, it simplifies the maintenance of ledger systems as there are fewer systems to manage [11]. Miners play a crucial role in the blockchain network by finding, verifying, and adding new transactions. Transactions are validated using cryptographic keys, with the private key accessible only to the owner while the public key is visible to everyone on the network. Each transaction is signed with the appropriate key pair, preventing the reuse of coins. Once confirmed by miners, transactions are tamper-proof and irreversible. This characteristic was pioneered by Satoshi Nakamoto to ensure blockchain integrity. The information stored on the blockchain is accessible globally, eliminating the need for traditional transactions as all activities are tracked and recorded securely [12]. The Nakamoto Consensus Protocol governs blockchain operations by establishing rules for validating transactions, accepting new blocks, and selecting block paths, thus preventing redundancy. It distinguishes between global and local consensus methods. In the worldwide model, exemplified by Bitcoin, the genesis block is shared by all nodes, validating all transactions. Conversely, the regional model requires consensus only from participating users, reducing storage requirements and enhancing scalability. Nakamoto's consensus relies on proof-of-work (PoW), which is resource-intensive and challenging to quantify [13]. Since no central body monitors laws and regulations, proof-of-work ensures that each transaction validator acts honestly. Miners in blockchain networks play a critical role in maintaining consensus, ensuring all nodes have identical copies of the blockchain. This uniformity makes changes to previous blocks costly and challenging, as subsequent transactions must re-verify any modifications. Solving complex hash functions is a prerequisite for adding new blocks, with validators certifying the correct hash value. Successful miners receive Bitcoin and transaction fees, with higher fees prioritizing transactions. Peck likens introduced hash functions that identify one key for multiple locks, explaining the process as selecting the appropriate key and leaving it in place for confirmation by other network users [14], [15]. Figure 1 shows blockchain work behavior and Figure 2 represents the blocks of blockchain technology that consist of a decentralized database, data, and hash.

FIGURE 1: BLOCKCHAIN WORK BEHAVIOR

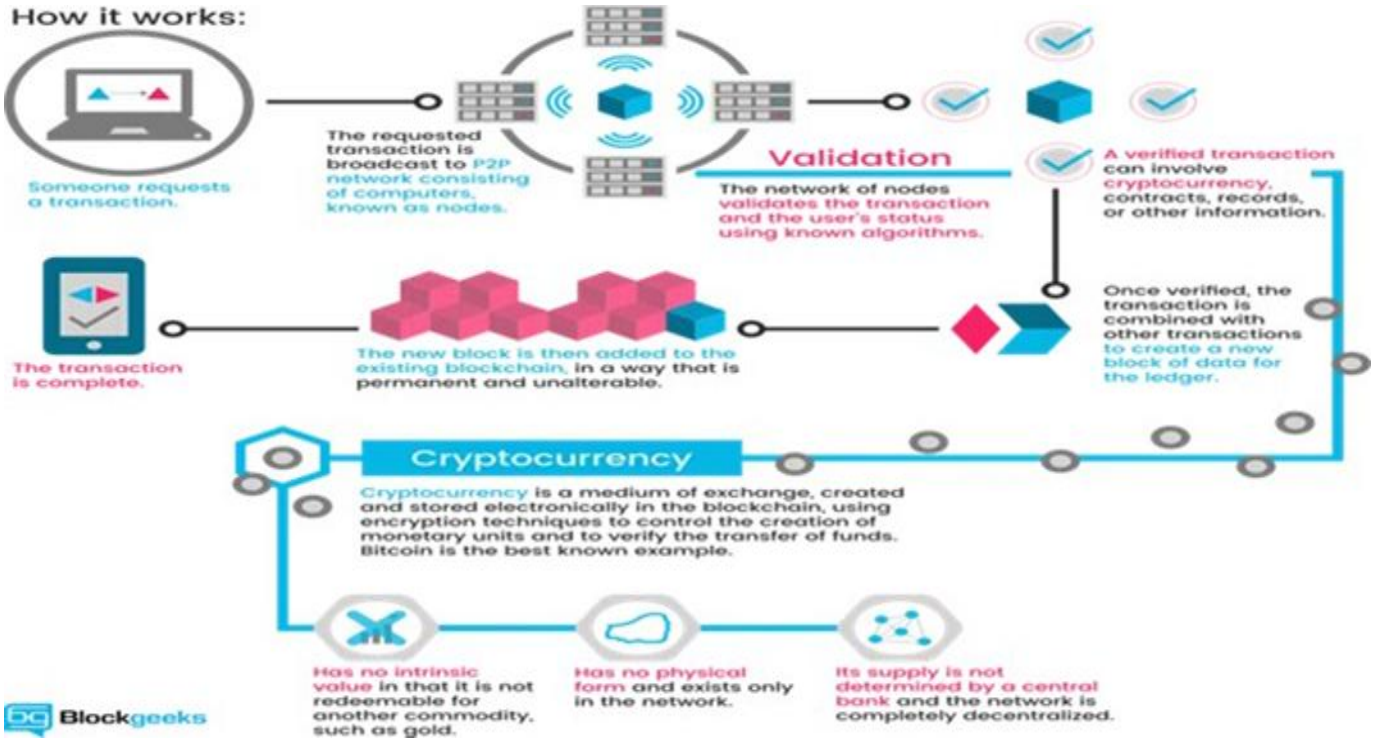
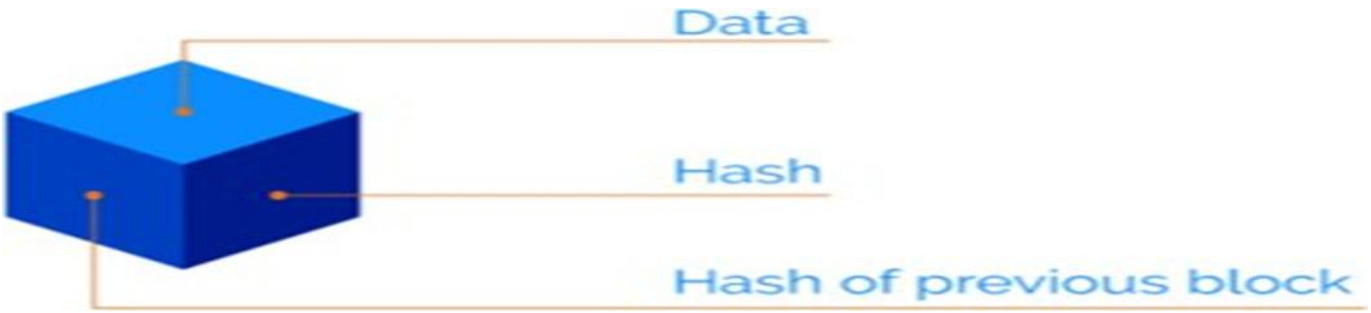


FIGURE 2: REPRESENTATION OF EACH BLOCK IN A BLOCKCHAIN



BLOCKCHAIN ELEMENTS

Blockchain technology consists of a decentralized network where each node holds a copy of a distributed ledger, ensuring transparency and eliminating a single point of failure. Transactions are secured through cryptographic techniques, making them immutable and tamper-proof. Consensus mechanisms like Proof-of-Work (PoW) and Proof-of-Stake (PoS) validate transactions and maintain integrity. In addition, Smart contracts enable automated, self-executing agreements without intermediaries. Blockchain protocols govern the creation and validation of blocks. The system balances transparency with anonymity, offering robust security features. Decentralized apps (DApps) take advantage of these properties to propose novel solutions to various industries [16, 17].

Decentralized Database: A decentralized database is data storage that is integral to blockchain-based systems, information is spread across multiple network participants to increase fault tolerance, reliability, and resistance to alteration. Blockchain utilizes distributed ledgers that are cryptographically secure, have centralized data storage, and lack authority. Consensuses like the PoW and the PoS authenticate and regulate transactions. Decentralized databases facilitate fast access from any node, which enhances security by preventing malicious attacks. They provide a powerful solution for secure, transparent, and decentralized data storage and management [18]. A unique aspect of blockchain-based healthcare systems is the concept of decentralized data management. This innovation promotes decentralized control over the data of patients, shifting the ownership of these data from institutions like hospitals or insurance companies to the patients themselves. Blockchain's cryptographic principles ensure the safe store, access, and sharing of patient's medical information. This paradigm shift promotes data privacy, transparency, and patient autonomy, all of which are responsible for empowering individuals to control their healthcare.

FIGURE 3: BLOCKCHAIN DECENTRALIZED DATABASE

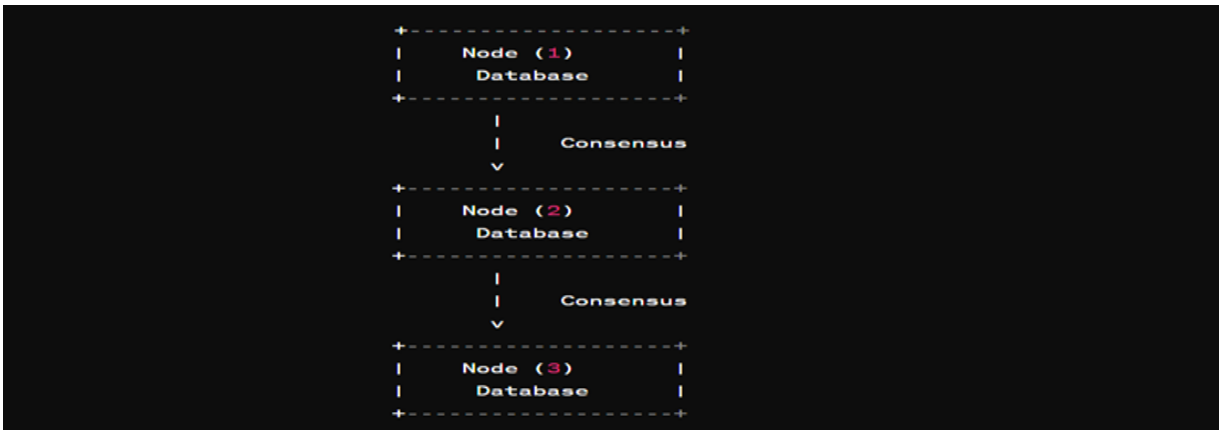


Figure 3 illustrates the decentralized database within a blockchain network. Each node represents a participant, storing a copy of the database. Arrows signify communication and consensus mechanisms, ensuring agreement on the database state. Transactions are validated and added to the database independently by each node, providing transparency and security [19].

1) Block: The block is the main nerve in blockchain technology, containing data related to many transactions. The blocks are linked with each other by mixing the previous block with the new block and surrounding it with a tight circle in the Blockchain [20].

2) Hash: A mathematical process known as hashing converts an input of any length into an encoded output of a given length. The hash is constant in size regardless of the original amount of data. Since hash functions are" one-way", they cannot be used to reverse engineer by taking the encrypted information out of the hashed output. However, if you apply the same function to the same data, the hash will be the same, allowing you to verify that the data is identical and correct. [23]

FIGURE 4: BLOCKCHAIN STRUCTURE

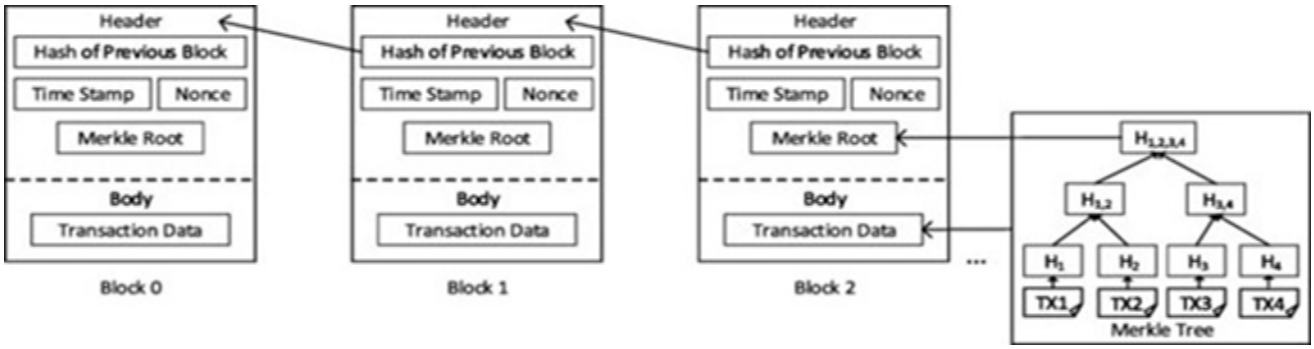


Figure 4 shows the structure of blockchain blocks, each block is divided into two parts, a header, and a body of transactions. The header contains the data description of the block containing all the details about the block in the blockchain [21]. The latest release to monitor program and protocol updates is among the fields in the block header. A timestamp, the number of transactions, and the block size are also included in the header. The hash value of the most recent block is displayed in the Merkle root field. In decentralized systems and P2P networks, Merkle tree hashing is frequently employed for effective data verification [22].

FIGURE 5: SHA-256 HASH FUNCTION

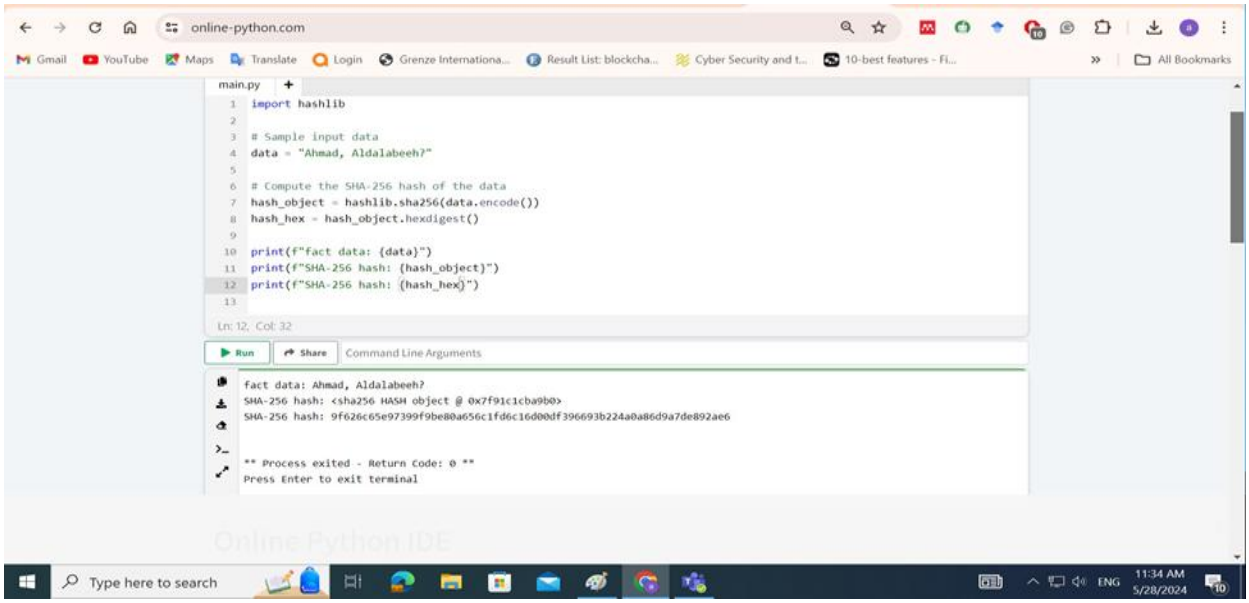


Figure 5 shows the SHA-256 hash function, which produces a 256-bit hash and proves it by Python code. Hash functions are vital for maintaining the integrity and security of data in various applications, from simple data verification to complex cryptographic systems. Their deterministic, efficient, and secure nature makes them indispensable in modern computing.

3) Minor: A CPU that attempts to solve complex computational problems to discover a new block is known as a miner. As miners are a group of people who sit at a computer and work on blockchain applications to solve emerging

problems in the technology, miners can also work Individually or in groups to try to find a solution to the mathematical problem [24].

4) Transaction: A transaction is a computational unit that implements and stores records in the blockchain after verifying user identity in the network. Blockchain allows users to review previous transactions at all times and prevent any changes [25].

5) Consensus Mechanism: Consensus mechanisms include proof-of-stake (POS) and Proof-of-Work (POW), which are important in authorizing, verifying, and managing transactions. For instance, PoS manages large-size transactions to control transaction costs and resource consumption. In addition, PoW manages the blocks that miners can add to the network [26].

BLOCKCHAIN TYPES

Blockchain is partitioned into three permission classes: public, private, and federated permission [27]. Public blockchain networks are accessible to anyone who wishes to add blocks allowing various transactions and information to be added. These commonly used blockchains are accessible. For example, Ethereum is a public network that enables miners to compete for Ether. Public blockchain networks have no privileges, which allows anyone to participate and verify transactions [28]. Furthermore, it utilizes consensus mechanisms like PoW or PoS to authenticate transactions. This is caused by the lack of a centralized authority that typically necessitates security mean- sure implementations that require significant computational resources to prevent malicious users from affecting the system. While private blockchain systems, similar to federated chains, offer data-writing privileges to participants based on their performance and safety [74]. They excel in securely storing confidential data, particularly in applications like e-payment companies and online shopping sites such as Amazon and PayPal [29]. In contrast to public blockchains, private ones prioritize reliability and performance. Finally, federated blockchains, used by multiple organizations, share similarities with private blockchains, preserving transparency while facilitating transactions. These blockchains offer shorter transaction processing times but are not fully decentralized [30]. Federated blockchains are a type of blockchain where a consortium oversees the permissions. Based on how the blockchain was configured, the consortium nodes manage the decision and determine whether an operation is public or private [31, 32]. A brief comparison of these three types is represented in Table 1.

TABLE 1: COMPARISON OF PUBLIC, PRIVATE, AND FEDERATED BLOCKCHAIN ATTRIBUTES

Attributes	Public	Private	Federated
Consensus	All miners	One organization	The selected set of nodes
Consensus process	Permissionless	Permissioned	Permissioned
Read permission	Public	Can be restricted	Can be restricted
Immutability	difficult to modify	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Yes	Partially

Table 1 presents a comparative analysis of the attributes of three distinct blockchain types: Public, Private, and Federated. The table elucidates six key attributes across these blockchain variants, offering insights into their operational characteristics and structural differences. The attribute" Consensus," delineates the entities responsible for achieving agreement within the network. In public blockchains, consensus involves all miners, while private blockchains restrict this to a single organization. Federated blockchains occupy a middle ground, with consensus determined by a selected set of nodes. The" Consensus process" row distinguishes between permission-less systems, characteristic of public blockchains, and per-mission systems that are employed in private and federated blockchains." Read permission" refers to the accessibility of blockchain data. Public blockchains offer unrestricted access, whereas private and federated blockchains allow for potential restrictions on data visibility. The" Immutability" attribute addresses the resistance to modification of recorded data. Public blockchains are noted for their high resistance to alterations, while private and federated blockchains are potentially more susceptible to tampering." Efficiency" compares the blockchain's operational speed

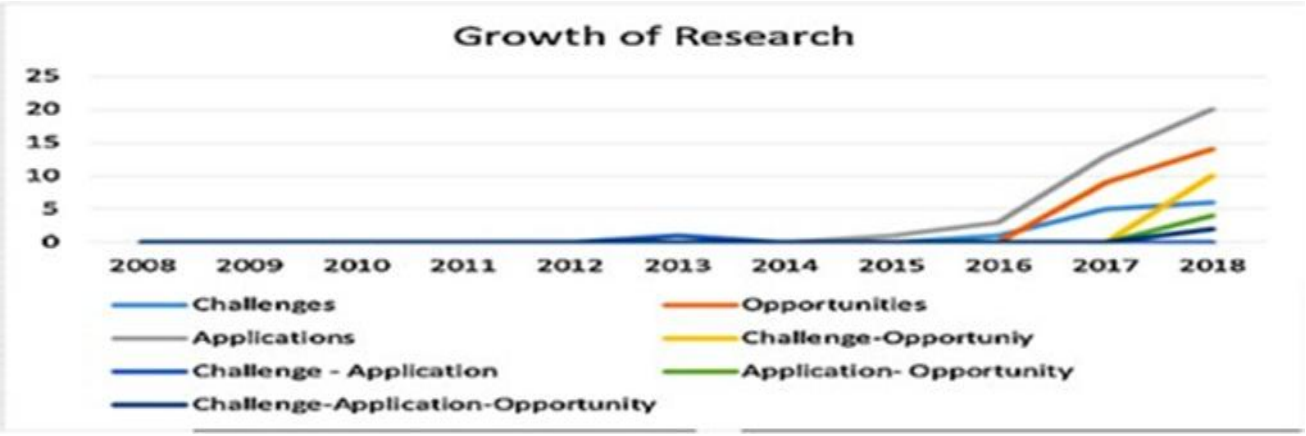
and resource utilization. Private and federated blockchains are categorized as highly efficient, in contrast to the lower efficiency of public blockchains. The final attribute," Centralized," examines the degree of centralization in decision-making and control. Public blockchains are characterized as non-centralized, private blockchains as fully centralized, and federated blockchains as partially centralized. This comprehensive comparison provides a nuanced understanding of the trade-offs and design choices inherent in different blockchain architectures, facilitating informed decision-making in blockchain implementation and research.

BLOCKCHAIN CHALLENGES

Blockchain technology is one of the most advanced technologies that result in difficulties if combined because of the business need for clarity. Figure 6 shows that the blockchain has become valuable over the past years since its inception in 2008. Despite published research explaining this technology, it still lacks clarity and sufficient maturity to become approved by many companies securely [33]. Early adoption of modern technology like blockchain can lead to unforeseen challenges, such as high transaction costs, incompatible models, and uncertain operational expenses. Integrating blockchain with existing systems poses another challenge, as the blockchain must seamlessly extract information from necessary sources to function effectively [34]. Blockchain implementation confronts various challenges, with scalability being a primary concern. Current blockchain systems struggle to manage high transaction volumes per second (TPS) [35]. In addition, blockchains are susceptible to hacking and unauthorized access to sensitive information, which raises concerns about security and privacy [36]. Developing blockchain-based healthcare systems faces several barriers, including interoperability, security, privacy, reliability, integrity, scalability, and patient involvement. Ensuring communication between software applications developed by different suppliers or for various platforms is challenging without clear rules and standards. Further, cost of implementation and maintenance requires financial resources for infrastructure development.

However, transferring information between platforms like Ethereum and Hyperledger fabric complicates the development of remote patient monitoring applications [37]. Blockchain-based healthcare systems encounter scalability challenges due to the substantial data volume stored. Storing extensive personal information for diverse individuals can result in usability issues and impracticality. Additionally, blockchain processing mechanisms, such as Ethereum's verification process, involve participation from every network location leading to significant processing delays, especially during high data loads [38] as shown in Figure 6.

FIGURE 6: THE RAPID EXPANSION OF RESEARCH ON BLOCKCHAIN



DISCRETE WAVELET TRANSFORM (DWT)

(DWT) is a mathematical technique used to transform a signal or data set into a series of wavelets. Wavelets are functions that can represent data or other functions in terms of orthogonal basis functions. This transform provides both time and frequency information, making it useful for analyzing various data types, such as signals and images, which can be defined using Python code shown in Figure 7.

FIGURE 7: ALGORITHM FOR DWT-BASED ENCRYPTION

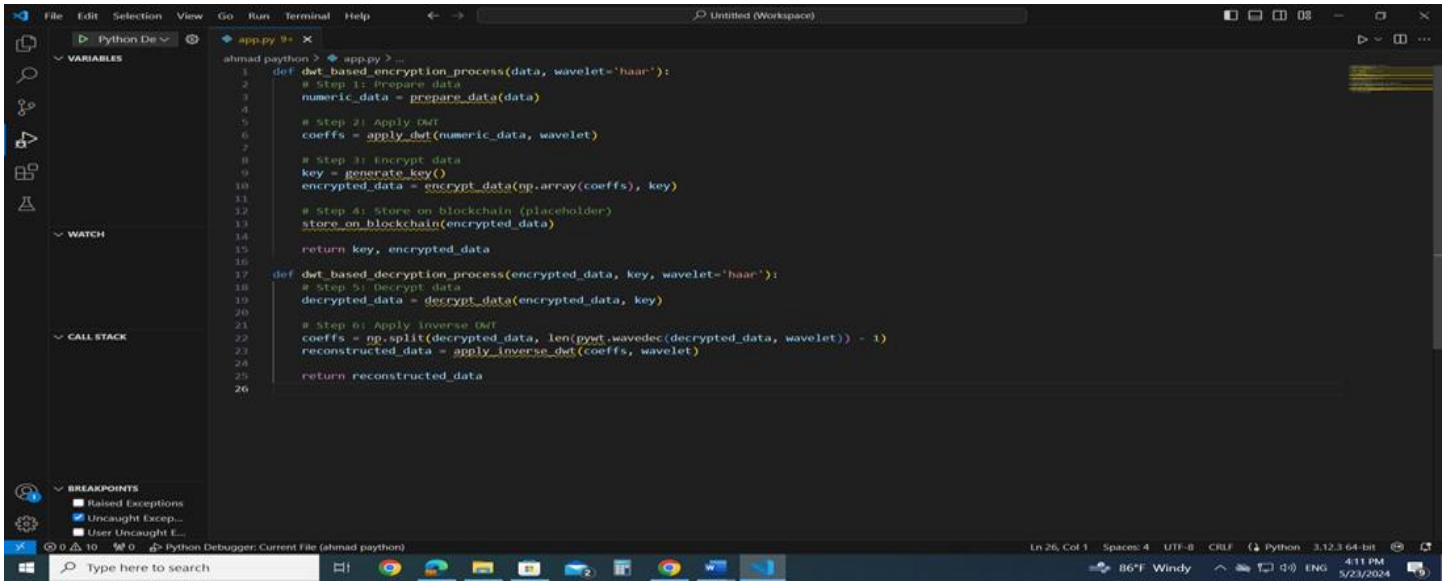


Figure 7 shows how to encrypt data within the blockchain, data encryption steps are explained by [39] as follows:

1. Function Declaration: Define the function (DWT) Based Encryption Process with parameters data, wavelet, and NumPy(np).
2. Data Preparation: Call prepare data(data) to convert the input data into a numeric format, storing the result in numeric data.
3. Apply DWT: Apply DWT [40] to transform the numeric data using the specified wavelet, storing the resulting coefficients.
4. Generate Key: Generate a cryptographic key by calling generate key () and storing it in the key.
5. Encrypt Data: Convert the wavelet coefficients to a NumPy array and store the result in the encrypted data.
6. Store on Blockchain: Securely store the encrypted data on a blockchain by calling the store on the blockchain.
7. Return Results: Return the cryptographic key and the encrypted data as a tuple.

BLOCKCHAIN-BASED HEALTHCARE

Healthcare is one of the world's largest and most important industries, providing essential services to individuals and communities. Germany spent 11.2% of the total gross domestic product (GDP) on healthcare in 2018, considered the third highest globally [41]. However, the industry faces several challenges that impact its ability to deliver high-quality, accessible, and affordable care. These challenges include high rates of fatness, an aging population, the Cost of healthcare, Pandemics (Corona pandemic) and global health emergencies, and shortages of healthcare professionals. The healthcare industry faces significant administrative challenges that divert resources from patient care signifying the need to explore innovative solutions to address these issues and support the evolving needs of patients and communities. Collaboration among policymakers, healthcare providers, and stakeholders is essential for developing and implementing effective solutions. This may involve investing in recruiting and training healthcare professionals, exploring new care delivery models like telemedicine and nurse-led care, and implementing measures to reduce administrative burden in healthcare [42]. Further, addressing lifestyle factors and promoting healthy living can reduce healthcare costs and improve health outcomes. According to Di Bonaventura et al. (2018), this entails employing policies and programs that encourage a healthy diet, boost physical exercise, and lower the prevalence of obesity and associated diseases. Developing solutions to fulfill the increasing need for healthcare services, especially for chronic illnesses that are more frequent among older persons, is crucial as the world's population ages [43]. Therefore, maintaining the integrity of technology in healthcare is essential for better communications. Electronic health records (EHRs), telemedicine, and other digital tools can facilitate better communication between medical practitioners, ease administrative burdens, and increase patient access to care. Telemedicine, for instance, can assist in addressing the scarcity of medical personnel

and make treatment more accessible to patients, especially in isolated or rural locations [44] [45]. These healthcare-based elements are shown in Figure 8.

FIGURE 8: BLOCKCHAIN-BASED HEALTHCARE COMPONENTS

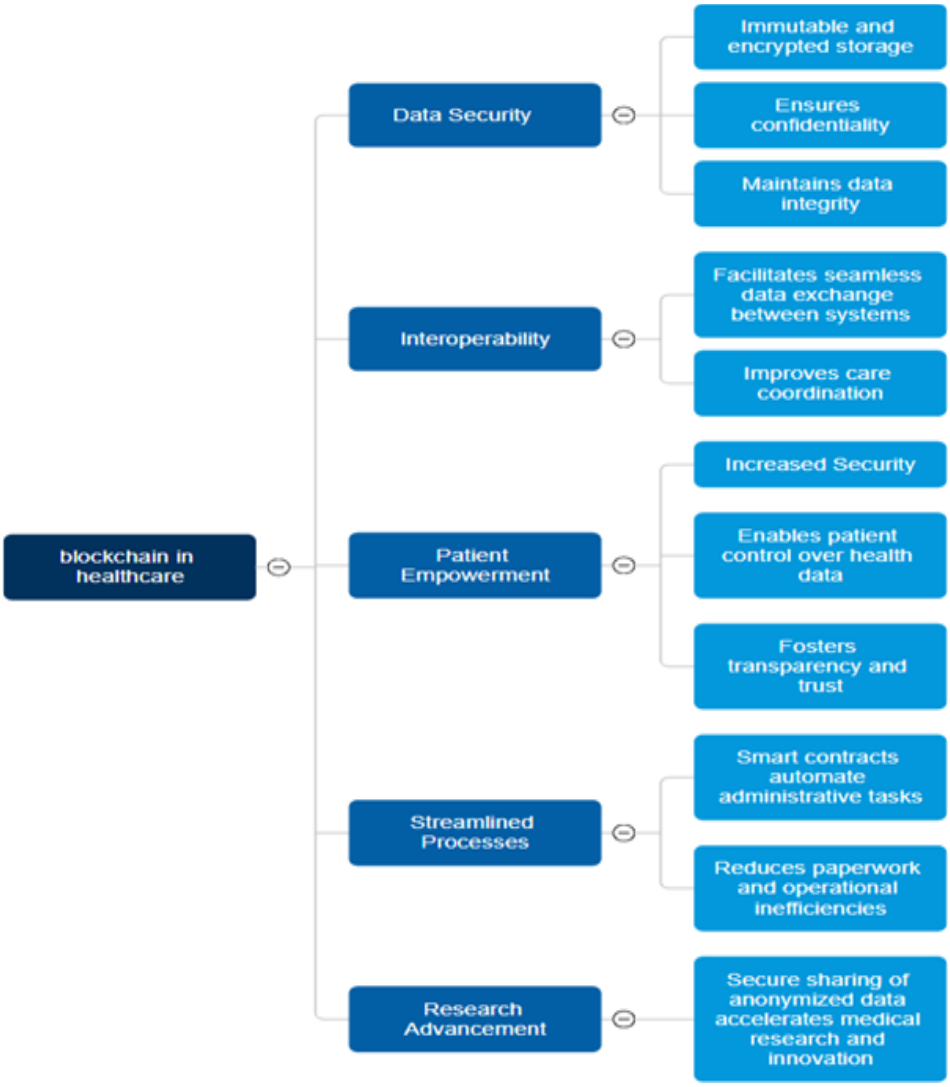


Figure 8 presents the different components of blockchain-based healthcare, including data protection, compatibility, patient information autonomy, reduced processes, and scientific research advancement.

HEALTHCARE DATA MANAGEMENT

Healthcare data management is crucial to ensure that data are used to enhance patient outcomes in healthcare, data must be maintained ethically. Thus, a full picture of a patient's records, treatment choices, and effective communication tools are all made available to medical professionals [46]. The relationship between blockchain technology and the General Data Protection Regulation (GDPR) is debated in Europe. However, blockchain appears compliant with the General Data Protection Regulation (GDPR) regarding data portability, such as tracking and legal auditing of how data is accessed and managed. Sharing data depends on reliable cooperation between the mutual parties during the operations process depending on the shared data and how they are shared [47]. Data privacy represents the ethical standards and laws that must be adhered to according to (HIPAA) and (GDPR) standards [48]. Therefore, most healthcare organizations adhere to such standards and rules to secure sensitive information using blockchain technology [49].

JORDAN DATA PROTECTION LAW

Jordan does not have a comprehensive data protection law equivalent to GDPR or HIPAA. However, there are some regulations and guidelines related to data privacy and security, such as the Electronic Transactions Law (2001) and the Cybercrime Law (2010). These laws provide some level of protection for personal data, but they are not as detailed or stringent as GDPR or HIPAA [74]. The lack of a comprehensive data protection law in Jordan could pose challenges for blockchain implementation, especially in terms of ensuring patient data privacy and security. Blockchain's decentralized nature might conflict with existing regulations that require data to be stored in centralized systems under the control of specific entities [52].

ELECTRONIC HEALTH RECORDS (EHR)

EHRs are cloud-based data storage used for healthcare records exchange between healthcare suppliers. Data exchange between suppliers raises security and trust risks of data attack and forgery [50], [51]. Blockchain technology manages EHRs effectively using different techniques to protect patients' information [52]. Thus, EHR is widely used in blockchain technology in healthcare. [53].

FIGURE 9: BLOCKCHAIN HEALTHCARE RECORDS

Figure 9 shows how patients' medical data are recorded in a digital domain called the Electronic Health Record (EHR). For example, the patient's general medical history, signs, symptoms, and historical illnesses are stored in the database. Each patient's electronic health records may include important data, such as a summary of their general health, administrative data, and legal paperwork [54, 55].

INTEROPERABILITY WITH EXISTING SYSTEMS

Jordan's healthcare system relies on a mix of public and private healthcare providers, each with its own electronic health record (EHR) systems. The lack of a unified regulatory framework for interoperability could hinder the integration of blockchain technology, which requires seamless data exchange between different systems emphasizes the importance of standardization in healthcare data management, which is currently lacking in Jordan [25, 27]. Without clear standards for data formats and protocols, integrating blockchain with existing EHR systems could be challenging.

REGULATORY UNCERTAINTY

Jordan, like many other countries, does not have specific regulations governing the use of blockchain technology in healthcare. This regulatory uncertainty could deter healthcare providers from adopting blockchain, as they may be unsure about compliance requirements [16]. Also, [48] suggests that regulatory clarity is essential for the successful implementation of blockchain in healthcare. If Jordan were to adopt GDPR-like regulations, it could create a more favorable environment for blockchain by providing clear guidelines on data protection and privacy.

DATA PRIVACY AND SECURITY IN BLOCKCHAIN

Blockchain technology utilizes tools to maintain data privacy and security which has arisen since using such technology in Bitcoins. Blockchain maintains Bitcoin data privacy and security through consistency, tamper-resistance, and resistance to a distributed denial-of-service (DDoS) attack. These features are still used by other sectors such as the Internet of Things (IoT) and healthcare [56]. Data privacy and security have many characteristics as follows:

Information Uniqueness

Information uniqueness indicates the lack of compatibility between two parties or two of the entities monitored for the system with excellent trust. Although blockchain technology verifies the provision of a false identity as a form of support to hide user identity, the user cannot be protected by using an anonymous name except by guaranteeing the user's pseudonym [57].

Confidentiality

Blockchain data privacy refers to the features of confidential sensitive data stored in the database. Although the blockchain was designed as a distribution system for digital currencies, it has become more widely used in applications such as smart contracts and copyrighted works. The security feature in digital currencies is not active, such as maintaining the confidentiality of the available amounts. Unfortunately, it is available to the public despite pseudonym use instead of the real identity. Even with the use of smart contracts in the Ethereum application, for example, when transferring an amount of money to another party, and the other party has information, this party may link this part of the information to its identity, so it requires the design of stronger protection mechanisms for contracts that maintain information privacy [58].

METHODOLOGY

This study utilized a mix of exploratory and survey methods to collect the required data to achieve the study aim by using a set of keywords from the available literature and the distributed questionnaire. Through this method, the problems related to utilizing blockchain technology in healthcare institutions in Jordan were investigated.

ETHICAL CLEARANCE

This study was conducted in accordance with the ethical standards and the National Health and Medical Research Council guidelines. Approval for the study was obtained from the Ministry of Health (MoH) in Jordan. All participants were informed about the purpose of the research, and informed consent was obtained before their involvement. The study ensured the confidentiality and anonymity of all participants, adhering to national and international ethical standards for research involving human subjects.

INSTRUMENT

The study hypotheses were tested based on the collected data from a questionnaire survey. The questionnaire was composed of constructs developed based on the extensive review of the published studies on healthcare and blockchain to ensure its validity and reliability. The distributed questionnaire was designed to assess the challenges used in the study. Questionnaire items were measured based on a five-point Likert scale, ranging from 1 (Strongly agree) to 5 (Strongly disagree)

SAMPLE AND PROCEDURE

This study was created to measure the use of blockchain technology in healthcare technology as a case study in Jordan, where 31 questions were used to address four potential challenges that the healthcare sector faces. The questionnaire was distributed based on the approval of the Ministry of Health to government hospitals, including Al-Bashir Hospital, and the private sector is represented by Hakeem Health Company and Health Laboratories such as Biolab, and Med Labs. Also, it was distributed to professionals such as doctors, software developers, and nurses. The total of the distributed questionnaires was 120 samples. 100 valid responses were obtained and considered valid for analysis, where 40 samples were omitted from the study due to incomplete answers. This high rate of response 80% is due to the questionnaire's convenient design, which required 10-15 minutes to complete.

QUESTIONNAIRE DESIGN

The questionnaire assessed the impact of security, privacy, reliability, and integrity on adopting blockchain technology in healthcare. The questionnaire consisted of two parts: the first part collects personal information about the respondent demographic data such as gender, age, educational level, job title, and work experience. The second part consisted of 31 questions to measure the impact of the four challenges across 4 axes each axis included a set of questions.

1. The first axis assessed the impact of security on the healthcare industry switching to blockchain-based cloud computing services.
2. The second axis assessed the impact of privacy on the healthcare industry when shifting to blockchain-based cloud computing services.
3. The third axis assessed the impact of reliability on the healthcare industry when shifting to blockchain-based cloud computing services.
4. The fourth axis assessed the impact of Integrity on the healthcare industry when shifting to blockchain-based cloud computing services.

Also, to remark on the arithmetic average of the variables, the study utilized the following equation to determine their respective importance [59]:

$$\text{Relative importance} = \frac{\text{maximum value} - \text{minimum value}}{\text{number of levels}}$$

$$= \frac{5-1}{3}$$
$$= 1.333$$

The score results of the applied equation indicate that <2.33 represents a poor level of importance, 2.33-3.67 represents an average level of importance, and >3.67 represents a high level of importance.
The following hypotheses were derived from the published studies:

1. The first hypothesis: Blockchain technology provides security features in healthcare.
2. The second hypothesis: Blockchain technology ensures patient privacy in healthcare.
3. The third hypothesis: Blockchain improves reliability in healthcare systems.
4. The fourth hypothesis: Blockchain maintains data integrity in healthcare records.

RESULTS

This section represents the results of the analyzed data from the questionnaire and the derived hypothesis from other studies.

DESCRIPTIVE ANALYSIS

The collected demographic data of the study participants were analyzed as shown in Table 2.

TABLE 2: RESPONDENTS' DEMOGRAPHIC DATA

Category	Sub-category	Repetition	Ratio
Gender	Male	62	**62%**
	Female	38	**38%**
	Total	100	**100%**
Age	Less than 30	49	**49%**
	30-39	25	**25%**

	40-49	20	**20%**
	50 or above	6	**6%**
	Total	100	**100%**
Education	Bachelor's degree	58	**58%**
	Higher Diploma	8	**8%**
	Master's degree	19	**19%**
	Ph.D.	15	**15%**
	Total	100	**100%**
Job	Nurse	14	**14%**
	Developer	20	**20%**
	Consultant	8	**8%**
	Doctor	43	**43%**
	Manager	15	**15%**
	Total	100	**100%**
Experience	5-10 years	56	**56%**
	11-15 years	15	**15%**
	16-20 years	14	**14%**
	21 or more years	15	**15%**
	Total	**100**	**100%**

Table 2 shows the participant's demographic data; the results indicate that 62% of males and 38% of females participated in the study. Most participants were younger than 49 years 49%, 25% aged 30-39 years old, 20% aged 40-49 years old, and 6% older than 50 years old. The educational level consisted of four groups, with 58% bachelor's degree, 19% master's degree, 15% Ph.D. degree, and 8% higher diploma degree. The job title for the participants shows that 43% were doctors, 20% were developers, 15% managers, 14% nurses, and 8% were consultants. Finally, job experience shows that 56% of the participants have 5-10 years of experience, 15% have 11-15 years of experience, 15% have more than 21 years of experience, and 14% have 16-20 years of experience, respectively.

RELIABILITY TEST

TABLE 3: RELIABILITY TEST RESULT

Case Processing Summary			
		N	**%**
Cases	Valid	100	**100.0**
	Excluded	0	**0.0**
	Total	100	**100.0**
a. Listwise deletion is based on all variables in the procedure.			
Reliability Statistics			
Cronbach's Alpha		**No. of Items**	
0.854		**31**	

Table 3 shows the results of the reliability test for the questionnaire items. Cronbach alpha test was applied to verify the stability and internal consistency of the questionnaire items. Cronbach's value of 0.7 and above for questionnaire items indicates reliable and consistent items. All used items in the questionnaire have a Cronbach alpha coefficient of 0.854, indicating that stable and consistent items were used in the study questionnaire [60].

NORMAL DISTRIBUTION TEST

TABLE 4: TEST OF NORMALITY

Type	Kolmogorov-Smirnova			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Security	0.134	100	0.185	0.957	100	**0.073**
Privacy	0.111	100	0.256	0.908	100	**0.129**
Reliability	0.147	100	0.361	0.935	100	**0.226**
Integrity	0.190	100	0.281	0.926	100	**0.324**
a Lilliefors Significance Correction						

The" Smirnova-Kolmogorov and Shapiro-Wilk" test was performed to determine whether the data were normally distributed. This test is essential when evaluating hypotheses since most parametric tests demand that the data distribution be normal. The test findings are shown in Table 4, where each axis' probability significance value is larger than 0.05.

MEANS AND STANDARD DEVIATIONS

To find out the estimates of the participants' work in the healthcare sector within the functional levels on the axes of the study, the arithmetic mean (M) and standard deviations (SD) of their answers were calculated, and the results of each axis are presented as follows:

TABLE 5: M AND SD VALUES FOR THE SECURITY AXIS

No.	Security	M	SD
1	Blockchain can provide increased control and access to patient information.	3.5500	0.72995
2	Blockchain increases the security of the medical supply chain.	3.5700	0.71428
3	Blockchain technology allows doctors to access backup records to verify a patient's identity without permission.	3.5900	0.77973
4	The main limitation of turning off patient-physician interoperability is data centralization.	3.4400	0.67150
5	Healthcare includes details about encryption algorithms such as AES-256, Health Insurance Portability and Accountability (HIPAA), and General Data Protection Regulation (GDPR).	3.6300	0.83672
6	Off-chain transactions are not recorded on the blockchain; hence it's necessary to ensure their safety and security.	3.7400	0.84829
7	Healthcare information powered by blockchain technology.	3.7000	0.82266
8	The systems in the chain must be secure to prevent unauthorized access, hacking, and other types of fraud.	3.7400	0.78650
9	An off-chain healthcare system stores stakeholder information.	3.8400	0.88443
10	You can retrieve information stored in the off-chain healthcare system.	3.8300	0.91071
11	I feel comfortable sharing my personal health information with other healthcare providers via blockchain technology.	3.6800	0.89758
12	I feel that the benefits of using blockchain technology in the healthcare system outweigh any potential security risks.	3.5500	0.71598
13	Blockchain technology provides instructions about the privacy procedures in place to protect your personal health information before you use it.	3.7500	0.82112
Security as a whole		**3.6923**	**0.50871**

1) *The Security Axis*: The first axis of the study sample focused on security, and the mean and standard deviations of the responses were calculated. The results are presented in Table 5.

Table 5 shows the M and SD of the participants for the items of the security axis. The M value for security items ranged between 3.44-3.84 indicating the level of importance for all the used items for this axis. For instance, item 9 has the highest M value of 3.84 indicating the high importance of storing patient information for future use. While item 4 has the lowest M value of 3.44 indicating a medium level of importance due to the consistency of the stored data about the patient. However, the overall M value for information security suggests the high level of importance for information security when using blockchain in healthcare.

2) *The Privacy Axis:* The second axis of the study sample focused on privacy, and the mean and standard deviations of the responses were calculated. The results are presented in Table 6.

TABLE 6: M AND SD VALUES FOR THE PRIVACY AXIS

Num	Privacy Statement	Mean (M)	Standard Deviation (SD)
1	Blockchain healthcare system protects the privacy and security of patient information.	3.4800	0.73140
2	Do you have any concerns about the privacy of your information when using the electronic healthcare system?	3.5100	0.77192
3	Do you trust the healthcare system?	3.4500	0.84537
4	Blockchain supports scrutiny and is reviewed by health organizations, regulators, payers, and individuals while protecting individual privacy.	3.6700	0.89955
5	Off-chain systems provide high privacy to protect sensitive information.	3.6000	0.86457
6	On-chain systems do not reveal sensitive information, such as transaction details and user identities, which can be a concern for privacy-sensitive applications.	3.8100	0.89550
7	Blockchain technology provides instructions about the privacy procedures in place to protect personal health information before using them.	3.7100	0.72884
8	I feel that the benefits of using blockchain technology in the healthcare system outweigh any potential privacy risks.	3.8800	0.72864
Privacy as a whole	**Overall privacy perception in blockchain healthcare systems.**	**3.6887**	**0.53474**

Table 6 presents the M and SD of the respondents for the items of the Privacy axis. The M value for privacy items ranged between 3.45-3.88 indicating the level of importance for all the used items for this axis. For instance, item 8 has the highest M value of 3.88 indicating the high importance of using blockchain in the healthcare system in dealing with potential risks of patient information privacy. Item 3 has the lowest M value of 3.45 among the axis items indicating a medium level of importance due to the important role of trust in the healthcare system for preserving patient information. However, the overall M value for information privacy indicates the importance of blockchain.

3) *The Reliability Axis:* The third axis of the study sample examined reliability, and the responses arithmetic means and standard deviations were extracted. These findings are presented in Table 7.

TABLE 7: M AND SD VALUES FOR THE RELIABILITY AXIS

No.	Reliability Statement	Mean (M)	Standard Deviation (SD)
1	There are challenges associated with using the healthcare system.	3.6800	0.73691
2	The patient privacy policies and procedures in the healthcare system linked to the blockchain are up-to-date to meet the specific requirements of the user.	3.6100	0.77714
3	In an emergency case, patients can authorize healthcare personnel to access their health information.	3.5900	0.81767
4	Blockchain technology does not provide training on how to secure personal health information.	3.5600	0.76963
5	I trust the healthcare system to protect my personal health information when using blockchain technology.	3.5400	0.74427
Reliability as a whole	**Overall reliability perception in blockchain healthcare systems.**	**3.5960**	**0.53634**

Table 7 presents the M and SD of the respondents for the items of the reliability axis. The M value for reliability items ranged between 3.54 and 3.68 indicating the level of importance for all the used items for this axis. For instance, item 1 has the highest M value of 3.68 indicating the high importance of dealing with the challenges that face blockchain in healthcare to improve system reliability. Item 5 has the lowest M value of 3.54 among the axis items indicating an average level of importance due to the recency of blockchain in the healthcare system for preserving patient information. However, the overall M value for reliability indicates an average level of importance for the healthcare system's reliability.

4) *The Integrity Axis:* The fourth axis of the study sample examined integrity, and the responses' arithmetic means and standard deviations were extracted. These findings are presented in Table 8.

TABLE 8: M AND SD VALUES FOR THE INTEGRITY AXIS

No.	Integrity Statement	Mean (M)	Standard Deviation (SD)
1	The Electronic Healthcare System retrieves the Electronic Healthcare Record (EHR).	3.5800	0.66939
2	I am aware of the laws and regulations governing the use of blockchain technology in the healthcare system and how they affect my personal health information.	3.4800	0.84662
3	Blockchain technology manages healthcare information systems.	3.4900	0.81004
4	Many stakeholders in the healthcare system would benefit from a better understanding of how people use and trust healthcare services.	3.4600	0.84591
5	I feel comfortable about my level of control over my personal health information when using blockchain technology.	3.6700	0.82945
Integrity as a whole	**Overall integrity perception in blockchain healthcare systems.**	**3.5340**	**0.60306**

Table 8 presents the M and SD of the respondents for the items of the integrity axis. The M value for integrity items ranged between 3.48 and 3.67 indicating the level of importance for all the used items for this axis. For instance, item 5 has the highest M value of 3.67 indicating the high importance of user control of personal information stored on the cloud. Item 2 has the lowest M value of 3.48 among the axis items indicating a medium level of importance in the regulations and laws that govern the use of blockchain in healthcare to deal with patient information. However, the overall M value for integrity

indicates a medium level of importance for the healthcare system's integrity. However, the overall M value for information privacy indicates the importance of blockchain.

1) *The Reliability Axis*: The third axis of the study sample examined reliability, and the responses arithmetic means and standard deviations were extracted. These findings are pre-presented in Table 7.
2) *The Integrity Axis:* The fourth axis of the study sample examined integrity, and the responses arithmetic means and standard deviations were extracted. These findings are pre- presented in Table 8.

Table 8 presents the M and SD of the respondents for the items of the integrity axis. The M value for integrity items ranged between 3.48 and 3.67 indicating the level of importance for all the used items for this axis. For instance, item 5 has the highest M value of 3.67 indicating the high importance of user control of personal information stored on the cloud. Item 2 has the lowest M value of 3.48 among the axis items indicating a medium level of importance in the regulations and laws that govern the use of blockchain in healthcare to deal with patient information. However, the overall M value for integrity indicates a medium level of importance for the healthcare system's integrity.

HYPOTHESES TEST

Study hypotheses were tested using one Sample T-test to compare the arithmetic averages of the study sample's responses to the weighted arithmetic mean value. The T value is calculated and the significance level is extracted. The value of the weighted average that was compared is 3. If the significance level is ≤ 5, the results indicate a statistically significant difference in the answers of the study sample from the test average. Thus, the alternative hypothesis is accepted, but if the level of significance is >5, it indicates that there are no statistically significant differences in the answers of the study sample from the average of the test. This means the null hypothesis is accepted, and the alternative hypothesis cannot be accepted. The results are as follows:

THE FIRST HYPOTHESIS (H01)

H01: Blockchain technology provides security features in healthcare.

TABLE 9: ONE-SAMPLE T-TEST RESULTS FOR H01

One-Sample Statistics						
	N	Mean	Std. Deviation	**Std. Error Mean**		
Security	100	3.6623	0.50871	**0.05087**		
One-Sample Test						
	Test Value = 3					
	T	DF	Sig. (2-tailed)	Mean Difference	**95% Confidence Interval of the Difference**	
					Lower	**Upper**
Security	**13.019**	**99**	**0.000**	**0.6623**	**0.5614**	**0.7632**

Table 9 indicates that the (T) value of (13.019) is statistically significant because Sig. <0.05, while the M value of 3.66 reflects the significance of the positiveness of the first hypothesis. The M value is higher than the weighted test average of 3 and the significance level <0.05. Therefore, the null hypothesis is rejected and the alternative hypothesis is accepted. This indicates that security is available when using the blockchain from the viewpoint of workers in the healthcare sector in Jordan at a significant level (a ≤ 0.05).

THE SECOND HYPOTHESIS (H02)

H02: Blockchain technology ensures patient privacy in healthcare.

TABLE 10: ONE-SAMPLE T-TEST RESULTS FOR H02

One-Sample Statistics						
Variable	N	Mean	Std. Deviation	Std. Error Mean		
Privacy	100	3.6388	.53474	.05347		
One-Sample Test						
	Test Value = 3					
	T	DF	Sig.(2-tailed)	Mean Difference	**95% Confidence Interval of the Difference**	
	11.94	**99**	**.000**	**.63875**	**.5326**	**.7449**

Table 10 indicates that the (T) value of (11.94) is statistically significant because Sig. <0.05, while the M value of 3.63 reflects the significance of the positiveness of the second hypothesis. The M value is higher than the weighted test average of 3 and the significance level <0.05. Therefore, the null hypothesis is rejected and the alternative hypothesis is accepted. This indicates that privacy is important when using the blockchain from the viewpoint of workers in the healthcare sector in Jordan at a significant level ($a \leq 0.05$).

THE THIRD HYPOTHESIS (H03)

H03: Blockchain improves reliability in healthcare systems.

TABLE 11: ONE-SAMPLE T-TEST RESULTS FOR H03

One-Sample Statistics							
Variable	N	Mean	Std. Deviation	Std. Error Mean			
Reliability	100	3.5960	0.53634	0.05363			
One-Sample Test							
	Test Value = 3						
	T	DF	Sig. (2-tailed)	Mean Difference	**95% Confidence Interval of the Difference**		
	11.113	99	0.000	0.59600	**0.4896**	**0.7024**	

Table 11 indicates that the (T) value of (11.11) is statistically significant because Sig. <0.05, while the M value of 3.59 reflects the significance of the positiveness of the second hypothesis. The M value is higher than the weighted test average of 3 and the significance level <0.05. Therefore, the null hypothesis is rejected and the alternative hypothesis is accepted. This indicates that reliability is important when using the blockchain from the viewpoint of workers in the healthcare sector in Jordan at a significant level ($a \leq 0.05$).

THE FOURTH HYPOTHESIS (04)

H04: Blockchain maintains data integrity in healthcare records.

TABLE 12: ONE-SAMPLE T-TEST RESULTS FOR H04)

One-Sample Statistics					
Variable	N	Mean	Std. Deviation	Std. Error Mean	
Integrity	**100**	**3.5340**	**.60306**	**.06031**	
One-Sample Test					
	Test Value = 3				
	T	DF	Sig. (2-tailed)	Mean Difference	**95% Confidence Interval of the Difference**
	8.87	**99**	**.000**	**.53400**	**0.4143 to 0.6537**

Table 12 indicates that the (T) value of (8.85) is statistically significant because Sig. <0.05, while the M value of 3.53 reflects the significance of the positiveness of the second hypothesis. The M value is higher than the weighted test average of 3 and the significance level is <0.05. Therefore, the null hypothesis is rejected and the alternative hypothesis is accepted. This indicates that integrity is important when using the blockchain from the viewpoint of workers in the healthcare sector in Jordan at a significant level ($a \leq 0.05$).

Table 13 presents the accepted hypotheses and confirms them with other studies.

TABLE 13: SUMMARY OF THE RESULTS OF THE STUDY HYPOTHESES

Study Hypothesis	Results	References
H01: Blockchain technology provides security features in healthcare	Accepted	Attaran, M. (2022); Abu-elezz et al., (2020)
H02: Blockchain technology ensures patient privacy in healthcare	Accepted	Hussein et al., (2021)
H03: Blockchain improves reliability in healthcare systems.	Accepted	Hussein et al., (2021)
H04: Blockchain maintains data integrity in healthcare records.	Accepted	Zarour et al., (2021)

Table 13 presents the outcomes of four hypotheses tested in a study focusing on blockchain technology in the healthcare sector in Jordan. Each hypothesis (H01 to H04) examines a specific feature of blockchain technology from the perspective of healthcare sector workers in Jordan. The hypotheses are formulated as null hypotheses, suggesting the inactivity or ineffectiveness of these features at a significant level ($a \leq 0.05$).

The acceptance of all four hypotheses suggests that, from the perspective of healthcare sector workers in Jordan have important implications for the adoption and implementation of blockchain technology in Jordan's healthcare sector. It suggests a potential gap between the theoretical benefits of blockchain and its perceived effectiveness in practical application within this specific context. The references provided offer avenues for further investigation into the reasons behind these perceptions and potential comparisons with findings from other contexts or regions.

DISCUSSION

The results of H01 showed the use of the blockchain that provides information security. Published studies attribute such results to the fact that one of the main features of blockchain technology is its ability to provide secure and clear data storage. This is achieved using cryptographic algorithms and consensus mechanisms, which ensure that transactions recorded on the blockchain are immutable and can only be modified by the consensus of network participants.

Furthermore, because blockchain offers a high level of security, it is a good fit for applications like medical records that need to transmit and store sensitive data securely. Blockchain technology can improve security, but it's vital to remember that it's not a magic bullet and needs to be used correctly to be effective. Furthermore, if blockchain technology is not developed and maintained appropriately, it may be subject to assaults and is not impervious to all security risks. These findings are consistent with Swan's (2015) design for developing a new economy using blockchain technology.

The results of H02 demonstrated that blockchain offers information privacy. However, blockchain-based solutions growth and acceptance in numerous industries indicate that blockchain technology is a potential means of protecting personal information privacy. These results are consistent with the results of [61] who argues that blockchain enables information sharing while preserving the privacy of parties involved in the supply chain. Further, the author suggested that blockchain technology can help meet key supply chain management objectives, such as reducing fraud, enhancing trust, and improving efficiency. Also, [62] argue that blockchain technology can be used to protect personal health information. The authors noted that blockchain-based solutions can ensure data integrity, confidentiality, and availability are essential for maintaining personal privacy in healthcare. The results of H03 demonstrated how using the blockchain increases

reliability, which is crucial for consumer trust in such technologies. These findings are consistent with [63] study, which discovered that blockchain technology improves the supply chain management systems' dependability and transparency. According to the report, blockchain technology can offer a safe and impenetrable platform for tracking products and confirming their legitimacy, enhancing the supply chain system's dependability.

The results of H04 show how information integrity is protected by blockchain technology. These findings are consistent with those of [64], who examined the application of blockchain technology to the defence of intellectual property. The study concluded that the high degree of support for blockchain technology's integrity feature suggests that it has the potential to be a dependable and secure method for safeguarding intellectual property. The report emphasizes how blockchain technology can completely transform the healthcare sector in Jordan. Blockchain can offer a strong foundation for handling patient data by solving security, privacy, dependability, and integrity issues. This shift is essential for raising patient and provider trust, optimizing data management, and improving patient care.

This comprehensive analysis provides significant insights and a compelling case for blockchain technology implementation in the Jordanian healthcare system, highlighting the transformative benefits and addressing critical challenges.

CONCLUSION

Achieving patient data confidentiality and privacy requires the use of blockchain technology. The blockchain's ledger feature makes it possible for data secure exchange and keeps patient data protected against unauthorized access. Furthermore, when granting authorized people access to certain data smart contracts enhance patient privacy. Such technology's stability guarantees that every transaction is traced and documented, creating an open audit trail. However, several obstacles prevent such technologies in the healthcare industry, such as high cost, complexity, interoperability problems, and regulatory requirements. To protect patient privacy and information security, it's recommended to evaluate the utilized systems that provide healthcare facilities. To ensure that information is accessible by authorized individuals for designated purposes, stringent policies that control accessibility and usage purposes are also used. The restricted dispersed sample of the questionnaire might impact the validity and reliability of the study's findings. Furthermore, this constraint might impact how broadly the study's findings may be applied. Thus, to guarantee the validity and trustworthiness of the data, it is advised to raise the sample size. further to ensure that the healthcare system conforms with relevant rules and regulations. Therefore, ensuring the healthcare system has the proper tools and training to teach staff members how to access and utilize data stored on the blockchain is recommended. Furthermore, the blockchain should be checked and inspected to ensure its functioning correctly, that the data is safe, and that only authorized users may access it. Future blockchain research should concentrate on creating interoperable, scalable blockchain technologies that satisfy privacy concerns and legal constraints. To guarantee that blockchain technology can be efficiently applied in healthcare systems new consensus methods and privacy-preserving technologies need to be created. Thus, policy makers in Jordan must establish a regulatory framework for blockchain adoption in healthcare, ensuring its compliance with the existing healthcare and data privacy laws. Finally, infrastructure enhancements must be developed to be compatible with blockchain systems.

Future work should focus on developing scalable blockchain solutions that ensure interoperability and seamless integration with existing healthcare systems. Also, cost, infrastructure, and legal challenges for blockchain adoption must be investigated further in future research.

References

1. Reyna A, Martín C, Chen J, Soler E, Díaz M. On blockchain and its integration with IoT. Challenges and opportunities. Future generation computer systems. 2018 Nov 1;88:173-90.
2. Sultan K, Ruhi U, Lakhani R. Conceptualizing blockchains: characteristics & applications. arXiv preprint :1806.03693. 2018 Jun 10.
3. Siyal AA, Junejo AZ, Zawish M, Ahmed K, Khalil A, Soursou G. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography. 2019 Jan 2;3(1):3.
4. Darlington N. Blockchain for beginners: what is blockchain technology. A step-by-step guide. 2022.
5. Zhang R, Xue R, Liu L. Security and privacy on blockchain. ACM Computing Surveys (CSUR). 2019 Jul 3;52(3):1-34.
6. Szabo N. Winning strategies for Smart contracts. foreword by Don Tapscott, Blockchain Research Institute. 2017 Dec 4;4.
7. Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KK. A systematic literature review of blockchain cyber security. Digital Communications and Networks. 2020 May 1;6(2):147-56.
8. Peck ME. Blockchains: How they work and why they'll change the world. IEEE spectrum. 2017 Sep 28;54(10):26-35.
9. Attaran M. Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management. 2022 Jan 2;15(1):70-83.
10. Atlam HF, Wills GB. Technical aspects of blockchain and IoT. IAdvances in computers 2019 Jan 1 Vol. 115, pp. 1-39 Elsevier.
11. Buterin V. What Are Smart Contracts? A Beginner's Guide to Smart Contracts. 2016.
12. Kettunen P. *Feasibility of Distributed Ledger Technology and Blockchain in the Finnish Securities Industry* [master's thesis]. Hämeenlinna: Hämeen ammattikorkeakoulu; 2020.
13. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future generation computer systems. 2018 May 1;82:395-411.
14. Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press; 2016 Jul 19.
15. Mettler M. Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom) 2016 Sep 14 (pp. 1-3). IEEE.
16. Ahmed M, Pathan AS. Blockchain: Can it be trusted? Computer. 2020 Apr 9;53(4):31-5.
17. Katuwal GJ, Pandey S, Hennessey M, Lamichhane B. Applications of blockchain in healthcare: current landscape & challenges. arXiv preprint:1812.02776. 2018;10.
18. Swanson T. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. Report, available online. 2015 Apr 1;28.
19. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: Architecture, consensus, and future trends. In2017 IEEE international congress on big data (BigData congress) 2017 Jun 25 (pp. 557-564). IEEE.
20. Atzei N, Bartoletti M, Cimoli T. A survey of attacks on ethereum smart contracts (sok). In International conference on principles of security and trust 2017 Mar 28 (pp. 164-186). Berlin, Heidelberg: Springer Berlin Heidelberg.
21. Al Khaldy M, Alshdifat G, Almalahmeh T, Aldweesh A. Blockchain as a resilient infrastructure for e-business transactions. In 2024 2nd International Conference on Cyber Resilience (ICCR) 2024 Feb 26 (pp. 1-6). IEEE.
22. Upadhyay N. Demystifying blockchain: A critical analysis of challenges, applications and opportunities. International Journal of Information Management. 2020 Oct 1;54:102120.
23. Tschorsch F, Scheuermann B. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials. 2016 Mar 2;18(3):2084-123.
24. Agbo CC, Mahmoud QH, Eklund JM. Blockchain technology in healthcare: a systematic review. Healthcare 2019 Apr 4 (Vol. 7, No. 2, p. 56). MDPI.
25. Dimitrov DV. Blockchain applications for healthcare data management. Healthcare informatics research. 2019 Jan 31;25(1):51-6.
26. Ekblaw A, Asaf A. MedRec: Medical Data Management on the Blockchain. PubPub. PubPub websites. 2016.
27. Pagliari C, Detmer D, Singleton P. Potential of electronic personal health records. BMJ. 2007 Aug 16;335(7615):330-3.
28. Xia QI, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE access. 2017 Jul 24;5:14757-67.

29. Heart T, Ben-Assuli O, Shabtai I. A review of PHR, EMR and EHR integration: A more personalized healthcare and public health policy. Health Policy and Technology. 2017 Mar 1;6(1):20-5.
30. Ganiga R, Pai RM, Sinha RK. Security framework for cloud based electronic health record (EHR) system. International Journal of Electrical and Computer Engineering. 2020 Feb 1;10(1):455.
31. Li R, Niu Y, Scott SR, Zhou C, Lan L, Liang Z, Li J. Using electronic medical record data for research in a Healthcare Information and Management Systems Society (HIMSS) Analytics Electronic Medical Record Adoption Model (EMRAM) stage 7 hospital in Beijing: cross-sectional study. JMIR Medical Informatics. 2021 Aug 3;9(8):e24405.
32. KLAS Research. 2020. 2020 Best in KLAS Awards: Software & Services. Available https://klasresearch.com/report/2020-best-in-klas-awards-software-and-services (Accessed 3/4/2023)
33. Cerner Corporation. Cerner Corporation. Available : https://www.cerner.com/ (Accessed 5/2/2023)
34. Liu Z, Weng J, Li J, Yang J, Fu C, Jia C. Cloud-based electronic health record system supporting fuzzy keyword search. Soft Computing. 2016 Aug;20(8):3243-55.
35. JPC Rodrigues J, De La Torre I, Fernández G, López-Coronado M. Analysis of the security and privacy requirements of cloud-based electronic health records systems. Journal of medical Internet research. 2013 Aug 21;15(8):e186.
36. Bhagyoday R, Kamani C, Bhojani D, Parmar V. Comprehensive study of E-Health security in cloud computing. Int Res J Eng Technol. 2019 Nov;6(11):1216-28.
37. Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for secure ehrs sharing of mobile cloud based e-health systems. IEEE access. 2019 May 17;7:66792-806.
38. Surbiryala J, Rong C. Cloud computing: History and overview. In2019 IEEE Cloud Summit 2019 Aug 8 (pp. 1-7). IEEE.
39. Mell P, Grance T. The NIST definition of cloud computing. National institute of science and technology, special publication. 2011 Jan;800(2011):145.
40. Alashoor T. Cloud computing: a review of security issues and solutions. International Journal of Cloud Computing. 2014 Jan 1;3(3):228-44.
41. Sivan R, Zukarnain ZA. Security and privacy in cloud-based e-health system. Symmetry. 2021 Apr 23;13(5):742.
42. Zhang Y, Xu C, Ni J, Li H, Shen XS. Blockchain-assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage. IEEE Transactions on Cloud Computing. 2019 Jun 17;9(4):1335-48.
43. Halas M. Blockchain technology as a part of distribution system operators' platform business model [master's thesis]. Lappeenranta: LUT University; 2019
44. Wüst K, Gervais A. Do you need a blockchain? in '2018 Crypto Valley Conference on Blockchain Technology (CVCBT)'. New York: Institute of Electrical and Electronics Engineers-IEEE. 2018 Jun:01-10.
45. DiBonaventura M D, Nicolucci A, Meincke H, LeLay A, & Fournier J. Impact of overweight and obesity on healthcare resource utilization and costs in Germany. 2018; Value in Health, 21(1), S30- S38.
46. Swan, B A. Healthcare workforce shortages: a critical component of America's economic future. 2018; Nursing economic, 30(2), 63-67.
47. Shiau WL, Sarstedt M, Hair JF. Internet research using partial least squares structural equation modeling (PLS-SEM). Internet Research. 2019 Jun 13;29(3):398-406.
48. Kshetri N. 1 Blockchain's roles in meeting key supply chain management objectives. International Journal of information management. 2018 Apr 1; 39:80-9.
49. Masoud MZ, Jaradat Y, Jannoud I, Zaidan D. CarChain: A novel public blockchain-based used motor vehicle history reporting system. In2019 IEEE Jordan international joint conference on electrical engineering and information technology (JEEIT) 2019 Apr 9 (pp. 683-688). IEEE.
50. Makki Q, Abdelgani Y, Al Zu'bi S. Developing off-chain system interfaces in health and pharmaceutical blockchain applications. InAIP Conference Proceedings 2023 Oct 20 (Vol. 2979, No. 1, p. 030001). AIP Publishing LLC.
51. Hussien HM, Yasin SM, Udzir NI, Ninggal MI, Salman S. Blockchain technology in the healthcare industry: Trends and opportunities. Journal of Industrial Information Integration. 2021 Jun 1;22:100217.
52. Abu-Elezz I, Hassan A, Nazeemudeen A, Househ M, Abd-Alrazaq A. The benefits and threats of blockchain technology in healthcare: A scoping review. International Journal of Medical Informatics. 2020 Oct 1;142:104246.
53. Zarour M, Alenezi M, Ansari MT, Pandey AK, Ahmad M, Agrawal A, Kumar R, Klhan RA. Ensuring data integrity of healthcare information in the era of digital health. Healthcare technology letters. 2021 Jun;8(3):66-77.

54. Liang YC. Blockchain for dynamic spectrum management. Dynamic Spectrum Management: From Cognitive Radio to Blockchain and Artificial Intelligence 2019 Nov 16 (pp. 121-146). Singapore: Springer Singapore.
55. Dhillon V, Metcalf D, Hooper M. The hyperledger project. In Blockchain enabled applications: Understand the Blockchain ecosystem and how to make it work for you 2017 Nov 30 (pp. 139-149). Berkeley, CA: Apress.
56. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and informatics. 2019 Mar 1;36:55-81.
57. Swan M. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc."; 2015 Jan 24.
58. Haleem A, Javaid M, Singh RP, Suman R. Telemedicine for healthcare: Capabilities, features, barriers, and applications. Sensors international. 2021 Jan 1;2:100117.
59. Sammeta N, Parthiban L. Blockchain-based scalable and secure EHR data sharing using proxy re-encryption. Int. Arab J. Inf. Technol.. 2023 Sep 1;20(5):702-10.
60. Su PC, Su TC. Secure blockchain-based electronic voting mechanism. Int. Arab J. Inf. Technol.. 2023 Mar 1;20(2):253-
61. Al-E'mari S, Anbar M, Sanjalawe Y, Manickam S, Hasbullah I. Intrusion detection systems using blockchain technology: A review, issues and challenges. Computer Systems Science & Engineering. 2022 Jan 1;40(1).
62. Coleman CD. The Importance of Variable Importance. arXiv preprint arXiv:2212.03289. 2022 Dec 6.
63. Hussein AF, ArunKumar N, Ramirez-Gonzalez G, Abdulhay E, Tavares JM, De Albuquerque VH. A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. Cognitive Systems Research. 2018 Dec 1;52:1-1.
64. Sarmah SS. Understanding blockchain technology. Computer science and engineering. 2018 Aug;8(2):23-9.
65. Peters GW, Panayi E. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In Banking beyond banks and money: A guide to banking services in the twenty-first century 2016 Sep 1 (pp. 239-278). Cham: Springer International Publishing.
66. OECD. Health at a Glance 2017: OECD Indicators, OECD Publishing, Paris.
67. Bharimalla PK, Dash SR, Choudhury HS. An Extensive Survey on Blockchain-Based Electronic Health Record Systems. International Journal of Reliable and Quality E-Healthcare (IJRQEH). 2022 Apr 1;11(2):1-2.
68. Yanamadala S, Morrison D, Curtin C, McDonald K, Hernandez-Boussard T. Electronic health records and quality of care: an observational study modeling impact on mortality, readmissions, and complications. Medicine. 2016 May 1;95(19):e3332.
69. Hussain S, Rahman H, Abdulsaheb GM, Al-Khawaja H, Khalaf OI. A Blockchain-Based Approach for Healthcare Data Interoperability. International Journal of Advances in Soft Computing & Its Applications. 2023 Jul 1;15(2).
70. Katuwal GJ, Pandey S, Hennessey M, Lamichhane B. Applications of blockchain in healthcare: current landscape & challenges. arXiv preprint arXiv:1812.02776. 2018 Dec 6.
71. Atzei N, Bartoletti M, Cimoli T. A survey of attacks on ethereum smart contracts (sok). In International conference on principles of security and trust 2017 Mar 28 (pp. 164-186). Berlin, Heidelberg: Springer Berlin Heidelberg.
72. Al-Talafheh K, Aplop F, Al-Yousef A, Obiedat M, Khazaaleh M. Predictive big data analytics capability model to enhancing healthcare organization performance. International Journal of Advances in Soft Computing and its Applications. 2024 Nov 1;16(3).
73. Hussain S, Rahman H, Abdulsaheb GM, Al-Khawaja H, Khalaf OI. A Blockchain-Based Approach for Healthcare Data Interoperability. International Journal of Advances in Soft Computing & Its Applications. 2023 Jul 1;15(2).
74. Bardaweel SK, Al Muhaissen SA, Alkurdi NH, Tayyem HH. Data privacy and confidentiality from the perspectives of general public and health care providers in Jordan. International Journal of Clinical Practice. 2021 Jun;75(6):e14117.