Blockchain and emerging technologies for next generation secure healthcare: a comprehensive survey of applications, challenges, and future directions

Omar Cheikhrouhou, Khaleel Mershad, Maryline Laurent, Anis Koubaa

Blockchain and Emerging Technologies for Next Generation Secure Healthcare: A Comprehensive Survey of Applications, Challenges, and Future Directions

Omar Cheikhrouhou[a,b,*], Khaleel Mershad[c], Maryline Laurent[d], Anis Koubaa[e]

[a]*CES Laboratory, National School of Engineers of Sfax, University of Sfax, Sfax 3038, Tunisia*
[b]*Higher Institute of Computer Science of Mahdia, University of Monastir, Tunisia.*
[c]*Computer Science and Mathematics Department, School of Arts and Sciences, Lebanese American University (LAU), Beirut, Lebanon.*
[d]*Samovar, Télécom SudParis, Institut Polytechnique de Paris, France.*
[e]*Robotics and Internet of Things Lab, Prince Sultan University, Riyadh, Saudi Arabia.*

Abstract

Faced with multiple societal challenges, the healthcare sector has been compelled to leverage recent and emerging technologies to adapt. Blockchain is one of the leading technologies, offering transparency, process automation, immutability of traces and the ability to scale up in terms of both the volume of processes and the number of players interacting. The goal of the paper is to show the potential of blockchain technology - alone or merged with other technologies - to help the healthcare system evolve and provide scalable, efficient and secure solutions to four healthcare applications: electronic health record (EHR) storage, health data sharing, remote patient monitoring, and pharmaceutical supply chains. After identifying the functional and security requirements of healthcare systems, the paper conducts an in-depth review of the literature. The survey assesses the effectiveness of blockchain-based solutions in meeting functional, privacy and security needs. It is completed by an analysis of the synergies that can be expected between blockchain and emerging technologies, e.g. artificial intelligence, federated learning, the Internet of Things (IoT), and Large Language Models (LLM), to the benefit of security or privacy in healthcare.

Keywords: Blockchain, Healthcare, Security, AI, LLM, Federated Learning, Lightweight Blockchain, Survey.

1. Introduction

Among the 17 Sustainable Development Goals (SDGs) adopted by the United Nations Member States in 2015 [1], the third goal focuses on health and well-being for everyone. This task

*corresponding author
Email addresses: omar.cheikhrouhou@isetsf.rnu.tn (Omar Cheikhrouhou), khaleel.mershad@aul.edu.lb (Khaleel Mershad), Maryline.Laurent@telecom-sudparis.eu (Maryline Laurent), akoubaa@psu.edu.sa (Anis Koubaa)

is made more complex by the escalating costs of advanced medical care, and an ageing population. Cutting-edge technologies can help implement effective strategies for achieving optimal and scalable healthcare outcomes. Innovations such as remote monitoring of the elderly, an aid to diagnosis, and improved management of data and pharmaceutical supply chains can significantly contribute to this goal.

Blockchain technology is one the promising cutting edge technologies in this context. Indeed, it provides automation of cumbersome processes requiring specific conditions (e.g. patient consent, temperature of drugs during transport) and the involvement of several players in the healthcare sector (surgeon, hospital, health insurance company, drug manufacturer). Every condition, every stakeholder approval, every automated decision could be traced in the blockchain, bringing transparency to patients, auditability to legal entities, continuous monitoring and anomaly detection. However, it is crucial that these advances do not compromise the security of the system or the privacy of patients.

This paper proposes a survey on blockchain-based solutions offering security guarantees in the four following healthcare applications: electronic health record (EHR) storage, health data sharing, remote patient monitoring, and pharmaceutical supply chains. It presents real-world cases and comparative analyses to highlight the benefits and obstacles encountered by healthcare stakeholders in adopting blockchain technology.

The survey is complemented by an analysis of the synergies that can be expected between blockchain and emerging technologies, for the benefit of security or privacy in healthcare. The technologies examined include artificial intelligence, federated learning, the internet of things (IoT) and large language models (LLMs). The analysis looks at ethical and security considerations, discussing data ownership, patient privacy and the changing role of individuals in managing their health data.

The motivations behind the survey is to show the potential of the blockchain technology - alone or merged with other technologies - to help the healthcare system evolve and provide scalable, efficient and secure solutions to four healthcare applications: electronic health record (EHR) storage, health data sharing, remote patient monitoring, and pharmaceutical supply chains. More specifically, the contributions can be summarised as follows:

- Identification of specific healthcare challenges to better understand the technological, functional and security requirements of healthcare.
- Highlighting the benefits of blockchain in meeting the healthcare requirements thanks to its natural properties and the extensions proposed by the scientific community.
- Literature review on blockchain-based solutions that provide a solution to security needs in healthcare, resulting in summary tables that precisely identify technological features and limitations.
- A systematic review of four key healthcare applications, providing an in-depth understanding of the state of the art in how blockchain can meet functional and security requirements.
- A clarified summary mapping of the contributions examined with regard to the specific functional and security requirements of healthcare systems.

- An advanced analysis of work merging blockchain with other technologies, with identification of current gaps and suggestions for future research investigations of interest.

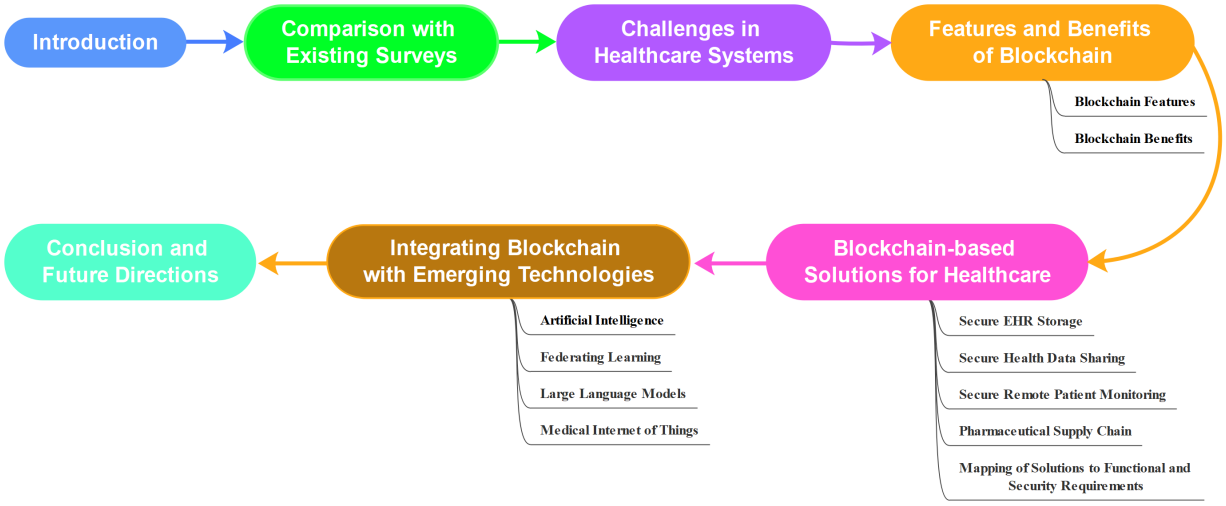

Figure 1: Structure of the paper

The remainder of this survey is organized as follows. Section 2 delineates the survey's unique contributions in contrast to existing literature. Section 3 identifies the prevalent challenges within healthcare systems including a list of functional and security requirements. Section 4 list the advantages blockchain technology offers to the healthcare sector. In Section 5, we conduct a comprehensive review of blockchain-based healthcare solutions, structured around four critical use cases, and summarized in detailed tables for ease of comparison. Section 5 also maps these solutions against the specific functional and security requirements of healthcare applications, critically assessing their applicability and effectiveness. Section 6 explores how blockchain technology can be seamlessly integrated with other emerging technologies, including Artificial Intelligence and Large Language Models (LLM), to drive innovation in healthcare. The survey concludes with reflections on the findings and suggestions for future research directions. Figure 1 illustrates the roadmap of the paper.

2. Comparison with Existing Surveys

Blockchain technology has recently emerged in the healthcare sector, prompting an array of studies examining its applications, challenges, and potential benefits [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]. However, the current literature features a discernible gap, with most surveys failing to address the security implications of implementing blockchain in healthcare. This review seeks to fill this void, offering an in-depth analysis of the existing literature while focusing on the security aspects of blockchain use in healthcare. A closer examination of existing literature reveals that [2, 5, 6, 8] partially broach the topic of security, although, their scope remains limited. For instance, [8] restricts its focus to the application of blockchain in Electronic Healthcare Record

(EHR) management. Similarly, [6] provides a superficial overview of the reviewed solutions and their security aspects. Moreover, while [2, 5] delve into security issues, they neglect to discuss the integration of blockchain with emerging technologies, an area of significant importance. In contrast, the present study offers a comprehensive review of the existing surveys, as summarized in Table 1, and critically compares them to highlight the similarities and differences in their methodologies, findings, and implications.

Table 1: Summary of **Blockchain for Healthcare** existing Surveys

Ref	Year	Scope	Description	Limits
[2]	2023	A Survey on Blockchain for Healthcare	An analysis of healthcare blockchain applications, various security attacks on the blockchain discussed, and a threat model proposed to categorize them	Few solutions were discussed, omitting Blockchain's integration with emerging technologies.
[3]	2023	A Systematic Review on Blockchain for Healthcare Management Systems	A systematic analysis of papers related to Blockchain for Healthcare Management Systems with a focus on security and interoperability	No description of the reviewed solutions
[4]	2022	A Survey on the integration of Blockchain and AI for Healthcare	Discuss the integration of blockchain and artificial intelligence technologies in the healthcare sector and Highlight their applications and benefits	Security aspects and healthcare requirements are omitted
[5]	2022	A Survey on Blockchain for Healthcare	Present functional components of healthcare systems and the interaction between the different entities. Make a systematic analysis of reviewed solutions according to the challenges, benefits and the defined functional components	No taxonomy presented and no classification of solutions according to use case applications
[6]	2021	A systematic review and review of two use cases: Telemedicine and E-health systems	A systematic review about the use of blockchain in healthcare, Analysis of the reviewed solutions according to security objectives. Moreover, recommendations to different stakeholders are presented	Lack of discussion on solutions and emerging technologies
[7]	2020	Blockchain platform for healthcare	Start-up companies involved in blockchain healthcare solutions. Review of 11 solutions. Potential research directions discussed	Solutions briefly discussed Several use cases not presented
[8]	2020	Blockchain for EHR management	Healthcare Systems Requirements. Blockchain features, applications and limitations. Mapping between reviewed solutions and healthcare security requirements. Discussion on potential research directions	Limited to EHR storage solutions only
[9]	2020	Systematic review of Blockchain in Healthcare	Healthcare System Requirements. Blockchain overview. Discussion on potential research directions	Solutions not discussed
[10]	2019	A comprehensive review	The paper reviews blockchain applications in healthcare and classifies them into three broad categories; data management, supply chain management, internet of medical things	Some redundancies

Table 1 – continued from previous page

Ref	Year	Scope	Description	Limits
[11]	2019	Limited to few solutions	Healthcare Industry Requirements. Blockchain features, applications and limitations. Review of 9 solutions. Discussion on potential research directions	Only few solutions presented
[12]	2019	Systematic Review	Classification of reviewed papers into six use cases including EMR management, remote patient monitoring, pharmaceutical supply chain, biomedical research, health insurance claims, and health data analytics	Lack of recent solutions missing, and future directions

◯ = Systematic review

For instance, [2] presents a working model, operations, architecture, and classification of blockchain in healthcare, and conducts a comparative analysis of present healthcare blockchain applications. However, their discussion is confined to a limited number of solutions. On the other hand, [3] presents a systematic review of blockchain for healthcare management systems, with a focus on security and interoperability.

In [4], the authors present a comprehensive review of the integration of blockchain and machine learning in healthcare, categorizing research works based on application scenarios and AI training paradigms. However, a critical analysis reveals a lack of discussion on healthcare requirements and security aspects, which are fundamental elements in healthcare technology integration. In [5], an examination of healthcare systems' components, challenges, and the advantages accrued from blockchain characteristics is undertaken. While this work provides a systematic review of blockchain-based solutions, it does not explicitly pinpoint the open issues related to the use of blockchain in current healthcare systems. Similar to [5], [10] reviews blockchain-based healthcare applications such as data management, supply chain management, and the Internet of Medical Things (IoMT), focusing on blockchain's role in ensuring interoperability, integrity, and privacy. However, the study falls short in investigating the blockchain's capacity to store and process extensive data access transactions, an area that requires thorough exploration. [13] provides an overview of the applications of the main pillars in healthcare 4.0: Internet of Things (IoT), BigData, and Cloud computing. However, the authors need to delve into the proposed solutions or present their main contributions, thus offering only a superficial understanding of the use of these technologies in healthcare. In contrast to the studies above, our current work delves into the requirements of healthcare applications, mapping existing solutions to these identified needs. Importantly, we extend the analysis to integrating blockchain with emerging technologies such as AI, federated learning, and LLM to bolster the security of next-generation healthcare applications. Moreover, given the rapid evolution of blockchain technology, our survey incorporates several recently published works not covered in previous reviews. Specifically, we explore and discuss lightweight blockchain solutions and their integration with the Internet of Medical Things, areas that have received scant attention in the existing literature. Table 2 summarizes the key features of the present survey compared to the existing ones.

3. Challenges in Healthcare Systems

The challenges posed by the digitisation of the healthcare system and healthcare data are considerable. Increasingly large volumes of healthcare data are being fed into large healthcare data lakes, offering the potential for new discoveries and new treatments. However, the format of this data needs to be standardised to make it usable, and researchers need to be able to access this data without compromising patient's privacy. Progress in artificial intelligence is particularly eagerly awaited to help doctors make increasingly accurate and rapid diagnoses. With everything permanently connected, data on patients in distress can be accessed very quickly, saving lives. This easier access makes it easier to cross-check information and combat fraud, which is known to have

Table 2: Comparison between existing surveys and this paper

Feature \ Reference	[2]	[4]	[5]	[6]	[7]	[8]	[3, 9, 10]	[11]	[12]	This paper
Discuss the benefits of Blockchain for healthcare	◑	○	●	◑	○	◑	○	○	●	●
Present a taxonomy of blockchain based solutions for healthcare	◑	●	○	◑	◑	◑	●	◑	●	●
Identify the NG healthcare requirements	◑	○	●	◑	○	●	○	◑	○	●
Map existing solutions to the identified requirements	◑	○	●	◑	○	●	○	○	○	●
Study the integration of blockchain with emerging technologies (such as AI, LLM)	○	◑	○	○	◑	◑	○	○	○	●
Review of recent blockchain-based solutions that were published between 2021-2023	◑	◑	◑	○	○	○	○	○	○	●
Suggest future research directions to enhance NG healthcare systems	◑	◑	◑	○	○	○	○	◑	○	●

○ = No, ◑ = Partially, ● = Yes

a particularly serious impact on the healthcare system. However, access to this data must be secure and must not allow data leaks, which can have disastrous consequences for patients' lives.

Ultra-digitalisation also brings with it new vectors of harm [14] that have flourished in recent years, such as ransomware, which aims to paralyse a hospital's information system until a ransom has been paid, social engineering, which relies on the credulity of staff to extract critical information such as a password, and data breaches, the latter having increased by 32% between 2022 and 2023 according to the study [15]. There are a number of reasons for this upsurge in attacks on healthcare systems: firstly, the lucrative nature of the attacks, with the resale price of a medical file at around $250 on the black market [15], but also the lack of resources hospitals have to secure their digital infrastructure, as their budgets are preferentially devoted to healthcare activities. From the hackers' point of view, a cyber attack on a health system has an added attraction because it demonstrates, in the eyes of the public, the inadequacy of a State to protect their interests and it puts pressure on the government to guarantee the protection of citizens while continuing to allocate limited budgets to IT infrastructures.

One of the most critical challenges facing healthcare systems today is technical, with an imperative need to take steps to secure healthcare data and patient privacy [2] [16]. A good digital identity management system is crucial for managing individuals, whether patients or medical staff, with their rights, their consent to the use of their data and control over their data. It makes it possible to implement the authentication, authorisation and accounting services needed to enforce security and protect against identity theft attacks, among other things. The physical and logical

security of infrastructures is also vital to prevent intrusions into a hospital's information system and data theft. The security of cryptographic keys and protocols is highly necessary, with an increasingly pressing need to integrate solutions that are resistant to quantum computers to guarantee long-term data protection. Finally, the approaches integrating blockchain, as we consider them in this article, inherit the vulnerabilities of blockchains [16].

Healthcare systems are of a very specific nature, as listed below, which necessitates adjusting or defining tailored technical approaches to meet their specific security and privacy needs:

- Patient life is an absolute priority. In any case, technology must never prevent medical staff from saving a patient's life or avoiding a loss of chance. This means that a means must be put in place for staff to access the EHR, with or without the patient's consent, because a patient is not capable of giving consent. This goes against a principle in cyber security, which is to specify a clear and unavoidable access control policy, which in this case would be to leave the patient alone in control of his or her data. This topic mainly concerns the EHR storage and health data sharing use cases (cf. Sections 5.1 and 5.2). This challenge is linked to the RH1, RH2, RH5, RH6 security requirements presented in Table 3.

- Volume and diversity of health data, e.g. MRIs, scans, and associated metadata (e.g. dates, hospitals, services, frequency). Whilst the confidentiality of health data is required because its content can reveal sensitive information about patients, the associated metadata also requires confidentiality protection because it can reveal a suspicion of disease. This is why total data protection is necessary. The greater the volume of data, the higher the cost of protection. This topic mainly concerns the EHR storage use case (cf. Section 5.1).). It is mainly linked to the RH3, RH4, RH6, RH7 and RH9 security requirements presented in Table 3.

- Extending the scope of data collectors (e.g. IoMT devices). Guaranteeing the authenticity, integrity and confidentiality of the data collected is already a complex task within the hospital. Extending data collection to devices that are purchased, used in the home and configured by patients, widens the attack surface, making indirect attacks on healthcare IT systems and poisoning of patient data possible [18]. Indeed, although some jurisdictions have adopted regulations requiring manufacturers to implement sufficient security measures in connected devices, such as the Cyber Resilience Act [19], devices currently in use are still riddled with misconfigurations or security flaws. This topic mainly concerns the use case of remote patient monitoring (cf. Section 5.3). It is mainly linked to the RH7 security requirement presented in Table 3.

- A large number of diverse IT-unaware people in interaction through healthcare systems, including patients, healthcare staff and administrative staff, in a variety of healthcare establishments. This requires a scalable and rigorously managed identity management system that is highly resistant to identity theft and fraud, while ensuring ease of use and high data availability. Sharing data within a healthcare establishment or between establishments must be supported as part of the patient's care pathway. This is linked to the security requirements RH1, RH2, RH5, RH8 presented in Table 3.

Table 3: Functional and Security requirements for Healthcare applications

Requirements for Healthcare (RH)	**Description**
RH1: Authentication (Ath)	Authentication is the first line of defense for any healthcare application. Indeed, to be secure a healthcare application needs to carefully authenticate every participant in the system including patients, doctors, care givers, etc.
RH2: Access Control (AC)	Access control methods permit to specify who can access the healthcare data and the privilege level (read only, read and write, etc.). In classical healthcare applications, patient data was managed centrally by the hospital.
RH3: Privacy (Prv)	The privacy of patients' data needs to be preserved. This can be done through cryptographic techniques such as homomorphic encryption. Privacy defines in which situation patient data might be accessed, utilized, and disclosed to a third party.
RH4: Integrity (Intg)	Patient stored data needs to be protected against any unauthorized modification. Moreover, any modifications or alteration of data need to be detected.
RH5: Traceability (Aud)	Also known as auditability or accountability, tracks and audits who accesses the patient data, with what aim, and the time-stamping of any operation in the entire life cycle.
RH6: Availability (Avai)	We mean here ubiquitous availability of data. More precisely, patient data can be accessed from anywhere and distant access is possible.
RH7: Interoperability (Itop)	This requirement guarantees that patient data issued by different organisations and with different formats can be understood by each other. This facilitates data sharing for research and educational purpose.
RH8: Patient-Centric access control (PCA)	This requirement indicates that the patient has the right to own his healthcare data and to control it. More precisely, the patient controls which data is accessible to whom.
RH9: Scalability (Scal)	Healthcare applications generally involve big data such as X-ray images, clinical data, etc. Therefore, healthcare solutions designers need to take into consideration the large volume of data generated.

List elaborated from [8] and [17]

- Diverse sources and diversity of pharmaceutical products. The size of the market for medicines and medical equipment is such that it is difficult to control the origin of products, their composition and their traceability to purchasers. Yet the need is real. Counterfeit medicines kill more than 250,000 children a year, and the most disadvantaged people are the most vulner-

able [20]. Scalable and rigorous management of players and products is needed to ensure accurate and reliable traceability. This topic mainly concerns the pharmaceutical supply chain use case described in Section 5.4. It is mainly linked to the security requirements RH1, RH2, RH5 and RH6 presented in Table 3.

4. Features and Benefits of Blockchain to healthcare applications

4.1. Blockchain features

Blockchain technology has received a lot of attention from both industry and academia due to its distinctive features. These features are explained as follows:

- **Distributed**: In blockchain, the storage of data is done in a distributed manner. A distributed ledger is stored in different nodes in the blockchain network. Moreover, the decision to add new data (new block) is taken through consensus protocol and not by a central entity.

- **Decentralization**: The blockchain system does not require a centralized third party and operate in a P2P manner. Transactions are endorsed in a decentralized manner by the peer-to-peer network and without the intervention of a central entity. This decentralized nature eliminates the need for a central authority, making the system more resilient to attacks and failures.

- **Immutability**: The distributed ledger in Blockchain is composed of a set of blocks linked together through a cryptographic hash. More precisely, Each block in the blockchain contains a hash of the previous block, creating a chain of blocks that are cryptographically linked together. Consequently, any change in a block would require the alteration of subsequent blocks, making the system highly resistant to tampering. This makes blockchain immutable and secure. Moreover, transactions are signed with the help of digital signatures.

- **Transparency**: All transactions on the blockchain are visible to network participants. Moreover, before addition to the ledger, transactions are validated by participant nodes. Therefore, participants can track and view the changes on the blockchain. This transparency helps to build trust among participants and enables auditing and accountability.

- **Traceability**: Blockchain enables the traceability of transactions or data. Each transaction or data entry on the blockchain is timestamped and linked to previous transactions, creating an audit trail that can be traced back to its origin. This feature is particularly useful in supply chain management and provenance tracking.

4.2. Blockchain benefits

The blockchain is a promising technology that will play a vital role in empowering and developing next-generation healthcare applications. The various benefits of the blockchain to the smart healthcare applications can be summarised as follows:

- **Decentralization**: healthcare applications are generally distributed over several stakeholders, which requires a distributed management system. Blockchain can provide this decentralized management, where all participants and stakeholders can control access to patients' data, without the need for a central authority.
- **Improved data security and privacy**: Blockchain technology is immutable and therefore helps protect the patients' data from alteration or corruption, reducing the risk of data breaches and unauthorized access. Patients can have greater control over their health data, and healthcare providers can ensure the integrity and confidentiality of patient records. Moreover, the real identities of patients are hidden through the use of cryptographic keys, which help protect the privacy of patients.
- **Health data ownership**: Through smart contracts, blockchain can deploy user centric healthcare applications, where the patient can control the access to his health data. Thanks to well-defined smart contracts, the user can decide to which medical staff he/she will give access and the access validity.
- **Availability and robustness**: The data is stored on the blockchain in a distributed manner and is replicated on multiple nodes. This permits to guarantee the availability of the data and increases the system robustness.
- **Transparency and trust**: By nature, the blockchain is an open and transparent system, which increases trust between the different participants and stakeholders. Additionally, blockchain can improve the traceability of pharmaceuticals in the supply chain, ensuring the authenticity and safety of medications.
- **Interoperability**: Blockchain can help standardize data formats and ensure interoperability among various healthcare systems and providers. It acts as a common platform for sharing data, making it easier for different healthcare systems and providers to access and share patient information seamlessly. This reduces the challenges associated with data silos and incompatibility.
- **Reduced Frauds**: Blockchain can help reduce fraudulent activities, such as insurance fraud and prescription drug fraud, by providing a transparent and auditable record of transactions. Moreover, smart contracts can automate various processes in healthcare, such as insurance claims, billing, and supply chain management, reducing frauds, errors, and delays.
- **Reduced bureaucracy and expenses**: Implementing blockchain in healthcare systems can reduce bureaucracy and expenses by streamlining processes and eliminating intermediaries.

5. Blockchain-based solutions for healthcare

Based on the reviewed papers we have identified four use cases of the applications of blockchain in healthcare including **secure EHR storage**, **secure health data sharing**, **secure remote patient monitoring**, and **pharmaceutical supply chain management**. Fig. 2 illustrates the taxonomy of healthcare applications studied in this paper.

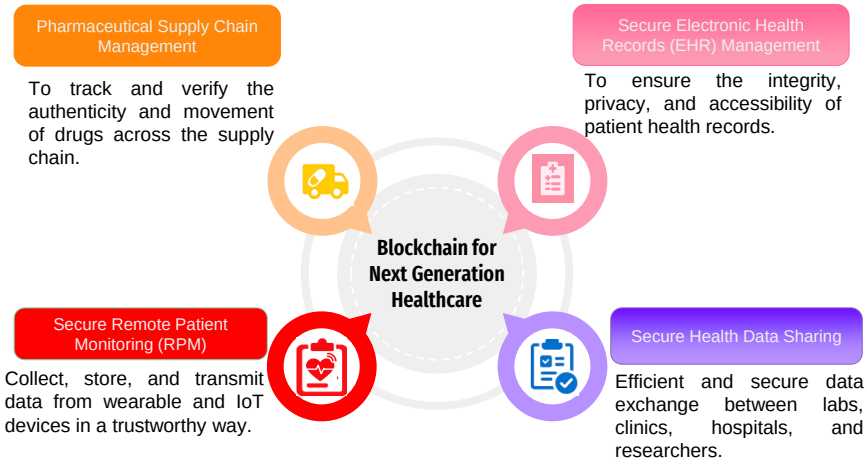

Figure 2: Taxonomy of Blockchain for Next Generation Healthcare Applications

5.1. Secure EHR storage

Patient health data are generally saved into an Electronic Health Record (EHR). One of the popular applications of blockchain in healthcare is the security of this EHR. In the literature, the term EHR is used interchangeably with Electronic Medical Record (EMR), and Personal Health Record (PHR). The security of the EHR needs to be achieved during its creation, storage, management, and sharing. The main blockchain based EHR secure systems are presented in Table 4 and are discussed as follows.

An early conception of using blockchain to provide confidentiality, authentication, and accountability of EHRs is described in [21], where the authors suggested using blockchain for medical data access control and permission management.

The authors in [22] proposed an identity and access management system to provide EHR authorisation and authentication. The proposed system is implemented using the Hyperledger Fabric Framework. [23] designed BHEEM, a blockchain-based framework to securely store and maintain EHRs.

[24] proposes a decentralized attribute-based signature scheme for privacy-preserving of user identity during signature verification. The proposed scheme is deployed for the security of EHR in healthcare. The decentralised EHR storage system based on blockchain guarantees integrity, auditability, and availability.

The authors in [31], similarly to [32], combine attribute-based encryption, identity-based encryption, and identity-based signature in one crypto-system, to provide authentication, confidentiality, integrity and traceability of medical data records in EHR. However, no implementation is carried out to evaluate the proposed system.

To overcome the scalability problem, due to the large volume of healthcare data, some solutions propose to store the healthcare data on the cloud and to keep on the blockchain only the pointers to that data, along with their hashes [33] [34] [25].

HealthChain [25] is a secure and scalable EHR management system. HealthChain is based on two blockchain networks; Private Blockchain for intra-regional communication and, Consortium

Table 4: Summary of **Blockchain for Secure EHR storage** solutions

Ref	Contribution/ Purpose	Blockchain Type	Framework	Consensus	Storage	Validation Tools	Merits/Limits
[21]	Decentralized blockchain based EHR access control and permission management	Public	Ethereum	PoW	Local database	Smart contracts	A local database representing a single point of failure
[22]	An identity and access management mechanism to support EHR authorisation and authentication	Consortium	Hyperledger Fabric	Not specified	CouchDB	Javascript + Hyperledger Fabric +PostgreSQL	+Implementation of the system
[23]	Blockchain-based framework for efficient storage and management of EHRs	Consortium	Ethereum	Not specified	Not specified	Not specified	No validation of the solution
[24]	Decentralized attribute-based signature to provide privacy for blockchain-based EHR security	Consortium	Not specified	PBFT	On-chain and off-chain storage	Security analysis + Prototype imp. in C	No standard framework used for the evaluation
[25]	Secure and scalable EHR management system	Two Blockchains; one Private and one Consortium	Ethereum	PoA	IPFS + Cloud	Mathematical analysis	No implementation
[26]	Privacy-preserving framework for the security and interoperability of EHR management	Private	Ethereum	Quorum-Chain	Local database		No implementation or validation provided
[27]	Design and implementation of different medical workflows	Private	Ethereum	PoW (Ethash)	Back-end distributed file system (DFS)	Solidity language+ Remix and Kovan test network	Only partial system developed
[28]	Performance evaluation of blockchain-based access control mechanism for EHR	Consortium	Hyperledger Fabric	BFT	CouchDB	Hyperledger Fabric +Hyperledger composer+ Docker	+Description of the algorithms including access control
[29]	MediBchain: a patient centric blockchain based EHR management system	Consortium	Hyperledger Fabric	BFT	On-chain on cloud	Solidity+ Java	+Using ECC
[30]	HealthBlock: A secure blockchain-based healthcare data management system	Private	Hyperledger Fabric	PBFT	OrbitDB with IPFS	Hyperledger Fabric +Hyperledger composer	+Using two channels to enhance privacy

Blockchain for inter-regional communication.

The authors in [26] propose Ancile, which is built on the Ethereum blockchain platform and utilizes smart contracts to achieve access control, data privacy and interoperability of electronic medical records. The QuorumChain Consensus algorithm [35] is adopted to determine the next block to be added to the chain. Additionally, the authors use the concept of proxy-encryption to store keys and small encrypted records directly on the blockchain. Moreover, Ancile define different smart contracts for each function of the system.

The work in [27] discusses and implements different medical workflows using Ethereum smart contract system for secure EHR management. These healthcare workflows involve complex medical procedures.

The authors in [28] use Hyperledger Fabric to evaluate the performance of blockchain-based EHR systems. The authors have also developed the algorithm for access control and patient, clinician and lab interaction with the blockchain network.

Recently, the authors of [30] proposed a new blockchain-based healthcare data management system. They have used blockchain to control access to the stored patient's medical data in a decentralized database which is OrbitDb with IPFS. They have adopted two channels: the device channel and the consultation channel. In fact, the concept of channels enhances data privacy. Moreover, they have adopted a patient-centric access control through the execution of smart contracts to allow or deny access to the patient's health data. Therefore, data confidentiality is preserved. Note that only the hash of data stored in OrbitDB with IPFS is saved in the blockchain to ensure data integrity and auditability. Besides, the adopted approach is fully decentralized providing no single point of failure which ensures data availability.

The authors in [36] presented a pioneering approach to Electronic Medical Record (EMR) sharing in the healthcare sector. The proposed scheme leverages consumer electronic devices and Mobile Edge Computing (MEC) to enable secure generation and uploading of EMRs and diagnosis reports, safeguarding the Health Information Exchange (HIE) process between patients and doctors. Notably, the system employs a combination of Advanced Encryption Standard (AES), Rivest Shamir and Adleman (RSA), Edwards-curve Digital Signature Algorithm (EdDSA), and Elliptic Curve Digital Signature Algorithm (ECDSA) techniques, alongside the Inter-Planetary File System (IPFS), to ensure the secure storage and availability of EMRs, thereby preventing unauthorized access and tampering. Furthermore, the proposed model addresses the need for scalability, high speed, and minimal computational complexities by implementing the Proof of Authority (PoA) consensus algorithm and IPFS, as evidenced by its superior performance compared to existing schemes.

5.2. Secure health data sharing

Facilitating the secure sharing of health data among healthcare providers, institutions, and authorized stakeholders is crucial for informed and effective patient care, yet it necessitates a delicate balance between data accessibility and patient privacy. Blockchain technology offers a compelling solution by providing robust data security through encryption and access control, ensuring that only authorized entities can access and modify patient records. Furthermore, the immutability and transparency of blockchain guarantee data integrity, mitigating the risk of tampering and fraud.

Table 5: Summary of **Blockchain for Secure health data sharing** solutions

Ref	Contribution/ Purpose	Blockchain Type	Framework	Consensus	Storage	Validation Tools	Limits
[37]	Sharing healthcare data in a trustless environment such as cloud	Consortium	Not specified	Not specified	Cloud Database	JMeter	No implementation
[38]	Sharing healthcare data for clinical and research purposes	Public	Not specified	An endorser is elected by more than half of the nodes. Then, the endorser validates the transactions	Local Database	Security analysis	Latency of service provider requests, The endorser is a central entity which minimizes the advantages of the distributed nature of blockchain, and No implementation
[39]	Healthcare Data Sharing	Consortium blockchain	Java	BFT-SMaRt [40]	Local Database	Implementing using Java	The frequent intervention of healthcare providers needed
[41]	Secure and scalable healthcare data sharing for collaborative clinical decision making	Private	Ethereum	Not specified	Hybrid on-chain/off-chain	Javascript + solidity	Limited to healthcare system supporting FHIR [42] only
[43]	Healthcare data sharing with a decentralized Trusted Third Party Auditor (TTPA)	Private	Ethereum platform	Two Ethereum nodes deployed in Amazon servers responsible for mining	Cloud database	Testnet of Ethereum+ Solidity language	Security issues inherent in using cloud servers
[44]	Blockchain-based hierarchical data sharing framework	Private	Ethereum platform	Two Ethereum nodes deployed in Amazon servers responsible for mining	Cloud database	Testnet of Ethereum+ Solidity language	Security issues inherent in using cloud servers

The authors in [45] [37] propose MedShare to securely share medical data stored on the cloud. The proposed system implements smart contracts and an access control mechanism to provide traceability and permissions on data.

[38] proposes MedBlock to share healthcare data for clinical and research purposes. MedBlock combines access control protocols with symmetric encryption to provide high-level security. One limitation of MedBlock is that it focuses solely on hospital medical records of patients collected from medical examinations and does not store the vital signs of patients.

To transcend this drawback, Shen et al. [39] propose MedChain: a blockchain based healthcare data sharing system. In addition to the EHRs of patients, MedChain shares also their vital signs collected from the IoMT devices.

FHIRChain [41] was proposed to meet the Office of the National Coordinator for Health Information Technology [46] requirements for secure and scalable clinical data sharing. These requirements include user identifiability, user authentication, controlled data access, secure data exchange, consistent data formats, and system modularity. In FHIRChain each participant possesses a public/private key pair. The public key serves for user identity and the private key for user authentication. To address the scalability requirements, FHIRChain suggests keeping protected data off-chain and only pointers of it are stored on the blockchain.

In [43], the authors propose a blockchain based framework method called BiiMED. It permits to manage and share Electronic Health Records (EHR) stored on the cloud between different medical organisations. Additionally, a Trusted Third Party Auditor (TTPA) based on blockchain technologies is introduced. TTPA permits to validate the exchanged data and ensures data interoperability and integrity.

In [44] a groundbreaking blockchain-based hierarchical data sharing framework (BHDSF) is introduced in the context of Healthcare Internet of Things (H-IoT). The framework addresses the critical need for secure and trustworthy personal health records (PHR) sharing, especially in remote healthcare scenarios, emphasizing user privacy and PHR integrity. BHDSF offers fine-grained access control and efficient retrieval of encrypted PHRs with a focus on low overhead hierarchical key distribution and robust key leakage resistance. Notably, it simultaneously considers untrusted cloud services and malicious auditors, employing blockchain for trustworthy PHR integrity auditing and metadata verification. Additionally, BHDSF introduces efficient aggregative authentication for source records from H-IoT devices, a feature often absent in existing data sharing frameworks. Table 5 summarizes the blockchain-based solutions for secure health data sharing.

5.3. Secure remote patient monitoring (RPM)

To secure the remote patient monitoring systems, Griggs et al. [47] propose to use a consortium blockchain based on Hyperledger. The proposed RPM system Gateway implements a smart contract to analyse collected data (from sensors) and sends notification to the medical staff. The action of data read or doctors commands are considered as transactions, which are stored in the blockchain. One challenge of this solution is how to perfectly choose the transmission time of the aggregated data to the blockchain network.

The authors in [48] propose a two-tier architecture; the first one ensures vital sign streaming and storage, whereas the second one is responsible for key management. The lower tier includes

Table 6: Summary of **Blockchain for Secure RPM** solutions

Ref	Contribution/ Purpose	Blockchain Type	Framework	Consensus	Storage	Validation Tools	Limits
[47]	Sharing healthcare data for clinical and research purposes	Private/ Consortium	Ethereum	PBFT	Designed EHR storage database	Solidity + Smart contracts	Sensors data sent regularly to the patient phone, which consumes its energy and makes the solution not practical and dependent on the user phone
[48]	Continuous patient monitoring using body sensors network. Security and blockchain based functions are integrated into a PCA	Private	Not specified	PoW with miner selection based on capacity	On-chain+ Cloud	Java + Ethash	Partially evaluated on non standard platform, and Limited patient mobility as the PCA needs a computer to run
[49]	Ring signature used for anonymity and nodes organized into clusters for scalability purpose	Not specified	Not specified	Cluster Heads behaving as miners	Cloud database	Not specified	No description of how clusters are formed, and No validation
[50]	Remote Patient Monitoring	Private	Hyperledger Fabric	PBFT	Blockchain database	Go language + Application SDK	The capacity limit of direct storage in blockchain
[51]	Vital signs real time remote monitoring	Private	Hyperledger Fabric	PBFT	Distributed ledger technology (DLT)	Hyperledger composer + Caliper	Particularly heavy storage of patient data in the blockchain network
[52]	New architecture of a blockchain based RPM system	Private	Hyperledger Fabric	PBFT	Cloud	Hyperledger composer + Caliper	- Potential breach of patient privacy due to storage of patient data in the cloud
[53]	Access control to patient data through proxy re-encryption	Private	Ethereum	PoA	IPFS	Implementation	Experiment limited to a small number of nodes

a patient centric agent (PCA), which is connected to a blockchain network and a cloud system. The PCA is a software that needs to be executed on a computer or server and ensures three functionalities: medical Data Management Module (DMM) responsible for storage management and compression, Security Service Module (SSM) responsible for key management, and Miner Management Module (MMM) is responsible for miner selection and blockchain interaction. The proposed system used a modified version of the PoW consensus algorithm, where only one miner is selected based on its characteristics to add a new block to the network. Moreover, the authentication of the different components of the system is proposed, which is mainly based on XOR operation and hash functions.

To provide anonymity and authenticity, [49] proposes to use a lightweight privacy-preserving ring signature scheme [54]. In ring signature, the signature is mixed with other groups (named ring), to keep the identity of the signer private. Moreover, the authors introduce the concept of clustering the blockchain network to provide scalability. More precisely, nodes are organized into clusters and in each cluster the cluster head is responsible for the addition of new blocks. However, the the authors do not specify how the groups are formed and do not evaluate their work.

[51] proposes an IoT-based blockchain platform for the secure remote monitoring of patients physiological parameters. One limit of this solution is that it stores the high volume of data generated by the medical sensors into the blockchain nodes. This design choice requires nodes with big storage space and leads to scalability problems.

Attia et al. [50] propose to use two separate blockchains to secure the remote monitoring of patients. One blockchain manages the medical wearable devices and stores their collected data, and the other blockchain manages the consultations and contains all the history of patients records. Moreover, the NDN paradigm [55] is used to retrieve data from the patient wearable devices. A prototype of the proposed architecture was implemented using Hyperledger Fabric Framework.

Recently, the authors of [52] proposed a new architecture for a remote patient monitoring system based on blockchain technology. The overall architecture of the proposed RPM system is composed of a perception layer, a network layer and an application layer deployed in the cloud. In the application layer, the authors used Hyperledger fabric integrated with Hyperledger Composer to implement the business model of the RPM system in the blockchain network. Note that the ledgers and transactions are deployed in the cloud to ensure the scalability of the proposed system. Moreover, the wearable health devices and the IoT gateway are considered assets of the blockchain network which ensure data integrity and auditability. Besides, the participants which are patients and doctors must be registered and enrolled in the blockchain network to benefit from RPM services. This fact ensures data confidentiality. Finally, the proposed system is fully decentralized with no single point of failure which ensures data availability.

To provide access control to patient data collected from IoT devices, the authors in [53] propose to adopt proxy re-encryption. The scheme uses IPFS to protect data integrity and ensure non-repudiation.

The authors in [56] introduced a distributed application (DA) designed for an IoT-based healthcare system, specifically focusing on the generation, storage, and maintenance of medical certificates. The DA serves as an interface between the blockchain-based system and various application users, including hospitals, physicians, and regulatory agencies. Additionally, the paper emphasizes the importance of ensuring the security and privacy of healthcare documents, controlling unautho-

Table 7: Summary of **Blockchain for Secure Pharmaceutical Supply Chain Management** solutions

Ref	Contribution/ Purpose	Blockchain Type	Framework	Consensus	Storage	Validation Tools	Limits
[57]	Blockchain-based drug management to check drug integrity	Private	Hyperledger Fabric	Not specified	couchDB + Offchain	Hyperledger Composer/Caliper	Consensus algorithm and consensus manager selection not specified
[58]	Blockchain-based drug management to detect counterfeit drug + A machine learning based drug recommendation module	Private	Hyperledger Fabric	Not specified	couchDB + Offchain	Implementation in Hyperledger	Consensus algorithm not specified
[59]	Convergence of IoT and Blockchain to monitor drug temperature and preventing the counterfeiting of pharmaceutical products	Private	Hyperledger Fabric	Raft	Cloud	Security Analysis	No implementation and several components required
[60]	Ethereum smart contracts for end-to-end tracking and traceability of pharmaceuticals	Public	Ethereum	PoW	offchain(IPFS)	Implementation and Security Analysis	Scalability issues
[61]	Blockchain-based smart tracking and tracing platform for the drug supply chain, employing a four-level IoT-based traceability approach to recognize and manage drug identities at different levels	Private	Hyperledger Fabric	pBFT	Elasticsearch	Implementation in virtual machines	Limited number of stakeholders tested and scalability issues
[62]	Integration of Blockchain with IoT to offer decentralized tracking and tracing of medical products	Public	Ethereum	PoW	Offchain	Implementation with web interfaces	Smart contracts not explained
[63]	Blockchain-based framework to enhance access control management in the medical device supply chain	Private	Hyperledger Fabric	Kafka and Solo	Onchain	Implementation of smart contracts	No interface designed and no comparison with other systems

rized access, maintaining the integrity of medical certificates, and preventing fraud. Furthermore, the paper presents experimental results, security features, and a comparative analysis, demonstrating the superior performance of the proposed scheme when compared to existing systems.

Table 6 summarizes blockchain-based solutions for secure remote patient monitoring.

5.4. Pharmaceutical supply chain

The pharmaceutical industry faces a myriad of challenges related to the integrity, safety, and efficiency of its supply chain. Counterfeit drugs, regulatory compliance, and the need for transparency have all made supply chain management a critical concern. Blockchain technology is emerging as a transformative solution to address these challenges. Here, we delve into the key applications of blockchain in the pharmaceutical supply chain.

An overview of Pharmaceutical Supply Chain Management (SCM) systems is presented in [64]. The authors discuss their benefits, issues (including counterfeiting, improper labeling, im-

proper temperature controls and handling, transportation and storing issues), and challenges.

Blockchain's ability to create a transparent and immutable ledger of transactions is invaluable in tracking the journey of pharmaceuticals from manufacturing facilities to end-users. Each step of the supply chain, from production to distribution, can be recorded in a tamper-proof manner, allowing for real-time visibility. This ensures the authenticity and safety of medications, while also making it easier to identify and recall products if quality or safety issues arise. The authors in [57] propose a blockchain-based SCM to check the drug integrity. The proposed system enables the medical staff, patients, and pharmacists to manage, control access, and share personal medical records and the complete patient drug life cycle in a secure and transparent way. The system is implemented using Hyperledger Fabric and tested using Hyperledger composer [65].

To address counterfeit drugs, the authors in [60] use Ethereum smart contracts to propose an end-to-end tracking and traceability system for pharmaceutical supply chains. The smart contract ensures the origin of data, removes the necessity for intermediaries, and delivers a secure and unchangeable record of transactions to all involved stakeholders.

The paper [61] (1) introduces a blockchain-based smart tracking and tracing platform for the drug supply chain, employing a four-level IoT-based traceability approach to recognize and manage drug identities at different levels. This enhances traceability and transparency within the supply chain while fostering a transparent environment for stakeholders. (2) The paper offers a practical roadmap for drug industry stakeholders, providing insights into blockchain architecture selection, data management principles, and integration with external systems. (3) It proposes smart contract-based alert mechanisms to enhance drug quality information access and counterfeit drug detection. However, the paper acknowledges several limits, including practical application, scalability, and the test with more stakeholders.

The authors in [62] integrate Blockchain technology with IoT to offer decentralized tracking and tracing of medical products, effectively mitigating the risk of counterfeit drugs and delivering real-time status updates throughout the entire pharmaceuticals journey from manufacturers to end-users.

The paper [63] proposes the integration of Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) models within a blockchain-based framework to enhance access control management in the medical device supply chain. By combining these two access control models, the paper addresses issues of complex rights retrieval and assignment, provides granular and dynamic permission management through ABAC, and simplifies overall system permissions using RBAC. The implementation of this access control model through blockchain's smart contracts offers fine-grained and dynamic authority management for medical equipment within the supply chain, ensuring the security and privacy of sensitive medical device information. Moreover, it establishes a traceable and tamper-proof medical supply chain system, promoting transparency and trust between transaction parties while preventing medical accidents caused by unreliable equipment.

Counterfeit pharmaceuticals pose a significant risk to public health. Blockchain provides a robust defense against this threat. By assigning unique identifiers or serial numbers to each drug unit, stakeholders can easily verify the authenticity of medications by checking their history on the blockchain. The authors in [58] propose a drug supply chain management and recommendation system. The authors use blockchain to track the drug delivery and detect the counterfeit drugs.

Moreover, a machine learning module is proposed to recommend the best medicines. The authors use Hyperledger Fabric as a blockchain framework and the N-gram, LightGBM models as the machine learning method.

Pharmaceuticals often require strict temperature control during transport and storage. Blockchain can record temperature and environmental data at every point in the supply chain, ensuring that drugs are stored under the required conditions. If temperature fluctuations are detected, immediate corrective actions can be taken, preserving the quality of medications. The authors in [59] propose an SCM for drugs that takes into consideration the temperature of the drug during transit and storage. The solutions necessitate the presence of a sensor in the drug box. Moreover, a QR code was used to store drug information. To address the scalability issue the bloXroute [66] servers are introduced. bloXroute are a scalable blockchain distributed network. Moreover, the authors suggest using the Raft consensus protocol. A security analysis is proposed. However, the solution requires the presence of several pieces of hardware which can be difficult to provide such as smart transportation box, sensor nodes, and dynamic QR code in each packet.

Table 7 summarizes blockchain-based solutions for secure Pharmaceutical Supply Chain Management.

5.5. Mapping of existing solutions to functional and security requirements

Table 8 shows the mapping of the previously reviewed solutions to the specified healthcare requirements previously described. On the other hand, Figure 3 illustrates the percentage of papers satisfying each requirement. It is worth noting from the table and figure that some requirements such as authentication, access control, integrity, and auditability are well fulfilled by the proposed solutions. This can be explained by the fact that these security services are inherent to blockchain technology. However, the interoperability requirement is fulfilled by only 32% of the studied solutions. This is due mainly to the different formats of data used in healthcare. Moreover, proposed healthcare solutions use generally a private blockchain, which fails to scale to a very high number of participants. Therefore, scalability is another issue that needs to be resolved in healthcare solutions (only 25% of the papers proposed scalable solutions). Additionally, the majority of healthcare solutions store patient data either on the blockchain or in the cloud. However, blockchain cannot fit the large volume of patient data. This explains why some solutions opted for cloud storage solutions. However, storing data in the cloud might reveal the privacy of the patient and expose the system to several attacks. From Figure 3, we observe that only 50% of the papers satisfy the privacy requirement. Finding a storage solution that overcomes these limits is another future research direction.

Figures 4 - 8 summarize the results of Tables 4 - 7. We notice from Figure 4 that most systems use private blockchain platforms (54%), with some systems (23%) utilizing a consortium blockchain. With respect to the implementation framework, most systems use Ethereum (40%) and Hyperledger (40%). In Figure 6, we notice that most of the consensus algorithms used in healthcare applications are PoW (17%), PBFT (17%), and custom algorithms (13%); with many authors not specifying the consensus algorithm they used (34%). As for the storage method, most systems use cloud-based solutions (23%), with some systems using a local database (17%) and custom mechanisms (17%). Finally, with respect to the validation method (cf. Figure 8), most authors implemented their systems using various implementation frameworks (70%).

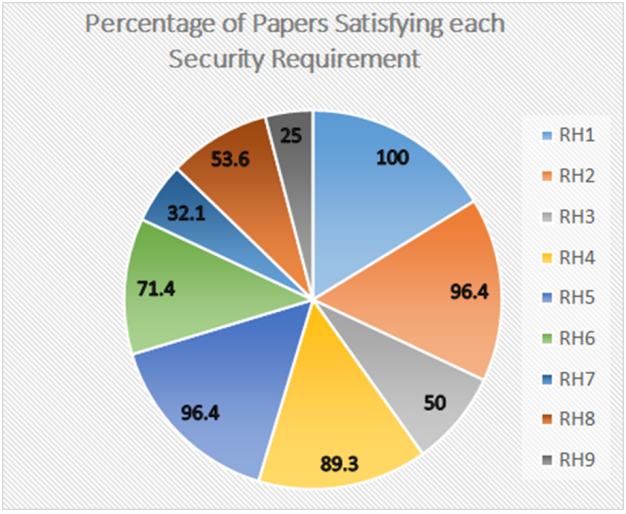

Figure 3: Mapping of studied solutions to security requirements

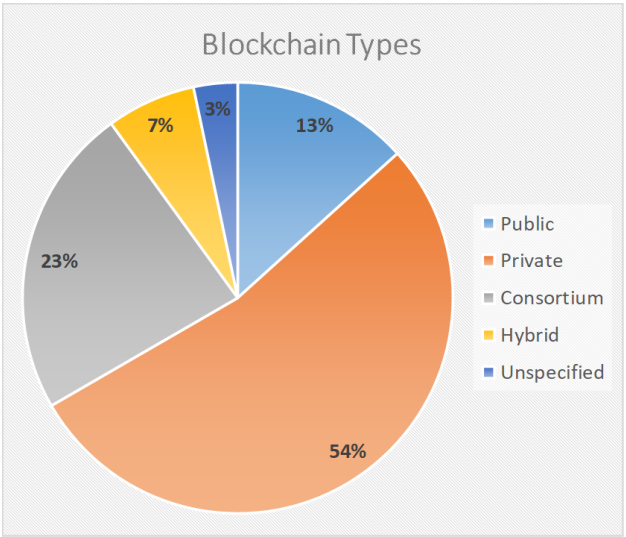

Figure 4: Mapping of studied solutions to blockchain types

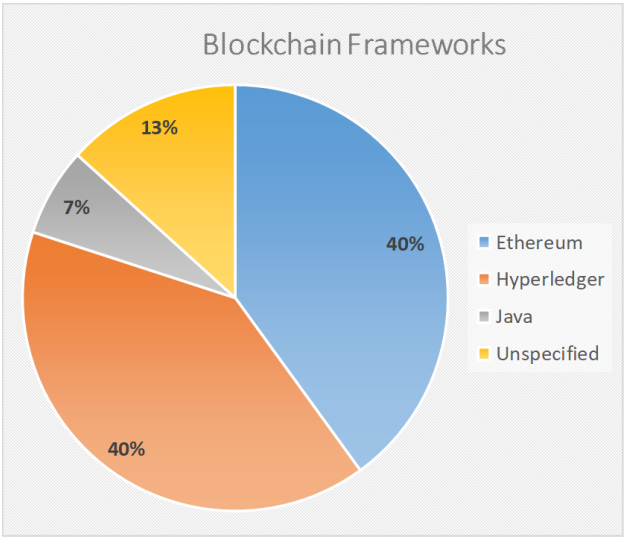

Figure 5: Mapping of studied solutions to blockchain frameworks

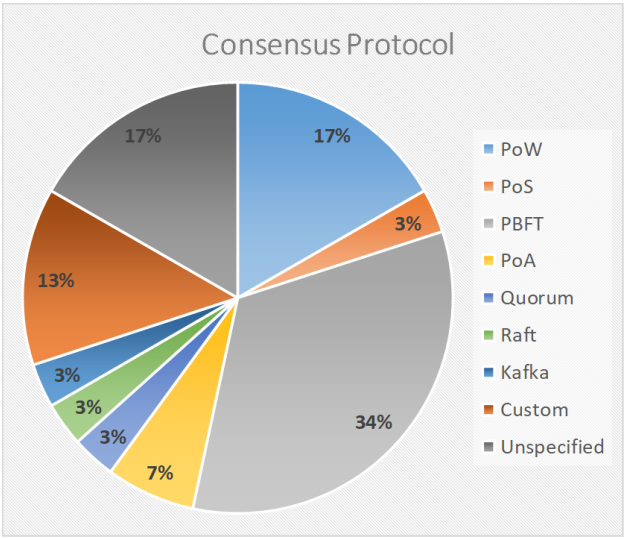

Figure 6: Mapping of studied solutions to consensus algorithms

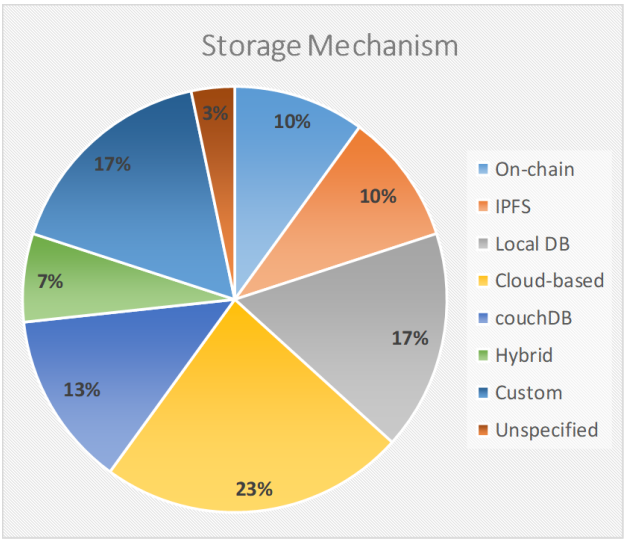

Figure 7: Mapping of studied solutions to storage mechanisms

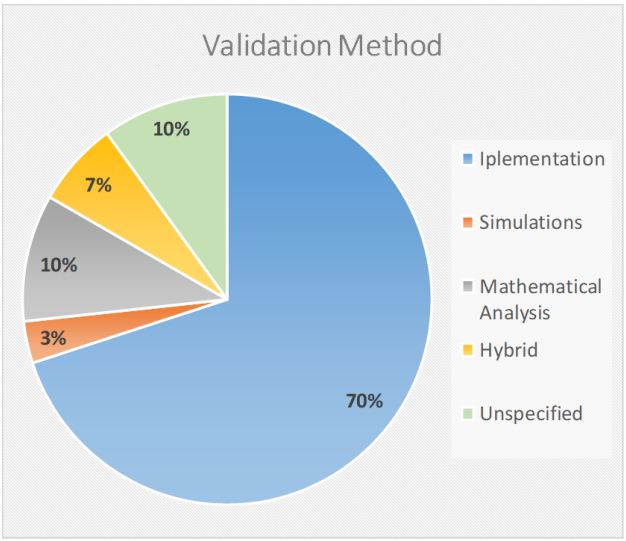

Figure 8: Mapping of studied solutions to validation methods

Table 8: Mapping of **Blockchain for Healthcare** solutions to functional and security requirements

Ref	Use case	RH1 (Ath)	RH2 (AC)	RH3 (Prv)	RH4 (Intg)	RH5 (Aud)	RH6 (Avai)	RH7 (Itop)	RH8 (PCA)	RH9 (Scal)
[21]	SEM	✓	✓	✓	✓	✓	✓	✓	✓	✗
[22]	SEM	✓	✓	✗	✓	✓	✗	✗	✓	✗
[23]	SEM	✓	✓	✗	✓	✓	✗	✗	✓	✗
[24]	SEM	✓	✓	✗	✓	✓	✓	✗	✓	✗
[25]	SEM	✓	✓	✓	✓	✓	✓	✓	✓	✓
[31]	SEM	✓	✓	✗	✓	✓	✓	✗	✓	✗
[26]	SEM	✓	✓	✓	✓	✓	✗	✓	✓	✗
[27]	SEM	✓	✓	✗	✓	✓	✓	✓	✓	✗
[28]	SEM	✓	✓	✗	✓	✓	✗	✗	✓	✗
[30]	SEM	✓	✓	✓	✓	✓	✓	✓	✓	✓
[38]	SDS	✓	✓	✓	✓	✓	✓	✗	✓	✗
[37]	SDS	✓	✓	✗	✓	✓	✗	✗	✗	✓
[41]	SDS	✓	✓	✗	✓	✓	✗	✓	✓	✗
[43]	SDS	✓	✓	✗	✓	✓	✗	✗	✗	✗
[47]	SRPM	✓	✓	✓	✓	✓	✓	✗	✗	✗
[48]	SRPM	✓	✓	✓	✓	✓	✓	✗	✓	✗
[49]	SRPM	✓	✓	✓	✓	✓	✓	✓	✗	✓
[50]	SRPM	✓	✗	✗	✓	✓	✓	✗	✗	✗
[51]	SRPM	✓	✓	✓	✓	✗	✓	✗	✗	✗
[52]	SRPM	✓	✓	✓	✓	✓	✓	✓	✓	✓
[53]	SRPM	✓	✓	✓	✓	✓	✓	✓	✗	✗
[57]	PSCM	✓	✓	✗	✗	✓	✓	✗	✗	✗
[58]	PSCM	✓	✓	✗	✗	✓	✓	✗	✗	✗
[59]	PSCM	✓	✓	✓	✗	✓	✓	✗	✗	✓
[60]	PSCM	✓	✓	✓	✓	✓	✓	✗	✗	✗
[61]	PSCM	✓	✓	✓	✓	✓	✓	✗	✗	✗
[62]	PSCM	✓	✓	✗	✓	✓	✓	✗	✗	✓
[63]	PSCM	✓	✓	✗	✓	✓	✗	✗	✓	✗
SEM: Secure EHR Management, SDS: Secure Data Sharing, SRPM: Secure Remote Patient Monitoring, PSCM: Pharmaceutical Supply Chain Management.										

6. Integrating Blockchain with emerging technologies

This section explores the integration of Blockchain with emerging technologies, such as Artificial intelligence, Federated Learning, Large Language Models, and Lightweight Blockchain with Internet of Medical Things. Figure 9 illustrates the synergies between these technologies, highlighting their collective potential to enhance security, efficiency, and patient-centric care in

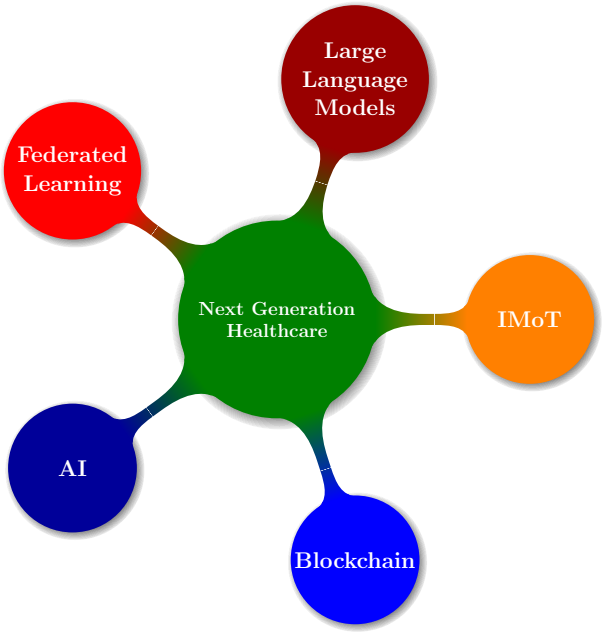

Figure 9: Integrating Blockchain with emerging technologies

healthcare systems. The integration of these technologies not only addresses the challenges faced by current healthcare systems but also paves the way for future advancements.

6.1. Integrating Blockchain with Artificial Intelligence

A large number of studies proposed various models for the integration of blockchain with AI within the context of several healthcare applications. A review of these models is depicted in Figure 10.

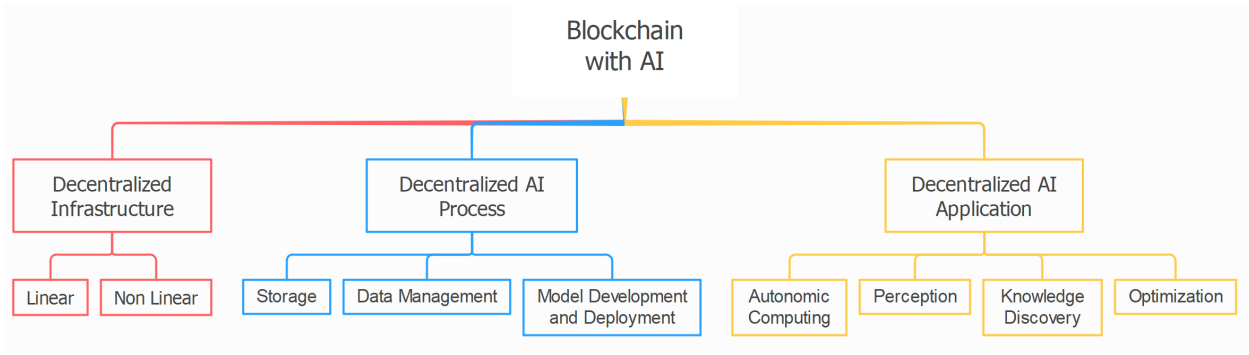

Figure 10: The various venues of integrating blockchain technology with AI

The paper [67] proposes the use of blockchain technology to address the challenges of secure data sharing and collaboration among multiple organizations in the healthcare domain. They propose to upload healthcare data to blockchain and then use AI for lung cancer detection. More precisely, they propose a method to secure medical data by only sharing the weights of the trained

deep learning model via a smart contract. Then distributing the local deep learning model weights to a blockchain decentralized network to train a global model. The integration of blockchain with deep learning models allows for the distribution of the training task across a decentralized network. Participants in the network compute training gradients locally, and the blockchain securely aggregates the local weights without leaking private information. This distributed learning approach reduces time and utilizes decentralized resources, leading to improved model performance. Blockchain enables the collaboration of multiple organizations in training a deep learning model. By sharing data and model weights over the decentralized network, a collaborative deep learning model can be constructed, leveraging the diverse and evolving data from different sources. This collaborative approach enhances the accuracy and performance of the deep learning model for lung cancer detection [67].

The paper [68] proposes an AI-assisted blockchain-based framework for electronic medical record management. The goal is to store and process medical records using various AI techniques, such as optical character recognition (OCR), to create a single patient medical history report. This report presents only the crucial information in a concise manner for convenience and secure storage. The framework utilizes a decentralized model, using IPFS and Ethereum decentralized application, to provide data and identity protection. The stored records, including handwritten and printed prescriptions and reports, are uploaded to a distributed network on the Ethereum platform. AI techniques like OCR and Microsoft Azure Computer Vision are used to extract relevant information from the documents. The extracted data are then collectively stored as a single document. The summary report of the patient's medical history can be accessed and updated by doctors, attendants, and patients, providing a quick and illustrative overview. The framework aims to improve the efficiency of accessing and managing medical records while maintaining data security.

The authors in [69] propose a machine learning integrated blockchain model for minor medical consultations. The model includes patients, doctors, and other medical experts as users. Patients provide their personal information and medical history, while doctors and experts provide their credentials and experience. Smart contracts on the blockchain verify the information provided. A patient wanting to consult for minor medical issueshas to post their query on the blockchain network. Doctors and experts respond to the queries, and a natural language processing-based machine learning model rates their responses. The model considers reputation, expertise, supporting documents, and detail orientation to determine the reward payable to the respondents.

To identify fraud in medical insurance, Zhang et al. [70] propose a deep learning model using blockchain technology. The model focuses on the problem of healthcare providers changing low-cost disease codes to high-cost codes to receive more money from insurance companies. Patients upload their chief complaint and assigned International Classification of Diseases (ICD) code to a medical consortium blockchain. The deep learning model uses a text classification task to determine the appropriateness of the ICD code. The model consists of seven layers, including a BERT layer for text encoding and a character-ICD match layer for calculating matching scores. The authors also propose using a consortium blockchain governed by multiple parties and a data storage method combining off-chain and on-chain storage. The model outperforms other state-of-the-art models in terms of precision, recall, and F1-score. The model's explainability is demonstrated by giving more weight to disease symptoms mentioned in the chief complaint. However, a limitation of the study is that the data is collected from only two hospitals.

The authors in [71] propose a framework called BinDaaS, which integrates blockchain and deep-learning techniques for healthcare 4.0 applications. BinDaaS combines blockchain and deep-learning techniques to securely store and manage patient Electronic Health Records (EHRs). Blockchain ensures trust, security, and privacy among healthcare users, while deep learning is used to predict future diseases based on current indicators and features of patients. To address the challenges of privacy, confidentiality, and data consistency in sharing EHRs, the framework uses lattice-based cryptography, a quantum-resistant solution, to ensure privacy and authentication of EHR records. This approach resists quantum and collusion attacks and complies with HIPPA guidelines.

The authors in [72] present an approach, referred to as "BDSDT," which combines Blockchain technology and Deep Learning to ensure secure data transmission in IoT-enabled healthcare systems. The proposed system leverages a scalable blockchain architecture with Zero Knowledge Proof (ZKP) to guarantee data integrity and security, while integrating with the InterPlanetary File System (IPFS) for efficient off-chain storage and Ethereum smart contracts for enhanced data security. Additionally, a deep learning model, combining Deep Sparse AutoEncoder (DSAE) and Bidirectional Long Short-Term Memory (BiLSTM), is used for intrusion detection within healthcare networks. Experiments on two public datasets demonstrate that BDSDT surpasses existing methods in both non-blockchain and blockchain settings, achieving remarkable accuracy levels close to 99%.

6.2. Integrating Blockchain with Federating Learning

Federated Learning (FL), a distributed machine learning approach, can be combined with blockchain to enable secure and decentralized AI model training. Federated learning allows multiple healthcare organizations to collaborate and train AI models without sharing sensitive patient data. Blockchain ensures the integrity and traceability of the training process, enhancing data privacy and security.

A review of the applications of federated learning in healthcare is illustrated in Figure 11.

The authors in [73] propose a framework that combines blockchain and federated learning to detect COVID-19 patients using CT imaging while preserving privacy. The primary motivation behind this framework is the shortage and reliability of testing kits for diagnosing COVID-19 patients, as well as the need to share data among hospitals globally while maintaining privacy. The authors collect data from various hospitals and use a data normalization technique to handle the heterogeneity of the data gathered from different CT scanners. To address the privacy concerns, they utilize blockchain technology to authenticate the data and federated learning to train the global deep learning model while preserving the privacy of the organizations.

The authors in [74] present a lightweight hybrid federated learning (FL) framework that enhances the security and provenance of Internet of Health Things (IoHT) data. The framework utilizes blockchain smart contracts to manage various aspects of the FL process, including edge training plans, trust management, authentication of federated nodes, distribution of trained models, reputation management, and encryption of datasets and model training. Federated learning is employed to train the FL model using private IoHT data that remains on the owner's premises. The FL process takes place within smartphones or edge devices that have IoHT attached to their edge nodes. This decentralized approach addresses privacy concerns by allowing training to occur

Figure 11: Applications of federated learning in healthcare

locally without sharing raw data. Each federated edge node performs additive encryption, and the blockchain uses multiplicative encryption to aggregate the updated model parameters. The framework also incorporates differential privacy (DP) to ensure the privacy and anonymization of IoHT data.

The paper [75] proposes a platform that addresses the challenges of data privacy, service integrity, and network adaptability in wearable Internet of Things (IoT) devices used in predictive healthcare. The platform utilizes federated learning and private blockchain technology within a fog-IoT network to secure data and create an adaptive network for wearable IoT devices. The authors design a testbed to evaluate the platform's ability to preserve the integrity of a classifier, and the experimental results demonstrate the effectiveness of the implementation in preserving patient privacy and predictive service integrity.

The authors in [76] introduce a blockchain-based Federated Learning framework for the fifth-generation healthcare, enabling the construction of a collaborative model across various edge devices and overseeing the entire training process. The scheme enhances the security of blockchain-based FL with a Real-Time Deep Extreme Learning System (RTS-DELM) method, striking a balance between privacy and model accuracy through noise adjustment. Additionally, the system accommodates multiple medical organizations, allowing locally trained models to improve the healthcare 5.0 system by sharing a global model. It also designs an Intrusion Detection System (IDS) within the healthcare 5.0 system to augment security and privacy by detecting intrusions and attack patterns.

The authors in [77] present a blockchain-empowered FL framework for healthcare-based CPSs, wherein a distributed ledger, governed by a task agreement committee representing hospitals, ensures secure FL model training and consistent block generation. Moreover, the system introduces a contribution point-based incentive mechanism to fairly reward FL participants for sharing their local data.

The authors in [78] introduce a novel approach to collaborative machine learning for image classification in the context of Healthcare 4.0. By leveraging secure multi-party computation-based ensemble federated learning with blockchain technology, it enables healthcare institutions to collectively train machine learning models while safeguarding user privacy and ensuring data integrity. The proposed method addresses the challenge of heterogeneous model structures across different hospitals through a weighted ensemble Deep Learning approach, where model accuracy determines contribution weights. Privacy guarantees are maintained through a secure multi-party computation-based evaluation process. Furthermore, blockchain technology is used to provide data integrity, auditability, and version control, eliminating the need for centralized trust in a server. This comprehensive framework offers a secure and privacy-conscious solution for collaborative machine learning in healthcare.

6.3. Integrating Blockchain with Large Language Models

In the healthcare sector, blockchain technology's potential has been recognized for ensuring data integrity, privacy, and interoperability. However, as the field evolves, the convergence of blockchain with other advanced technologies is creating new paradigms that promise even greater innovations. A particularly intriguing development is the integration of Large Language Models (LLMs) with blockchain infrastructures. LLMs, owing to their capacity to process vast amounts

of data and generate human-like textual content, present a unique opportunity for enhancing blockchain's utility in healthcare. In this section, we present the pioneering works that demonstrate this intersection of blockchain and LLMs. From real-time anomaly detection in transactions to dynamic adaptability and the verification of generative AI outputs in decentralized systems, these emerging studies [79], [80], and [81] underscore the possibilities that this combination can bring in for healthcare applications.

Figure 12 summarizes the various use cases for integrating the blockchain with LLMs in Healthcare. This integration revolves around four main topics: 1) using the LLM to detect and resolve smart contracts' vulnerabilities, 2) using NLP for extracting useful information from healthcare data, 3) applying sentiment analysis and opinion mining to deduce patients' status and development, and 4) executing predictive modeling to deduce important statistics from blockchain data.

In [79], the paper introduces BLOCKGPT, a tool designed for real-time anomaly detection in blockchain transactions. By generating trace representations of blockchain activities, BLOCKGPT uses a large language model trained on Ethereum transactions to detect anomalies without depending on predefined rules. It successfully identifies abnormal transactions in a dataset spanning 68M transactions and achieves a throughput of 2284 transactions per second. Unique contributions include the use of unsupervised learning for anomaly detection in smart contract execution traces and a custom data encoding tailored for Ethereum's architecture. However, the system might produce false positives, and while the model detects many attacks, it doesn't catch all, necessitating further refinement for comprehensive security.

In [80], Yuanhao Gong proposes a novel method of training and deploying dynamic large language models (LLMs) on blockchains. The decentralized nature of blockchains offers high computational performance and the opportunity for the LLMs to evolve continuously based on user input even after initial training. This contrasts with traditional LLMs that are static post-training and operate on centralized GPUs. The proposed system enables LLMs to be more adaptable and relevant over time. However, a potential limitation is the risk of biases in data sets amplifying during training, and concerns about the misuse of LLMs in generating misinformation, which needs to be addressed for ethical and responsible use.

In [81], The study explores the verification of generative AI outputs in decentralized, trustless networks. Researchers conducted a billion locality-sensitive hash comparisons of artificially generated data samples, striving to ascertain the "correctness" of AI-generated outputs. They created millions of data samples from open-source models, analyzing the balance between deterministic and non-deterministic outputs. The study introduced a new training dataset, ImageNet-Gen, for improving training processes. Results revealed a 99.89% probability of detecting perceptual collisions in AI-generated images and achieved 100% consensus in language model outputs. The work paves the way for reliable AI verification in decentralized networks, minimizing trust issues.

The marriage of Large Language Models (LLMs) and blockchain in healthcare promises both improved data handling and stronger security. Studies have shown that this blend can spot unusual blockchain transactions in real-time, let LLMs learn and adapt even after their initial setup, and ensure AI-generated outputs are genuine on decentralized networks. This could lead to sharper disease prediction, more secure patient data, and treatments better suited to individual patients. Yet, there are hurdles. Some anomalies might go unnoticed, LLMs could pick up and amplify

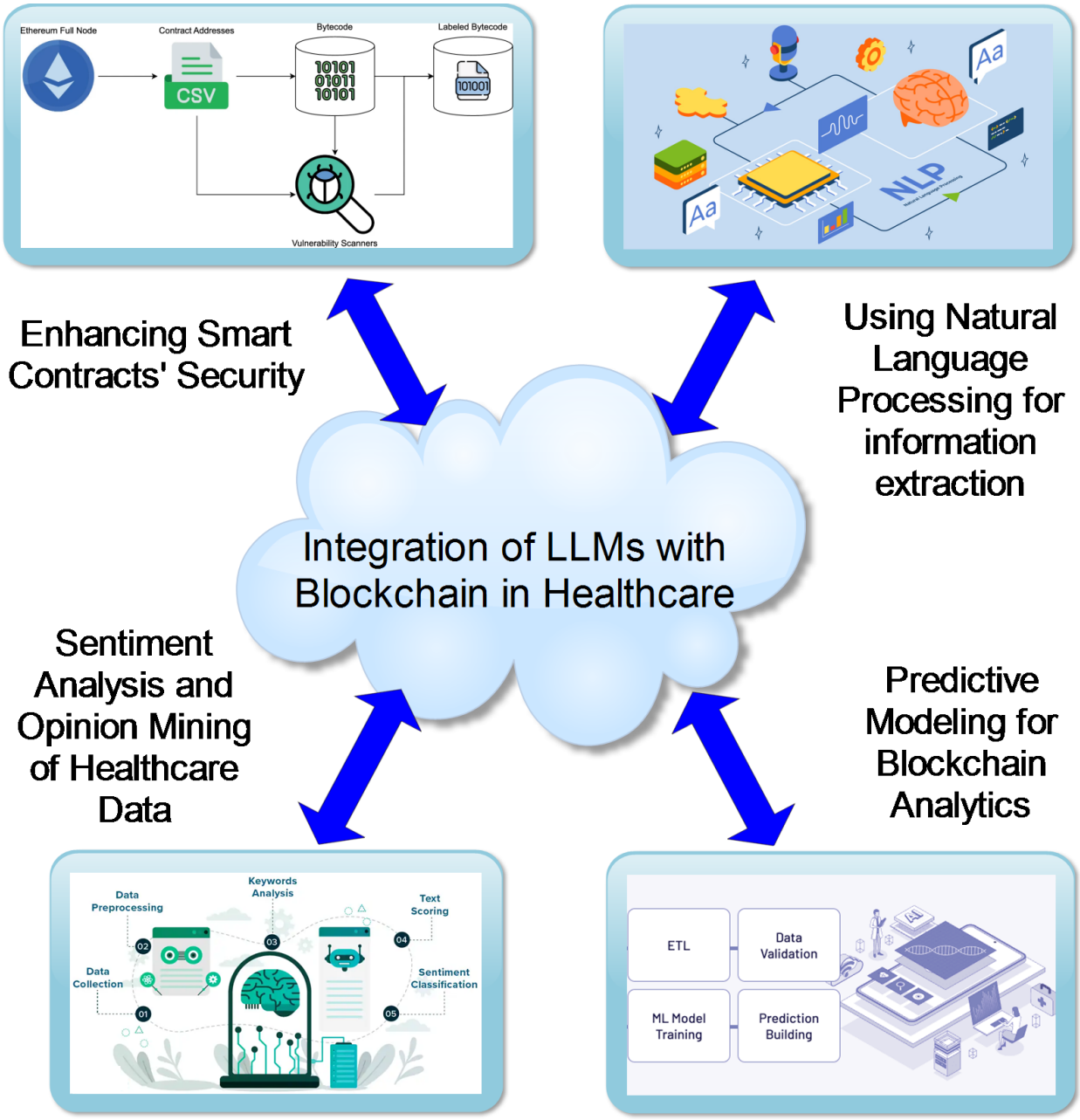

Figure 12: Integrating LLMs with Blockchain in healthcare

biases over time, and there's a risk of AI creating inaccurate medical data. Given the high stakes in healthcare, addressing these tech challenges is crucial.

Building on these insights, the future trajectory for the amalgamation of LLMs and blockchain in healthcare offers tantalizing prospects. One promising avenue is the creation of domain-specific LLMs honed for niches within healthcare, such as cardiology, pediatric care, or infectious diseases. When integrated with blockchain, the potential for a secure and precise delivery of domain-centric medical advice or predictions becomes tangible. Furthermore, the convergence of LLMs' capability to structure vast patient data with blockchain's ability to authenticate can significantly enhance the efficacy of electronic health records. As we move forward, it's essential that the healthcare community collaborates closely with technologists to harness these potentials while diligently mitigating the identified challenges. This partnership could be the bedrock for a more reliable, efficient, and patient-centric healthcare system in the coming years.

6.4. Integrating Lightweight Blockchain with Internet of Medical Things

Several healthcare applications comprise different types of IoT devices. These devices are typically resource-constrained in terms of their processing power, storage capability, and available power. The integration of common blockchain systems into such devices is impossible, due to the high resource-demanding nature of the blockchain. For this reason, a large number of researchers studied the possibility of modifying one or more characteristics of the blockchain in order to make it suitable for Internet of Medical Things (IMoT) applications. In general, it is expected that the future of smart healthcare will involve extra-lightweight blockchain frameworks, due to the abundance of lightweight devices in most healthcare applications, and the inability of these devices to support traditional blockchain systems.

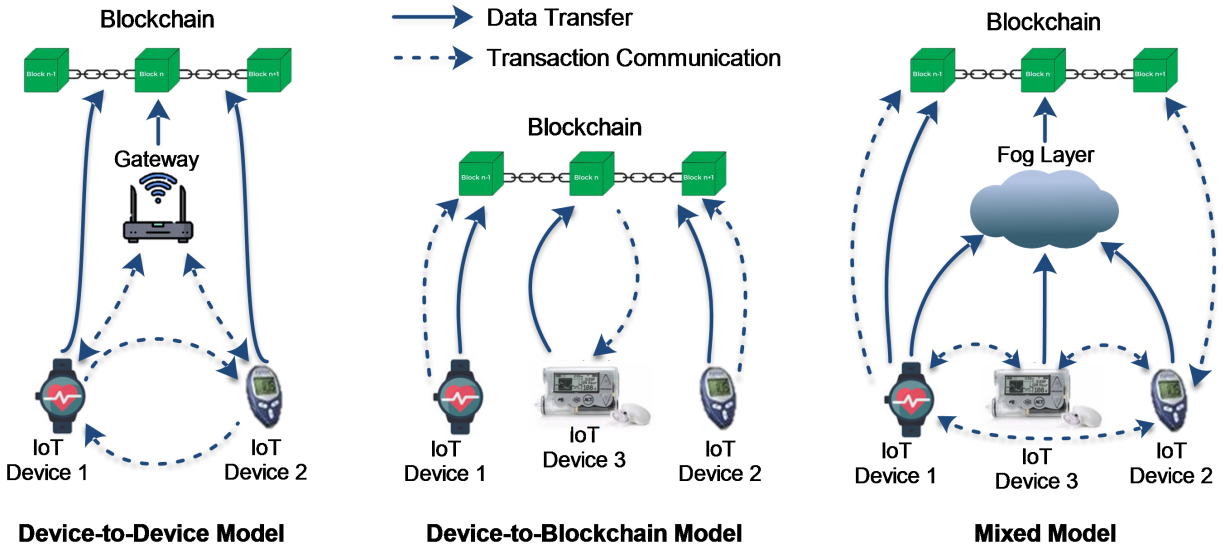

Figure 13: The three architectures for Blockchain and IoT integration.

Three architectures for integrating blockchain with healthcare IoT have been proposed in the literature. These architectures are illustrated in Figure 13. In the first architecture, which is the

device-to-device model, the IoT nodes perform the required tasks locally, outside the premises of the blockchain. Only the metadata of transactions are stored in the blockchain. In the second architecture, all operations' details are stored in the blockchain. Hence the blockchain is utilized for both data storage and transaction management. The third architecture (mixed model) allows IoT users to select the blockchain network for certain event interactions and the remaining events are executed directly through IoT devices.

The authors in [82] propose a lightweight blockchain system for remote patient monitoring that is integrated with fog computing. The system architecture comprises three layers: the IoT devices layer contains medical sensors that monitor the patient and transmit their readings to the blockchain-enabled fog gateways. The second layer includes fog devices that are utilized for the registration of IoT devices in the blockchain, authorization of each IoT device when it connects to the network, and validation of the medical data transactions. The third layer consists of cloud servers that play the role of full blockchain nodes. The IoT gateways and sensors at each healthcare organization and patient's home are grouped into a cluster and become responsible for storing and overseeing a local blockchain. Within each cluster, the sensor nodes retain only the block headers of the blockchain, whereas the gateways retain both the block headers of the full blockchain and the complete blocks of the local blockchain.

An authentication framework for medical sensors that utilizes blockchain and physically unclonable functions (PUF) is proposed in [83]. At the start of the system, the administrator configures each cluster of gateway nodes (GWN) and initializes the blockchain. In the proposed system, the GWNs oversee the blockchain operations by implementing the Proof of Work (PoW) consensus. Next, the sensor controllers (SCs) generate the secret private keys and facilitate the mutual authentication of the GWNs. After that, the sensor devices (SDs) and medical professionals (MPs) are registered with the blockchain via a secure channel. Each device uses its PUF to create and send a unique identity and a set of challenge/response to its GWN. In the login and authentication phase, each MP that wishes to access an SD's data must first mutually authenticate with the SD and establish a shared secret key with it. The authors prove that their scheme is safe against man-in-the-middle, impersonation, replay, session key disclosure, and physical capture attacks.

In [84], a Patient Agent (PA) software, replicated at the medical sensors and edge devices, is used to handle medical data and guarantee dependable, secure, and confidential communications. The PA employs a streamlined blockchain consensus mechanism and a task-offloading algorithm enhanced by blockchain to safeguard the patient's privacy when offloading tasks. The system utilizes a lightweight modified Proof of Stake consensus algorithm that is executed at the edge nodes to analyze and process the data of medical IoT sensors. The proposed consensus algorithm utilizes the edge devices' faster communication capacity to add data to the blockchain in a fast manner. Periodically, the older blocks are offloaded to the cloud servers that are responsible for the permanent storage of the whole blockchain. The proposed system implements a task migration algorithm that offloads tasks to nearby sensor nodes or distant fog agents based on data sensitivity. The agents' profiles are managed by the blockchain smart contracts to establish trust between the various entities.

The industrial Internet of Things (IIoT) is characterized by its autonomous system configuration and cross-platform application connectivity. In the context of E-healthcare, IIoT collaborates with medical sensors to attain, assess, save, and document real-time patient transactions. The fu-

sion of E-healthcare and IIoT creates a platform that is capable of managing vast amounts of data at a cost-effective rate by leveraging cloud-based scalable storage. However, during this transition, there is a potential risk to patients' personal information when exchanged. The authors in [85] propose a Hyperledger-enabled blockchain with healthcare IIoT-based distributed application architecture (BHIIoT). The system uses two communication channels, mainly on-chain and off-chain, for node-to-node interactions and data distribution. It also utilizes four different chain codes to process E-healthcare transactions via a customized DApp that controls the execution of consensus protocols and digital signature mechanisms.

A lightweight secret-sharing model between smart medical devices, medical workers, and medical institutions is proposed in [86] to strengthen medical data-sharing security and efficiency. It uses the interleaving encode technology to reduce the size of the transmitted message into n pieces. These pieces enable data transmission and processing in a more energy-efficient manner. In addition, the proposed method protects privacy by removing the overall semantic meaning of the transmitted data. Furthermore, it requires only some of the pieces to restore the original message, which makes the overall process more efficient. The authors propose a fault tolerance threshold function that enables the receiver to recover parts of the original message when some pieces are lost. The performance evaluations show that the proposed system produces low transaction throughput, acceptable transaction latency, and much lower energy consumption than the base model.

In [87], the authors describe a decentralized EHR and smart-contract-based service automation framework that uses the blockchain to secure EHR transactions. The authors introduce a decentralized selective ring-based access control (SRAC) mechanism that maintains the patient record anonymity. Furthermore, user-friendly smart digital agreements are utilized to establish dynamic digital service agreements among various parties. Patient medical raw data, generated by the sensors, undergoes a process where it is enriched with supplementary information and then encrypted using the public key of the respective edge computer. This prepared data is subsequently transmitted to the consumer layer. Within the middle layer, a hybrid computing system takes charge of data processing, analysis, and decision-making. Additionally, it handles tasks related to data storage, access control, anonymity, and manages a blockchain-based distributed data storage system (DDSS). Furthermore, the hybrid computing layer is responsible for creating and deploying smart contracts. Finally, in the consumer layer, the actuators and terminals execute events specified within a particular smart contract.

7. Conclusion and Future Directions

This paper has elucidated the potential of blockchain technology for advancing contemporary healthcare systems, particularly in terms of security and integrity. By summarising existing surveys and providing a taxonomy of blockchain-based solutions, this research serves as an invaluable resource for professionals in healthcare technology. The potential of the integration of blockchain with other emerging technologies for transformative impacts on healthcare was also explored.

However, despite the promising prospects, several challenges remain for the broader deployment of blockchain-based healthcare systems. These include data storage constraints, scalability issues, and the choice of blockchain type. In addition, interoperability and privacy concerns, as

well as the need for standardisation and regulations, are also significant challenges that require further research focus.

- **Storage**: New storage systems need to be explored, on a distributed basis for greater coherence and complementarity with the operation of the blockchain. The idea is to take advantage of this decentralization to provide greater storage capacity, given that healthcare systems generate large volumes of healthcare data [88, 89, 90], and greater availability of stored data, for example by intelligently replicating data and appropriately choosing the position of these nodes with respect to stakeholders. The challenge is to provide resilience to such a system in the event of storage node failures, while ensuring that data access and content are secure, that no sensitive information is leaked, and that storage and recovery operations are efficient, with reasonable administration costs.

- **Scalability**: The need for scalability covers the need to store large volumes of heterogeneous data, but even more obviously, the need for performance in validating transactions using an appropriate consensus protocol [91, 92], and in writing and accessing information in the blockchain. The objective is for each operation to take a reasonable amount of time and for the solution to be viable on a national scale, for example. The need for scalability also relates to the large number of interacting healthcare stakeholders, who need to be managed by associating specific rights that are strictly respected.

- **Type of blockchain**: Although the blockchain consortium seems to be the most appropriate choice for healthcare systems, balancing the need for confidentiality and data sharing, it is worth continuing works on public blockchains and incorporating security properties for certain healthcare uses, such as Healthcare IoT.

- **Interoperability**: The heterogeneity of data formats and healthcare systems based on blockchain needs to be studied in greater depth. To enable medical data to be shared between stakeholders, a standard format for storing and exchanging data within the blockchain is needed [93, 94]. To enable different healthcare systems to cooperate, it is also necessary to design and implement distributed inter-blockchain approaches that enable switching from one system to another, for example in the form of a blockchain-hub.

- **Standards and regulations**: To improve economic acceptability, interoperability and widespread adoption, it is necessary to standardise the format of health data and cooperative health systems based on blockchain. There is also a need for extensive regulatory works to integrate the use of blockchain and other digital technologies.

- **Privacy**: The transparency of blockchain transactions and identity management pose a risk to patient privacy, warranting the selection of combined privacy-preserving blockchain components (DID method, VC and VP), and the investigation of more advanced privacy-preserving mechanisms [95].

In conclusion, this work contributes to the foundational knowledge required to navigate the multifaceted landscape of blockchain in healthcare. Our findings underscore the potential of

blockchain technology in paving the way towards a more secure, efficient, and patient-focused healthcare ecosystem, while also highlighting key areas for future research.

Declarations

Compliance with Ethical Standards

This article does not contain any studies with human participants or animals performed by any of the authors.

Competing interests

The authors declare no conflict of interest, financial or otherwise.

Authors' contributions

O.C. wrote the main manuscript text and O.C. and K.M prepared figures. All authors reviewed the manuscript.

Acknowledgments

This research was supported by the Tunisian Ministry of Higher Education and Scientific Research, the Agence Nationale de la Recherche under the France 2030 programme (TracIA project, reference ANR-22-PESN-0006), and International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (CybAlliance, Project no. 337316).

Availability of data and materials

This manuscript has no associated data file.

References

[1] United Nations. United nations sdgs. `https://sdgs.un.org/goals#History`, 2024. Accessed: 2024-02-28.

[2] J Andrew, Deva Priya Isravel, K Martin Sagayam, Bharat Bhushan, Yuichi Sei, and Jennifer Eunice. Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. *Journal of Network and Computer Applications*, 215:103633, 2023.

[3] Edgar R Dulce Villarreal, Jose García-Alonso, Enrique Moguel, and Julio Ariel Hurtado Alegría. Blockchain for healthcare management systems: A survey on interoperability and security. *IEEE Access*, 11:5629–5652, 2023.

[4] Siva Sai, Vinay Chamola, Kim-Kwang Raymond Choo, Biplab Sikdar, and Joel JPC Rodrigues. Confluence of blockchain and artificial intelligence technologies for secure and scalable healthcare solutions: A review. *IEEE Internet of Things Journal*, 2022.

[5] Mohammad Salar Arbabi, Chhagan Lal, Narasimha Raghavan Veeraragavan, Dusica Marijan, Jan F Nygård, and Roman Vitenberg. A survey on blockchain for healthcare: Challenges, benefits, and future directions. *IEEE Communications Surveys & Tutorials*, 24(4):2984–3009, 2022.

[6] Hassan Mansur Hussien, Sharifah Md Yasin, Nur Izura Udzir, Mohd Izuan Hafez Ninggal, and Sadeq Salman. Blockchain technology in the healthcare industry: Trends and opportunities. *Journal of Industrial Information Integration*, 22:100217, 2021.

[7] Ahmed Farouk, Amal Alahmadi, Shohini Ghose, and Atefeh Mashatan. Blockchain platform for industrial healthcare: Vision and future opportunities. *Computer Communications*, 151:24–35, 2020.

[8] Shuyun Shi, Debiao He, Li Li, Neeraj Kumar, Muhammad Khurram Khan, and Kim-Kwang Raymond Choo. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security*, page 101966, 2020.

[9] Emeka Chukwu and Lalit Garg. A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations. *IEEE Access*, 8:21196–21214, 2020.

[10] Seyednima Khezr, Md Moniruzzaman, Abdulsalam Yassine, and Rachid Benlamri. Blockchain technology in healthcare: A comprehensive review and directions for future research. *Applied sciences*, 9(9):1736, 2019.

[11] Thomas McGhin, Kim-Kwang Raymond Choo, Charles Zhechao Liu, and Debiao He. Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, 135:62–75, 2019.

[12] Cornelius C Agbo, Qusay H Mahmoud, and J Mikael Eklund. Blockchain technology in healthcare: A systematic review. *Healthcare*, 7(2):56, 2019.

[13] Giuseppe Aceto, Valerio Persico, and Antonio Pescapé. Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. *Journal of Industrial Information Integration*, 18:100129, 2020.

[14] Health-ISAC and Booz Allen Hamilton. 2023 health cybersecurity annual threat report. `https://h-isac.org/2023-health-cybersecurity-annual-threat-report/`, 2023. Accessed: 2024-10-20.

[15] Splunk. The state of security 2023, global research: How leading organizations engage the entire business to build resilience, splunk. `https://www.splunk.com/en_us/form/state-of-security.html`, 2024. Accessed: 2024-10-20.

[16] Yourong Chen, Hao Chen, Yang Zhang, Meng Han, Madhuri Siddula, and Zhipeng Cai. A survey on blockchain systems: Attacks, defenses, and privacy preservation. *High-Confidence Computing*, 2(2):100048, 2022.

[17] Jigna J Hathaliya and Sudeep Tanwar. An exhaustive survey on security and privacy issues in healthcare 4.0. *Computer Communications*, 153:311–335, 2020.

[18] Ramamoorthy Somasundaram and Mythili Thirugnanam. Review of security challenges in healthcare internet of things. *Wireless Netw*, 27, 2021.

[19] European Commission. Proposal for a regulation of the european parliament and of the council on horizontal cybersecurity requirements for products with digital elements and amending regulation (eu) 2019/1020 com/2022/454 final. `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454`. Accessed: 2024-11-14.

[20] Shambhu Sarkar. Drug counterfeiting: Key factors affecting vulnerable people in the world. *Journal of Advances in Medical and Pharmaceutical Sciences*, 25:27–34,, 2023.

[21] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. Medrec: Using blockchain for medical data access and permission management. In *Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30, Vienna, Austria, 2016. IEEE.

[22] Tomas Mikula and Rune Hylsberg Jacobsen. Identity and access management with blockchain in electronic healthcare records. In *2018 21st Euromicro conference on digital system design (DSD)*, pages 699–706. IEEE, 2018.

[23] Jayneel Vora, Anand Nayyar, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, Mohammad S Obaidat, and Joel JPC Rodrigues. Bheem: A blockchain-based framework for securing electronic health records. In *2018 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6, Abu Dhabi, United Arab Emirates, 2018. IEEE, IEEE.

[24] You Sun, Rui Zhang, Xin Wang, Kaiqiang Gao, and Ling Liu. A decentralizing attribute-based signature for healthcare blockchain. In *2018 27th International conference on computer communication and networks (ICCCN)*, pages 1–9. IEEE, 2018.

[25] TP Abdul Rahoof and VR Deepthi. Healthchain: A secure scalable health care data management system using blockchain. In *International Conference on Distributed Computing and Internet Technology*, pages 380–391. Springer, 2020.

[26] Gaby G Dagher, Jordan Mohler, Matea Milojkovic, and Praneeth Babu Marella. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable cities and society*, 39:283–297, 2018.

[27] Asma Khatoon. A blockchain-based smart contract system for healthcare management. *Electronics*, 9(1):94, 2020.

[28] Sudeep Tanwar, Karan Parekh, and Richard Evans. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, 50:102407, 2020.

[29] Abdullah Al Omar, Md Zakirul Alam Bhuiyan, Anirban Basu, Shinsaku Kiyomoto, and Mohammad Shahriar Rahman. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future generation computer systems*, 95:511–521, 2019.

[30] Bessem Zaabar, Omar Cheikhrouhou, Faisal Jamil, Meryem Ammi, and Mohamed Abid. Healthblock: A secure blockchain-based healthcare data management system. *Computer Networks*, 200:108500, 2021.

[31] Hao Wang and Yujiao Song. Secure cloud-based ehr system using attribute-based cryptosystem and blockchain. *Journal of medical systems*, 42(8):152, 2018.

[32] Xiaodong Yang, Ting Li, Xizhen Pei, Long Wen, and Caifen Wang. Medical data sharing scheme based on attribute cryptosystem and blockchain technology. *IEEE Access*, 8:45468–45476, 2020.

[33] Christian Esposito, Alfredo De Santis, Genny Tortora, Henry Chang, and Kim-Kwang Raymond Choo. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Computing*, 5(1):31–37, 2018.

[34] Tareq Ahram, Arman Sargolzaei, Saman Sargolzaei, Jeff Daniels, and Ben Amaba. Blockchain technology innovations. In *2017 IEEE technology & engineering management conference (TEMSCON)*, pages 137–141, San Jose, CA, USA, 2017. IEEE, IEEE.

[35] ConsenSys. Quorumchain consensus. `https://github.com/ConsenSys/quorum/wiki`, 2024. Accessed: 2024-11-14.

[36] Sagnik Datta and Suyel Namasudra. Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile edge computing. *IEEE Transactions on Consumer Electronics*, 70(2):211–221, 2024.

[37] QI Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, and Mohsen Guizani. Medshare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, 5:14757–14767, 2017.

[38] Kai Fan, Shangyang Wang, Yanhui Ren, Hui Li, and Yintang Yang. Medblock: Efficient and secure medical data sharing via blockchain. *Journal of medical systems*, 42(8):136, 2018.

[39] Bingqing Shen, Jingzhi Guo, and Yilong Yang. Medchain: efficient healthcare data sharing via blockchain. *Applied sciences*, 9(6):1207, 2019.

[40] Joao Sousa and Alysson Bessani. From byzantine consensus to bft state machine replication: A latency-optimal transformation. In *2012 Ninth European Dependable Computing Conference*, pages 37–48. IEEE, 2012.

[41] Peng Zhang, Jules White, Douglas C Schmidt, Gunther Lenz, and S Trent Rosenbloom. Fhirchain: applying blockchain to securely and scalably share clinical data. *Computational and structural biotechnology journal*, 16:267–278, 2018.

[42] FHIR. Fast healthcare interoperability resources. `https://www.hl7.org/fhir/`. Accessed: 2024-11-14.

[43] Rateb Jabbar, Noora Fetais, Moez Krichen, and Kamel Barkaoui. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pages 310–317, Dubai, United Arab Emirates, 2020. IEEE, IEEE.

[44] Jiawei Zhang, Yanbo Yang, Ximeng Liu, and Jianfeng Ma. An efficient blockchain-based hierarchical data sharing for healthcare internet of things. *IEEE Transactions on Industrial Informatics*, 18(10):7139–7150, 2022.

[45] Qi Xia, Emmanuel Boateng Sifah, Abla Smahi, Sandro Amofa, and Xiaosong Zhang. Bbds: Blockchain-based data sharing for electronic medical records in cloud environments. *Information*, 8(2):44, 2017.

[46] ONC. Office of the national coordinator for health information technology. `https://www.healthit.gov/`, 2024. Accessed: 2024-11-14.

[47] Kristen N Griggs, Olya Ossipova, Christopher P Kohlios, Alessandro N Baccarini, Emily A Howson, and Thaier Hayajneh. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems*, 42(7):130, 2018.

[48] Md Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. Continuous patient monitoring with a patient centric agent: A block architecture. *IEEE Access*, 6:32700–32726, 2018.

[49] Ashutosh Dhar Dwivedi, Gautam Srivastava, Shalini Dhar, and Rajani Singh. A decentralized privacy-preserving

healthcare blockchain for iot. *Sensors*, 19(2):326, 2019.

[50] Oumaima Attia, Ines Khoufi, Anis Laouiti, and Cedric Adjih. An iot-blockchain architecture based on hyperledger framework for healthcare monitoring application. In *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–5, Paris, France, 2019. IEEE, IEEE.

[51] Faisal Jamil, Shabir Ahmad, Naeem Iqbal, and Do-Hyeun Kim. Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals. *Sensors*, 20(8):2195, 2020.

[52] Bessem Zaabar, Omar Cheikhrouhou, Meryem Ammi, Ali Ismail Awad, and Mohamed Abid. Secure and privacy-aware blockchain-based remote patient monitoring system for internet of healthcare things. In *2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 200–205, Madrid, Spain, 2021. IEEE, IEEE.

[53] Kebira Azbeg, Ouail Ouchetto, and Said Jai Andaloussi. Access control and privacy-preserving blockchain-based system for diseases management. *IEEE Transactions on Computational Social Systems*, 9(3):633–643, 2022.

[54] Lukas Malina, Jan Hajny, Petr Dzurenda, and Sara Ricci. Lightweight ring signatures for decentralized privacy-preserving transactions. In *ICETE (2)*, pages 692–697, 2018.

[55] Asadullah Tariq, Rana Asif Rehman, and Byung-Seo Kim. Forwarding strategies in ndn-based wireless networks: A survey. *IEEE Communications Surveys & Tutorials*, 22(1):68–95, 2019.

[56] Pratima Sharma, Suyel Namasudra, Naveen Chilamkurti, Byung-Gyu Kim, and Ruben Gonzalez Crespo. Blockchain-based privacy preservation for iot-enabled healthcare system. *ACM Transactions on Sensor Networks*, 19(3):1–17, 2023.

[57] Faisal Jamil, Lei Hang, KyuHyung Kim, and DoHyeun Kim. A novel medical blockchain model for drug supply chain integrity management in a smart hospital. *Electronics*, 8(5):505, 2019.

[58] Khizar Abbas, Muhammad Afaq, Talha Ahmed Khan, and Wang-Cheol Song. A blockchain and machine learning-based drug supply chain management and recommendation system for smart pharmaceutical industry. *Electronics*, 9(5):852, 2020.

[59] Rajani Singh, Ashutosh Dhar Dwivedi, and Gautam Srivastava. Internet of things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention. *Sensors*, 20(14):3951, 2020.

[60] Ahmad Musamih, Khaled Salah, Raja Jayaraman, Junaid Arshad, Mazin Debe, Yousof Al-Hammadi, and Samer Ellahham. A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE access*, 9:9728–9743, 2021.

[61] Xinlai Liu, Ali Vatankhah Barenji, Zhi Li, Benoit Montreuil, and George Q Huang. Blockchain-based smart tracking and tracing platform for drug supply chain. *Computers & Industrial Engineering*, 161:107669, 2021.

[62] Saroj Kumar Nanda, Sandeep Kumar Panda, and Madhabananda Dash. Medical supply chain integrated with blockchain and iot to track the logistics of medical products. *Multimedia Tools and Applications*, pages 1–23, 2023.

[63] Jiatao Li, Dezhi Han, Zhongdai Wu, Junxiang Wang, Kuan-Ching Li, and Arcangelo Castiglione. A novel system for medical equipment supply chain traceability based on alliance chain and attribute and role access control. *Future Generation Computer Systems*, 142:195–211, 2023.

[64] D Kapoor, RB Vyas, and D Dadarwal. An overview on pharmaceutical supply chain: A next step towards good manufacturing practice. drug des int prop int j 1 (2)-2018. *DDIPIJ. MS. ID*, 107, 2018.

[65] Hyperledger. Composer. `https://hyperledger.github.io/composer/latest/introduction/introduction.html`, n.d. Accessed: 2024-11-14.

[66] Uri Klarman, Soumya Basu, Aleksandar Kuzmanovic, and Emin Gün Sirer. bloxroute: A scalable trustless blockchain distribution network whitepaper. *IEEE Internet Things J.*, 2018.

[67] Rajesh Kumar, WenYong Wang, Jay Kumar, Ting Yang, Abdullah Khan, Wazir Ali, and Ikram Ali. An integration of blockchain and ai for secure data sharing and detection of ct images for the hospitals. *Computerized Medical Imaging and Graphics*, 87:101812, 2021.

[68] Vinay Chamola, Adit Goyal, Pranab Sharma, Vikas Hassija, Huynh Thi Thanh Binh, and Vikas Saxena. Artificial intelligence-assisted blockchain-based framework for smart and secure emr management. *Neural Computing and Applications*, pages 1–11, 2022.

[69] Vikas Hassija, Rahul Ratnakumar, Vinay Chamola, Soumya Agarwal, Aryan Mehra, Salil S Kanhere, and Huynh Thi Thanh Binh. A machine learning and blockchain based secure and cost-effective framework for minor medical consultations. *Sustainable Computing: Informatics and Systems*, 35:100651, 2022.

[70] Guoming Zhang, Xuyun Zhang, Muhammad Bilal, Wanchun Dou, Xiaolong Xu, and Joel JPC Rodrigues. Identifying fraud in medical insurance based on blockchain and deep learning. *Future Generation Computer Systems*, 130:140–154, 2022.

[71] Pronaya Bhattacharya, Sudeep Tanwar, Umesh Bodkhe, Sudhanshu Tyagi, and Neeraj Kumar. Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications. *IEEE transactions on network science and engineering*, 8(2):1242–1255, 2019.

[72] Prabhat Kumar, Randhir Kumar, Govind P Gupta, Rakesh Tripathi, Alireza Jolfaei, and AKM Najmul Islam. A blockchain-orchestrated deep learning approach for secure data transmission in iot-enabled healthcare system. *Journal of Parallel and Distributed Computing*, 172:69–83, 2023.

[73] Rajesh Kumar, Abdullah Aman Khan, Jay Kumar, Noorbakhsh Amiri Golilarz, Simin Zhang, Yang Ting, Chengyu Zheng, Wenyong Wang, et al. Blockchain-federated-learning and deep learning models for covid-19 detection using ct imaging. *IEEE Sensors Journal*, 21(14):16301–16314, 2021.

[74] Mohamed Abdur Rahman, M Shamim Hossain, Mohammad Saiful Islam, Nabil A Alrajeh, and Ghulam Muhammad. Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. *Ieee Access*, 8:205071–205087, 2020.

[75] Marc Jayson Baucas, Petros Spachos, and Konstantinos N Plataniotis. Federated learning and blockchain-enabled fog-iot platform for wearables in predictive healthcare. *IEEE Transactions on Computational Social Systems*, 10(1):112–121, 2023.

[76] Abdur Rehman, Sagheer Abbas, MA Khan, Taher M Ghazal, Khan Muhammad Adnan, and Amir Mosavi. A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. *Computers in Biology and Medicine*, 150:106019, 2022.

[77] Yuan Liu, Wangyuan Yu, Zhengpeng Ai, Guangxia Xu, Liang Zhao, and Zhihong Tian. A blockchain-empowered federated learning in healthcare-based cyber physical systems. *IEEE Transactions on Network Science and Engineering*, 2022.

[78] Veronika Stephanie, Ibrahim Khalil, Mohammed Atiquzzaman, and Xun Yi. Trustworthy privacy-preserving hierarchical ensemble and federated learning in healthcare 4.0 with blockchain. *IEEE Transactions on Industrial Informatics*, 18(3):1989–1999, 2022.

[79] Yu Gai, Liyi Zhou, Kaihua Qin, Dawn Song, and Arthur Gervais. Blockchain large language models, 2023.

[80] Yuanhao Gong. Dynamic large language models on blockchains, 2023.

[81] Edward Kim, Isamu Isozaki, Naomi Sirkin, and Michael Robson. Generative Artificial Intelligence Consensus in a Trustless Network. *arXiv e-prints*, page arXiv:2307.01898, July 2023.

[82] Omar Cheikhrouhou, Khaleel Mershad, Faisal Jamil, Redowan Mahmud, Anis Koubaa, and Sanaz Rahimi Moosavi. A lightweight blockchain and fog-enabled secure remote patient monitoring system. *Internet of Things*, 22:100691, 2023.

[83] Sungjin Yu and Youngho Park. A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions. *IEEE Internet of Things Journal*, 9(20):20214–20228, 2022.

[84] Md Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. Blockchain leveraged decentralized iot ehealth framework. *Internet of Things*, 9:100159, 2020.

[85] Abdullah Ayub Khan, Sami Bourouis, MM Kamruzzaman, Myriam Hadjouni, Zaffar Ahmed Shaikh, Asif Ali Laghari, Hela Elmannai, and Sami Dhahbi. Data security in healthcare industrial internet of things with blockchain. *IEEE Sensors Journal*, 2023.

[86] Chaoyang Li, Mianxiong Dong, Xiangjun Xin, Jian Li, Xiu-Bo Chen, and Kaoru Ota. Efficient privacy-preserving in iomt with blockchain and lightweight secret sharing. *IEEE Internet of Things Journal*, 2023.

[87] Bhaskara S Egala, Ashok K Pradhan, Venkataramana Badarla, and Saraju P Mohanty. Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet of Things Journal*, 8(14):11717–11731, 2021.

[88] Doriane Perard, Jérôme Lacan, Yann Bachy, and Jonathan Detchart. Erasure code-based low storage blockchain node. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and*

Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pages 1622–1627. IEEE, 2018.

[89] Xiaohai Dai, Jiang Xiao, Wenhui Yang, Chaofan Wang, and Hai Jin. Jidar: A jigsaw-like data reduction approach without trust assumptions for bitcoin system. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pages 1317–1326, Dallas, TX, USA, 2019. IEEE, IEEE.

[90] Yibin Xu and Yangyu Huang. Segment blockchain: A size reduced storage mechanism for blockchain. *IEEE Access*, 8:17434–17441, 2020.

[91] Pan Chen, Liu Zhiqiang, Liu Zhen, and Long Yu. Research on scalability of blockchain technology: Problems and methods. *Journal of Computer Research and Development*, 55(10):2099, 2018.

[92] Qiheng Zhou, Huawei Huang, Zibin Zheng, and Jing Bian. Solutions to scalability of blockchain: A survey. *Ieee Access*, 8:16440–16455, 2020.

[93] Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys (CSUR)*, 54(8):1–41, 2021.

[94] Hai Jin, Xiaohai Dai, and Jiang Xiao. Towards a novel architecture for enabling interoperability amongst multiple blockchains. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, pages 1203–1211, Vienna, Austria, 2018. IEEE, IEEE.

[95] Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, and Neeraj Kumar. A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, 126:45–58, 2019.