Security Risk Assessment of Blockchain-Based Patient Health Record Systems

Nedaa B. Al Barghuthi[1](✉), Huwida E. Said[2](✉), Sulafa M. Badi[3], and Shini Girija[2]

[1] Higher Colleges of Technology, Sharjah, UAE
Nedaa.albarghuthi@hct.ac.ae
[2] Zayed University, Dubai, UAE
{huwida.said,shini.girija}@zu.ac.ae
[3] The British University in Dubai, Dubai, UAE
sulafa.badi@buid.ac.ae

Abstract. Blockchain technology is receiving greater attention for enhancing the security of patient records systems; however, it is not a panacea, as many security risks have been found in these healthcare applications. This study conducts a state-of-the-art analysis of emerging risks in blockchain-based patient health record systems, their severity level, impact, and the corresponding countermeasures against them. In addition, we conclude our observations and indicate how blockchain security vulnerabilities may develop in the future. This study aims to promote more research on blockchain security challenges by offering researchers insights into future security and privacy developments in blockchain-based patient health record systems.

Keywords: Blockchain · Electronic health records (EHR) · Patient health records (PHR) · risks · impact · countermeasures · privacy · security

1 Introduction

The COVID-19 pandemic has worn out medical personnel, overburdened institutions, adversely affected and marginalized sizable population segments, and reduced demand for and access to non-COVID-19-related medical care [1]. Interoperability, lengthy procedures, delays in diagnosis and treatment, information-sharing delays, high operating expenses, long insurance processing times, and control, privacy, and security issues are just a few difficulties facing current healthcare systems. With the advent of blockchain technology, a distributed and decentralized ecosystem will be possible, ultimately securing and safeguarding critical medical data [2]. For example, an innovative decentralized record management system called MedRec was proposed by Azaria et al. [3], providing patients with a secure means to access an immutable medical log to store treatment details using blockchain technology.

The development of blockchain technology has created new research opportunities in some fields, including medical data preservation, data integrity, patient ownership of

M. Papadaki et al. (Eds.): EMCIS 2022, LNBIP 464, pp. 477–496, 2023.
https://doi.org/10.1007/978-3-031-30694-5_35

their data, simple medical data exchange, and efficient medical insurance claims [4, 5]. However, several studies [6–8] have concentrated on the security features of blockchain-based healthcare due to the growing demand for patient data and its associated security and privacy issues. These studies have paid little attention to the impact, severity level, and relevant countermeasures in the healthcare arena. Such a gap makes it challenging to properly tackle security threats in blockchain-based patient health record systems (BPHRS). Our research aims to identify potential security risks in BPHRS, analyze their severity level and impact, and identify the corresponding countermeasures available to lessen these dangers and secure BPHRS. The three main research questions that underpin this study are as follows:

RQ1: What are the emerging security risks in blockchain-based patient health record systems (BPHRS)?
RQ2: What are the severity levels and impacts of these risks?
RQ3: What are the recommended countermeasures to mitigate these risks?

This paper is organized as follows: The background of blockchain technology is described in the next section. The methodology is presented in section three. The study's findings are described in section four. We summarize the results and study limitations and suggest areas for future investigation.

2 Background: Blockchain Technology

A blockchain collects chronologically ordered, publicly accessible records called blocks [9]. The information is encrypted using cryptography to protect user privacy and prevent data manipulation. Since the information is managed and stored in a decentralized ledger, no single central authority makes all the decisions. Instead, a consensus of all the network's participating nodes, which are dispersed around the globe, is used to make most choices [10]. Security, transparency, decentralization, immutability, and distribution are some of the distinctive characteristics of blockchain technology. Blockchain does not rely on centralized, trustworthy entities to process data transactions. Therefore, no intermediary third party is required to audit and confirm the data exchanges [11]. According to their characteristics and network behavior, blockchains can be classified into public, private, and hybrid [12] (Table 1).

Table 1. Features of different kinds of blockchains.

	Public	Private	Hybrid
Type of database	Decentralized	Partially decentralized	Partially decentralized
Definition	Anyone can join and complete transactions on this permissionless distributed ledger [10]	A permissioned blockchain network functions in a private setting, such as a closed network, or is managed by a single identity [11]	It allows businesses to build private, permission-based, and public permission-less systems [10]
Advantages	Trustable, secure, and transparent [12]	Faster transactions and scalable [12]	Safe and cost-effective [12]
Disadvantages	Scalability issues and high energy consumption [2]	Trust-building issues, lower security, and centralization [2]	Lack of transparency and less incentive [3]
Examples	Ethereum [10]	Hyperledger [10]	Ripple [11]

3 Methodology

Using the search terms (TS = "Healthcare" or "Risks" or "Assessments" or "Countermeasures" AND TS = "Blockchain"), we performed a literature search using the Web of Science (WoS) and Scopus databases, establishing a time constraint from 2017 and beyond, and obtained 18 results. The IEEE and Science Direct search engines produced 20 and 13 papers, respectively, which were used to retrieve the supplemental material for the study. Thus, for the systematic literature review, 51 articles published between 2017 and 2022 were found and reviewed for inclusion and exclusion. The inclusion criteria included the study's publishing period (2017–2022) and applicability to blockchain-based healthcare systems. A PRISMA diagram is shown in Fig. 1 to illustrate the steps the researchers performed to identify relevant published materials and choose whether to include or exclude them. These steps include identification, screening, eligibility, and final inclusion.

4 Findings

This section discusses the findings of the systematic literature review organized according to the three research questions, RQ1, RQ2, and RQ3.

4.1 RQ1: What Are the Emerging Security Risks in BPHRS?

The healthcare industry faces challenges and inefficiencies, including fraud, erroneous healthcare data, a lack of stakeholder participation, and privacy and security concerns. Blockchain is seen as a logical technological solution for solving these issues and shortfalls [13–15]. However, significant problems must be resolved before a safe BPHRS is effectively deployed. We present the outcome of our systematic literature review in Fig. 2, which represents a taxonomy of the risks associated with BPHRS based on its features and network behavior. The most significant risks related to BPHRS are technical, threat/security, privacy, organizational, and regulation. The terms risk register, risk profile, and risk treatment are used to provide detailed explanations of each of the risks. A risk register is utilized to detect possible risks associated with a project or an enterprise. An organization's risks are analyzed in a risk profile to determine their severity and likelihood. Risk treatment is selecting and implementing actions to reduce the risk [39].

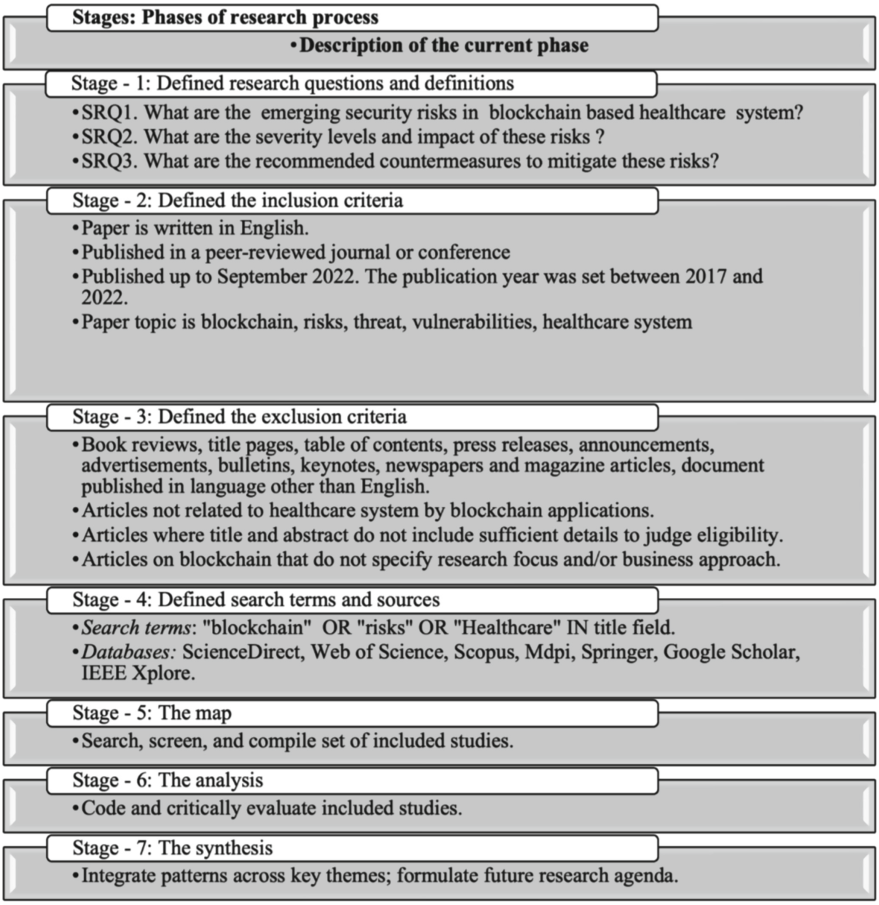

Fig. 1. Research phases

A. Technical risks

Before implementing a blockchain, several technical risks to its fundamental functions must be assessed and mitigated. The technical analysis concentrates on the characteristics of the created blockchain-based system, including its applications, the Blockchain it uses, and the consensus algorithm it employs [24]. The most prominent technical risks are scalability, smart contract bugs, poor consensus mechanism, and high energy consumption. As the number of nodes increases, validating every node and every transaction becomes a **scalability** [25] challenge. Data duplication makes it difficult to scale blockchain networks in the healthcare industry [25]. The poor consensus mechanism is mainly due to the lack of proper selection of consensus protocols [28]. Smart contract bugs occur due to poor contract code that generates an invalid result [31]. The Proof of Work (PoW) consensus mechanism used by the blockchain network requires considerable energy. Blockchains consume high energy levels because, no matter how many miners are on the network, blocks can only be added to the chain at set times. Most Ethereum-based healthcare blockchain uses this consensus algorithm, leading to **high energy consumption** [27]. In addition, several other technical risks are associated with BPHRS, as listed in Table 2.

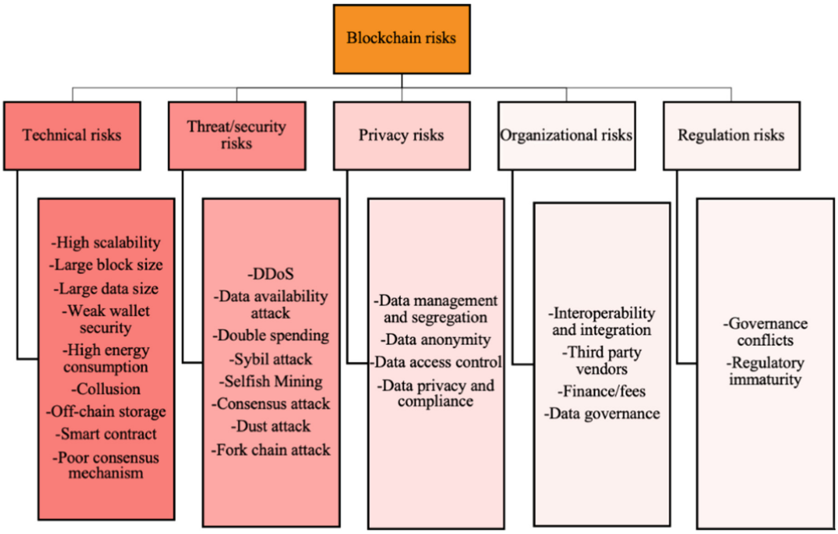

Fig. 2. Taxonomy diagram of blockchain risks of the healthcare system

B. Threat/security Risks

Even though Blockchain is considered safe and there is no participation by third parties, attacks such as double spending [16], consensus attack [17], Sybil attack [18], DDoS [17], and others have become a serious issue, especially in healthcare. When hacking, many cybercriminals aim directly at customers' financial information stored in their wallets. Hackers often try to boost their earnings by generating network congestion and unnecessary mining blocks. The most prominent security

Table 2. List of technical risks in BPHRS

Risk register	Risk profile	Blockchain types	Healthcare domain
High scalability	Difficulty in scale to a large number of transactions [25]	Public	Covid trace tracking and PHR
Large block size	Maximum number of transactions that can be added to a block at once [20]	Public/private	EHR
Large data size	Difficult to handle data with high temporal resolution [6]	Public	EHR
Weak wallet security	Poor key management [27]	Public/private	EHR
High energy consumption	The PoW consensus mechanism requires a considerable amount of energy	Public	E-healthcare App
Collusion	Transaction time delay [26, 29]	Public/private	PHR
Off-chain storage	No network record of off-chain transactions is available in the event of a dispute between the parties [30]	Private	EHR, IoT
Smart contract bugs/logic/process	Poor contract code [31]	Public/private	EHR, IoT
Poor consensus mechanism	Decision-making by consensus may not always be guaranteed [28]	Public	EHR

risk is the **double-spending attack**, in which several transactions can occur in the network without a fair exchange [16]. Every participant must adhere to the fundamental principle of equitable exchange, which states that they are not permitted to discover more messages about other participants' inputs than they would while implementing the consensus protocol [6]. A **consensus attack** occurs in Blockchain when a group of miners or a single miner controls more than 50% of the network's mining hash or computer [17]. Attackers use a 51% attack to reverse transactions on a blockchain and hinder the process of storing new blocks. During a **Sybil attack**, the attacker disrupts information flow, blocks the trustworthy nodes, and refuses to receive or send information after false identities are recognized by the blockchain system [17]. In a **DDoS attack**, an attacker can fill up blocks with spam transactions if they submit many blockchain transactions to the network, causing valid transactions to sit in "*mempools*." If legitimate transactions are not included in blocks, they are not added to the ledger, and the Blockchain will not be able to function [1]. Table 3 illustrates the list of security risks that disrupt the proper functioning of BPHRS.

Table 3. List of threat/security risks in BPHRS

Risk register	Risk profile	Blockchain types	Healthcare domain
DDoS attacks	Transaction flooding [17]	Public	EHR, PHR
	Dust transactions [20]	Private	EHR
Data availability attack	Receive an erroneous block by concealing the malicious part of the block from other nodes [21]	Public	E-healthcare App
Double spending	Double spending without fair exchange [16]	Public	EHR, PHR
Sybil attack	Run several fake nodes [18]	Public	EHR
Selfish mining	Allowing nodes with more than 51% computational power to reverse transactions in a blockchain [20]	Public	PHR
Consensus attack (51% attack)	The majority of the mining power is controlled by entities [17]	Private	EHR, PHR
Dust attack	Dust transactions [22]	Public	EHR
Fork chain attack	A fork on the Blockchain and more than one chain exist [23]	Public	EHR

C. **Privacy Risks**

When patient records in BPHRS are shared with other organizations without the data owners' consent for research or medication advertising, serious data privacy problems arise. Maintaining the integrity and confidentiality of outsourced data leads to a significant burden on stakeholders and blockchain nodes in computation and communication [37]. Table 4 shows the list of privacy risks in BPHRS.

Table 4. List of privacy risks in BPHRS

Risk register	Risk profile	Blockchain types	Healthcare domain
Data management and segregation	Poor data management results in an information overload [37]	Public/private	EHR
Data anonymity	Leakage of sensitive patient information [37]	Public/private	EHR, PHR
Data access control	Unauthorized access to medical data [38]	Public/private	EHR, PHR
Data privacy and compliance	Compliance issues with privacy laws such as HIPPA and GDPR [38]	Public/private	EHR

D. **Organizational risks**

Information about patients can be shared securely with healthcare organizations via Blockchain. Blockchain technology has helped organizations by making it easier to manage the clinical trials required for drug trials. Since copies of the shared ledger are stored across users' devices, Blockchain allows organizations to keep and back up medical insurance [7, 31]. However, investigating Blockchain's internal and external organizational challenges should be considered. Table 5 presents the list of organizational risks associated with BPHRS.

Table 5. List of organizational risks in BPHRS

Risk register	Risk profile	Blockchain types	Healthcare domain
Interoperability and integration	Occurs due to a lack of trust between parties, and a lack of open standards [7, 31]	Public/private	PHR
Third-party vendors	Risks of sensitive information leakage due to the involvement of third-party vendors [32]	Public/private	PHR
Finance/Fees	A large number of transactions and fraud activities contribute to the high cost of these services [13]	Public/private	EHR
Data governance	Lack of guidelines and standards to control the accuracy, security, and use of sensitive data [31]	Public/private	EHR, E-healthcare App

E. **Regulation risks**

Regulation risks such as governance conflicts and regulatory immaturity were other significant risks identified within BPHRS (see Table 6). The majority of BPHRS are created to be Health Insurance Portability and Accountability Act (HIPAA) [33] and General Data Protection Regulation (GDPR) compliant [34]. The implementation of these regulations has been hampered by decentralization and a lack of involvement from reliable third parties. However, because these regulations will link various social, economic, and healthcare systems, patients and service providers may find it difficult to follow the applications' results in the absence of a legal or compliance code, which results in governance conflicts [35]. Regulatory immaturity involves difficulties in defining the rules that will consider the cooperation of diverse stakeholders to develop an entire ecosystem that also considers the current regulatory system [36].

Table 6. List of organizational risks in BPHRS

Risk register	Risk profile	Blockchain types	Healthcare domain
Governance conflicts	Difficult to follow the applications' results in the absence of a legal or compliance code [35]	Public/private	EHR, E-healthcare App
Regulatory immaturity	Problems in defining the rules that will consider the cooperation of diverse stakeholders to develop an entire ecosystem [36]	Public/private	PHR

4.2 RQ2: What are the Severity Levels and Impacts of These Risks?

An in-depth analysis of the risks' immediate impact and severity level in blockchain-based healthcare systems is conducted. The projected harm or unfavorable outcome from exposure to the risk is known as risk severity (also known as risk impact). Using an ordinal scale is one of the most popular techniques to describe risk severity. Low, moderate, high, and severe are the most typical qualitative values on an ordinal scale [39]. Table 5 lists the impacts of all security risks in BPHRS. Table 7 illustrates the effects of emerging security risks in BPHRS.

A. **Impact of technical risks**

Scalability, consensus, smart contract bugs/logic, and transaction time delay/real-time are the most severe technical risks [25, 29]. BPHRS has a scalability issue that forces users to pay considerable fees and wait hours for transaction approval, delaying the provision of services [25]. The systems cannot manage millions of healthcare records in real time due to transaction time delays [29], and there is a probability that a medical history error will occur. The lack of records may cause treatment to be delayed [29]. Blockchain demands a tremendous amount of computer power, which is energy-intensive; it is estimated that Bitcoin mining alone uses 0.5% of the world's electrical supply [28].

B. **Impact of threat/security risks**

The most severe vulnerability risks that expose healthcare data to hackers and cyberattacks are consensus attacks and double spending [16, 17]. Transaction data integrity is compromised during a 51% attack assault, and the network's resources are depleted. The availability of services and the integrity of the data, which are crucial for healthcare applications, are adversely affected [17]. The possibility of double spending undermines the ledger's credibility. Numerous dangers can result in double spending, including Sybil-based double spending and 51% attacks, among others [16]. DDoS attacks have a high severity level, which can immediately interrupt network operations and prohibit access to essential data [20]. The patients and the medical staff may be unable to converse or exchange information because of this attack. Massive data requests block the server. As a result, the attack impacts demand and response generation [20].

C. **Impact of privacy risks**

Important security and privacy issues are brought up by introducing a single interoperable platform to make all healthcare data available in one place. Recent cyberattacks like WannaCry and the breach of medical data at Anthem are evidence of this [41]. When medical data is uploaded to the cloud to be shared in a healthcare blockchain, it can raise essential privacy issues that previous studies have largely ignored. For example, in cloud blockchain networks, hackers can become curious about medical resources and steal sensitive patient data without the patients' permission [20].

D. **Impact of organizational risks**

Interoperability, integration, and data governance are the most severe organizational risks. Premier Healthcare Alliance estimates that a lack of interoperability costs 150,000 lives and US$18.6 billion annually [40]. Most EHR products now available on the market impose restrictions on the open exchange of patient data across different product platforms. Although blockchain technology is intended to be more secure than traditional methods of data exchange, a lack of industry standards may make it difficult for devices to communicate with one another [31]. Industry standards are essential to the success of the healthcare blockchain market as it evolves [7].

E. **Impact of regulation risks**

Governance conflicts have a significant impact on how well BPHRS operates. Major security regulations must be followed, which apply to EHR contents [35]. For instance, anyone can access the data on a blockchain, and no one is responsible for ensuring its availability or security. Users are the data controllers under GDPR; however, Blockchain's immutability cannot erase or modify their data. Who should be held responsible for breaking the rules and regulations is a crucial concern for regulators in governance [31].

Table 7. Summary table for impacts of all the emerging security risks

Risk register	Risk Impact	Blockchain types
High scalability	Increase in processing needs across the entire BPHRS infrastructure [25]	Public
Large block size	Unprocessed patient data, including genomic, critical organs, and others, resulting in unnecessary operating costs [20]	Public/private
Large data size	Issues with handling multi-dimensional medical data and high computational costs [6]	Public
Weak wallet security	If the key is stolen, it puts both patients' sensitive data and finances in jeopardy [27]	Public/private
High energy consumption	Critical performance degradation of patient healthcare systems [28]	Public
Collusion	Unable to handle millions of healthcare records in real-time [26, 29]	Public/private
Off-chain storage	Introduces a single point of failure, which continuously limits the availability of medical records [30]	Private
Smart contract bugs/process/logic	User revocation is expensive and results in a significant blockchain computation overhead. [31]	Public/private
Poor consensus mechanism	Impact on how consensus decisions are made [28]	Public
DDoS attacks	Massive medical transaction backlogs and higher mining fees [19]	Public/private
Data availability attack	Prompt diagnosis and treatment would be delayed [21]	Public
Double spending attack	Blocks specific IP addresses and transactions between various hospitals on the blockchain network [18]	Public
Sybil Attack	Targets sensitive data such as personal information, insurance details, and patient medical records [18]	Public
Selfish mining	If the patient's treatment record transactions are reversed, it could pose a significant threat to the patient [20]	Public

(*continued*)

Table 7. (*continued*)

Risk register	Risk Impact	Blockchain types
Consensus attack	Threatens the integrity of medical data on the Blockchain [17]	Private
Dust attack	Unavailability of patients' records during the treatment [22]	Public
Fork chain attack	A potential threat to the accuracy and integrity of medical data [23]	Public
Data management and segregation	Problems in managing and storing enormous numbers of EHRs locally and communicating secure data [37]	Public/private
Data anonymity	Conceals the actual identity of the nodes accessing the data [37]	Public/private
Data access control	Lack of authorization and distribution of medical records among healthcare providers [38]	Public/private
Data privacy and compliance	Raises concerns about compliance with international privacy and security laws, including the GDPR and HIPAA [38]	Public/private
Interoperability and integration	Problems in sharing medical data across many blockchain-based BPHRS [7, 31]	Public/private
Third-party vendors	Risks of sensitive information leakage are considered when a patient shares part of their medical records with an authorized third party [32]	Public/private
Finance/Fees	Insurance frauds and medical trials without planning contribute to high transaction fees [13]	Public/private
Data governance	Lack of framework for all healthcare stakeholders is not available [31]	Public/private
Governance conflicts	Both patients and service providers may find it difficult to follow the applications' results in the absence of a legal or compliance code [35]	Public/private
Regulatory immaturity	Unsure of responsibility for breaking privacy rules and regulations [36]	Public/private

4.3 RQ3: What are the Recommended Countermeasures to Mitigate These Risks?

Here, we outline the current security and privacy-preserving methods and detection techniques that BPHRS can apply. Table 8 presents the list of countermeasures to mitigate BPHRS risks.

A. **Countermeasures for technical risks**

The technical study examines the features of the developed blockchain-based system, including its applications, the Blockchain it uses, and the consensus algorithm it employs. A variety of techniques are investigated to address scalability problems (such as permissioned blockchains, the lighting protocol, delegated proof of stake, and directed acyclic graphs) [25, 44]. The Practice Byzantine Fault Tolerance (PBFT) algorithm instead of the PoW consensus algorithm can be used to solve scalability issues since it is better suited for BPHRS [25]. Segregated Witness restricts block sizes to 1MB, which minimizes DDoS attacks because forged blocks with larger sizes would be checked out and thrown away [45].

Ethereum attempted to tackle the security limitations of proof of work, the lower danger of centralization, and high energy consumption using the Proof of Stake (PoS) mechanism [42]. To reduce data size, metadata is stored in a blockchain, and its sensitive and significant data is stored in a separate storage system such as the cloud [14].

The techniques mainly used for tackling weak wallet security are using a multi-level authentication method when accessing wallets or generating wallet keys. In addition, we might use multi-signature wallets and cold wallets and not share the private keys of wallets with anyone [45]. Estimable PoW estimates how much work has been done and if the corresponding agreement reached a consensus [46]. IoT sensors can measure a patient's health conditions in real-time, which can be used in public blockchains such as the Ethereum environment [47].

B. **Countermeasures for threat/security risks**

Increased authentication that permits pairing with blockchain blocks is required to reduce double spending attacks, which calls for more confirmations. It is also possible to apply non-interactive non-knowledge proof (NIZK), which aids in spotting anomalies in blockchain systems and allows for the addition of detection criteria to the network, making it impervious to fraudulent and early detection [4]. When nodes surpass a specified threshold, the power monitoring tool should impose restrictions to ensure that no single miner or mining pool has more than 50% of the network hash rate [25]. This helps to track node computing power continually to protect against consensus attacks. It is common practice to detect DoS/DDoS using anomaly detection techniques and reactive defense strategies. While unsupervised learning is frequently used for anomaly and novelty detection, machine learning (ML) techniques are now being utilized to predict harmful and legitimate traffic. Fee- and age-based designs are reactive defense strategies [42]. The mempool accepts an incoming transaction in the fee-based architecture if it pays the minimum relay and mining fees [19]. By only taking transactions that will be added to the Blockchain via mining, the main goal of this approach is to thwart an attacker's plan of attack. The authors calculated the inputs or parent transactions for each incoming transaction in an age-based process and set the "average age" variable to zero [19]. By randomly requesting/sampling portions of the block from the malicious node, Coded Merkle Tree (CMT) was developed to help light nodes identify data availability attacks [21]. Anti-Dust is offered to defend against various dust attacks effectively [22]. Through PBFT consensus, communication with peers can be done directly, reducing the chance of forgery and eliminating financial costs [28]. To protect from fork chain attacks, users should ensure the nodes they connect to are reliable to prevent multiple forks [23]. Selfish mining can be reduced by a backward-compatible protection method in which the fork resolution strategy ignores blocks not released in time [43]. The smart contracts should be designed with formal verification, which checks that a computer program executes as per the standard specification anticipated by the stakeholders [48].

C. **Countermeasures for privacy risks**

BPHRS must develop privacy policies to guarantee that only the patient and healthcare professionals can access patient medical records with the patient's express authorization. Healthblock is used to prevent security risks observed in widely used systems for intelligent healthcare and to strengthen the resiliency of healthcare data management systems [51]. Town Crier maintains anonymity using encrypted variables while allowing smart contracts to leverage data from sources beyond the Blockchain [19]. Ancile uses advanced cryptographic algorithms and smart contracts in an Ethereum-based blockchain for increased access control and data encryption [50]. No direct personal data should be stored on the Blockchain to ensure privacy. Some methods for dealing with this involve adding a cryptographic hash to the chain [38].

D. **Countermeasures for organizational risks**

The effectiveness of blockchain systems depends on organizational security controls for blockchains. As a result, we intend to examine countermeasures for corporate risks associated with BPHRS. Interoperability and integration can be controlled by building future capabilities, training, funding, and setting a suitable regulatory framework for blockchain adoption in the healthcare sector [6]. Smart contracts could implement agreements to secure agreements from healthcare professionals and patients before granting third-party vendors access to their content [31]. The system would be more effective if disintermediation led to lower transaction costs and near-real-time processing [13]. Organizations should agree on a framework for defining the data, size, and format that will be saved to solve data governance issues. This framework should be familiar to all healthcare stakeholders [6].

E. **Countermeasures for regulation risks**

All stakeholders in the healthcare industry should agree on a framework for specifying the data, size, and format that organizations will save to overcome **regulatory immaturity** issues [6]. To ensure that blockchains comply with national and international laws, the legislative frameworks must be evaluated and the required changes enacted. This may reduce **governance conflicts** by gaining certification from the International Standardization Authority, which will facilitate the rapid and secure development of BPHRS [49].

Table 8. List of countermeasures for all emerging security risks

Risk register	Risk severity level	Risk treatment
Large scalability	Severe	Use the PBFT algorithm instead of the PoW consensus algorithm [25]
Large block size	High	Minimize the block size to 1 MB by Segregated Witness [45]
Large data size	Medium	Separate storage areas into the cloud [14]
Weak wallet security	Medium	Implement multi-level authentication, wallet keys, multi-signature wallets, and cold wallets [45]
High energy consumption	High	Introduce a hybrid consensus algorithm based on the PBFT algorithm, and the POS algorithm [42]
Collusion/Transaction time delay	Severe	Estimable PoW [46]
	High	Use IoT sensors [47]
Off-chain storage	Low	Applying masking blocks [30]
Poor consensus mechanism	Severe	Use PBFT consensus [28]
Smart contract bugs/logic/process	Severe	Verifying the logic of the intelligent contract programs within the Blockchain [48]
DDoS attacks	High	Anomaly detection methods [19]
	High	Fee-based design and age-based design [19]
Data availability attack	Medium	Coded Merkle Tree (CMT) [21]
Double spending	Severe	Non-interactive non-knowledge proof (NIZK) [4]
Sybil attack	High	Pure PoW consensus protocol [18]
Selfish mining	Low	Backward-compatible protection approaches [43]
Consensus attack	Severe	Power monitoring tool [25]
Dust attack	High	Anti-Dust [22]
Fork chain	High	Use reliable nodes [23]
Data management and segregation	Low	Healthblock to strengthen the resiliency of healthcare data management systems [51, 52]

(*continued*)

Table 8. (*continued*)

Risk register	Risk severity level	Risk treatment
Data anonymity	High	Town Crier maintains anonymity [19]
Data access control	Severe	Use Ancile for increased access control [50]
Data privacy and compliance	Severe	Add a cryptographic hash to the chain [38]
Interoperability and integration	Severe	Set the suitable regulatory framework for blockchain adoption in the healthcare sector [6]
Third-party vendors	Medium	Smart contracts [31]
Finance/Fees	high	Disintermediation techniques [13]
Data governance	medium	A standard framework for defining the data, size, and format [6]
Governance conflicts	medium	Legislative frameworks need to be evaluated [6]
Regulatory immaturity	high	Gaining certification from International Standardization Authority [49]

5 Discussion

A systematic review of published blockchain-based healthcare systems literature identified the critical area where Blockchain may be used to address data management and access control problems in the EHR. Blockchain technology can reduce costs while increasing the process quality and efficiency in many different areas of healthcare. According to the research, private blockchains are less vulnerable to security risks than public blockchains. The network's scalability, technological risks, rising transaction fees, and security and privacy threats are the ongoing problems that must be resolved for a safe and effective BPHRS. Numerous studies and real-world applications offer countermeasures against these hazards. The best solutions identified are the PBFT algorithm and the PoS consensus protocol, which reduce the overhead of scalability, transaction delay issues, and transaction cost to a large extent [25, 28, 46]. However, there are still difficulties and unresolved research problems with developing reliable and efficient security solutions that can guarantee the proper operation of BPHRS. There is still a regulatory issue with defining the rules and conditions of usage for all parties interested in the BPHRS. One of the primary potential techniques for adopting a blockchain into various healthcare areas is to create a compliance code with consistent standards, standardizations, and international legislation. BPHRS would benefit from adopting AI-based methods like machine learning and deep learning with Blockchain to improve clinical trial verdicts, medical research, and treatment processes.

6 Conclusion

This research examined emerging risks related to BPHRS and identified numerous technological security and vulnerability issues. To conduct an in-depth analysis, the authors reviewed 51 publications using PRISMA's inclusion and exclusion criteria in response to the RQs. We provided an overview of BPHRS security and identified vulnerabilities, threats, and viable countermeasures for security specialists and researchers. This study mainly concerns the severity level and impact of these hazards on the patient record system. To forecast the potential harm caused by these threats and confirm whether the current technology is sufficient to survive persistent hacking, it is essential to evaluate the severity level and impact of security and privacy concerns in BPHRS. The study found that, compared to public blockchains, private blockchains are less susceptible to security risks. The ongoing issues that must be fixed for a secure and reliable BPHRS include the network's scalability, technological hazards, increased transaction fees, and security and privacy threats. Future work on BPHRS will center on more secure architecture, creating a robust consensus mechanism, a standard regulatory framework, and a more thorough smart contract detection.

References

1. Behnke, R.: How Blockchain DDoS Attacks Work (2022). Halborn.com. https://halborn.com/how-blockchain-ddos-attacks-work/
2. Marbouh, D., et al.: Blockchain for COVID-19: review, opportunities, and a trusted tracking system. Arab. J. Sci. Eng. **45**(12), 9895–9911 (2020). https://doi.org/10.1007/s13369-020-04950-4
3. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A.: MedRec: using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30. IEEE, August 2016
4. Alsunbul, A., Elmedany, W., Al-Ammal, H.: Blockchain application in healthcare industry: attacks and countermeasures. In: 2021 International Conference on Data Analytics for Business and Industry (ICDABI), pp. 621–629. IEEE, October 2021
5. Kumar, T., Ramani, V., Ahmad, I., Braeken, A., Harjula, E., Ylianttila, M.: Blockchain utilization in healthcare: key requirements and challenges. In: 2018 IEEE 20th International conference on e-health networking, applications and services (Healthcom), pp. 1–7. IEEE, September 2018
6. Attaran, M.: Blockchain technology in healthcare: challenges and opportunities. Int. J. Healthc. Manag. **15**(1), 70–83 (2020). https://doi.org/10.1080/20479700.2020.1843887
7. Onik, M.M.H., Aich, S., Yang, J., Kim, C.S., Kim, H.C.: Blockchain in Healthcare: Challenges and Solutions. Big Data Analytics for Intelligent Healthcare Management, pp. 197–226. Academic Press, Cambridge (2019)
8. Ismail, L., Materwala, H.: Article; a review of blockchain architecture and consensus; protocols: use cases, challenges, and solutions. Symmetry **11**(10), 1198 (2019). https://doi.org/10.3390/sym11101198
9. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008). Accessed 20 Aug 2018. https://bitcoin.org/bitcoin.pdf
10. Rifi, N., Rachkidi, E., Agoulmine, N., Taher, N.C.: Towards using blockchain technology for eHealth data access management. In: 2017 4th International Conference on Advances in Biomedical Engineering (ICABME 2017), pp. 1–4. IEEE (2017)

11. Vacca, A., Di Sorbo, A., Visaggio, C., Canfora, G.: A systematic literature review of blockchain and smart contract development: techniques, tools, and open challenges. J. Syst. Softw. **174**, 110891 (2021)
12. Morkunas, V.J., Paschen, J., Boon, E.: How blockchain technologies impact your business model. Bus. Horiz. **62**(3), 295–306 (2019)
13. Noon, A.K., Aziz, O., Zahra, I., Anwar, M.: Implementation of Blockchain in Healthcare: A Systematic Review. In 2021 International Conference on Innovative Computing (ICIC), pp. 1–10. IEEE, November 2021
14. Chen, Y., Ding, S., Xu, Z., Zheng, H., Yang, S.: Blockchain-based medical records secure storage and medical service framework. J. Med. Syst. **43**(1), 1–9 (2018). https://doi.org/10.1007/s10916-018-1121-4
15. Abunadi, I., Kumar, R.: Blockchain and business process management in health care, especially for COVID-19 cases. Secur. Commun. Netw. **2021**, 1–16 (2021). https://doi.org/10.1155/2021/2245808
16. Khan, S.N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., Bani-Hani, A.: Blockchain smart contracts: applications, challenges, and future trends. Peer-to-Peer Netw. Appl. **14**(5), 2901–2925 (2021). https://doi.org/10.1007/s12083-021-01127-0
17. Wang, H., Wang, Y., Cao, Z., Li, Z., Xiong, G.: An overview of blockchain security analysis. In: Cyber Security: 15th International Annual Conference, CNCERT 2018, pp. 14–16 August (2018), Revised Selected Papers 15, pp. 55–72. Springer Singapore (2019)
18. Iqbal, M., Matulevičius, R.: Exploring Sybil and double-spending risks in blockchain systems. IEEE Access **9**, 76153–76177 (2021)
19. Hasanova, H., Baek, U.J., Shin, M.G., Cho, K., Kim, M.S.: A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. Int. J. Netw. Manag. **29**(2), e2060 (2019)
20. Jabarulla, M., Lee, H.: A Blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: opportunities and applications. Healthcare **9**(8), 1019 (2021). https://doi.org/10.3390/healthcare9081019
21. Mitra, D., Tauz, L., Dolecek, L.: Overcoming Data Availability Attacks in Blockchain Systems: LDPC Code Design for Coded Merkle Tree (2021). arXiv preprint arXiv:2108.13332
22. Wang, Y., Yang, J., Li, T., Zhu, F., Zhou, X.: Anti-dust: a method for identifying and preventing Blockchain's dust attacks. In: 2018 International Conference on Information Systems and Computer Aided Education (ICISCAE), pp. 274–280. IEEE, July 2018
23. Ploder, C., Spiess, T., Bernsteiner, R., Dilger, T., Weichelt, R.: A Risk Analysis on Blockchain Technology Usage for Electronic Health Records. Cloud Computing And Data Science, pp. 1–16 (2021). https://doi.org/10.37256/ccds.222021777
24. Wright, S.: Technical and legal challenges for healthcare blockchains and smart contracts. In: 2019 ITU Kaleidoscope: ICT for Health: Networks, Standards, and Innovation (ITU K) (2019)
25. Panda, S.K., Jena, A.K., Swain, S.K., Satapathy, S.C. (Eds.): Blockchain Technology: Applications and Challenges. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-69395-4
26. Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T.: Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J. Med. Syst. **42**(7), 1–7 (2018). https://doi.org/10.1007/s10916-018-0982-x
27. Beinke, J., Fitte, C., Teuteberg, F.: Towards a stakeholder-oriented blockchain-based architecture for electronic health records: design science research study. J. Med. Internet Res. **21**(10), e13585 (2019). https://doi.org/10.2196/13585
28. Wu, Y., Song, P., Wang, F.: Hybrid consensus algorithm optimization: a mathematical method based on POS and PBFT and its application in Blockchain. Math. Probl. Eng. 2020 (2020)

29. Siyal, A.A., Junejo, A.Z., Zawish, M., Ahmed, K., Khalil, A., Soursou, G.: Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. Cryptography **3**(1), 3 (2019)
30. Castillo, J.: Blockchain: a decentralized solution for secure applications (doctoral dissertation, university of texas at San Antonio) (2022)
31. Xiong, H., Chen, M., Wu, C., Zhao, Y., Yi, W.: Research on progress of blockchain consensus algorithm: a review on recent progress of blockchain consensus algorithms. Futur. Internet **14**(2), 47 (2022). https://doi.org/10.3390/fi14020047
32. Esmaeilzadeh, P.: Benefits and concerns associated with blockchain-based health information exchange (HIE): a qualitative study from physicians' perspectives. BMC Med. Inform. Decis. Mak. **22**(1), 1–18 (2022)
33. Gostin, L.O., Levit, L.A., Nass, S.J. (Eds.): Beyond the HIPAA privacy rule: enhancing privacy, improving health through research (2009)
34. Wachter, S.: Normative challenges of identification in the Internet of Things: privacy, profiling, discrimination, and the GDPR. Comput. Law Secur. Rev. **34**(3), 436–449 (2018)
35. Nguyen, D., Pathirana, P., Ding, M., Seneviratne, A.: Blockchain for secure EHRs sharing of mobile cloud based E-Health systems. IEEE Access **7**, 66792–66806 (2019). https://doi.org/10.1109/access.2019.2917555
36. Min, M., et al.: Learning-based privacy-aware offloading for healthcare IoT with energy harvesting. IEEE Internet Things J. **6**(3), 4307–4316 (2019). https://doi.org/10.1109/jiot.2018.2875926
37. Bernal Bernabe, J., Canovas, J., Hernandez-Ramos, J., Torres Moreno, R., Skarmeta, A.: Privacy-preserving solutions for blockchain: review and challenges. IEEE Access **7**, 164908–164940 (2019). https://doi.org/10.1109/access.2019.2950872
38. Sookhak, M., Jabbarpour, M.R., Safa, N.S., Yu, F.R.: Blockchain and smart contract for access control in healthcare: a survey, issues and challenges, and open issues. J. Netw. Comput. Appl. **178**, 102950 (2021)
39. Lagrama, E.R.C.: Preventing Disaster: Quantifying Risks at the UP Diliman University Library (2009)
40. DeVore, S., Champion, R.W.: Driving population health through accountable care organizations. Health Aff. **30**(1), 41–50 (2011)
41. Ghafur, S., Grass, E., Jennings, N.R., Darzi, A.: The challenges of cybersecurity in health care: the UK national health service as a case study. Lancet Digit. Health **1**(1), e10–e12 (2019)
42. Rodrigues, B., Stiller, B.: Cooperative signaling of DDoS attacks in a blockchain-based network. In: Proceedings of the ACM SIGCOMM 2019 Conference Posters and Demos, pp. 39–41 (2019)
43. Zhang, R., Preneel, B.: Publish or perish: a backward-compatible defense against selfish mining in bitcoin. In: Handschuh, H. (ed.) CT-RSA 2017. LNCS, vol. 10159, pp. 277–292. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-52153-4_16
44. Singh, S., Sanwar Hosen, A.S.M., Yoon, B.: Blockchain security attacks, challenges, and solutions for the future distributed IoT network. IEEE Access **9**, 13938–13959 (2021)
45. Wen, Y., Lu, F., Liu, Y., Huang, X.: Attacks and countermeasures on blockchains: a survey from layering perspective. Comput. Netw. **191**, 107978 (2021)
46. Hsueh, C., Chin, C.: EPoW: solving blockchain problems economically. In: 2017 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computed, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation, SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI, 2017, pp. 1–8 (2017)
47. Pham, H.L., Tran, T.H., Nakashima, Y.: A secure remote healthcare system for a hospital using blockchain smart contract. In: Proceedings of the IEEE Globecom Workshops, pp. 1–6 (2018)

48. Hewa, T.M., Hu, Y., Liyanage, M., Kanhare, S.S., Ylianttila, M.: Survey on blockchain-based intelligent contracts: technical aspects and future research. IEEE Access **9**, 87643–87662 (2021)
49. Pinter, K., Schmelz, D., Lamber, R., Strobl, S., Grechenig, T.: Towards a multi-party, blockchain-based identity verification solution to implement clear name laws for online media platforms. In: Business Process Management: Blockchain and Central and Eastern Europe Forum. BPM 2019. LNBIP, vol. 361, pp. 151–165. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-30429-4_11
50. Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B.: Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain. Cities Soc. **39**, 283–297 (2018)
51. Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., Abid, M.: HealthBlock: a secure blockchain-based healthcare data management system. Comput. Netw. **200**, 108500 (2021)
52. Papadaki, M., Karamitsos, I., Themistocleous, M.: Covid-19 digital test certificates and Blockchain. J. Enterp. Inf. Manag. **34**, 993–1003 (2021). https://www.researchgate.net/publication/353272635_ViewpointCovid-19_digital_test_certificates_and_blockchain