UNIVERSITY OF TURKU

Enhancing Information Security Compliance in Healthcare through Cryptography and Blockchain Technology

Cryptography/ MDP in ICT

Master's thesis

Author:

Mohammad Ashraful Islam

08.04.2025

Turku

Master's thesis

Subject: Cryptography
Author: Mohammad Ashraful Islam
Title: Enhancing Information Security Compliance in Healthcare through Cryptography and Blockchain Technology
Supervisor(s): Prof. Ion Petre, Docent Yury Nikulin

Number of pages: 132 pages

Date: 08.04.2025

The subject of the thesis is integrating blockchain technology and advanced encryption methods to enhance information security in the healthcare sector. This thesis tries to reach the following three objectives: determination of the current landscape regarding compliance in healthcare information security, finding several techniques of encryption for data protection, and monitoring the application of blockchain technology for data transactions' protection.

The research has also elucidated actual case scenarios indicating the usage of cryptographic techniques such as public key infrastructure algorithms and secure multi-party processing in various solutions. We found that adequate encryption greatly enhances patients' medical record security, secures personal information, and enhances regulatory compliance.

We conclude that the kind of challenges that face the health sector necessitate cryptographic techniques to be carried out on top of blockchain technology. The advantages of deploying such advanced technologies are that the organizations will be able to guarantee patient data confidentiality and availability, where integrity is ensured by applicable laws. This research study contributes to the steadily growing body of literature on healthcare cybersecurity and also offers some key lessons learned for policymakers, industry practitioners, and scholars interested in hardening information security levels in healthcare organizations.

Key words: Information security, healthcare, cryptography, blockchain, transparency, data breach prevention, and regulatory compliance.

Table of contents

1 Introduction

Cyber threats in healthcare are expected to rise as internet-enabled apps and medical equipment become more common. Healthcare is a huge human concern, and cyberattacks may interrupt patient treatment and endanger lives [1]. EHR applications digitize paper-based patient health records. Paper medical records were formerly used. Information and communication technology has helped medical records move from paper to electronic. In healthcare, user data privacy is crucial. Enhancing EHR systems for data privacy without compromising efficiency and interoperability is the main concern [2]. The idea of patient registries built from data collected in EHRs is gaining popularity. Electronic health records (EHRs) and patient registries both collect and make use of clinical information at the patient level, but they serve distinct conceptual functions [3]. EHR allows clinicians at multiple medical facilities or hospitals in different cities, regions, or countries to view the patient's records. EHRs assist doctors in prescribing new drugs by providing a patient's medication history. Other benefits of EHR include leveraging patient medical information for research and therapy development [4]. With ubiquitous health data access, privacy is an issue. EHR issues include medical institutions holding patients' data, not patients. Patients' privacy includes clinicians and researchers accessing their EHR without their consent for treatment and research.

Electronic Health Record systems face various security challenges because of growing IoT sensor devices and wearable technology, but these create greater exposure to cyberattacks [5]. The pharmaceutical supply chain faces serious problems with fraud detection because counterfeit drugs can result in significant adverse outcomes [6]. The HITECH Act of 2009 created a major push for Electronic Health Records (EHR) adoption because it encouraged healthcare digitalization to improve service efficiency [7]. The EHR systems are beneficial in the sense of effective management of public health services, enabling patients to retrieve their data online, and allowing data integration [8],[9]. The emergence of COVID-19 stressed future reliance on remote patient monitoring as well as the importance of data connection systems for medical services [10],[11]. Nevertheless, with privacy hazards involved, centralized server systems still cause major security issues [12]. This investigation is noteworthy since the protection and confidentiality of EHRs is essential in ensuring quality healthcare services. As the threats posed by cybercriminals and data violations have increased, effective storage, use, and management of information are paramount given the rise

of EHRs in health care systems [13]. Blockchain technology's data management advantages include both improved security elements and more openness [14]. This thesis investigates the use of blockchain in healthcare in order to improve the existing healthcare data management system for the benefit of patients, healthcare providers, and researchers.

This thesis will have several parts. Chapter two will focus on privacy in electronic health records. Interesting research questions that arise from this literature are; Chapter three will focus on the current state of information security in healthcare. Chapter four will focus on blockchain technology in healthcare. Cryptography in Healthcare is in chapter five. Chapter six is the applications of blockchain in healthcare. Chapter seven is Challenges and Limitations. Chapter eight will analyze various cases and success factors. Chapter nine discusses the blockchain innovation and ethics in healthcare, and ultimately, the chapter titled Conclusions summarizes the thesis.

2 Health care privacy laws and regulations

Over the last several decades, medical professionals have benefited from the assistance that information and communication technology (ICT) provided in the management of patient care and research records [15]. Delivering top-notch patient care is intimately tied to healthcare systems' capacity to digitally gather, store, retrieve, analyze, and communicate information on patients' health records [16]. Information and communication technologies (ICTs) offer great promise for enhancing healthcare service delivery, combating diseases, managing health, conducting research, and preventative care [17]. The data quantity has become significant and reaches terabyte levels. Raw health data continues to scale up as medical organizations implement digital documentation while creating opportunities for peta (1015) to exa (1018) bytes of data storage that prove challenging to handle and interpret. Multiple data silos prevent a combination of healthcare information from being both related and retrieved for analysis [18]. This growth is due to the increased adoption of biomedical technologies, electronic health records, and the IoT [19]. The increased application of big data in medicine is triggered by the frequent advancement of cheap computing hardware, available study designs, and cultural and societal shifts that enable easier access to information [20]. There is still a lot that big data may help uncover the patterns of health and generate new solutions. However, some of the issues include international law, data ownership, privacy, and security [21].

2.1 Health Insurance Portability and Accountability Act (HIPAA)

Federal and state laws and rules give patients the right to access their health information and control the disclosure of this information while at the same time ensuring that healthcare data is shared for care delivery and research. All kinds of personally identifiable information are protected and secured under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which was passed on a national level and applies to different healthcare companies [22]. There are some other relevant laws, like the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act, the Patient Safety and Quality Improvement Act, and the Health Information Technology for Economic and Clinical Health Act. Security threats and the protection of individually identifiable health information are the goals of these laws [23]. However, increasing usage of new healthcare technology requires local and international patient data regulations, ethics, and legislation. The many healthcare stakeholders and organizations involved make patient privacy difficult [24]. With the goal of improving patient care and

making medical data used for research and public health efforts more reliable, health privacy laws are important [25]. HIPAA protects information relative to users' health data processed or shared by the institution in any format, including electronic, manual, or verbal. The privacy regulation is commonly known as the healthcare privacy regulation or Protected Health Information (PHI) under HIPAA [26].

2.2 Directive on Data Protection in the European Union

For cost efficiency in the provision of healthcare, health information technology, specifically the use of electronic health records (EHRs), is vital. That means, however, that there could be risks to privacy and security. Computer security is also considered vital because privacy can easily be violated online, and such violations are sometimes very difficult to undo. Privacy laws in health in the United States can be categorized into constitutional, statutory, and regulatory laws. In this respect, the EU laws are much broader and cover personally identifiable medical data [27]. A lot of concern has been raised over patient data as regards the integration of EHR within the European Union. The GDPR in the EU mandates that data protection be initiated and integrated into EHR systems [28]. This methodology is essential for safeguarding privacy and security in electronic health records, which include sensitive patient data [29]. The secondary use of EHR data for clinical studies poses a problem in reconciling patient privacy with potential societal advantages [30]. Addressing these challenges, a complete data security by design paradigm for EHRs has been designed. The model enshrined not only the organizational protection but also the technological protection [31]. Data controllers and developers might use this model as a guide or check to see if they are aligned with GDPR provisions. Despite the various benefits of applying EHRs in healthcare and research, these records should follow the legal requirements of the European Union and preserve patients' trust through the proper consideration of the criteria of data safety [28]. In order to analyze personal information, organizations have to meet at least six legal bases under the GDPR before they may process personal information. However, with regard to medical records, such standards are even more rigorous [32]. It is believed that GDPR seeks to advance the EU's laws on the process of personal data and grant sovereignty to people with respect to their data alongside setting standards. OpenEHR is a standard that facilitates interoperable and secure EHR software and is believed to be the best method to build hospital information systems [33]. It is particularly noteworthy because there is a conflict between patients' right to privacy and the potential dangers of compromising such

sensitive data, as well as the possible social benefit of using the data to further medical research [30].

2.3 NIST Cybersecurity Framework for Healthcare Data

The use of the NIST Cybersecurity Framework (CSF) extends to healthcare data protection. It gives a framework for enhancing cybersecurity in such important sectors as the health sector [34]. It is also scalable and can be applied together with other standards, specimens of which include HITRUST in evaluating the advancement of security in healthcare settings [34]. In the last couple of years, the studies in the subject have logically catalogued regulations, standards, and guidelines specifically for the healthcare domain by employing NIST CSF as a classification model [35]. Frameworks like ISO/IEC 27799, HIPAA, and GDPR are out there, but NIST CSF has better solutions for cybersecurity issues [36]. The NIST risk framework has been used to identify risks and assess vulnerabilities in the Asia region that continues to experience a rising number of healthcare cyberattacks, though risk analysis forms a good foundation when trying to institute preventive measures and modalities for risk management [37]. In recent years, care has been taken to develop a myriad of rules, standards, and recommendations to address and avoid incidents in terms of healthcare cybersecurity. Guidelines from ENISA, NIST SP 800-66, ISO/TR 21332, and ISO 27799 are important [35]. In the EU, the Medical Device Regulation (MDR) and In Vitro Diagnostic Medical Device Regulation (IVDR) have brought new cybersecurity obligations for medical devices [38].

The central message of this chapter is that, while there has been enormous effort and resources being put in place to ensure health data security through laws, regulations, and policies, the incidences of data breaches are still rampant and increasing globally. Despite having the HIPAA laws, data breaches have not yet been eradicated [39]. The subsequent chapter covers the current scenario of healthcare information security.

3 Present Condition of Information Security in Healthcare

The amount and type of data in the healthcare sector obtained and processed have grown exponentially because of the advancement of technology in providing care to the people. This so-called big data contains diverse types of data, such as EMRs, biological and medical records, data gathered from sensors, and data accumulated from other medical devices [40]. Several threats associated with healthcare business can be singled out, primarily due to the nature of collected, stored, and processed personal and medical data. Due to the fact that patient records are valuable and contain information such as protected health information, financial information, and other individually identifiable data, healthcare organizations receive higher risks of hacker attacks [41]. Leakage of personally identifiable health information (PHI) may produce several social, financial, and legal consequences for people, thus making it important to devise secure ways of handling healthcare data [42].

3.1 An Overview of Healthcare Data Sensitivity

Healthcare data is voluminous in nature and also considered sensitive personal data; it should not be mismanaged [43]. As the set amounts and kinds of healthcare data and their further use for decision-making and patient treatment are rather large and sensitive, recommend evaluating classification algorithms concerning such parameters as accuracy, sensitivity, and specificity for choosing the most appropriate ones [44],[45]. In order to advance patient results, healthcare data analysis needs assessment. One of the biggest considerations of data analytics is how to properly manage sensitive information, which concerns ethical issues around patients and data security [46]. The increasing importance of metrics can negatively impact the qualitative work being delivered to the patients, implying that a rather broader view of healthcare metrics is needed [47]. Since patient information is safeguarded, confidentiality and strong security measures must be employed since the current algorithms fail to handle the amount and diversity of the healthcare data [48]. These methods are often employed in patient data to conceal their identities but often fail when reconstructing attacks are used on them [49]. A recommendation for analyzing the categories of data at a more detailed level is made to enhance ethical decision-making and to offer suitable protection to research subjects [50]. It is noted that Mobile Health Data Collection Systems (MHDCS) encounter specific issues concerning the protection of data, for which the sensitivity of health data varies depending upon several contextual factors. To cope with this, the multi-level data

sensitivity model has been designed for mobile health attribute-based access control to provide more granular security measures while collecting the clinical data [51].

Security of healthcare data in blockchain is greatly enhanced by anonymization techniques. Several techniques have been used in order to increase data privacy and anonymity in smart healthcare networks [52]. These methods have the objective to safeguard individual health data and permit the data mining aim as well as medical decisions boosting in addition to the avoidable costs decrease [49]. It should be noted that the anonymization cannot completely remove risks associated with re-identification; however, it is a critical stage in data de-sensitivity steps if performed correctly [53]. Some of the frequently used anonymization processes are k-anonymity and hash functions to be used in geolocation and IP address values [52]. A study done on privacy-preserving blockchains provides proof that ensuring both data utility and privacy is a major concern in development [54]. A systematic literature review demonstrating that privacy and anonymization are positively correlated in different blockchain applications. This includes methods such as ring signature, homomorphic encryption, and k-anonymity that can be used in increasing privacy. Combining these papers in one work indicates constant work on anonymization techniques in blockchain systems that can help minimize privacy concerns while maintaining data usefulness [55].

Healthcare data is comprised of EHRs, human wearables, genomic data, and patient self-reported data. Thus, it poses tremendous challenges to processing and analysis [56],[57], and [58]. Conventional methods of data management become ineffective due to the volumes, velocity, and variety of data. Nonetheless, big data analytics in healthcare presents one of the greatest opportunities for real-time disease tracking, outbreak forecasting, and one-to-one patient care [57]. To overcome these challenges, researchers have sustained effective methods in data accrual, preservation, and amalgamation for different forms of data from many sources [59]. The existence of data heterogeneity in the healthcare system creates a lot of complexity in data integration and analysis [60]. That’s why blockchain’s decentralized structure becomes a solution, as it guarantees data’s reliability and its inability to change. Using cryptographic algorithms and the creation of trust ledgers, blockchain provides an open and traceable environment for storing and protecting medical data that cannot be altered. The technology also allows for timely and selective acquisition of medical histories to improve patient care and for enhanced collaboration between caregivers [61].

3.2 Cybersecurity risks in healthcare

Due to the increase in the use of patients records in healthcare facilities, the use of electronic health records, and the aspects of healthcare cybersecurity, have become crucial [62],[63],[64], and [65]. Hospitals are lucrative targets for cybercriminals with risks including data loss, ransom, and potential compromising of medical devices [66]. They are even more so when the Internet of Things (IoT) is integrated into a healthcare environment [67]. Healthcare requires practical and detailed cybersecurity risk management frameworks that will help healthcare organizations address these issues. Key strategies are the development of an integrated systems management program, assessment of risks, and implementation of risk mitigation mechanisms [68]. These indicate that addressing cybersecurity in healthcare requires avoiding human elements such as behaviour and the use of technology and processes. In addition to a multi-disciplinary collaborative approach, particularly involving IT, clinical, and administrative staff [62],[67]. Reducing threats in the healthcare sector needs a proactive as well as a reactive strategy in the domain of cybersecurity. Key proactive measures include rightful staff education programs appropriate to staff members' positions because human mistakes remain the primary causes of breaches, having a 95% success rate [69]. Due to the ever-increasing new threats, it is possible to detect security flaws in the security system and prevent such incidents by conducting regular security audits and applying upgrades [70].

Primary measures of security have been found to be cheaper and related to low incidences of failure compared to measures that are taken after an incident has occurred [71]. It is also important for several healthcare organizations to sometimes check on third-party vendors to make sure they are secure enough [70]. There is a major security threat for healthcare institutions, especially when it comes to patients' data security in connection to various regulatory requirements. Transitioning to the proper cybersecurity frameworks is necessary for risk control and maintaining business processes sustainability [72]. Key regulations like HIPAA, GDPR, and other standard frameworks and guidelines comprise the ISO/IEC 27799 and NIST CSF Cybersecurity frameworks, each of which possesses its own strengths when approaching security issues, which I highlighted in chapter two.

3.3 Healthcare data breaches and incidents

There has been a marked increase in the number of reported healthcare data breaches in the last few years, with most of the attacks falling under the hacking and IT accidents' category [73].

This sector is the most vulnerable to hacking because of the personal information of the patients [74]. Between 2010 and 2018, as many as 2,529 breaches included 194.74 million individual records in the United States; concerning the most often targeted were the healthcare providers [75].

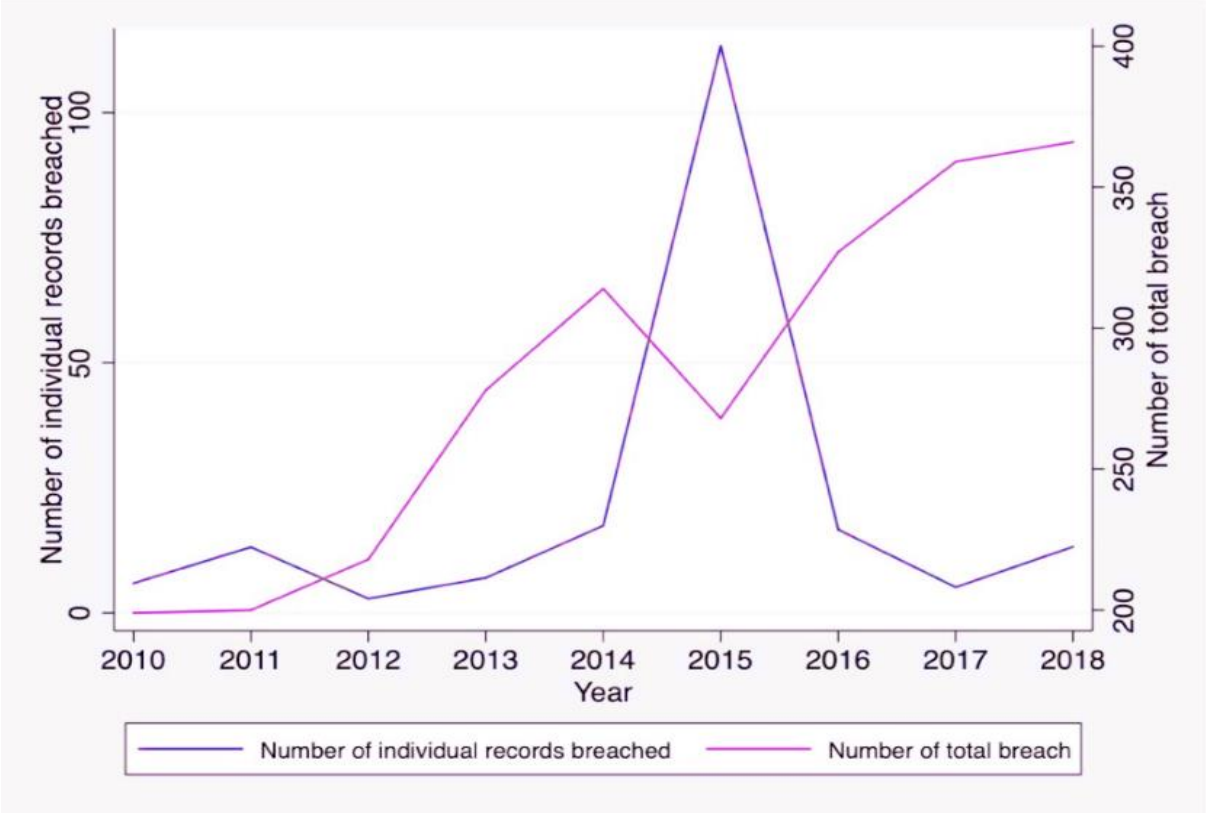

Figure 1 Number of U.S. data breaches and impacted records between 2010 and 2018 [75].

Hacking/IT incidents make up 87% of all healthcare data breaches, with network server breaches at 67% and email breaches at 23% within the year 2020 [76]. The cyberattacks on the healthcare industries increased drastically from the year 2016 to the year 2021, with the patient's protected health information compromised to almost 42 million [77]. There is a marked rise in the average cost of healthcare data breaches, which is set at US$ 10.93 million in 2023, and the percentage increase in the incidence of phishing is 60 percent. For instance, as much as 82% of cyberattacks started mainly with hospitals, showing that there were serious weaknesses within the health sector [78]. There are high levels of breaches across the healthcare sectors, for example, costing $575 billion each year. Such events usually pertain to the loss of customers' personal, financial, and health data, which is often reported to the victims long after the breach, causing much harm [79].

Table 1 Sector-Based Data Breach Representation [73].

Name of the Sector	Number of Breaches (2005–2019)	Percentage % (2005–2019)	Number of Breaches (2015–2019)	Percentage % (2015–2019)
Educational Organizations	671	10.55	64	3.08
Businesses – Financial	410	6.45	194	9.36
Businesses – Other	426	6.7	113	5.45
Healthcare Service Providers	3912	61.55	1587	76.59
Government and Defense Institutes	561	8.82	45	2.17
Non-Governmental Organizations	75	1.18	7	0.33
Business – Retail (incl. Online)	300	4.72	62	2.99
Total	6355	99.97	2027	99.97

The table presents data about the number of data breaches that occurred in different sectors over two time periods: the outcomes of the last 15 years (2005-2019) and the outcomes of the last 5 years (2015-2019). Based on data from 2005 to 2019 and 2015 to 2019, healthcare has been subjected to the most data breaches among all the industries included in the study. Out of the 6355 records of breach instances from 2005 to 2019, the healthcare business experienced 3912 data breach incidents, and 1587 were recorded in the healthcare sector, which accounts for 76.59% of the total number of recorded breach instances from 2015 to 2019. The foregoing evidence is clear testimony that the healthcare sector has become the biggest loser through data breaches. However, the incidence of healthcare data breaches is rising at an even higher rate more recently [73]. The main disclosure types of protected healthcare information again included hacking/IT incidents, unauthorized use (internal), loss (theft), and improper disposal of data that is not needed [75].

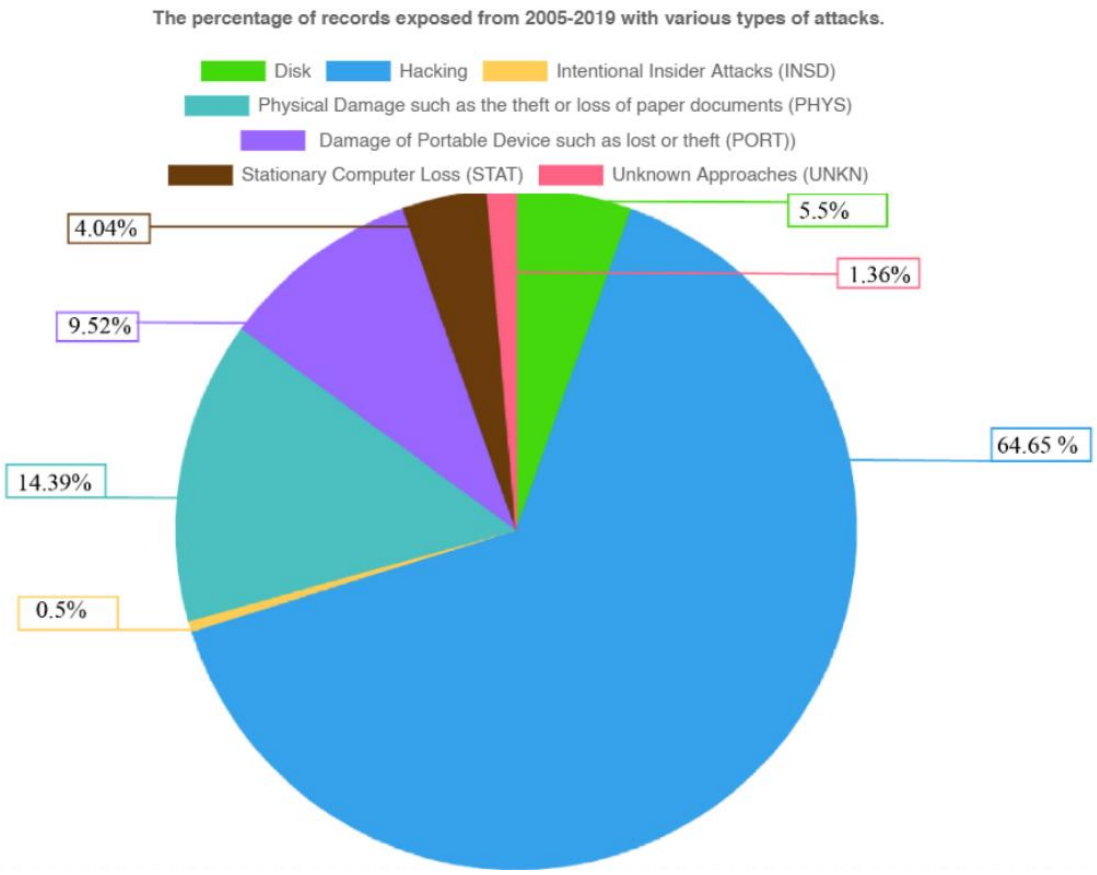

Figure 2 The percentage of records exposed from 2005 to 2019 with various types of attacks [73].

Figures 2 present the percentage share of records exposed to each type of attack from 2005 through 2019 and confirm that hacking is the main source of very sensitive health data leakage.

Ejiofor Oluomachi and Akinsola Ahmed use a Gradient Boosting Classifier (GBC) model to forecast the severity of data breaches. GBC, an effective ensemble method, is well suited for enhancing patient data security in healthcare cybersecurity. This approach develops a very precise predictive model by sequentially integrating several weak learners, usually decision trees, with each iteration rectifying mistakes from prior iterations to enhance accuracy and mitigate overfitting. The final model,

$$F_M(X) = F_0(X) + \sum_{m-1}^{M} \alpha_m \, h_m(x)$$

consolidates the weak learners to produce a robust, cohesive prediction. Their breakdown of breach types also shows that there have been 695 cases of hacking/IT incidents, making it the most common type of breach [42]. Paweł Dymora, Mirosław Mazurek, and Mariusz Nycz are

to provide new insights into the method that future data analysts use when selecting and applying statistical methods, data mining techniques, and IT tools. Predicting future data breaches, the authors constructed a time series model utilizing data from 2010 to 2022. In order to aggregate and analyze patterns in the data, a bespoke tool was developed. The data was then divided into two categories: those with discernible trends and those that were just random noise. Group II's (noise data) models relied only on moving averages, in contrast to Group I's (trend data) mix of linear regression plus moving averages. Validated using simulations and visualizations generated using Python, the overall data leakage projection is the combined prediction from each sub-series [80].

For group one, they calculated an "error" value $\varepsilon_j(t$) which is equation (1), which is the difference between the model's linear prediction $(at + b)$ and the actual leak count $X_J(t)$ for each month:

$$\varepsilon_j(t) = (at + b) - X_J(t), \qquad (1)$$

where X(t) is the actual number of data leaks for a particular month t and x(t) are the model's prediction of leaks for month t:

$$x_j(t) = \max\,(at + b + \varepsilon\_j(t),0). \qquad (2)$$

Equation (2) shows how much the prediction is off from the actual value. They averaged these errors over the last few months to smooth out random fluctuations. This average error, $\varepsilon_{-j}(t)$ which is a moving average of errors, provides a more stable correction factor. makes the correction factor more stable. In the final prediction, for each month t, they add up the linear prediction $(at + b)$ and the average error from recent months:

$$\varepsilon_{-j}(t) = \frac{\varepsilon_j(t-w)+\varepsilon_j(t-w+1)+\cdots+\varepsilon_j(t-1)}{w}. \qquad (3)$$

While working with the data of Group II, where data appears to be random and trends are not easily discernible, they eliminate the linear regression step and just use the moving average. This approach functions better for noisy data, where trends cannot be identified. This modeling framework employs autocorrelated plots to detect periodicities of sample data and then partitions the data into subsamples for modeling. Some of them include defining parameter values of the model, compiling monthly data values, calibrating simulated models, and synthesizing sub-series leakage forecasts into an overall leakage forecast. Using records

obtained from the Department of Health and Human Services, this paper provides a literature review of data leakage in U.S. healthcare institutions from the year 2009 to the year 2023. The authors identified several trends during the analysis, and they also stated that IT incidents such as hacking have emerged as the leading category over the decade [80].

There are some major security vulnerabilities in the healthcare industry, like A Russian hacker organization dubbed “Ryuk” targeted the University of Vermont Health Network on October 28, 2020. This ransomware attack locked down almost every server of UVM Medical Center serving around 1,300 in the organization and contaminated more than 5,000 devices. The attackers just sent an anonymous file with contact instructions and locked the patient data. Many staff members lost their phones and emails, and such patient details and records and systems covering their overtime allowance were among the items and services that were attacked and halted at the facility. Whereas users were able to perform read-only operations on medical information in three days, full recovery was attained in 42 days. It was estimated to have cost about $63 million. Security Breach at Trinity Healthcare, Overall, it is estimated that the Trinity Healthcare Breach has affected 3,320,726 individuals [81],[82],[83], and [84].

The case of the Vastaamo psychotherapy data breach in Finland revealed the critical cybersecurity problems facing the mental health sector. This case clearly shows why de-identification, encryption, and multi-factor authentication should be implemented and practiced [85]. The breach procedure had a high social effect of increasing consciousness of cybersecurity and the ensuing Vastaamo bankruptcy [86]. It also exposed the risks introduced by the platform of psychotherapy as a service, as well as the necessity for stronger governance of healthcare givers [87]. More recent targeted cyberattacks involving Medibank and Australian Clinical Labs show that electronic health records contain vulnerabilities involving blackmail, fraud, and identity theft. These incidents bring about the decreased collection of personal information as well as the government increasing its control of electronic health record privacy and security [85].

This section captures increasing cybersecurity threats in healthcare because of big data in EMRs devices that constantly attract hackings and ransomware. When it comes to protecting such valuable data, preventive measures, intelligent data analysis techniques, and deep periodic assessments must become indispensable. Prominent examples include the Ryuk attack on the University of Vermont Health Network, for which proper protection must be set up in healthcare. Problems with interoperability and privacy protection are encountered by

EHRs. One promising approach to these problems is blockchain technology, which offers a distributed, trustworthy, and auditable method for handling electronic health records [88]. The use of blockchain means that the patient data is more secure, protected via cryptographic techniques, and put into the hands of the patients [89].

4 Blockchain Technology in Healthcare

Applying the blockchain technology is becoming an attractive solution for numerous issues in the sphere of healthcare while providing the secure, transparent, and efficient data processing [90],[91]. Telemedicine, clinical trials, medication supply chain management, and patient data management are some of the key uses [92]. The benefits that the technology brings include maintaining trust for decentralized transactions without control from a central authority as well as data sharing, real-time patient information access, and better outcomes [93]. Through analysis, it was understood that blockchain technology has prospects for solving security and data exchange issues in the healthcare sphere [94]. Blockchain solutions in healthcare can include cybersecurity and privacy, invoicing, and supply chain management issues [95]. Blockchain's immutable ledger makes sure that medical records are tamper-proof and reduces the risk of unauthorized access [96]. More specifically, blockchain technology improves interoperability by allowing many parties, such as patients, healthcare providers, and insurance, to easily share data [97].

4.1 Fundamentals of blockchain technology

Success with Bitcoin as a digital currency has led to the expansion of blockchain technology. A peer-to-peer electronic cash system was published in 2008 by Satoshi Nakamoto, who invented the Bitcoin mechanism [98]. Key properties of decentralization, persistency, anonymity, and auditability are claimed to provide increased levels of security and effectiveness for digital data systems [99]. The technology has the ability to revolutionize current business structures by authenticating commodities, facilitating decentralization, and reducing transaction costs [100]. By eliminating the need for centralized servers, blockchain's decentralized, peer-to-peer network design improves security and resilience [99]. Blockchain uses cryptographic methods to ensure they maintain data integrity, and it is immutable; hence, it is trusted and auditable. Beyond the realm of cryptocurrencies, blockchain technology has many possible applications in fields including healthcare, supply chain management, finance, and identity governance [101]. The opportunities and risks associated with the use of blockchain technology are potential in affecting several industries because they are still in the growing phase [100].

The data kept in a blockchain is organized into blocks that are connected to create a linear chain: the blockchain itself. Every blockchain rests on a foundation of blocks. Together, they constitute the blockchain and store all data. A digital fingerprint, unique to each block in the blockchain, represents each block and allows for its unambiguous identification [102]. While fingerprints may be used to uniquely identify individuals, they must be associated with other data, such as names, in a database in order to disclose a person's identity. Just like a person's unique "digital fingerprint" (or hash), each block in a blockchain may be recognized without disclosing its contents [103]. This unique identifier makes it possible to verify the integrity of any blockchain copy by looking for blocks that are missing. Additionally, every block checks the fingerprint of the block before it, making it possible to trace the order of blocks in a linear fashion [102]. The genesis block is the initial block on a blockchain, and each block is referred to by its parent block [104].

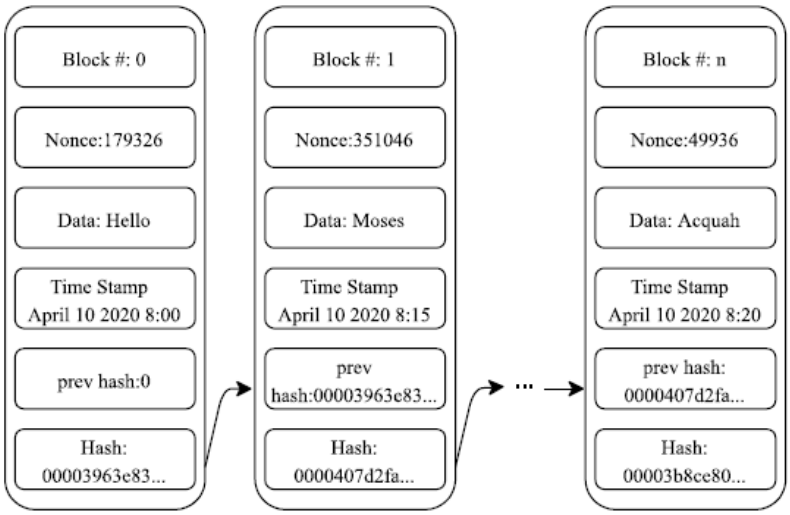

Figure 3 Typical Blockchain Blocks [105].

4.2 Decentralized and immutable ledger technology

Decentralized Consensus Technology (DCT) includes blockchain and other Distributed Ledger Technologies (DLT) that operate autonomously with no central authority and encourage decentralization, trust minimization, and consensus-building mechanisms among members [106]. Blockchain technology uses a one-way function in immutable distributed databases, which improves cybersecurity and is applicable in many industries such as cryptocurrency, smart contracts, and supply chains [107]. One-way functions are very

significant in providing security to numerous cryptographic tasks, such as those applied within blockchain systems [108]. In practice, if the output of a one-way function and find an input that produces that exact output, there's no shortcut or another method to do so. The only option is to try every possible input one by one (a brute force search) until find one that works. Instead of referring to a single function, one-way hash functions are more accurately characterized as a family of functions [109].

If n represents the length of the input string, then f_n is the function that operates on those n bit input strings so that a pseudoinverse F_n would satisfy the f_n.

$$f_n\left(F_n\left(f_n(x)\right)\right) = f_n(x)$$

This means that assuming the input x, applying f_n and then F_n should return an input that goes back to the same output of f_n. A pseudoinverse F_n of f_n is a function that can provide some input x' such that applying f_n to x' yields the same output as applying f_n to the original input x.It is important that, F_n doesn't need to recover the exact input x, it just needs to find some x' that maps to the same output. F_n isn't required to be one-to-one. It only needs to give a valid preimage for the given output of f_n.

Let $f = \{f_n\}_{n=1}^{\infty}$,this represents a family of one-way functions, one for each input length n and $F = \{F_n\}_{n=1}^{\infty}$,in a similar way, it defines a family of pseudoinverse functions, one for each f_n . In average-case hardness, it is difficult and hard for a pseudoinverse function F_n to reverse the function f_n for most inputs, even when considering all possible n -bit inputs. For any pseudoinverse F_n for which efficient computation is possible (in polynomial time relative to n), the proportion of inputs x for which F_n efficiently satisfies the relationship $f_n\left(F_n\left(f_n(x)\right)\right) = f_n(x)$ becomes very small as the input size n increases [110]. This ensures that inverting f_n is not just hard in rare cases but also in the average case, which makes it practically infeasible with larger inputs, at least as far as classical computations are concerned. This definition just underlines that it is hard to address one-way function inversion on average. It demonstrates that, for large inputs, no efficient algorithm can invert the function in more than a very small percentage of cases, even if one allows the use of randomized algorithms. This property is particularly important specifically in the cryptographic applications because the integrity of these functions depends on the practical impossibility of efficiently inverting such functions.

4.3 Digital signature

Coming to the components of blockchain, it has to be mentioned that digital signatures are needed and used to make the transactions safe and non-repudiable [111],[112]. The methods utilized include ECDSA, RSA, and DSA. ECDSA's usage of elliptic curve cryptography makes it very effective [111],[113]. It has been used in confirming the identity of the source of a message, guaranteeing the content has not been altered, and safe storage of electronic goods. They are also used in smart contracts and digital document signing [113]. For the purpose of transferring transactions and verifying their authenticity, blockchain employs asymmetric cryptography. Each transaction requires signature authorization by the sender using their private key before moving through the P2P network. Most current blockchains use the ECDSA, or elliptic curve digital signature algorithm [114]. In a peer-to-peer (P2P) network, all related nodes are considered equal participants, and the transaction is published to all of them once sent. Upon receipt by other nodes, the transaction's credibility is checked against established block validation criteria using the sender's public key. Once one node has received and verified a transaction, it will be forwarded on to the next node if it is legitimate. This method will be disregarded it if it is not the case. The new block in the blockchain network can only contain transactions that are legitimate [104].

The Method of the Digital Signature

In digital communication, to make the communication secure and authenticated, digital signatures come under the cryptographic technique [115]. The process includes creating two keys – a public and a private key [116]. The sender generates a digital signature by combining two steps. The first step is hashing the message, and the second one is using their private key to encrypt the hash result [117]. The original message and this signature are sent to the recipient [118]. When the receiver receives the message, he decrypts the hash using the sender’s public key and checks with a new hash of the received message [117]. If the hashes match, then it authenticates the message and assures the sender’s identity [115].

- Digital Signature Algorithm

Digital Signature Algorithm, commonly known as DSA, is the standard in the development of digital signatures, which is based on the principle of public-key cryptography using factorization, logarithmic, and modular exponentiation computing [119]. It employs two

cryptographic keys, both public and private, to enhance the security and reliability of data collected [120]. In implementing the DSA process, public and private keys must be created, hash values of documents must be generated, and specific signatures must be verified [121]. It is using the Secure Hash Algorithm SHA-1 in the message digestion process and consists of parameters based on the ElGamal signature algorithm [121].

- DSA Parameters

Let, p is a large modulus prime number, slightly larger than 2^{511} but smaller than 2^{512}. q is another prime number that divides $p-1$ slightly larger than 2^{159} but smaller than 2^{160}.g is value derived from p , q and an integer h, where h must meet certain conditions to make g valid.

$$g = h^{(p-1)/q} \bmod p > 1 \; ; \quad 0 < h < p.$$

Each user has a private key x and public key y . The private key x is a random number smaller than q

$$0 < x < q.$$

And the public key y is calculated from

$$y = g^x \bmod p.$$

A message m needs to be signed. A one-way hash function H is used to create a unique fingerprint of the message, assuring that no two messages yield identical hash values. A secret random number k is used during the signing process. This value of k must change for every new signature

$$0 < k < q.$$

The variables p , q and g are public and may be disseminated among a group of users. Nonetheless, private key x and random number k must consistently stay confidential. To make sure that communications are secure and cannot be altered, the hash function H makes it very difficult to locate two messages that have the same hash value [116].

- Create and Validate Signatures

The sender picks a random number k and calculates $r = (g^k \bmod p)\ mod\ q$; where p , q and g are public values. $s = k^{-1}(H(m) + xr)\ mod\ q$; where k^{-1} multiplicative inverse of k. $H(m)$ is the hash of the message, and x is the sender's private key. The pair (r, s) is the digital signature, which is sent along with the message m to the recipient. In signature verification process, the recipient checks that r and s are valid numbers

$$0 < r < q \text{ and } 0 < s < q;$$

If not, the signature is invalid. If valid, the recipient computes

$$w = (s')^{-1} \bmod q$$

w is the modular inverse of s'. It will assist in reversing the impact of s' during the verification procedure. u_1 scales the hash of the message using w and make sure that, the original message content contributes to the verification process

$$u_1 = ((H(m'))w) \bmod q$$

and u_2 is connected with r', which is the component of the signature that is obtained from the sender's private key.

$$u_2 = ((r')w) \bmod q$$

where s', m' and r' are the received values. And

$$v = (((g)^{u_1}(y)^{u_2}) \bmod p) \bmod q.$$

If $v = r'$, the signature is valid and signature verifies that the message was transmitted by the owner of the private key and has not been altered. If $v \neq r'$ the signature isn't trustworthy, it's possible that someone altered with the message, signed it incorrectly, or transmitted it as someone else [116].

4.3.1 Methods for digital signatures regularly used

The popular algorithms of digital signatures in blockchain are RSA, DSA, and ECDSA. As these algorithms will demonstrate, security, decentralization, and transparency can be delivered across multiple domains, including finance, particularly in the form of cryptocurrencies, and the healthcare system [122]. In healthcare delivery, electronic

signatures are very important because of their use in the development of other processes and the law. Several purposes have been incorporated by the healthcare organizations in the use of the digital signature solutions, including the generation of a disability report online or electronic submittance [123]. This means that digital signatures within healthcare have to consider technical and legal as well as organizational factors [124]. Different digital signature algorithms that are used in healthcare settings are RSA, Lamport, ECDSA, and EdDSA, but all of them function differently [125].

The RSA algorithm is probably the best-known public-key cryptosystem published in 1977, which uses the basic idea based on number theory, such as Fermat's Little Theorem [126]. It relies on public and private keys for encryption and decryption, which are based on modular arithmetic and prime numbers, accordingly. Since it is difficult to factor big non-prime numbers into their prime factors, the technique is secure [127]. Here are the three steps: generating keys, creating signatures, and verifying signatures are followed [125],[128],[129].

- Generate RSA Key Pairs

Public key $\big(VK = (n, e)\big)$ for encryption and signature verification.

Private key $(SK = d)$ for decryption /signature creation.

Input	Security parameter $\boldsymbol{l}$, which determines the size of the keys (2048 bits)
Generate Primes	Randomly select two large prime numbers p and q each with l / 2 bits.
Compute Modulus $\boldsymbol{n}$ and Euler's Totient Function $\boldsymbol{\phi}$	$n = p \times q$ $\phi = (p - I) \times (q - 1)$
Select public exponent $\boldsymbol{e}$	$1 < e < \phi$ and $\gcd(e, \phi) = 1$
Compute Private Exponent $\boldsymbol{d}$	$1 < d < \phi$ and $ed = 1 \bmod \phi$
Returns	(n, e, d)

- RSA Signature Generation

Create a digital signature s for a message m to ensure authenticity and integrity

Input	Public key $(\boldsymbol{VK} = (\boldsymbol{n}, \boldsymbol{e}))$, Private key $(\boldsymbol{SK} = \boldsymbol{d})$ *and* message $\boldsymbol{m}$
Hash the Message	$h = H(m)$, H using a cryptographic hash function (SHA-256)
Sign the Hash	$s = h^d \bmod n$
Returns	(s)

- RSA Signature Verification

Verify whether a signature s on a message m is valid.

Input	$(\boldsymbol{VK} = (\boldsymbol{n}, \boldsymbol{e}))$, received message $\boldsymbol{m}$ and signature $\boldsymbol{s}$.
Hash the Message	$h = H(m)$, using the same hash function as in the signing process.
Verify the Signature	$h' = s^e \bmod n$ using the public key e,
Check Validity	If $h = h'$, the signature is valid, the output is Accept the signature Otherwise, the output is "Reject the signature

Distributed Attribute-Based Signature (DABS) has the following benefits over RSA and ECDSA signature schemes in health care applications. DABS offers confirmation of EHR data and the signer's identity while keeping the identity of the signer secret [130]. DABS is decentralized to avoid risks related to single points of failure that occur in centralized systems[131]. DABS advocates for attribute-based access control to fine-grain authorization of healthcare data. It also enables flexible updates of attributes and uses blockchain to achieve better verifiability [132]. While it is shown that ECDSA has higher performance and security even with a smaller number of keys than RSA [133], extra features related to healthcare needs are offered by DABS. One of them is server-aided computation to reduce the burden on resource-limited devices [131] and protection against inference attacks that threaten user anonymity in the pseudonym-based systems [130].

In their paper A Decentralizing Attribute-Based Signature for Healthcare Blockchain, Sun et al. come up with a Decentralized Attribute-Based Signature (DABS) algorithm. In the DABS proposed by the authors, users get attributes and private keys from several authorities that belong to different organizations. Every user in the system has a universally unique identifier

(GID), which brings the keys given by different authorities to the same user. The structure of the DABS algorithm is seen below.

- Global setup

The system generates a composite-order (N) bilinear group G, which is a group where cryptographic operations can be performed efficiently. The group is formed according to the specified security input parameter λ with generator g. Upon the establishment of the bilinear group, the global public parameters GP are formed.

$$GP = (N, g)$$

a cryptographic hash function H that associates a user to its global identity (GID) to an element in G. G, maintaining the identity of users without revealing the actual identity of the users. Key creation, signing, and verification are all part of cryptographic operations that are laid out in the Global Setup. The hash function is employed to securely map each user's identity to the group. This phase is very important because it provides the level of privacy, proper handling of the user identities, and attribute-based authentication in a decentralized environment.

- Authority Setup

The authority setup phase is to be held for creating signing keys (SIK) and the verification keys (VK) for each attribute i. The described process provides the cryptographic mechanisms for attribute-based signing. Here the input is global public parameters GP. For each attribute i, the algorithm selects random values α_i and y_i from a mathematical space $\mathbb{Z}_N$ (a set of integers modulo N). The verification key (VK) for attribute i is calculated as:

$$VK = \{e(g, g)^{\alpha_i}, g^{y_i} \forall i\},$$

here $e(g, g)$ is a bilinear pairing used for cryptographic computations and signing key for attribute i

$$SIK = \{\alpha_i, g^{y_i} \forall i\}.$$

- Key Generation (KeyGen)

Input GP, GID, Attribute i and the signing key SIK generated in the previous step

$$(GP, GID, i, SIK) \rightarrow SIK_{i.GID}\ ),$$

The authority uses the user's GID to create an attribute-specific signing key

$$SIK_{i.GID} = \{ g^{a_i} H(GID)^{y_i} \forall i \}.$$

here, $H(GID)$ is a cryptographic hash function that performs a function mapping of the user's global identity to a value in the required mathematical space.

- Signing Algorithm (Sig)

A user then signs a message M based on their attributes by using the signing keys. It guarantees that the signature confirms the attributes of a user without necessarily exposing his identity.

$$\left(GP, M, (A, \rho), \{SIK_{i,GID}\}\right) \rightarrow \sigma$$

Here input, GP Global parameters, M message to be signed, A is the access control matrix defining the attributes required for signing, ρ mapping of matrix rows to attributes and $SIK_{i,GID}$ generated for the user's attributes. In process, randomly select $s \in \mathbb{Z}_N$ and a vector $v = \mathbb{Z}_N^l$.where l is the number of attributes. For computing, $\lambda_x = A_x \cdot v$, whereA_x is the x-th row of A. $\omega_x = A_x \cdot \omega$, ω with being a random vector where the first element is 0. r_x a random value for each rowA_x where $r_x \in \mathbb{Z}_N$.Now let's compute the signature components

$$s_{ig_0} = e(g, g)^{sH'(M)},$$

this is the first part (s_{ig_0}) of the signature, which combines a cryptographic pairing $e(g, g)^s$ (using the group generator g) with the hash of the message $H'(M)$. It ensures that the signature is tied to the message M.The second part ($s_{ig_{1,x}}$) of the signature is specific to the user's global identity (GID) and includes randomness r_x to ensure security

$$s_{ig_{1,x}} = H(GID)^{r_x},$$

the third part of the signature is ($s_{ig_{2,x}}$) and this is the complex part incorporating cryptographic pairings of the message, attributes (λ_x, ω_x) and user identity. Validation terms related to the user's signing keys ($\alpha_{\rho(A_X)}, y_{\rho(A_X)}$) and attributes mapped from the access matrix A_X. It computed as

$$s_{ig_{2,x}} = \frac{e(g, g)^{\lambda_x} . e(H(GID), g^{\omega_x}}{e\left(g^{\alpha_{\rho(A_X)}}, g\right), e(H(GID)^{y_{\rho(A_X)}}, g^{r_x})}.$$

These three components are then integrated into creating the full signature

$$\sigma = \left(s_{ig_0}, s_{ig_{1,x}}, s_{ig_{2,x}}\right).$$

- Verification Algorithm (Ver)

The verifier checks that the signature is indeed a legitimate one and the signer satisfies the attributes defined in the access control matrix A

$$Ver\left(GP, M, \sigma, \{VK\}, (A, \rho)\right) \rightarrow \{0,1\},$$

here as an input GP global parameters, the signed message M,signature σ, verification keys $\{VK\}$ which corresponding to attributes, access control matrix A and mapping ρ. The Ver algorithm calculate c_x by the access matrix A

$$\sum_x c_x \ A_x = (1,0,\ldots.,0).$$

c_x is a constant and then hash the message $H'(M)$ and finally check the verification equation

$$s_{ig_0}{}^{\frac{1}{H'(M)}} = \prod_x (e(g,g)^{\alpha_{\rho(Ax)}} \cdot e\left(s_{ig_{1,x}}, g^{y_{\rho(Ax)}}\right) \cdot s_{ig_{2,x}})^{c_x}.$$

If the equation is hold, the signature is genuine and the verifier will output 1. Otherwise, the signature is invalid [130].

4.3.2 A New Concept in Digital Security: Quantum-Immune Keyless Signature Systems

Current studies show that various forms of electronic signatures require quantum-resistant cryptographic techniques for secure communications. Some of the existing traditional public key infrastructures (PKI) have become vulnerable to security threats due to recent drifts in quantum computing [134],[135]. In response to this, post-quantum cryptographic (PQC) techniques are being designed and tested for their applicability in preserving evidential value for the long term [136]. Another recommendation focuses on the utilization of CrystalsDilithium, which is a lattice-based algorithm, and Long-Term Validation (LTV) to validate documents over time [134]. Another technique adds quantum resistance to classical digital signature algorithms through the use of zero-knowledge proofs, which can ensure

cryptographic protection as well as compatibility with future post-quantum environments while keeping compatibility with prior pre-quantum environments [137]. Ahto Buldas, Risto Laanoja, and Ahto Truu, the authors, explain how current electronic signature systems suffer from centralized key management, the requirement for large, hard-coded secret keys, and the vulnerability to quantum attacks. These systems are vulnerable to compromise resulting from technical breakdowns or human errors and rely on the PKI model that brings problems such as revocations and verification. Some of the harms include while traditional cryptography tools are vulnerable to attacks resulting from quantum computation, such as in the RSA algorithm. It emphasizes the problem of obtaining the necessary high degree of long-term verifiability and non-repudiation in today's systems, with a special regard to the constantly growing possibility of quantum attacks.

In view of these concerns, the authors have designed a quantum-immune, keyless digital signature system utilizing hash functions and Merkle hash trees. This server-assisted strategy does not require the use of trapdoor one-way functions and is thereby immune to quantum attacks, but the integrity of the signatures remains compromised. The scheme enables constructing small, checkable signatures without requiring interactions with other peers. The proposed system is expected to offer a viable, more efficient, and sustainable substitute to conventional digital signatures through the use of client authentication, timestamping, and hash-based solutions.

It starts with overviews of typical signature approaches, which are based on the usage of private-public key pairs from conventional cryptography. These systems rely on independent third parties to authenticate the signature, that is, Certification Authorities (CAs) and Time-Stamping Authorities (TSAs). However, they have problems such as key revocation complexities, require multiple trusted entities, and quantum-computational attacks to trapdoor one-way functions like RSA. It also introduces quantum computing as a growing threat to traditional cryptographic systems, with algorithms like Shor's capable of breaking RSA and Grover's reducing the security of hash functions. Nevertheless, hash functions continue to hold their defenses pretty well against quantum assault. Moreover, it also describes hash-tree digital signature schemes in which Merkle trees are employed to construct succinct and elegant data signatures. These schemes ensure the data's auxiliary state is hashed and its integrity published in a globally verifiable manner. New concepts such as hash calendars and the Keyless Signature Infrastructure (KSI) are also defined, illustrating their use for assigning tamper-evident digital signatures that are both scalable and verifiable by any third party. This

model explores the trust problems and limitations of server-based signature systems, the importance of verifiable client authentication, and quantum-immune approaches.

A Merkle tree combines multiple inputs $x_1, x_2, \ldots\ldots, x_N$ into a single root hash r through recursive hashing. For example, given leaves x_1, x_2, x_3, x_4 the intermediate hashes are $r_{12} = h(x_1, x_2)$ and $r_{34} = h(x_3, x_4)$ and the root $r = h(r_{12}, r_{34})$. To verify that x_1 is part of the tree, the verifier uses x_2 (its sibling), r_{34} (subtree hash), and r (root hash). The security of the aforementioned scheme relies on a collision resistant hash function h and it make sure that, no two distinct inputs $x \neq x'$ produce the same hash value $h(x) = h(x')$.Data signature is a means of data protection, and in this scheme, a Merkle tree is used to provide data integrity. Merkle hash tree produces a root hash r which is then made available as a trust anchor and it acts as a secure summary of all the data. Each data record x_i is signed by including its path to the root which makes verification without needing the entire tree. In signature verification, verify x_i using its path $\{x_j, r_k\}$ in the tree. The signatures are stylized by compact proofs (hash chains) that enable the verification procedure that takes $O(logN)$ time and guarantees the data's non-tampering without points to secret keys. A specific kind of a hash tree is the hash calendar, where the tree is ordered by time; thus, it is possible to assign a certain data point to a certain timestamp in a rather effective and even secure manner.

This is fortified in keyless signature schemes by incorporating identities into the global hash tree using further authentication details such as one-time hash-password chains. These chains are generated as, $z_{i-1} = h(z_i)$, It arose where each password is valid for only a predefined time $t_0 + i$.This precludes even if a password is compromised from being used wrongfully. It does not use trapdoor functions, and that makes the scheme quantum resistant. The incorporation of server-based structures and efficient search methods makes signatures still admissible for independent checks while solving trust problems by means of time-limited proofs and strong identities. Binding is also used. This combination makes the signatures compact, scalable, quantized, and secure for the long-term application requirement.

In their article, in the "3 New Keyless Signature Scheme" section, the author describes a signature technique that does not require the regular cryptographic keys, which makes it safe from quantum attacks. The scheme used one-time password chains together with Merkle hash trees in order to produce compact and efficient signatures. A client creates a random seed z_N and derives a sequence of one-time passwords $z_0, z_1, \ldots., z_N$ using $z_{i-1} = h(z_i)$. The root hash r of the Merkle tree, along with z_0 serves the public key. To sign a document M, the

client computes $m = h(M)$, combines it with a one-time password z_i and it makes $x = h(m, z_i)$ after that send x and their identity to the server. The server places x to a Merkle tree, time-stamps it, and returns the signature. This makes sure that the signature is of high authenticity by checking that z and its hash chain leads to the tree's root r and confirming $t = t_0 + i$. Finally, the scheme is logically secure since each of the passwords can only be in a usable state during the time slot assigned to it; hence, it cannot be reused or even exploited. It is compact, with $O(logN)$ sized signatures and efficient verification. With the elimination of trapdoor functions, the scheme remains quantum resistant and free from secret keys, offering thus a comprehensive means for long-term digital signatures [138].

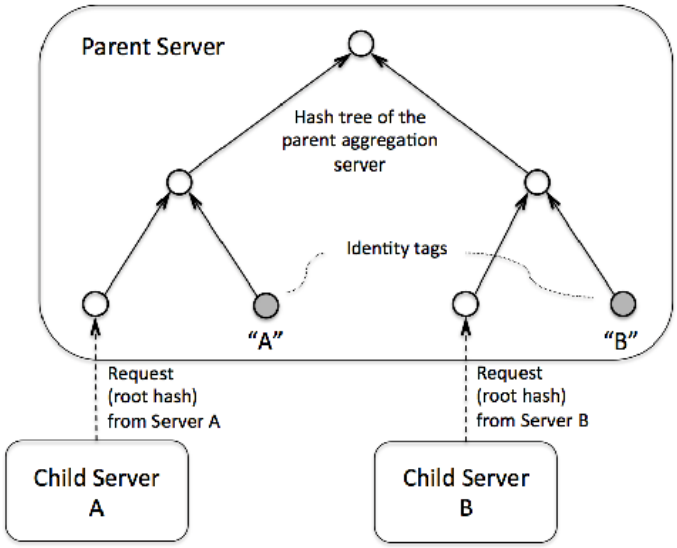

Figure 4 Identifications in keyless signatures [138].

4.4 Consensus algorithms

Consensus algorithms are very vital in the accomplishment of security and the functionality of blockchains as far as reaching general agreement on the state of the network [139],[140]. Three consensus algorithms currently gain widespread usage in blockchain technology, which include Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS) [139]. These algorithms also exhibit differences in resource demands, including computing assets and connected nodes [141]. Different consensus models have been proposed for the healthcare sector, such as proof of work, practical Byzantine fault tolerance, and proof of authority [142]. There are researchers who have suggested the development of more adaptive consensus methods that will enhance the reliability and security of IoT-based systems in healthcare [143]. Reputable blockchains are resistant to two problems. As to Byzantine

generals and double expenditures, there are two questions. However, these problems may cause the blockchain network to fail when an attacker acquires more than 51% of network power. Therefore, the consensus method needs to be well designed to avoid such kinds of assaults [144].

4.4.1 Importance of Consensus

The term ‘blockchain’ is used for the distributed digital ledger database that has details arranged in blocks one behind the other and has a timestamp and link to its previous block [145]. Its structure contains a number of blocks, and each block has a hash value that relies on the previous block, and thus to change data, one has to change the following blocks, which is virtually impossible. This makes the system very secure and impossible to hack because even when one key is lost, the entire structure remains intact [146]. The blockchain is governed by decentralized computers known as nodes that monitor transactions and endorse documents that parties have explicitly consented to use in contracts or funds. In order to keep the distributed ledger in consensus, only certain nodes known as miners approving transactions and adding blocks onto the chain adhere to rules for consensus [147]. Often transactions pass through digital signatures and inter-node checks before being hashed and bolted into the blockchain through a consensus process. This procedure prevents conflict and ensures that all the nodes always update in a like manner. The process, however, begins with the creation of the genesis block. Blockchain systems in real-world industries are dependent on consensus techniques to handle problems like Byzantine faults and the double-spending problem [144].

The classification of blockchains has been made as public, private, or consortium blockchains with interfering characteristics [148]. Nowadays, consensus algorithms are divided into three categories. When categorized by the nature of the blockchain, the consensus models described here can be classified as public blockchain consensus, private blockchain consensus, and consortium blockchain consensus [149]. Permissionless public blockchains are decentralized systems available for anyone with internet access. Typical applications include cryptocurrency mining and trading and are mostly used Consensus algorithms: Proof of Work (PoW), Proof of Stake (PoS) and Delegated Proof of Stake [150]. Private blockchains, on the other hand, are more controlled or limited to an organization and are exclusive to users within an organization, along with being a closed system for an organization’s internal use only [93]. Consortium blockchains are somewhat decentralized, operated by several organizations, and used in industries such as the healthcare, insurance, and finance industries. As a result, the

public blockchains, although providing high levels of transparency and security, may not be altogether appropriate for corporate use; thus the private and consortium blockchains are more appropriate for specific organizational requirements [144]. Blockchain in healthcare is being implemented through consortium blockchain to enhance the issues of data sharing and management. It allows for two or more healthcare providers to undertake business on the same system for secure transactions, as well as the exchange of information about electronic health records (EHRs) [151]. Health care-oriented consortium-based blockchains have superior resource utilization ratios and transaction throughput rates compared to public and private blockchains [152]. These systems usually use methods such as attribute-Based encryption and the interplanetary file system (IPFS) that provide high levels of security and privacy when managing data [153],[151].

Table 2 Blockchain categorization comparison [149].

	Public blockchain	**Private blockchain**	**Consortium blockchain**
Centralization	No	Yes	Yes
Consensus	POW	RAFT	PBFT
Participant	Everyone	Control center decision	Designated members
Benefit	Accessible to all users and simple to implement.	No threat of assault and energy consumption is very low.	Access regulation and significant scalability.
Drawback	Excessive energy usage	Node restricted	Conspiracy attack

4.4.2 The Use of Blockchain Consensus Algorithms in Healthcare

New studies look into the use of Practical Byzantine Fault Tolerance (PBFT) consensus toward healthcare decentralized systems. A well-known consensus algorithm in the blockchain family is the Practical Byzantine Fault Tolerance algorithm (PBFT) that outperforms traditional solutions based on the Byzantine fault tolerance idea [154].

- **PBFT Algorithm**

PBFT is a consensus mechanism designed to solve the Byzantine Generals Problem in a distributed system. It involves three main protocols:

1. Consistency Protocol, which checks for consistency of data that is located in the distributed nodes, and it operates in three stages. The stages are Pre-Prepare, Prepare, and Commit. In Pre-prepare the primary node broadcasts the message, and the message format is <Pre-prepare, view, n, digest>. View is the view number of the request message, n is the proposal number, and the digest is the digital digest of the request message. In the Prepare stage node send, this message <Prepare, view, n , digest, i > to others if the Pre-prepare message is valid. i is the number of the replica code. All nodes broadcast <Commit, view, n, digest, i > when they receive $2f + 1$ valid prepare messages. As a whole, the function of the master node is to receive request information from the client; if the check passes, the master node relays the request to all other replica nodes in the system.

2. In the View-Change Protocol consensus mechanism Triggered when the primary node fails and a new primary node is selected, changing the view number, and the view number shifts from v to v+1.

3. In Checkpoint Protocol, removes the size of logs by deleting data that has been validated by a consensus algorithm and guarantees the system's coordination even with network or node perturbation.

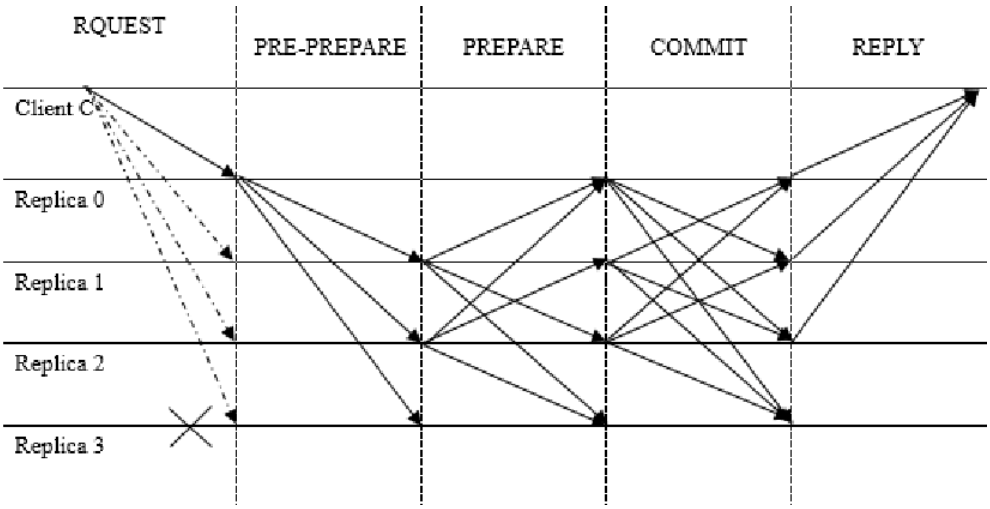

Figure 5 PBFT algorithm execution process [155].

Figure 5 represents the PBFT algorithm, which includes the request process, pre-prepare, prepare, commit, and reply process. Among them, Replica3 shows the information that the node is faulty and cannot send/receive any messages.

- **Drawbacks of PBFT**

As it was explained earlier, the PBFT algorithm, which is for the consensus in the distributed systems, has certain drawbacks. It has a high communication cost, which grows quadratically, using $2N(N-1)$ messages in the consensus process, which is not efficient with a large number of nodes. Additionally, if all nodes are not functioning optimally, then its fault tolerance is up to one-third of the total nodes; the system only works efficiently if less than one-third of the nodes are faulty. Furthermore, PBFT does not have a mechanism for choosing trusted master nodes, which means that it is possible for the wrong nodes to be selected as master nodes so that they compromise the efficiency and security of the system [156].

Nonetheless, PBFT has issues when dealing with larger numbers of nodes in terms of communication growth [157]. In response to this, several improvements have been proposed by researchers. Example includes the adoption of voting methods for categorizing nodes and enhancing the consensus process [158], the adoption of dual random selection methods for forming consensus groups [157], and the minimization of the phases of consensus to reduce the complexity of the algorithm [158]. Although the PBFT algorithm is highly efficient in terms of fault tolerance and throughput, it has its disadvantages, such as the potential misbehaviour of the primary node, besides coming with high network communication overhead. Current research is focused on improving PBFT efficiency and security and its ability to be applied in various types of blockchains [149].

Based on this, Pang et al. introduced an organization-controlled EHR sharing system using a node-state-checkable PBFT algorithm to advance the handling capability and decrease consensus latency [159]. Hegde & Maddikunta propose a PBFT-based lightweight secured blockchain for healthcare management using the Eigen Trust model and Verifiable Random Function (VRF) [160]. This consensus algorithm can be powerful for networks up to 70 nodes, block sizes of 5-20 transactions, and data generation periods of 5-10 seconds. This makes PBFT relevant for most types of IoT systems, such as implanted medical devices and telemedicine devices that are completely self-contained. [161]. The next section outlines some enhancements made on the PBFT's algorithm.

- **Reputation-based Byzantine Fault Tolerance (RBFT)**

One of the most utilized consensus algorithms in consortium blockchains is the Practical Byzantine Fault Tolerance (PBFT), which originally takes time to recognize a compromised

node as faulty and has a weakness for cyber-attacks on the primary node. Equal voting rights for consortium members could also not work in situations when weighted decision-making is necessary. To overcome these drawbacks, the proposed Reputation-based Byzantine Fault Tolerance (RBFT) algorithm is introduced. The RBFT protocol is faster and more efficient than the PBFT protocol in terms of average throughput, which also increases by 15%; delay, which decreases by 10%; and reduced rates of faulty node participation in the network over time, indicating better performance and security [162].

- **Proof of Authority (PoA)**

Proof of Authority (PoA) is a kind of consensus permissioned blockchain algorithm whose relevance has risen to the popularity of blockchain. Because of performance improvement with respect to the usual Byzantine Fault Tolerant algorithms. Proof of Authority (PoA) depends on a set of N trusted nodes. known as authorities, each identified by a unique ID. The system expects at least a majority, precisely at least $\frac{N}{2} + 1$ of those authorities are honest so as to guarantee a reliable consensus and the generation of blocks in permissioned blockchains. In the healthcare overlay network, the nodes are grouped into clusters where the elected leaders are the Cluster Heads (CHs), responsible for the public key for the healthcare providers or patient devices to ensure protected transactions [163].

- **Modified PBFT (mPBFT)**

PBFT has a fault tolerance of up to 33% and may ensure the accuracy of a block creation by broadcasting messages to all nodes multiple times, but this may lead to the network connection slowing down if many nodes are participating in the connection [164],[165]. Youn-A Min develops the modified Practical Byzantine Fault Tolerance (mpBFT) algorithm as a development of the standard PBFT. This modification is intended to address some problems of PBFT, especially in private blockchains where nodes are often believed to be trustworthy.

The mPBFT consensus process requires a primary node to start the consensus process delegated to the leader node and, at the same time, inform all nodes that the process has commenced. In the case of high-importance messages, the leader nodes get cross-verified through a very intensive process mainly taking a computational cost of

$$(N/3) \times (N/3) + \frac{N}{3} = N^2/9,$$

to ensure the validity of the messages. Generally, it is given to the leader node for consensus, and the leader nodes go through the process of delivering it to the primary node, which incurs a computational cost of

$$N / 3 + N / 3 = 2N / 3.$$

This modified approach significantly improved computational cost when the conventional PBFT computational cost is $2N^2$. Consensus node ration in modified PBFT

$$2/N = 3f + 1.$$

N represents the total number of nodes and f error nodes and fault tolerance ≥ 16.66 %.That means while PBFT sacrifices 33.3% of nodes, mPBFT reduces this to 16.7%. It is also shown that in mPBFT Network Communication Cost (NCC), it significantly minimizes than PBFT, While PBFT cost $2N^2$ but mPBFT need $\frac{2N}{3} + \gamma$ and $\frac{N^2}{3} + \gamma$, here γ The computational cost is associated with the frequency of use (α1) and the reliability of the institution (β1). To increase the number of nodes, mPBFT achieves higher Transactions Per Second (TPS) compared to PBFT [166].

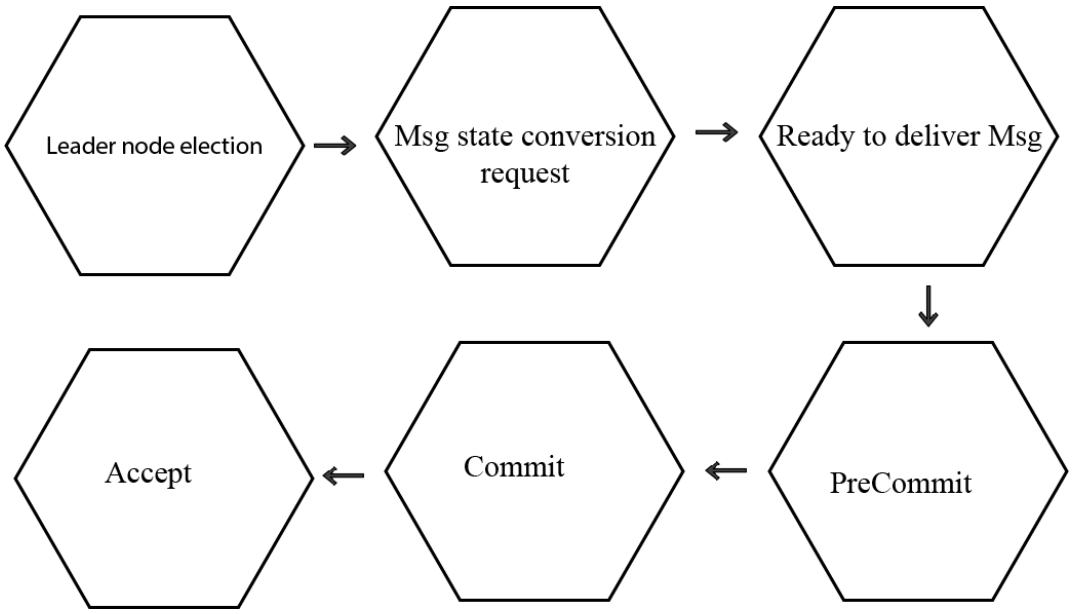

Figure 6 Diagram illustrating the mpBFT processing [166].

This paper presents Youn-A Min's mPBFT as an improvement over PBFT in scalability, efficiency, and resilience in private blockchain networks. By minimizing communication costs, introducing a flexible algorithm for a safer and faster method of managing internodal data, and improving leader node selection, mpBFT provides a more practical solution for

environments with trusted participants, such as government agencies or inter-organizational networks, or in healthcare also.

- **Trust Mechanism (TM-PBFT) Algorithm**

A trust mechanism is introduced by TM-PBFT, and it consists of

1. Trusted Node Voting

In Trusted Node Voting Cycle V, and All N nodes vote for trusted candidates. Trusted nodes build a subset N_T and the one trusted node becomes the master node ($N_M = 1$). Trusted nodes selected by ordinary nodes. In vote distribution, each node i receives n_i votes and satisfy

$$N = \Sigma_{i=1}^{\pi} n_{i.}$$

Top node, which is denoted by H, the top H nodes are chosen based on their highest n_i values.

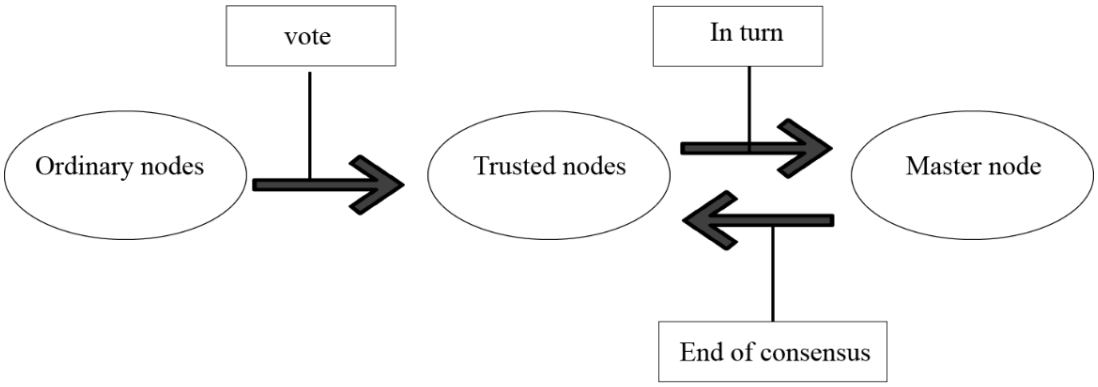

Figure 7 The TM-PBFT algorithm's network model [156].

2. Trust Degree Modelling

In the TM-PBFT algorithm, a voting period V includes multiple consensus periods T, and the number of consensus periods can be either adjusted. The consensus period T is also divided into several intervals t and the packaging of a block occurs within one interval t.The trust degree of node i in the current production interval t is defined as $Cr(i)_{pro}$.Trust $Cr(i)_{pro}$ comprises three components. One is voting trust $Cr(i)_{vote}$

$$Cr(i)_{vote} = \frac{n_i}{N}$$

where, N is the total number of votes and in the current voting period, node i collected number of votes n_i.Another one is performance trust $Cr(i)_{beh}$

`

$$Cr(i)_{beh} = \sum_{x-1}^{n} f(x) - \alpha \times \sum_{x-1}^{n} g(x).$$

Where, n is the number of consensus processes when node i has engaged in during the current voting period V. $f(x)$ indicates correct actions (1 for normal, 0 for abnormal) and $g(x)$ indicates malicious behaviour (1 for malicious, 0 otherwise) in each production interval t. A penalty factor α is used, where α = 1 in case the normal actions are more common than the malicious ones and increases in case those are more frequent in order not to reward negative behaviour. The final one is Accumulated Trust $Cr(i)_{acc}$ which is depends on the accumulated trust degree of node i as of the end of the last voting period, which is designated here as V-1

$$Cr(i)_{acc_v^1} = Cr(i)_{pro_{v-1}^{last}}.$$

Combined trust,

$$Cr(i)_{pro} = \lambda_1 \times Cr(i)_{vote} + \lambda_2 \times Cr(i)_{beh} + \lambda_3 \times Cr(i)_{acc}$$

where, λ_1 λ_2 λ_3 are weights ($\lambda_1 + \lambda_2 + \lambda_3 = 1$). λ_1 is voting parameter, λ_2 is the performance parameter and λ_3 is the growth parameter.

3. Reward and Punishment via Shapley Value

The TM-PBFT assigns penalties and rewards to its master node and to other nodes that vote for this node, therefore guaranteeing that all nodes vote for credible candidates. Voting nodes work collectively, not competitively. They unite to elect a single master node; the model is a cooperative, which is denoted as $\big(N, V(S)\big)$. where N represents voting nodes, S is a subset of cooperating nodes, and $V(S)$ denotes their collective benefit. In addition, the algorithm employs the Shapley value in providing each alliance's member with a recompense proportionate to his contribution, ensuring that every member inclines towards accountable behavior instead of destructive actions. The Shapley value awards the reward in a fair way and makes certain that no single player receives all the credit all the time. The Shapley value has a specific formulation written as an equation

$$\delta_i(S) = V(S \cup \{i\}) - V(S).$$

where, $\delta_i(S)$ The marginal contribution of node iii to the alliance S , $V(S)$ The total benefit of the alliance S without node i and $V(S \cup \{i\})$. The total benefit of the alliance after including node i.There will be an incentive for nodes to provide great input as rewards depend on the contribution of the node upon the benefit of all possible strategic partnerships, improving equity fundamentally. The Shapley value φ_i, which determines the fair share of a node i based on its contribution to different alliances in a cooperative game

$$\varphi_i = \sum_{i \in j} \delta_i(S_i(j))/N!.$$

The Shapley value for node i , calculated by summing its marginal contributions across all S subsets of the node set N. Each marginal contribution is analyzed with respect to the probability of S occurring in all possible orderings of the nodes. The reward is allocated to node i based on its contribution.

$$E_I = E \times \varphi_i$$

E is the total reward for distribution after a successful consensus in TM-PBFT. Time factor adjustment helps to take into account both the proactivity and punctuality of nodes, which promptly provide support to the reliable master nodes and at the same time, penalizes those who make delays from a self-interested point of view. This would lead to having a better, faster, and efficient consensus mechanism for decentralizing trust

$$Reward_{adjusted} = \varphi_i \times T_f.$$

where, T_f is time factor.

The TM-PBFT algorithm is better with communication efficiency than the PBFT algorithm, as the number of rounds required for the voting and consensus are reduced, and the communication space needed for voting is minimized; also, TM-PBFT achieves higher throughput

$$TPS = \frac{N_{transaction}}{\Delta t}.$$

This is due to higher reliability in the node section and reduced communication complexity [156]. While compared with its predecessor PBFT, TM-PBFT makes enhancements in communication expense, expansibility features, fault resistance, and security. TM-PBFT

improves the efficiency and security and actively adapts to large-scale blockchain systems using a trust mechanism, dynamic node election, and a fair reward/punishment system.

4.4.3 Overview of current PBFT consensus methods

Several works that focus on the performance evaluation of various consensus algorithms in the context of distributed healthcare blockchain systems have been reviewed to illustrate their feasibility and deployment depending on required characteristics [167]. Pawan Hegde and Praveen Kumar Reddy Maddikunta briefly review the current PBFT consensus algorithms [160], which are described below.

Table 3 Overview of current PBFT consensus methods [160].

Consensus Algorithm	Security	Privacy	Overhead	Remarks
Geographic-PBFT	MID	MID	HIGH	G-PBFT represents a location-based consensus protocol that employs fixed IoT nodes as part of its scalability model, Sybil attack protection, and performance improvement. The system minimizes consensus time and network load.
EPBFT	MID	LOW	HIGH	EPBFT extends PBFT to address issues in dynamic networks, communication overhead, and Byzantine nodes. It does not deeply assess node dependability.
Reputation-based PBFT	MID	LOW	MID	This model selects nodes with high reputation values and

Consensus Algorithm	Security	Privacy	Overhead	Remarks
				prioritizes them in the voting process.
HRPBFT	MID	MID	LOW	Uses a hash ring to categorize nodes and selects the primary node from defined groups.
MBFT	HIGH	MID	LOW	MBFT applies a two-layered consensus method using sharding and layered technology.
Trust PBFT	HIGH	MID	LOW	T-PBFT is an optimized PBFT variant that uses the EigenTrust model to improve blockchain environment stability.

4.5 Smart contract

The use of smart contracts built on blockchain technology was found to present solutions to some of the issues facing the healthcare domain, such as data protection, privacy, and integration [168],[169]. Smart contracts can help to create decentralized applications (DApps) that interact with a blockchain for multiple applications in healthcare, like multi-center clinical trials and pharmacovigilance [169]. Smart contracts are tamper-resistant digital programs, self-executable, self-actualizing contracts that execute transactions on a blockchain without involving third parties [170],[171]. Based on distributed consensus networks, operate on the premise of trustless transactions of digital assets or information [171]. Smart contracts have brought the idea of using blockchain beyond the realm of cryptocurrencies with various usage in industries such as healthcare, IoT, supply chain, and so on [172].

4.5.1 Smart Contract Engineering (SCE)

Smart Contract Engineering (SCE) can be described as a relatively novel architecture concept designed to further develop the creation of smart contracts [173]. It applies software engineering, mathematical measures, legal axioms, and algorithms in a way that minimizes mistakes in contract drafting. Theorem proving, symbolic execution, model checking, and other formal specification and verification methods are used in SCE to find vulnerabilities and make sure of its accuracy [174],[175]. These methods are essential in the handling of security threats and developments linking to smart contracts. The process incorporates requirements specifications crafted in an informal manner, the use of a set of formal mathematical descriptions, and the creation of models accompanied by their transformation into models that are refined from a set of given transformations [173]. Another key concept for SCE is legal compliance as well as automatic code generation through checked models. When smart contracts crop up in a number of industries, formal methods become rather essential for mitigating hazards and excluding probable costs [176]. Kai Hu, Jian Zhu, Yi Ding, Xiaomin Bai, and Jiehua Huang also describe the smart contracts in terms of formal models and show how mathematical models are used in the smart contract formalization and analysis. To describe and analyze the behavior of a smart contract, the authors use finite state machines (FSM), known as automata as follows [173].

A. The Smart Contract: A Detailed Explanation

1. Smart Contract Model

A smart contract C is defined as

$$C = (I, M^*\{M_1, M_2, \dots M_m\})$$

where, I represents the Information about the contracting parties, M^* The overall contract automata represent combined individual contract execution automata $\{M_1, M_2, \dots M_m\}$. Contract automata M^* is a quintuple

$$M^* = (Q\ \Sigma, \delta^*, s^*,\ F^*\ )$$

where, Q is the set of all states of the contract execution

$$Q = \{(q_1^*, q_2^* \cdot \dots q_m^*), L\}$$

where, L may contain information about the execution background or context for the contract or be in the form of the current state of the contract, past transactions, or external conditions influencing the contract execution. $(q_1^*, q_2^* \cdot \ldots q_m^*)$ This is a set of states where each state q_1^* corresponds to a particular contracting party P_i. Σ is the set of possible input events that cause a transition of the state. An input event could be an event of action or condition to happen, such as receipt of payment, confirmation of delivery, submission of documents etc. δ^* represents the collection of transition functions. The transition function δ specifies the system proceeds from one state to another based on input, and it could be written as,

$$\delta^*: Q \times \Sigma \to Q.$$

This means the transition function takes the current state from Q and an input event from Σ and it outputs a new state in Q . Transition function guarantees that the conduct of the contract shifts when a particular event is activated by the party or circumstances. s^* stands for the starting state of the corresponding contract automaton meant to determine the beginning of the contract's implementation. The initial state s^* must be one of the states from the set Q.

$$s^* \in Q$$

F^*refers to the end situations for the contract, which are the states where the contract will be brought to a close. These states are a subset Q

$$F^* \subset Q$$

M_i is the contract execution automaton for contracting party P_i, which is represented as a quintuple

$$P_i = (q_i, \Sigma, \delta_i, s_i, F_i),$$

where, F_i The set of termination states for party P_i . All contract execution automata $M_1, M_2, \ldots \ldots, M_m$ for each party $P_1, P_2, \ldots \ldots, P_m$ share the same set of input events Σ. This makes sure that the actions and transitions among all parties are synchronized and triggered by the same events.

In simple terms, the contract automaton works by having many states that capture the conditions of the contracting parties. This it does according to input events, which drive the

contract's flow. The contract is formed and initially established without being terminated until it reaches one of the defined termination states. Coordination to model the dynamic behaviour of the smart contract by simply controlling and regulating all the actions and transitions.

2. Transaction Model

The transaction model describes how transactions and their elements are located in the Smart Contract System architecture. Transaction is a basic form of processing in the smart contract system characterized by the term T . It is the process of transferring data or assets from one party to another. A transaction T can be represented

$$T \equiv \langle T_f, T_t, T_p, T_n, T_v, T_r, T_d \rangle.$$

Where every element of the tuple means a different part of the transaction. T_f : from -It refers to the address of the sender in the transaction, which is a 20-byte address $T_f \in \mathbb{B}_{20}$, $\mathbb{B}$ stands for character sequence. $\mathbb{B}_{20}$ stands for a 20-character sequence. T_t : to-The recipient's address in the transaction and that is also $T_t \in \mathbb{B}_{20}$.The type of transaction is an 8-bit positive integer represented by , T_p so $T_p \in \mathbb{P}_8$. Where, $\mathbb{P}$ is stands for positive integer. A transaction sequence number T_n used to identify the order of transactions, which is a 32-bit positive integer expressed by $T_n \in \mathbb{P}_{32}$. The value of the transfer transaction expressed by T_v is a 64-bit binary positive integer, indicated by $T_n \in \mathbb{P}_{64}$. T_r is the result of the transaction, which is 8-bit positive binary integer, $T_r \in \mathbb{P}_8$. T_d is the number of bytes that is variable-sized and usually includes information such as smart contract bytecode. The source and destination address in the transaction are indicated by a 20-byte hash, as mentioned earlier

$$T_f, T_t \in \mathbb{B}_{20}.$$

For the sake of the user's anonymity and security, the transaction addresses employ a 20-byte hash string.

3. State Transition in Transactions

An execution of a transaction in a smart contract is the process defined by a state transition function γ. For a transaction to be executed, it has to go through the initial validity checks, which include, among others, checking its well-formedness (well-formed RLP), having a

valid signature, the account balance of the sender being enough to cover the upfront cost v0, and all other parameters being valid. These checks make certain that only legal and executable transactions transact through the smart contract system. The state transition is represented by the function

$$\sigma' = \gamma\,(\sigma, T),$$

where, σ indicates the state of the system. σ' is the new state after the transaction is applied, and T stands for the transaction. This transition helps in order to guarantee that when the transaction is done the states of the system are changed in the right way.

4. Transaction Status TStatus

TStatus is the status of the transaction that can be represented by T which is a tuple

$$T \equiv (S, L, R)$$

where the finished set S accounts that were abandoned during the transaction operation. L represents both the VM execution log and the status of the smart contract within the log memory.

In simple terms, in the transaction model, a transaction is defined as an exchange of assets or data and is depicted by a series of components in a tuple form, and these are the sender, receiver, transaction type, sequence number, value, result, and data. Every transaction leads to a modification of the system, and the status of the transaction is identified by the record of performed actions, by the log, and by the contract balance. The model also employs a state transition function that is used to effect a change in the system after a transaction has taken place.

The formal description of smart contracts offers an exhaustive explanation and execution of smart contracts. Based on the Automata, the smart contract model rectifies and describes the pattern from which a smart contract is formed and how all the participating parties shall act in synchronization in response to the substance of it. In an effort to bring structure to all transactions, the Transaction Model explicates components such as the sender, receiver, and the value of the transaction. The state transition in transactions shows a systematic way through which a system uses a transition function to enforce integrity and correct transformations after every transaction. Finally, Transaction Status (TStatus) captures and

documents the results of transactions, relying on logs, completed actions, and balance changes throughout the entire process of the contract's execution.

B. Attribute Description

This section provides information on how formal descriptions of the attributes of smart contracts are conducted in order to make the smart contract run in the expected manner. Based on the categorization type, attributes are functional and non-functional attributes.

1. Functional attributes

Service behaviour, invocation, and communication are explained in functional descriptions, which are the operating attributes. They provide down the rules for how communications should be crafted and how network protocols should be set up in order to facilitate communication. Functional attributes make sure that the model runs smoothly. If there are any lexical or grammatical errors, it will modify the model to run smoothly.

2. Non-Functional Attributes

Non-functional attributes concern such specifications of the contract as performance, security, and reliability. It justifies the putative effectiveness of the contract in completing arranged clauses and its correct functioning through these properties. No deadlock prevents the contract from being stuck with all entities waiting endlessly

$$Q_{(t+1)} = \delta^*(Q_t) \quad , t > min\ \Delta t.$$

In no Livelock, avoid infinite loops where the fault lies in failure to make any progress

$$Q_{(t+1)} = \delta^*(Q_t) \quad , t < max\ \Delta t.$$

In boundedness, its verifies that the resources or parameters used in the contract are within defined limits

$$Q = \{(q_1^*, q_2^* \cdot \dots q_m^*), L\} \quad , q_i^* \in q_m^*.$$

In recoverability, it critically ensures the contract may return back to a normal state when an error has been generated

$$Q_t = \delta^*\left(Q_{(t+1)}\right).$$

Stateless Ambiguity Ensures that contracts remain in a steady state at any given point

$$\exists_{(unique)} Q_t \ \ , t = t_0.$$

In termination or progress, it makes sure that the contract fulfills its service within a limited period

$$\forall M^*, \exists F^* = \delta^*\left(Q_{t_0}\right) \ , \ \ t_0 < \max\ (\ \Delta t).$$

More simply, the attributes guarantee smooth running of the contract, nonconcurrence of glitches such as deadlock or loop, appropriate utilization of resources, fault tolerance, stability, and timeliness in finishing the contract's tasks. This ensures a proper and efficient smart contract delivery system for the benefit of all those parties involved in a smart contract.

C. Generate Code Automatically

Smart contract code automation is crucial for developing mass production in the digital society. It takes advantage of formal models together with the Model-Driven Architecture (MDA) so as to easily come up with contract code, which is both verified and executable. The process that occurs entails the engineering of models with the right forms, the development of rules for converting models into target platform code, and the use of template-based technology for transformation. Transformation templates are dynamic and can be easily realized to fit the different platforms they are going to be used on. This systematic approach allows for the creation of platform-specific contract code contained within the model information and converts it through a conversion engine to provide optimized code based upon the model information contained within the code.

D. Verification of Smart Contracts

Smart contract verification is a generic process intended to prove the completeness, accuracy, safety, and compliance of smart contracts during the development life cycle. This is followed by contract modeling, where the contract is translated to a formal expression of a mathematical model. Model checking and deductive proof are formal verification methods that ensure logical correctness and specification conformity. With model-driven architecture (MDA) techniques, the translated validated models are converted to executable code, thus reducing the chances of an error. Runtime monitoring implemented contracts to observe and respond to contraventions, whereas conformance testing checks whether the contract implementation corresponds to its formal specification. This systematic approach uses tools

such as SPIN, Rodin, and Event-B so as to ensure highly dependable, responsive, and legally sound smart contracts.

E. Conformance Testing

The authors have also done conformance testing, which means the systematic check to see whether the implemented code of the smart contract is in compliance with its specification. Include the generation of test sequences, the execution of tests, and the result analysis to determine whether or not the contract behaves as designed. They mention the utilization of several algorithms for generating tests. Sequences Include the following: UIO Method: This relies on the creation of unique sequences of inputs and outputs of the FSM in the smart contract to identify specific states and transformations. W and D Methods: These extend UIO by adding additional sets or sequences of state transitions. In Testing Methods, they employed the Local Testing Method. This is a direct method where the smart contract and the testing system being tested are in the same machine. This simplifies things significantly, as it gives a granular method for thinking about the contract's behaviour without requiring the transmission of a contract across contexts.

4.5.2 Quantitative Assessment of Smart Contracts

In recent years, researchers have shifted towards quantitative analysis and automated methodologies of analyzing smart contracts on the Ethereum platform. Chatterjee et al. suggested a framework for quantitative analysis, focusing on game theory and including utility modelling [177]. In a study, Durieux et al. performed a large-scale empirical analysis of nine automated analysis tools for smart contracts and concluded that only 42% of the issues are identified by all the tools, wherein Mythril is identified to be the most accurate among them [178]. Luu et al. found a new security threat of smart contract execution and developed Oyente, a smart contract vulnerability tool, which found security issues in 8,800 out of 19,336 Ethereum contracts [179]. Feist et al. introduced Slither, which is a tool for the quantitative analysis of smart contracts on Ethereum by using static analysis in order to identify specific weaknesses and potential improvements. Finally, the results of these studies underscore the significance of performing automated analysis in the vulnerability detection and optimization of smart contracts and indicate the difficulties in attaining a complete and precise picture of the smart contracts' state as well as a thorough comparison of the outcomes acquired via different approaches and tools.

Smart contracts are self-executing programs on blockchain networks and hold the promise of revolutionizing industries but are insecure due to code defects [180],[181]. Due to the immutability characteristics of blockchain, it is of great importance to avoid the presence of bugs within smart contracts before they are implemented because any errors that may be identified cannot be rectified [182],[181]. There are some solutions regarding this problem, such as the automation of transforming contracts into a more secure form [180] and the use of deductive software verification [182]. In contrast, most smart contract languages, such as Solidity, are reasonably complex, making it difficult to write secure smart contracts [183]. The stabilization of smart contracts is also important since their flaws are potentially damaging in actual-world usage [183],[182]. Bigi et al. noted that while a smart contract is decentralized, the interactions exhibit features of game theory, and this is why game theory and formal methods should be used to establish decentralized smart contracts [184]. Chatterjee et al. suggest that there is a lack of a framework that includes a game-theoretic perspective to measure incentives to behave dishonestly in smart contracts and present a simple programming language and an abstraction-refinement approach. In their article Quantitative Analysis of Smart Contracts, present four keys, to deconstruct and understand smart contracts. The authors propose the following approach: (i) flag a new simple programming language developed to facilitate game-theoretic modelling and interaction concurrency. (ii) Synthesize contracts as state-based games that can exhibit all possible interactions and adversarial behaviours. (iii) Introduce the concept of abstraction-refinement to tackle large state spaces to solve these games efficiently and (iv) use real-world-inspired contracts such as auctions. This enhances smart contracts by allowing the discovery of bugs (for example, overselling tokens or in unfair ways) as well as the analysis of the economic implications, all in a beneficial manner, and designing them as well to be robust in adversarial scenarios. This raises its practical usefulness as a valuable tool for building reliable blockchain applications concerning the scale and accuracy of evaluating the behaviour of contracts [177].

4.5.3 Smart contracts within the PBFT-based blockchains

The open public blockchain technology utilizes consensus algorithms in its components, including Proof of Authority (PoAu), Proof of Work (PoW), Byz coin, Delegated Proof of Stake (DPoS), Proof of Stake (PoS), Leased Proof of Stake (LPoS), Omni Ledger, Elastico, and Proof of Burn (PoB). Open public blockchains face the primary disadvantage today because their present state value fails to match the current system capabilities. P.

Parthasarathi, S. S. Askar, and Mohamed Abouhawwash suggest using PBFT with the PoW consensus algorithm to increase security for accessing the records of the healthcare in blockchain networks. Furthermore, they also incorporate the feature of smart contracting to validate health data, as it successfully offers an effective user-authenticating mechanism.

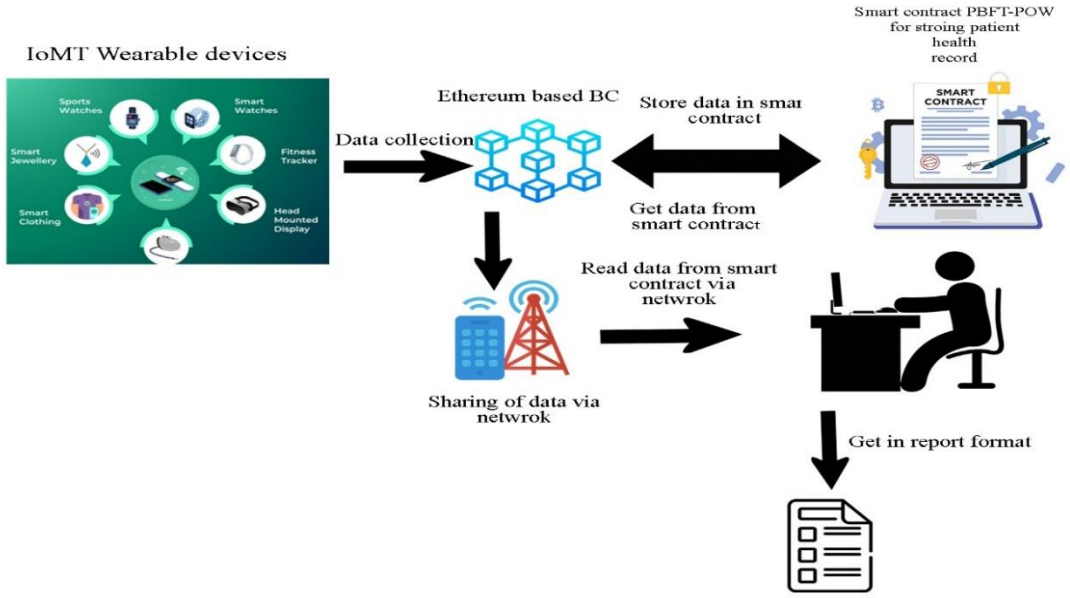

Figure 8 Architecture of PBFT-PoW with Smart Contact [185].

The new PBFT-PoW methodology pertaining to IoMT encompasses electronic storage of patient healthcare e-records through sensor devices and wearable devices that collect health condition details using established parametric measures, including oxygen saturation, pulse rate, calories, temperature, blood sugar, etc. Ethereum's blockchain receives data from

wearable devices, which get stored permanently within it. Health information remains private for all patients; therefore, healthcare providers must maintain utmost security and confidentiality. This paper endorses the execution of Ethereum blockchain smart contracts through PBF partnership combined with PoW (PBFT-PoW) consensus protocols. The proposed work achieves minimum consumption time during its comparison against existing algorithms. The PBFT-PoW system operates as a distributed data storage solution that secures data confidentiality. A lower number of sealers than total network nodes generate the optimal outcome for PBFT-PoW implementation. The system cuts down the duration required for synchronization and propagation. The accuracy percentage of PBFT stands at 90.15%, while the proposed work PBFT-PoW reaches 99.88% and PoW achieves 92.75% [185].

On the other hand, Rodrigo D. Garcia, Gowri Ramachandran, and Jó Ueyama explore the use of smart contracts within Byzantine Fault Tolerant (BFT) blockchain platforms. In particular, they consider Tendermint and Hyperledger Besu and discuss their performance when implementing a case study of a decentralized e-prescription system. The technical activities implemented within the system include the utilization of smart contracts for the validation of doctor transactions as well as medication sales. A typical patient works on two contracts: a prescription with the doctor and the contract that is buying medication with a pharmacy. Doctors generate transactions that contain prescription information, then put their digital signatures, which are their private keys, on the prescription contract address. Other nodes make use of a doctor's public key in order to validate such prescription records with the aim of combating fake records. As noted, the verified transactions are incorporated into the blockchain by use of a consensus mechanism.

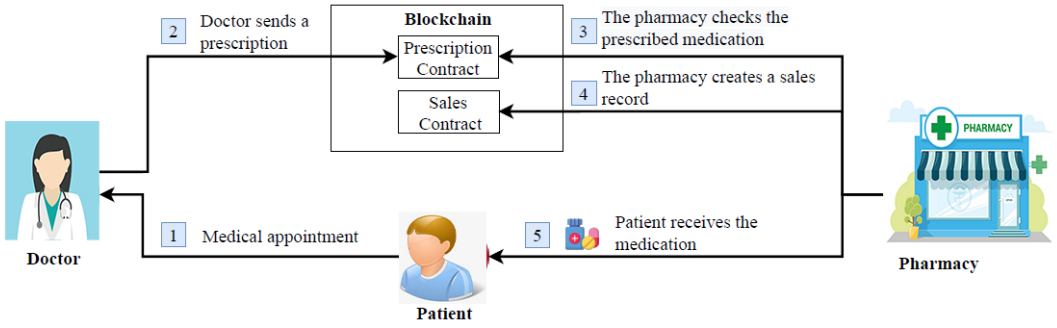

Figure 9 Decentralized architecture for electronic prescribing model [186].

In the comparison of smart contracts among Tendermint (CosmWasm), Hyperledger Besu (IBFT2), and Ethereum (PoW), the result shows that based on the BFT consensus (Tendermint and Hyperledger Besu), they are much faster and more stable than the PoW of Ethereum. Tendermint had an average block generation time of 5.40 s and a standard deviation of 0.06 s, while Hyperledger Besu had an average time of 5.00 s within a standard deviation of 0.49 s. While in Ethereum, the average block mining time was 23.79 seconds, with a high standard deviation of 17.78 seconds caused by the PoW. These results show the feasibility of BFT platforms for applications such as the proposed decentralized e-prescription solution for which low latency and consistency are paramount [186].

5 Cryptography in Healthcare

Blockchain and cryptography seem to affirm a suitable approach to address future healthcare data security requirements. These approaches deal with various concerns such as data sharing and privacy as well as the integrity of the systems in the healthcare segment [187],[188]. Fourthly, the use of blockchain results in increased soundness and decentralization, and the cryptography guarantees data security and privacy [188],[189]. In the context of cryptographic methods augmented by blockchain technology, enormous potential can be seen in developing solutions for data security in healthcare. It can support a decentralized and secure registry and improve the interoperability of data between healthcare stakeholders [190]. Both public key cryptography and blockchain can deal with the problems of authentication and data security in healthcare environments [188]. The application of superior cryptographic methods integrated with blockchain and smart contracts shows the possibilities to handle the drawbacks in existing approaches, such as AES, RSA, or ABS, providing enhanced efficiency, accuracy, and security to the EHRs preserved in the cloud [189]. Cryptography is the use of keys to encode information and decode it to keep the information safe from unauthorized parties [191],[192]. It converts plaintext to ciphertext using different algorithms such as AES and DES [191]. Cryptography plays significant security features, commonly confidentiality, authentication, and data integrity [193]. Since the protection of data has gained significance in the current world through technology use, cryptography is useful in the protection of data and restricting access [191],[192].

5.1 Cryptography

There are three main types of cryptography, namely symmetric key, asymmetric key, and hash functions [194]. Symmetric cryptography encrypts and decrypts data using the same secret key [195], and asymmetric cryptography encryption uses two keys: one is the public key and the other is the private key. But asymmetric cryptography is safer because it employs higher key parameters; however, it is slower and used more often for the key exchanges only [196],[197]. While in symmetric cryptography, it is much faster for encryption as well as decryption and requires a small key size, but it’s relatively weak for secured data [198]. The time taken to generate, encrypt, decode, and exchange keys depends on the kind of cryptographic technique used as well as the length of the key. Whereas RSA, ElGamal, and ECC fall in the asymmetric category, DES, 3DES, and AES in the symmetric category [199]. Hash functions, such as MD5, also play an important role in cryptography [194]. In section

4.3, I discussed digital signatures and illustrated how cryptography is used in the "Digital Signature Algorithm" (DSA). I also delivered on RSA and Distributed Attribute-Based Signature (DABS). In this part, I will discuss particular innovative uses of cryptography in healthcare blockchains, and at the end of the chapter, a table (Table 4) will show a summary of cryptographic concepts in blockchain.

5.2 A blockchain-based secure biomedical image processing system

Information security has been achieved by applying cryptographic techniques in securing medical images and patients' details. In some areas, the cryptography technique is employed just for the medical images or the patient's data [200]. Researchers focus their studies on using blockchain technology to establish secure biomedical image processing systems. It is for these reasons that these approaches seek to solve for privacy and secure data in healthcare organizations. Blockchain technology is used to openly share and store patients' medical images, such as X-ray, CT, and MRI scans, through a secure network. The frameworks proposed incorporate efficient cryptographic methods, including lightweight cryptography like elliptic curve cryptography, to enable the encryption and decryption of image data [201]. Hemant B. Mahajan and Aparna A. Junnarkar present the blockchain-based secure biomedical image processing solution for the healthcare 4.0 era designed to overcome the issues regarding secure and private processing of medical data, especially multimedia ones like X-rays and CT scans. It employs edge computing, fog computing, cloud storage, and blockchain layers while assembling, transmitting, and storing biomedical data to anonymize them. For encryption and decryption, the system employs only the Elliptic Curve Cryptography (ECC) with the ECDH method encrypting; for signatures, the system uses the ECDSA method signature; consequently, the system provides high security with low computational complexity. The effectiveness of the proposed idea is verified experimentally using datasets available to the public, and the evaluation of encryption and decryption times, improved Peak to Signal Noise Ratio (PSNR), and minimized Mean Square Error (MSE) confirm that it is a suitable solution for healthcare 4.0 for secure medical data management. They noticed Some measures of medical image protection identified include hybrid encryptions, for instance, stationary wavelet transformation (SWT) and singular value decomposition (SVD). It also condemns the fact that many of the current systems show an absence of edge-layer security, while some of the methods use encryption for protecting the medical images. The protection during the transfer of the images from the edge layer to the cloud is seldom protected. They

prove that there is a necessity to develop a more effective means of protecting the privacy and genuineness of medical images in transit. It is possible to classify their approach into several stages, and these stages are explained below [201].

- **Pre-Processing and Noise Reduction**

It is essential to perform pre-processing to improve the quality of the input X-ray image before encryption. Next, the intensity values of the image are modified using

$$M1 = imadjust\ (I),$$

where $M1$ is the contrast-enhanced image and I represents the original X-ray image. One of the main characteristics of this is the use of median filtering in order to remove noise. The median filter is commonly used in image processing for noise reduction

$$M(x, y) = median\ \{M1(x, y)|\ (xyj)\ \in p\}.$$

Here p represents the 3×3 neighborhood window. Such steps make the image clean and suitable for encryption.

- **ECC Key Generation**

To ensure security of the data ECC keys are generated. Private key Pr generated randomly, and it's calculated by

$$Pr = rand\ (1, n - 1),$$

where n is the multiplicative order of the base point G on the elliptic curve. Public key (Pu) is calculated by

$$Pu = Pr \times G.$$

The base point of the elliptic curve is designated as G. An important aspect is that these keys are used for both encryption and decryption as well as to create a secure signature.

- **Shared Secret Key Generation**

Using Elliptic Curve Diffie-Hellman (ECDH), a shared secret key (Sh) is generated. The shared secret key was then combined with the AES-128 in order to perform an encryption

$$Sh = Pu \times Pr.$$

- **Encryption and Indexing**

The medical data (x-ray images) is encrypted with the aid of a shared secret key (Sh) which is encrypted with the help of the AES-128 encryption algorithm

$$M_{encrypt} = Encrypt(M, Sh).$$

When encrypting the data, a unique index (i) is built from the IoT Node ID (IN) and the current time (TS). Which can be expressed by

$$i = Index\ (IN, TS).$$

The index makes sure the encrypted data is singularly distinguishable in the cloud and blockchain store and can be applied in search operations or access log reviewing.

- **Digital Signature Creation**

To make the data that is processed safe from any kind of malicious intervention, such a digital signature is created using the Elliptic Curve Digital Signature Algorithm (ECDSA). First, the hash of the encrypted message ($M_{encrypt}$)is computed using the SHA-2 hashing algorithm. Which can be expressed by

$$M_{hash} = H\left(M_{encrypt}\right).$$

In the next step the signature pair (r, s) is generated by applying the private key (Pr) to the hashed message and checking whether the encrypted data is legitimate and has not been changed by third parties.

- **Validation and Storage**

The encrypted data and its signature will be forwarded to the fog node (FN) and Cloud storage (CS) to validate the hash of the encrypted message ($H\ (M_{encrypt})$), the signature, and public key (Pu). It can be expressed by this,

$$Verify(H\left(M_{encrypt}\right), signature, Pu)$$

If the signature is valid, both the encrypted data and its index, together with the keys, are stored in cloud storage (CS), where the index, time, and signature information are also stored in the private blockchain (PB). If the validation process fails, then the encrypted data, associated keys, and index are erased, and an alarm is signaled to the hospital administration and the IoT node to take corrective action.

- **Secure biomedical image extraction**

The proposed mechanism of extraction ensures that the biomedical image remains secure because its data is well protected in terms of confidentiality, integrity, and traceability via an integrated cryptographic platform. A Medical User (MU) provides a search request to Cloud Storage (CS) with an IoT Node (IN) ID, index, and a signature created with an external current time of the present moment. The request needs to undertake the signature verification process at the Fog Node (FN) as well as at the CS. If the verification is successful, the signed encrypted biomedical data is obtained and sent to the MU through the FN for another round of verification. The MU decrypts the data using the shared secret key, which is $Sh = Pu \times Pr$ using the Elliptic Curve Diffie-Hellman (ECDH) protocol and restores it to its original form with AES-128 decryption. Such execution guarantees data authenticity by allowing signatures, data security by allowing encryption, and auditability through the metadata stored in the private blockchain (PB). It also shields against quantum threats and builds confidence in decentralization by using ECC-based cryptography and blockchain.

- Results Analysis

The evaluation of the proposed model involved the use of lightweight ECC-based cryptography, which provided the model with the best encryption time of 12.46 seconds and shortened the decryption time to 8.31 seconds. It also provided enhanced image quality with measured PSNR (average 49.02), higher than the rest, and MSE (average 509.71), comparatively lower than the others, showing that it has minimal error and high accuracy between the original and decrypted images. The model offers significant benefits by decreasing encryption time (18.5%) and decryption time (17.55%), enhancing PSNR by 8.5% and decreasing MSE by 9.66% compared to other methods [201].

5.2.1 The method of data hiding within encrypted images functions in a reversible manner.

Reversible data hiding (RDH) in encrypted images is a steganographic technique that permits the complete recovery of the images after the extraction of hidden data. This technique works with cryptography and steganography so that the present image and the hidden information can be secured [202]. Reversible data hiding in encrypted images RDHEI is a new technology that can be used in image authentication, identification of content owners, and privacy. New results within RDHEI include perfect separation schemes for complete schemes that ensure

the error-free extraction of data from both cipher and plaintext domains [203]. Ji-Hwei Horng and Ching-Chun Chang along with their co-authors Guan-Long Li, Wai-Kong Lee, and Seong Oun Hwang, have put forward an RDHEI technique. This method enables one to wirelessly transfer sensitive information, including patient details or diagnostic reports with medical images, and the ability to perfectly retrieve both the image and the embedded information. While evaluating the existing RDHEI methods, the authors pointed out that these methods have low embedding capacity, which makes them prone to tampering and does not offer traceability. To overcome such challenges, they present an improved RDHEI scheme with improved embedding capacity via image block-wise encryption and shifting of histograms. Furthermore, the authors incorporate a lightweight consensus mechanism, such as PBFT, to employ the blockchain technology and guarantee the traceability and data integrity by storing the hash of the medical images on the distributed ledger. According to the authors, this RDHEI system based on the blockchain environment allows for secure transmission and exchange of encrypted steganographic medical images (CSMI) securely within the trusted network, and protect against unauthorized modification, and achieves full traceability. The outline of the proposed reversible data hiding scheme for medical images describes a three-step method of data embedding into the encrypted medical images while preserving the ability to reverse both the data and the image.

The proposed RDHEI scheme incorporates simple cryptographic methods to provide privacy, security, and invertibility of medical images. The active pixel is encrypted using stream ciphering through an XOR operation with an 8-bit key, resulting in computational effectiveness that is effective for real applications such as telemedicine. The safe and reversible method involves three keys: Key-I to perform the block permutation, Key-II for the construction of the stream cipher, and Key-III for decoding the obscured information. As well, histogram shifting helps to make space for data embedding through shifting of pixels using a threshold, which ensures that the image is secured during the data embedding process. Indeed, the incorporation of stream ciphering and key-based encryption, as well as histogram shifting, yields fairly good results concerning both security and efficiency, whereas the option to recover all records makes this algorithm particularly appropriate for the field of medicine. For that purpose, this scheme entails the use of high levels of cryptographic and data-hiding mechanisms that will provide the scheme with high levels of security, high embedding capacity, and reversibility. It is divided into three broad stages.

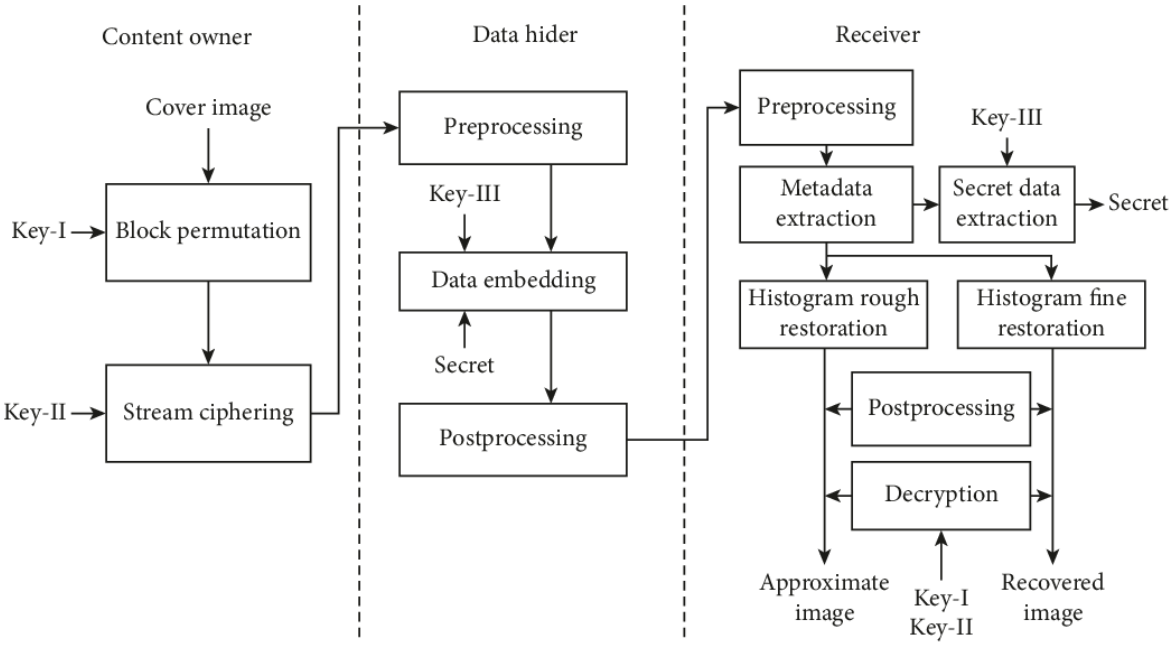

Figure 10 The RDHEI scheme proposed by Horng et al. [204].

- Cover Image Encryption Phase

The cover image encryption stage encrypts medical images to protect confidentiality and make them suitable for data embedding operations. The procedure starts with block permutation, where original image pixels are grouped into 3 × 3 blocks and rearranged randomly using Key-I in order to disrupt spatial correlation and obtain better security. Stream ciphering is then adopted again for each block pixel-wise through the formula $C = K \oplus P,\ C$ where is the encrypted pixel, P is the original pixel, and K is the 8-bits stream key using Key-II. An encrypted image is obtained at the end of the process, which obscures its original image and at the same time, is ready to be used for secure data embedding.

- Data Embedding Phase

The Data Embedding Phase of the Reversible Data Hiding in Encrypted Images (RDHEI) is to embed secrets in the encrypted image in blocks with histogram shifting and preprocessing. During preprocessing, an internal exclusive-OR operation is performed on each block of the encrypted image. The central pixel (c_c) and eight surrounding pixels ($c_1, c_2, \ldots \ldots c_8$) make up each image block. Perform an XOR operation between each surrounding pixel and the centre pixel, which can be expressed

$$g_i = c_c \oplus c_i,$$

where g_i are the output pixel values after preprocessing. This can also be expressed as

$$g_i = c_c \oplus c_i = p_i \oplus p_c,$$

where p_i and p_c stands for the original pixel values of the surrounding and centre pixels, respectively. In the smooth blocks, many g_i values approach zero as the pixel values are close to each other, resulting in a sparse histogram that facilitates efficient data embedding. A threshold value g_{th} is used to determine the modification of pixel values in order to create space for embedding secret data. Modify the pixel values (g_i) to create space

$$g_i' = \begin{cases} g_i \times 2, & g_i < g_{th}, \\ g_i + g_{th}, & g_i \geq g_{th} \text{ and } g_i < 128, \\ g_i, & g_i \geq 128 + g_{th}. \end{cases}$$

A vacating band of width g_{th} is developed after gray level 128 to accommodate secret data. The first g_{th} gray levels (0 to g_{th}) are shifted to even values to maintain their order, and the gray levels between g_{th} and 128 are shifted outward to fill the vacated band. The value g_{th} and information about the vacating band are then embedded as metadata so that the data extraction process is possible and the original image can be reconstructed. The binary secret stream is then encrypted using Key-III using a stream ciphering technique, resulting in an encrypted bitstream $S = \{b_1, b_2, b_3, \ldots\ldots, b_N\}$.Embedded pixels with $g_i' < 2 \times g_{th}$ are grouped according to the ordered Gray level and raster scan order for pixels belonging to the same gray level. Each secret bit is embedded by summing it to the adjusted pixel value g_i' . Postprocessing undoes the preprocessing in order to retain the block structure. The erased histogram band in the range $128 \leq g_i < 128 + g_{th}$ includes metadata with six bits for g_{th}, twelve bits for the number of pixels, three bytes per pixel for gray level, and coordinates. To gain the final encrypted image with embedded data, the process consists of image processing with Key I and Key II, histogram shift, encoding of metadata, embedding the encrypted data stream, and the final image processing stage.

- Data Extraction and Image Recovery Phase

Through the data extraction and image recovery phase, users achieve the recovery of hidden secret data and achieve complete image restoration. Here is the breakdown in detail. Preprocessing is implemented to reverse embedding for each picture block that has been embedded. After preprocessing the pixel values are calculated using $\hat{g}_i = \hat{g}_i' \oplus \hat{g}_c$,where i = 1, 2…., 8,. To obtain the threshold value g_{th} , the first six pixels with values of 0 or 1 are

accumulative in the raster-scan sequence. By combining these pixel values, a 6-bit binary number is generated and translated to the decimal form in order to get g_{th} to make sure that the value is securely encoded within the image for data embedding and retrieval. The embeddable pixels are collected in ascending order of $\hat{g}_i'/2$ Based on the threshold g_{th}. Metadata and the encrypted secret data stream are then extracted using an even-odd decision, as even pixel values represent 0 while odd pixel values represent 1, in order to get an accurate extraction of data. The secret stream, which is extracted from the image, is decrypted by Key-III. In order to undo the operations done during embedding, backward shifting employs a specific formula based on their range to bring back pixel values to the original state. Which can be expressed by,

$$g_i = \begin{cases} \left\lfloor \frac{\hat{g}_i}{2} \right\rfloor, & \hat{g}_i < 2 < g_{th}, \\ \hat{g}_i - g_{th}, & \hat{g}_i \geq 2 \times g_{th} \; and \; \hat{g}_i < 128 + g_{th}, \\ \hat{g}_i, & \hat{g}_i \geq 128 + g_{th}. \end{cases}$$

Additionally, the embedding process generates a vacating band, which is then recovered by the use of metadata. This ensures an accurate restoration of the loss of the exact distribution of pixel intensity as well as the structure of the picture. In this way, the original picture structure and pixel distribution are accurately reconstructed. Postprocessing reconstructs the internal pixel structure of each block.$c_i = g_i \oplus c_c$, i = 1, 2…., 8. The image obtained by decrypting the histogram-recovered image with Key-II is finally obtained, and the block permutation is reversed using Key-I to bring the image back to original spatial arrangement. These steps are important in order to ensure a full-blown recovery of the original image. Horng et al. also explained how their RDHEI scheme works on a consortium blockchain, making for an attractive solution for safeguarding and tracking medical images.

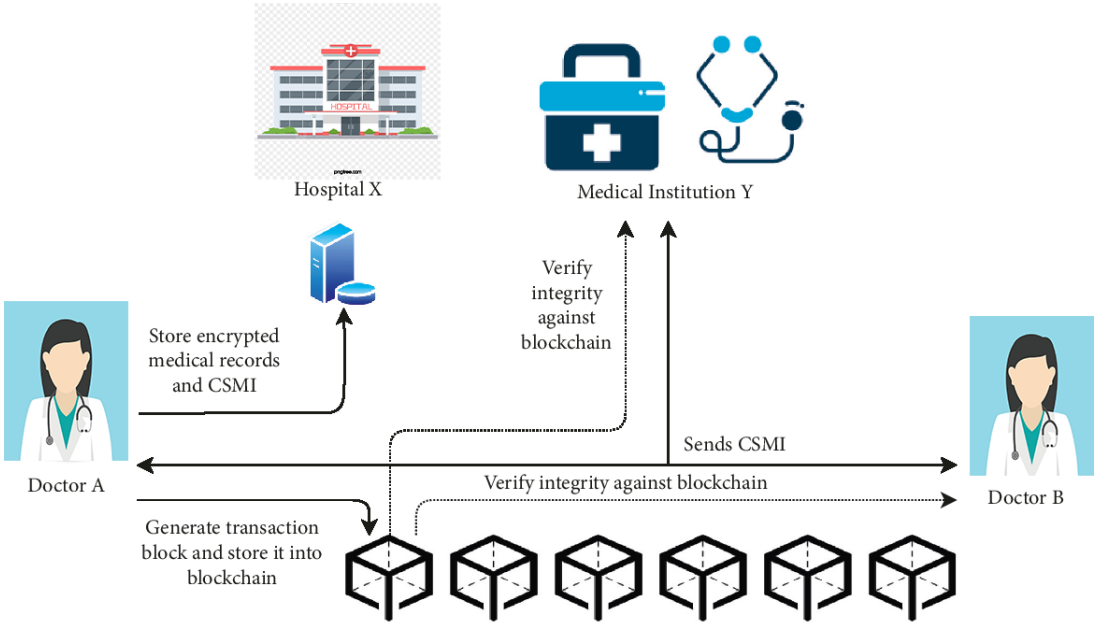

Figure 11 The architecture of the proposed blockchain system by Horng et al. [204].

- Blockchain Supported Reversible Data Hiding Scheme

The Blockchain-Based Reversible Data Hiding System (RDH) is a model using cryptographic algorithms and blockchain technology in the transmission of medical images. Protected patient information MR includes medical records that are encrypted with a symmetric key K_1. Which can be expressed by

$$C_{MR} = Enc(K_1, MR)$$

And this encrypted MR is embedded into images via stream ciphering and histogram shifting. These are the ciphered steganography medical images (CSMI), and they are created by means of reversible data hiding. A hash value

$$H_{curr} = Hash(H_{PREV}||CSMI),$$

where H_{PREV} is the hash of the previous blockchain block, and using this coordinate, the integrity of the images. Here $Hash$ refers to any standardized cryptographic hash function (SHA-2 & SHA-3 etc.) and H_{curr} is hash value of the current block. The hashes are stored on a consortium blockchain, so only the approved entities are capable of tracking image alterations. The method allows the reversible reconstruction of the original image and data

using decryption and backward histogram shifting. Users confirm received images by recalculating hash

$$H_{curr}{}' = Hash(H_{PREV}||CSMI),$$

and comparing it with the blockchain. The system was designed to protect information and have the ability to make it easy to audit and detect tampering. Owing to its being based on mathematical entities such as the modular arithmetic and cryptographic hashing of the histogram expansion, it provides a fairly sound solution for the protection of medical data in the telemedicine and healthcare application [204].

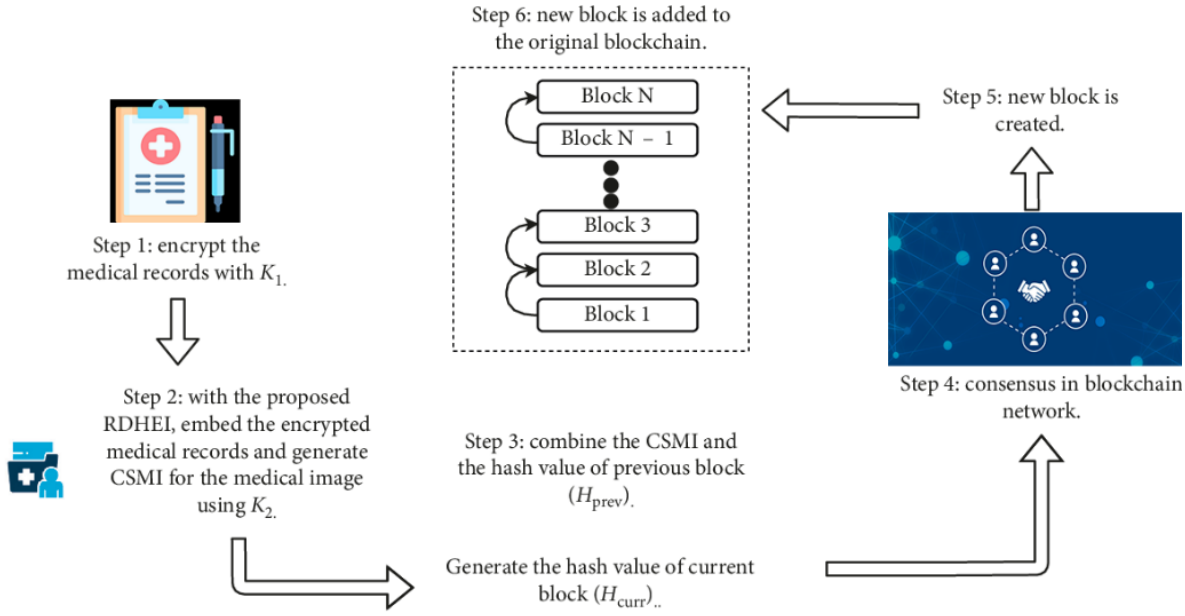

Figure 12 Blockchain system transaction flow based on the proposed RDHEI [204].

- **Experimental Results and Achievements**

The proposed RDHEI method optimizes the embedding rates and visual quality and is capable of providing better performance for smoother images and medical images. As such, medical images achieve higher embedding rates than standard images at similar thresholds, thus showing that the system is a good one for secure medical applications. The researchers were able to perform their experiments with both normal images, including Lena, Baboon, Airplane, etc., and medical images like MRI. Consequently, they provided in two tables a summary of the performance measurements of the standard images in figure 13 and the medical images in figure 14.

Image	Metrics	$g_{th}=4$	$g_{th}=8$	$g_{th}=16$	$g_{th}=32$	$g_{th}=64$
	Capacity	102125	140358	171658	190931	202715
	Metadata	42	66	162	6666	12858
Airplane	ER (bpp)	0.38	0.53	0.65	0.72	0.77
	PSNR	61.64	58.29	54.77	37.72	34.35
	SSIM	0.9999	0.9999	0.9999	0.995	0.9912
	Capacity	30506	56047	93320	134879	173447
	Metadata	1242	2298	4962	12810	51138
Baboon	ER (bpp)	0.11	0.21	0.35	0.51	0.66
	PSNR	42.61	40.32	36.99	32.79	26.12
	SSIM	0.999	0.9983	0.9961	0.9895	0.9516
	Capacity	79348	119982	153134	184078	209831
	Metadata	114	210	546	1866	10626
Boat	ER (bpp)	0.3	0.45	0.58	0.7	0.8
	PSNR	56.36	52.21	46.9	40.83	32.5
	SSIM	0.9999	0.9999	0.9996	0.9983	0.9879
	Capacity	83908	127070	164152	194295	209334
	Metadata	138	162	354	738	4506
Lena	ER (bpp)	0.32	0.48	0.62	0.74	0.79
	PSNR	53.11	52.07	48.24	45.27	36.04
	SSIM	0.9999	0.9999	0.9997	0.9993	0.9944
	Capacity	81892	127696	167267	195067	214845
	Metadata	258	498	954	1794	5586
Pepper	ER (bpp)	0.31	0.48	0.63	0.74	0.81
	PSNR	51.15	47.48	43.9	40.5	35.82
	SSIM	0.9998	0.9997	0.9993	0.9982	0.9944
	Capacity	56910	93681	134503	176246	195452
	Metadata	474	930	1794	3906	10122
Sailboat	ER (bpp)	0.21	0.35	0.51	0.67	0.74
	PSNR	45.23	41.76	39.11	35.87	31.43
	SSIM	0.9995	0.999	0.998	0.9958	0.9872

Figure 13 Different picture thresholds for performance analysis of the proposed method [204].

Image	Metrics	$g_{th}=4$	$g_{th}=8$	$g_{th}=16$	$g_{th}=32$	$g_{th}=64$
	Capacity	39671	43490	48507	52655	56038
	Metadata	66	114	234	738	1554
Medical A	ER (bpp)	0.6	0.66	0.74	0.8	0.85
	PSNR	70.1	57.02	42.68	37.44	35.34
	SSIM	0.9999	0.9999	0.9989	0.9971	0.9953
	Capacity	40608	43388	46851	50168	53448
	Metadata	138	258	546	1122	4338
Medical B	ER (bpp)	0.61	0.66	0.71	0.76	0.81
	PSNR	49.6	45.67	41.45	37.48	30.82
	SSIM	0.9999	0.9996	0.999	0.9976	0.9871

Figure 14 MRI medical image experiments with different thresholds [204].

As per the given information by the authors implementing their proposed RDHEI system, it is clear that high embedding rates are ensured with good or very good visual quality. For the standard images, the range of embedding rates varies up to a maximum of 0.8 bpp at a threshold(g_{th} = 64) as shown in Figure 13 above. For the case of the medical images, the embedding rates are always higher and are at 0.6 bpp at the lowest threshold of (g_{th}=4) and are comparable to those of higher thresholds and depicted in Figure 14. Taking into account

the specific measures of image quality, the Peak Signal-to-Noise Ratio (PSNR) varies from 34.35 dB (in the case of Airplane at g_{th}=64) up to 61.35 dB (at g_{th}=4), which also proves the fact that the method is not deteriorative to the image, keeping minimum distortion even at lower threshold values of g_{th}. Furthermore, the Structural Similarity Index (SSIM) is uniformly high at or above 0.99 for all the scenarios examined; deploying high embedding rates does not significantly impair structural similarity. Such findings show that the system can achieve a good trade-off between the embedding efficiency and visual quality, which means that it is ideal for applications with high data storage capacity and low distortion. The histogram-shifting approach was designed to be completely reversible and optimize the metadata, which eliminated unavoidable problems such as overflow and inefficiency in the other previous approaches. Furthermore, the combination of the system with blockchain ensured the greatest openness and immutability to ensure restored accuracy in the storage and transmission of medical records and data [204].

5.3 Cryptography techniques for securing clinical big data analytics

Clinical data encompass a range of clinical data gathered from clinical practice and consist of patients' demographics, medical histories, treatment results, and laboratory values. It would be useful for research and for decision-making as well as enhancing the quality of patient care, especially with clinical data repositories [205],[206]. Blockchain technology presents potential answers for mediated and off-site clinical data exchange with protection counts. Some suggested solutions include broadcast encryption and key regression for fine-grained access control [207]. Data encryption is another important genre of cryptography that keeps data secure and protected in the ambit of a network. The features of these algorithms are affected by the size of the key, size of the block, number of rounds, and the overall computational complexity [208],[209]. Some of the popular symmetric key algorithms used widely include DES, 3DES, AES, and Blowfish while the asymmetric algorithms include RSA, etc., and the comparative study has been made depending on parameters like speed and security, efficiency [196]. Steena Gracious, Geethu Nandanan, Dagma K. R., and Hari Narayana AG focus on cryptographic algorithms in providing security to clinical data on cloud platforms by comprehending the security issues relating to data integrity, confidentiality, authentication, and non-repudiation. It emphasizes the need to secure clinical information and posits the assessment of multiple encryption procedures, including RSA, DES, ECC, and AES, through measures of information security concerning clinical data sets

based on features such as time taken to encrypt data, time taken to decrypt the data, and memory size. The features of each algorithm are discussed, with RSA highlighted in regard to data encryption, ECC as effective with a small key length, AES as ideal for sensitive data encryption, and DES with fast processing even though less secure. The research results highlight that although DES works at the highest speed, it is less safe than AES and ECC, which are suggested for more critical applications [210]. A. F. Hussein, N. Arunkumar, G. Ramírez-González, E. Abdulhay, J. Tavares, and V. Albuquerque talk about a novel system for implementing medical records management. The identified system relies on the use of the blockchain in order to provide access to sensitive medical information. For improvement in security as well as performance, the approach used in the work utilizes an improved cryptographic method. This modification applies the popular DWT to produce a new bidimensional data sequence key (hash function) for an improved traditional cryptographic technique. The entire process of the proposed system is the following [211].

- Discrete Wavelet Transform

DWT is incorporated in the cryptographic part to generate a non-reusable hash-decrypted key. The wavelet transformations, used successfully in a vast number of applications within engineering sciences, successfully handle a large number of actual problems. The Wavelet Transform (WT) used a long-time window for precise, better-quality low-frequency resolution and a short time window for high-frequency information. This makes Wavelet Transform (WT) suitable for use to analyze non-stationary processes as well as multi-component and irregular data patterns, such as those characterizing impulses with random time intervals. The continuous wavelet transform (CWT) can be expressed,

$$CWT(a,b) = \int_{-\infty}^{\infty} g(t) \frac{1}{\sqrt{|a|}} \psi\left(\frac{t-b}{a}\right) dt.$$

where, $g(t)$ can be defined as the signal integral of a wavelet function multiplied by shifted and scaled versions of the wavelet function w and a and b are referred to as scaling (frequency shared) and shifting parameters, also known as time localization. DWT simplifies this one by employing dyadic scales (powers of two); hence, a computation is efficiently done. Which can be expressed

$$DWT(j,k) = \frac{1}{\sqrt{|2^j|}} \int_{-\infty}^{\infty} g(t) \psi\left(\frac{t-2^j k}{2^j}\right) dt.$$

As mentioned before, mathematically, DWT employs the methods of signal decomposition using high-pass and low-pass filters. In this context, it becomes possible to make an accurate analysis of multi-component non-stationary data and enhance the reliability of cryptographic hash functions, where 2^j represents a and $2^j k$ represents b.

- Cryptographic Hash Key

To ensure the integrity of data, the cryptographic hash function maps the input, regardless of its size, into a predetermined output size. When it comes to mathematics in hash functions like MD5, there are uses of bitwise operation and modular arithmetic in order to develop a digest that contains certain features. These properties include determinism in the output, non-invertibility (pre-image resistance), and collision resistance, which means that no two inputs can yield the same hash. The proposed method enhances the MD5 outputs by adding DWT coefficients; these coefficients increase the hash's entropy level and increase resistance to brute force attacks.

- Genetic Algorithm (GA)

In essence, the genetic algorithm is an evolution of the problem-solving approach. It takes a given issue, creates solutions at random, evaluates their appropriateness, and then optimizes them via generations of selection, mutation, and crossover. Through iteration of solutions, GA can effectively obtain the global or near-global solution for a problem. In mathematics, GA comes up with solutions through such processes; the fitness function helps determine how well a solution fits and hence will be selected for a solution. Selection guarantees the best solution survives, crossover allows blending of two solutions in an effort to produce offsprings and mutation prevents the algorithm from getting stuck in local optimum.

$$N(h.t+1) \geq N(h,t)\frac{f(h,t)}{\bar{f}(t)}\left[1 - p_c\frac{\delta(h)}{l-1} - p_m o(h)\right],$$

where, $f(h,t)$ represents the average fitness weight of schema h in generation t. $\bar{f}(t)$ stands for the average fitness weight of the entire population in generation t. p_c and p_m represents the probability of crossover and mutation respectively. $\delta(h)$ is the total length of schema h and $o(h)$ order of the schema. The number of bit positions in the string is represents by l. GA is needed here because GA optimizes the queuing system in the proposed architecture, reducing transaction node time.

- System Overview and Work Flow

The proposed system is an efficient architecture in the form of the blockchain system, which is particularly intended for medical records management and security. There are six major components: the user interaction networks nodes, cryptographic hash generator (CHG), utilizing the MD5 with discrete wavelet transform (DWT), request queuing system, genetic algorithm for optimizing queued requests, secure data repository, and applications employing the blockchain technology. The system successfully combines modern cryptographic approaches with optimization algorithms to promote a secure and effective method for managing the data owner's health records. The system starts with the creation of cryptographic keys using the cryptographic hash generator (CHG); users send keys for validation.

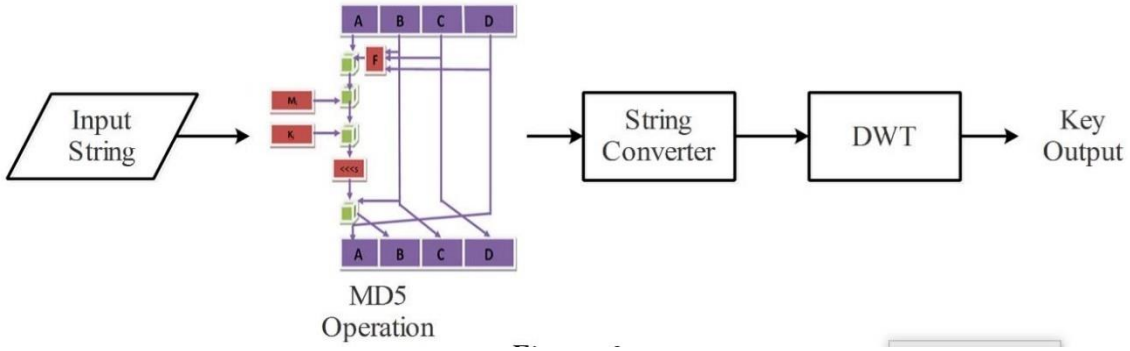

Figure 15 MD5 with Discrete Wavelet Transform (DWT) for Key Generation [211].

These are requests that have been authenticated and are entered into a list where the GA will categorize them depending on the level of efficiency. These optimized requests are then bundled into blocks that, through the consensus mechanism of the blockchain, are culminated. After that, the blocks securely go into the blockchain, allowing the users to receive the concrete information they have requested. The blockchain's property of non-tampering makes medical records secure, and the integration of DWT and GA also offers security and fast processing, hence a secure, efficient system. It is worthy of note, however, that in MD5, CHG, an encrypted hash generator that is the most commonly used one, featured in this proposed system. This research proposes an improved procedure to adopt the cryptographic hash generator through a better cryptographic encryption method. In the encryption mechanism, this enhanced technique uses the DWT for boosting the security level.

- Result and achievements

Based on the simulations, the proposed system identified some improvements compared with the previous system, such as increased security of the keys generated by MD5 and DWT coefficients for better fixed-length keys with low complexity. GA optimizes key management, thus increasing time efficacy and reducing delays, while exhibiting greater efficiency in key transfer than other approaches.

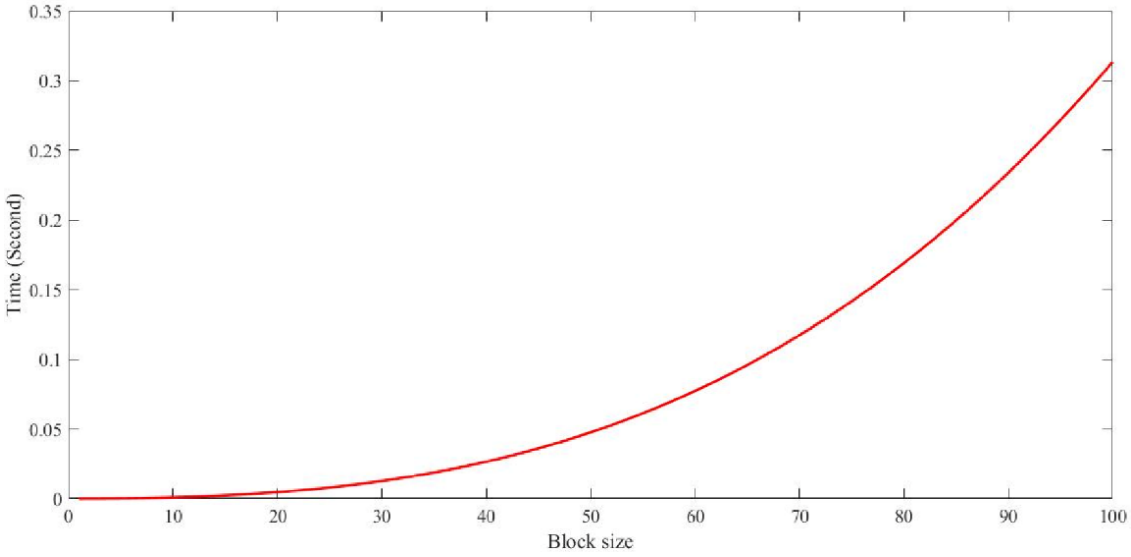

Figure 16 The block generation required time [211].

Figure 16 shows block generation efficiency, in which predefining block numbers is critical to prohibiting exponential time increases after 25 blocks and keeping low latency.

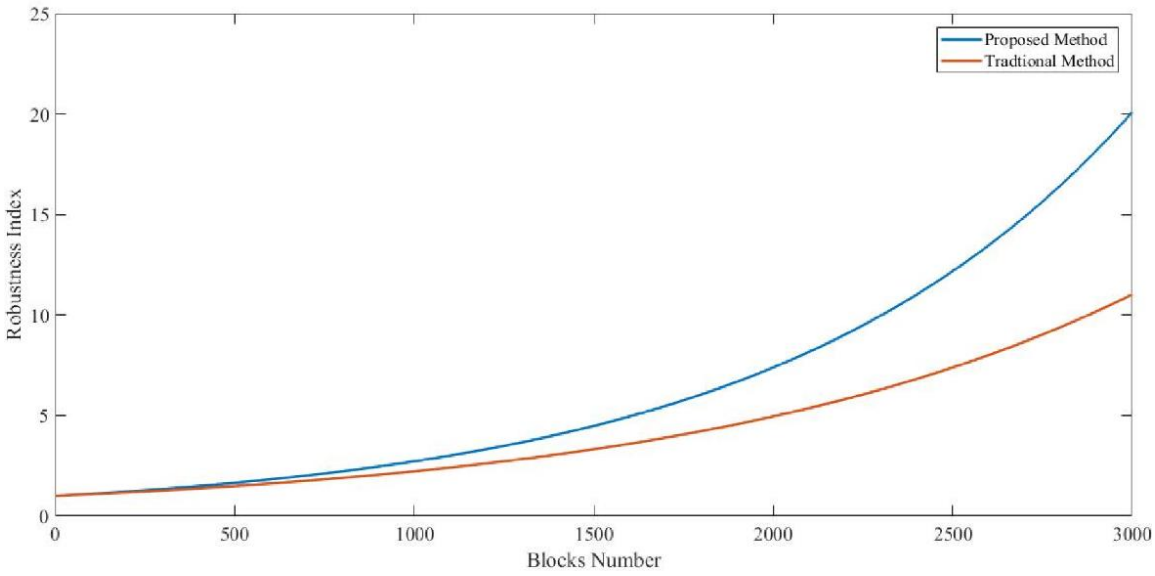

Figure 17 Evaluations of robustness [211].

Further, Figure 17 shows that the proposed system has a higher robustness index and can process more valid transactions to make sure of the dependability and data integrity of the medical records in a blockchain-based system. The average execution time of each node is computed to be 0.19 seconds, which is faster than other approaches [211].

5.4 Utilization of Artificial Neural Networks for Cryptography

New studies show that AI and cryptography are becoming closely intertwined as their application is increasingly interlinked, with each discipline benefiting from the other. Machine learning is increasingly explored in its applicability to encryption, decryption, and steganalysis [212]. Neural networks and evolutionary computing are being used for the creation of the new ciphers and the testing of the random nature of binary numbers for cryptanalytic application [213]. Popular cryptosystems that are already in use, including AES, RSA, and LWE, are also having their security enhanced by AI [214]. The field of adversarial robust neural cryptography is on the rise, where the neural network tries to learn with adversarial strategies for data security [215]. Further, AI is being used in authentication procedures and devices, for instance, the validation of high-value documents using smartphones with details encrypted on radio frequency tags [213]. The synergistic relationship between AI and cryptography is the driving force behind the advancement of novel positive cryptography. As of contemporary machine learning (ML) capabilities, it is possible to predict the weather, find directions, sort images and videos, and even write codes, texts, and films. AI helps the advancement of blockchain, cybersecurity, and other critical technologies. The properties of cryptography used in cybersecurity and in the blockchain can be enhanced by the employment of AI. AI, particularly neural networks, improve the security margins of proven cryptographic schemes such as AES, RSA, LWE, and Ascon by detecting flaws, emulating attacks, and redesigning portions. For AES, AI enhances resistance against side-channel and fault attacks, enhances S-boxes for higher nonlinearity and differential uniformity, and aligns it to meet the different cryptographic criteria such as the Strict Avalanche Criterion (SAC). In RSA, AI minimizes side-channel and fault attacks, chooses the better candidate primes to prevent factorization using Number Field Sieve (NFS) and Fermat’s method, and also verifies private keys against Wiener's or partial key exposure attacks.

In post-quantum cryptography, AI enhances the LWE-based system and also probes the hardness of lattice problems, Shortest Vector Problem (SVP), and others to set up novel parameters balancing between complexity and performance. Likewise, AI enhances lightweight ciphers like Ascon, for example, by analyzing their susceptibility to cryptanalysis, fine-tuning the configuration for resource-scarce environments, and assessing the cipher's resistance to more complex types of attacks. In all systems, it automates the efficient and effective penetration of vulnerabilities, recreates attacks that are complex, and guarantees that cryptosystems are resistant to modern threats, including quantum computing attacks [214].

Blockchain technology to a greater extent based on cryptographic solutions in ensuring security, confidentiality, and integrity of information [216]. The principles of cryptography that apply to blockchain include encryption, hashing, digital signatures, and public key cryptography [217]. Such techniques preserve the data of users, ensure the data is valid, and verify transactions. Specific cryptographic algorithms used in the blockchain systems include the hash functions and the group X algorithm, which is more emphasized on stability rather than speed [218]. Although the cryptography in blockchain delivers high security, challenges such as potential quantum attacks on public-key cryptography exist [217]. Hash-based, code-based, multivariate, and lattice-based public key cryptography are potential post-quantum cryptography methods that are identified by researchers [216]. Also, ideas in cryptography, such as homomorphic encryption, zero-knowledge proofs, and secure multi-party computation, are emerging for blockchain use cases [219]. Mayank Raikwar, D. Gligoroski, and Katina Kralevska, as shown below, provide a comprehensive overview of the various cryptographic techniques used in blockchain technology.

Table 4 Overview of Cryptographic Principles in Blockchain [219].

Cryptographic Concept	**Properties**	**Instantiation**
Access Control	Data privacy	Hyperledger Fabric, FairAccess
Accumulator	Provides Membership Proofs, Anonymity	Batching Techniques for Accumulators in Blockchain
Aggregate Signature	Fast Signature Verification	Tested in Bitcoin
Commitment Scheme	Non-Repudiation	Used in Bulletproof and in Monero
Decentralized Authorization	Data Privacy	BlendCAC , WAVE
Encryption Scheme	Confidentiality and Anonymity	Kadena, Hyperledger Fabric, Tendermint

Cryptographic Concept	Properties	Instantiation
Identity-Based Encryption	No Public Key Distribution Infra.	BAVP, BLIC
Incremental Cryptography	Efficiency Improvement	Kadena
Lightweight Cryptography	Fast, less memory/energy consumption	LSB, EVCE
Obfuscation	Privacy	Tested in Bitcoin
Oblivious RAM	Confidentiality and Integrity	Solidus, EVORAM
Oblivious Transfer	Data Privacy	Searchain
Post-Quantum Cryptography	Quantum Resistant	Post-Quantum Blockchain
Private Information Retrieval	Data Privacy	Private Blockchain Queries from PIR
Proof of Retrievability	Cloud Data Recovery	Permacoin, Retricoin, Storj
Secret Sharing	Data privacy	SHARVOT, Wanchain
Secure Multiparty Computation	Privacy of Peers and Smart Contract	Enigma, Hawk, Wanchain
Signature Scheme	Integrity and Authentication	Multichain, CryptoNote
Verifiable Delay Function	Less Parallelism, Fast Verification	Chia Network
Verifiable Random Function	Verifiable Pseudorandom Output	Algorand , Ouroboros Praos , Dfinity
White-Box Cryptography	Data Privacy	Runtime Self-Protection in Blockchain Ledger
Zero-Knowledge Proof	User and Data Privacy	Zerocoin, Zerocash

6 Applications of Blockchain in Healthcare

Blockchain has been suggested as a solution for many of the existing problems in the healthcare system, providing better protection, clear information, and data control. Some of the key constituents are inpatient data management, pharmaceutical development, logistics, clinical trials, and many others [220]. Blockchain is useful in the enhancement of medical records' exchange, simplifying data analysis while being secure and accurate [90]. It also possesses the possibility of solving problems in drug discovery, counterfeits, and even the management of billing claims [220]. It facilitates tracking of a device across its life, informing patient safety and operational efficiency improvement [221]. Moreover, it is argued that blockchain can also support the creation of patient-centric care by synchronizing real-time clinical data to the blockchain [222]. However, the implementation of blockchain experiences technical, regulatory, and business barriers in the healthcare sector. The number and variety of blockchain projects in healthcare are simultaneously growing, and the majority of initiatives exhibit high levels of maturity, which is a positive sign for the future of the use of blockchain in healthcare [220].

6.1 Supply Chain Management

Blockchain technology appears to have the potential to eliminate some of the main issues surrounding the drug supply chain, such as fake drugs, opaqueness, and inefficiency [223] [224]. Blockchain, because of its inherent architecture of distributed ledgers, can facilitate and guarantee the end-to-end supply chain visibility to eliminate counterfeits [223],[225]. The technology enhances awareness of supply chain events in real-time so that the stakeholders can view information regarding the batches and instantly gain confirmation of the genuineness of products [226]. Blockchain also brings better security since scams and improper access are reduced through the system's decentralized attribute [223]. Thus, whilst integration with legacy systems, scalability issues, and asynchronous and real-time data transactions can pose significant problems to blockchain's efficient application in the supply chain. It is evident that blockchain can offer direct supply chain-related benefits, as well as support smart contracts and cooperative strategies among stakeholders [224]. On balance, blockchain has accurate, safe, and efficient solutions for the concerned issues of the pharma supply chain [226]. Ijazul Haq and Olivier Muselemu Esuka described the pharmaceutical supply chain management system based on blockchain. The approach guarantees the highest level of protecting the communication by using a permissioned blockchain where only trusted

parties can participate. Every drug receives a hash that goes on a blockchain as a digital asset with all the data about it and its movement from the manufacturer to the consumer. Sensitive information is created within the chain while larger files are stored off-chain but pointed to within the blockchain using hash digests. Purchases and sales transactions occur in this process, and all such activities remain unique, offering accountability at different levels. For the participants, including doctor or patient as a particular persona, a mobile application allows checking the drug using its identifier and getting its history before it reaches the consumer, essentially helping to prevent counterfeiting and providing a clear view of the supplies [225].

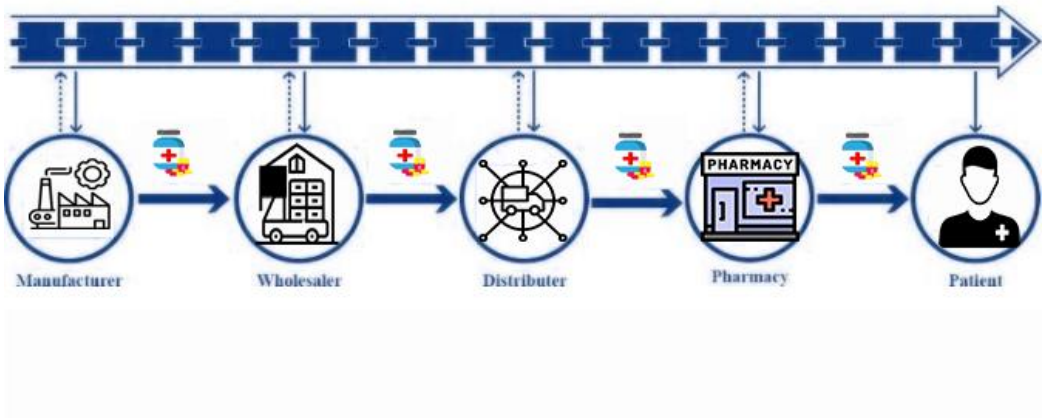

Figure 18 Blockchain-Based Management System for the Pharmaceutical Supply Chain [225].

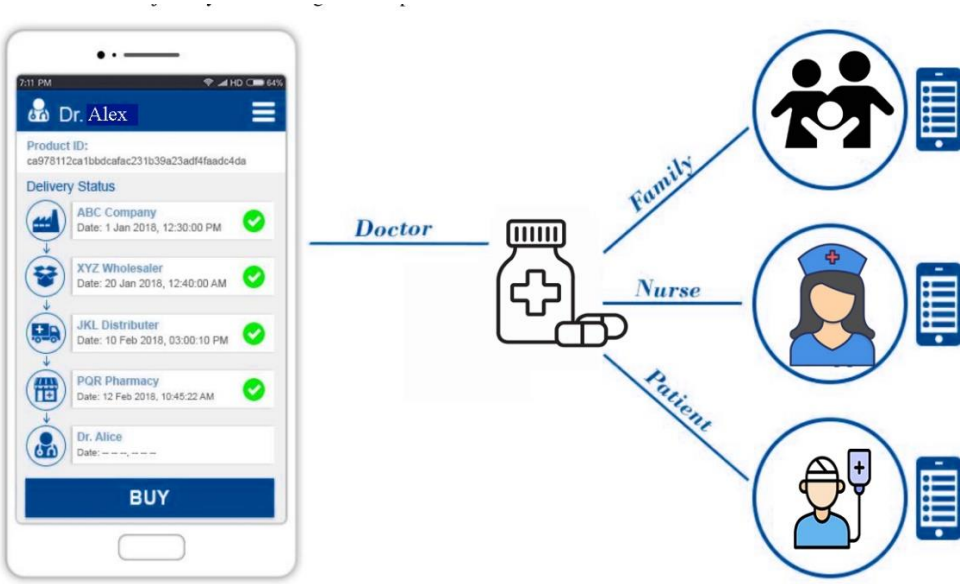

Figure 19 User Interface Layout for Blockchain-Based Pharmaceutical Supply Chain Management [225].

Figure 19 describes a basic plan of the front end of the system pertaining to the blockchain-based pharmaceutical supply chain management (SCM) system. This shows how users engage with the system through a basic and easily downloadable mobile application. It would demonstrate some functionalities that would include product registration, ownership transfer, product history search, and product authentication. The figure explains how friendly the app is while at the same time being secure in its provision of user interface and interaction with the blockchain.

6.2 Clinical Trials and Research

Smart contracts can be used to enable blockchain to automate different aspects of clinical trials, which reduces the error rates and the use of middlemen [227]. The technology allows stakeholders to communicate and share data in real time, reducing time and efforts to manage data information exchange, and ensuring privacy and data security [228]. Blockchain solutions can solve the problem of the patient recruitment process, proper regulation compliance, and cost issues in clinical research [229] and put patients in control of their information access [228]. Altogether, blockchain technology has a great potential to reshape the clinical trials and improve the public confidence in the resulting research [230],[227].

Table 5 Pros and cons of using blockchain technology for clinical trials [231].

Advantages	**Disadvantages**
Monitorization	General access to all key players (need to constrain access depending on its user)
Transparency	Implementation system difficulties
Immutability	Need for specialized technical resources
Decentralization	High levels of protection are needed
Real-time consent	Implementation costs
Real-time access to all key players involved	Scalability difficulties
	Appropriate software and hardware

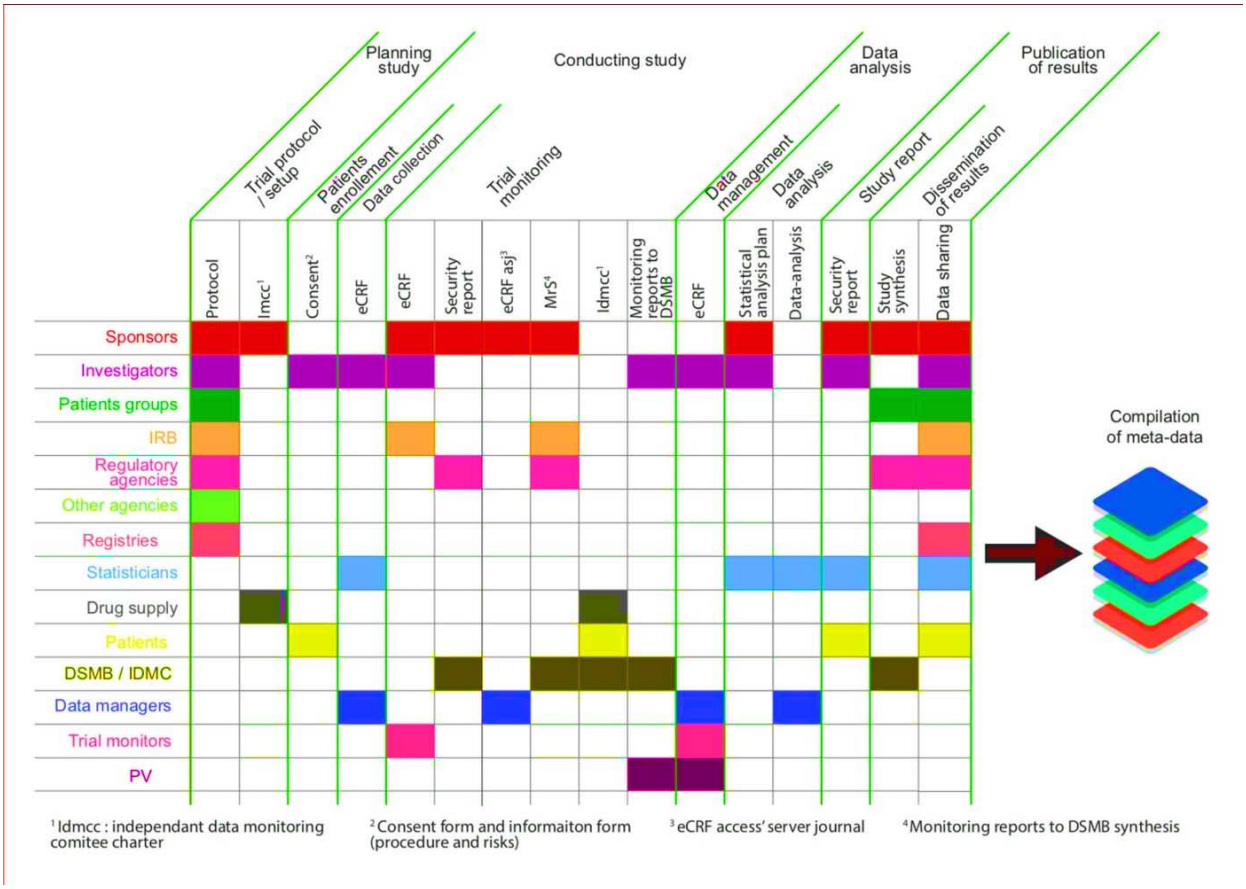

Figure 20 Detailed data structure related to a clinical trial implemented in blockchain with major parties and main steps [232].

Figure 20 illustrates an example of the clinical trial process improving through the implementation of blockchain to make it clearer, more secure, and more trustworthy. Key stakeholders are patients, investigators, sponsors, and regulators, which are described; the overall data processing is illustrated as well as options for consent handling, protocol management, and data storage. Blockchain features such as time-stamp solutions, traceability, and smart contracts deliver ethical conformance, data protection, and automated process solutions. The approach minimizes fraud, improves data quality, and ensures transparency across all phases of the clinical trial.

6.3 Insurance and Billing Management

With the use of blockchain technology, there are possibilities of removing many complications bordering on healthcare insurance and equally fighting fraud. It raises the security and accuracy of data and the openness of data in operation and boosts the effectiveness of clinical practices in the healthcare sector [233]. For instance, the Forti-Ins

framework shows how blockchain can be used to automate the claim-processing functionality and eliminate fraudulent double claims with smart contracts and distributed file systems [234]. Through the application of blockchain to insurance healthcare, the system achieves identification of insurance fraud by its transparency and unalterable nature [235]. Blockchain technology being utilized to store patient health records in an encrypted format at the servers facilitates healthy and secure claims processing where insurance companies can access bills and reports without the chance of being tampered with [236].

Table 6 Key Characteristics of Blockchain in Healthcare Insurance [235].

Characteristic	Support for Insurance Fraud Detection
Automation Using Smart Contracts	Smart contracts optimize procedures, management of insurance policy terms, integration with other datasets, and identification of deviations from the set patterns.
Digital Authentication and Access Rules	A digital wallet stores keys, and smart contracts integrate authentication and access rules for seamless management of access.
Shared Intelligence	The use of peer-to-peer (P2P) platforms facilitates collaborative efforts in the areas of claim processing, fraud detection, compliance, hospitalization control, and frequent prescription monitoring.
Transparency and Immutability of Data	Blockchain provides better security for healthcare records, governs dispensed medications by pharmacists, and enhances the Know Your Customer (KYC) and Anti-Money Laundering processes (AML) with higher safety.
Decentralization	P2P networks offer reliable, fault-tolerant storage that guarantees that the essential data is always available while also incorporating reputation scoring systems.

Vahiny Sharma, Ankur Gupta, N. Hasan, Mohammad Shabaz, and Isaac Ofori expose the transformational promise of applying blockchain technology in relation to secure health care systems. They derived the following potential application of blockchain technology within the health sector from 97 papers selected from 149 research articles.

Table 7 Healthcare domain, issues, and blockchain solutions [237].

Domain in Healthcare	Existing Problems	Blockchain-Based Solutions
Patient record management	Lack of access to complete medical records; ownership issues	Providing access to complete medical records, Restricting repeated diagnostic tests, allowing new doctors to learn about past patient histories.

Domain in Healthcare	Existing Problems	Blockchain-Based Solutions
Maintaining consistent permission	Accessing data takes a lot of time; permissions are not consistent.	Access to the data is fast-tracked, permissions are managed securely, minimizes time to obtain patient information,
Billing system	The system is not transparent; it takes a lot of time and resources.	Secure and transparent billing system, uses fewer resources, time, and cost.
E-medicine system	Security flaws in virtual connections; risk of data leaks.	Removes intermediaries, ensures secure, immutable, and untraceable distributed systems,
Drugs management	Fake medicines, pharmaceutical traceability, drug supply chain security, and multiple drug dealers.	Creates clear drug traceability, eliminates fake drugs and ensures data security.
Clinical trials and correctness of data	Incorrect data reporting; lack of transparency.	Improves data credibility, enhances the precision of analytics, and manages genomic sequences in personalized medicine.

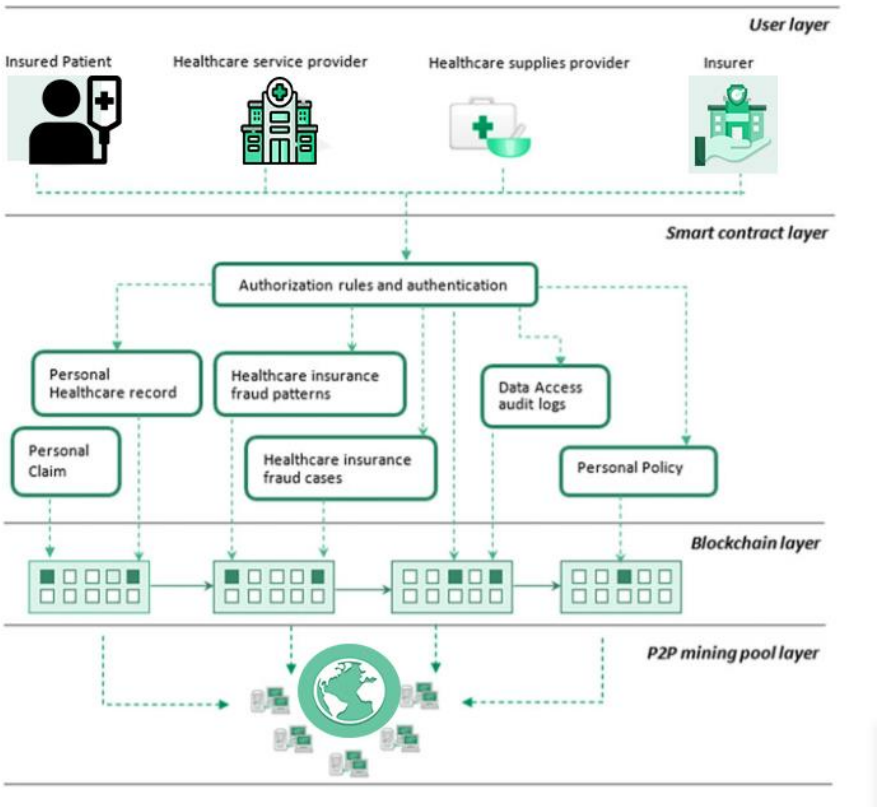

Figure 21 The blockchain-based healthcare insurance fraud detection layer [235].

7 Limitations and Challenges

However, there are challenges that blockchain experiences when implemented in healthcare. Challenges that are inherent to the deployment of blockchain refer to scalability issues such as block size constraints and large volumes of data [238]. Others are the compliance issues, compatibility issues, and issues to do with data privacy [239]. Other drawbacks of applying blockchain include technical challenges and power usage in some blockchain executions, which are also worth acknowledging [240]. In order to solve the above-mentioned challenges, researchers suggest possible solutions like storage optimization or redesigning blockchain [238]. Solutions include constructing rules to govern blockchain, working on real-world compatibility concerns, and funding other blockchain research and development [239],[237]. It is believed that with the development of technology, many technical issues will be addressed [237]. The following table offers a better structure of the problem area, pointing out the challenges of using blockchain in healthcare by their nature and areas of focus. This way, it helps stakeholders to be aware of some of the challenges that hinder its successful implementation.

Table 8 Categorization of Challenges in Blockchain Implementation for Healthcare [241].

Dimension	Category / Type
Technological	Security
	Privacy
	Integration
Adoption	Interoperability
	Compatibility
	Standardization
	Data Governance
Operational	Scalability
	Data Availability
	Accessibility
	Usability
	Data Sharing
	Data Processing Speed

7.1 Technological challenges

Actually, blockchain has a lot of potential for use in the grid, leading to the effective storage and exchange of medical data; however, there are problems with such usage. Privacy and security continue to be an issue since data leaks and unauthorized access to patient data, although encrypted, compromise patient information. Data must be protected against manipulations since they may result in adverse effects on the processes of patient treatment. Challenges include regulatory compliance as data access and sharing stay within specific legal guidelines, increasing the concern for compliance and making solutions hard to implement. The issue of access is also an issue demanding a system that provides restricted access to allow only certain personnel to access fortunes but provides patients with complete control over their data. Interactive connectivity is limited with preexisting healthcare systems, as many are antiquated and unable to integrate with blockchain technology cost-effectively. Additional barriers include high implementation costs and resistance to change because, despite its possible benefits, adoption of blockchain by healthcare organizations may be seen as too risky or difficult. The mentioned questions require attention as critical factors influencing the application of blockchain technologies in the healthcare field [241].

7.2 Adoption challenges

Exploring major issues concerning the implementation of blockchain technology in healthcare with special reference to issues such as interoperability, standardization, and data control. Lack of homogeneity, hence interconnectivity, is an interoperability problem that hinders various blockchain systems from securely sharing patients' sensitive health information. Lack of standards across organizations and lack of regulatory compliance cause the issue of standardization to be unclear with legal, ethical, and privacy issues. Data governance issues include privacy, which is essential to patients, and the need to secure patient consent for data sharing. Secondly, data quality, or accuracy, is important [241]. This decentralized, distributed ledger system encouraged trust of multiple parties without the need for central bodies. However, it could be seen that different operational models may demand the stakeholder to act as a regulator for satisfying the governance as well as the regulatory needs of the healthcare industry. Exercising such a governance structure in a system with diverse parties remains ambiguous and its relation to incentive structures. It will therefore be

anticipated that, as adoption of blockchain technologies advances in the healthcare domain, new and suitable governance strategies will be developed to overcome these issues [220]. R. D. Garcia and G. Ramachandran make headway with addressing data privacy and governance issues in multi-stakeholder applications through the implementation of blockchain technologies, proxy re-encryption (PRE), and BBS signatures. It guarantees immutable data storage and avoids centralized vulnerabilities, while PRE provides secure ways to transfer decryption privileges so that only relevant participants will have access to information that they are allowed to read. BBS signatures allow for partial disclosure of data while preserving the identity and confidentiality of a subject. Smart contracts help with truly informed and consensual processing since data owners can control the permissions and monitor further usage for transparency. This approach helps withstand proper and secure sharing of information that is also cost-effective and promotes trust amongst the stakeholders [242]. Accuracy and quality of data are essential for blockchain since the functioning of a blockchain system depends on such data. Data quality and accuracy is, however, likely to be an issue given the raw nature and heterogeneity of the healthcare data. The reliability and trustworthiness of the data that are involved in the blockchain-based healthcare systems depend on the parameters or regulations that describe the quality and correctness of data [243].

7.3 Operational challenges

A major problem for healthcare blockchain systems to address is related to their scalability that limits their applicability. Concerning system considerations, the first one is the block size that limits the size of data to be stored per block, and this is a challenge when trying to accommodate healthcare big data such as genomic data. Further, its presence in large quantities within healthcare systems hampers performance and raises power consumption and operating expenses. Transaction processing also poses immense challenges in scalability since current systems make all the validators approve each transaction regardless of the network speed or computational complexity. Another factor related to scalability is that networks have more nodes the higher the latency is, and more resources are needed. Another pretty significant issue is that of limited protocols, including such platforms as Ethereum, that hardly scale for security, speed, and flexibility. For example, immutable records create problems of accessibility during emergencies; lack of dynamic protocols for accessing records affects responsiveness. These have underlined the necessity for invention and effective ways, such as

enhancement of the storage optimality and restructuring of blockchain network models with a focus on scalability while keeping high-security possession and authenticity of health information. Overcoming these challenges is possible, and if achieved, blockchain can manifest itself as a reinvigorating solution to healthcare systems. Such proposed solutions can be of two types; to be more precise, the optimization of storage and redesign of blockchain [238]. Sharding, which is the division of the network into subgroups for parallel processing, has been brought forward as a probable solution to increase scalability in the application of the blockchain in healthcare [244]. Some other interesting prospects include the hybrid system and the off-chain computations [245]. Nevertheless, there are still a number of challenging issues that need to be solved in more detail in order to achieve better scalability of blockchain-based EHRS.

Figure 22 Scalability issue-solution mapping [238].

Data quality also has an influence on the application of blockchain in healthcare [241]. Some current shortcomings of the technology include the fact that as the technology develops, the processing speed, as well as duplicate data handling, is expected to be rectified [237].

7.4 Regulatory and legal considerations

There are legal and regulatory issues in the implementation of blockchain in healthcare. Data protection, data security, and consent, along with compliance, are the big focus [246]. As it will be seen, different countries have different legal requirements, thus causing the need to harmonize the set laws [247]. Adopting blockchain technology is advisable for healthcare institutions on the condition that they carry out business and technical due diligence [248]. Consequently, the technology has to leverage the impact and, at the same time, respect privacy rights and data protection realms. Continual cooperation with legal, health, and IT professionals is decisive to create valid structures [247]. The technical issues contain trusts and disparities between healthcare and cryptocurrency-based data. To reduce risks, it is advised that the project should go open source and be aligned to standard industry practices [249]. Although the views of European countries on the legal treatment of such technologies are diverse. Farouk and Alsamara stated that different legal systems of the states and their different interpretations of the EU law, including the GDPR, affect the fragmented ecosystem of using blockchain in the healthcare sector. An issue is the realization of the immutability feature of a blockchain to comply with the GDPR's 'right to be forgotten' provision, where a person's data will be erased. Solutions derived include permissioned blockchain or cryptographic techniques that would conform to data protection regulations. In the same respect, whilst the GDPR offers generalized legal requirements, national laws like the Data Protection Act 2018 in the United Kingdom and the Loi Informatique et Libertés in France add layers of complexity. Thus, deterministic legal integration is critical in promoting blockchain systems properly. Smart contracts solve problems like health insurance claims and contractual obligations in the healthcare industry but have legal problems. Legal complexities result from jurisdictional questions due to the fact that it is hard to define which law governs blockchain. Furthermore, the regulation of the law is challenging due to regional differences in the laws of different geographical locations; this makes the formulation and implementation of smart contracts quite a challenge. Finally, the document provides guidance on how to overcome common barriers to blockchain implementation in health care. One of them is to highlight that under the EU there must be some common set of rules with a focus on the measures to reduce the dissimilarities between national and Europe-wide legislation. To overcome the data privacy and compliance challenges, there are recommendations towards making use of permissioned blockchains and better cryptographic solutions. Further, the study

emphasizes the need for further awareness-raising of the possibilities and drawbacks of blockchain to policymakers, clinicians, and the general public to prevent ineffective and flawed implementation [246].

8 Case Studies and Real-world Examples

Blockchain has great potential within the healthcare industry, including the problems of data fragmentation, clinical trial reporting, and fake drugs. Some of the popular application areas are patients' information handling, the discovery of new drugs, procurement and distribution of medical products, and online doctor-patient consultations [220]. Yet, the experience of initiating blockchain in general is still to be expected to be gradual when it comes to applying it to healthcare in particular. The technology of shared, community, trusted ledgers across organizations that the technology affords has the potential to revolutionize the delivery of healthcare and the biomedical sciences [250].

8.1 Blockchain Applications in Clinical Trials

Blockchain technology integration in clinical trials is a new way of making changes to difficult issues in the healthcare and pharmaceutical sectors. Challenges that clinical trials experience include data integrity problems, patient recruitment problems, regulatory barriers, and opacity. The emerging breakthrough solutions to these challenges are provided by Blockchain – the decentralized, secure, and non-tampered platform that promotes trust and cooperation among the parties of interest [229]. Some of the groundbreaking platforms and initiatives, including Clinical Trials Intelligence, TriNetX, Innoplexus, Triall, and Embleema, are already implementing the blockchain to transform the clinical trial processes. All of these applications apply the blockchain in areas of data security, increased openness, optimization of processes, and patient-oriented studies. Many of them have the prospect of employing artificial intelligence and safe data transfer solutions to reform clinical trial effectiveness and reliability.

CTI, which stands for Clinical Trials Intelligence, is a blockchain solution created by ClinTex that aims to enhance some of the primary issues in clinical trials, including operational productivity, predictive analytics, patient enrollment, risk management, and data display. It controls access, payment of compensations, and storage of clinical data through the use of smart contracts laterated on Ethereum. They are ChainLink to access the data measuring decentralized and Storj to store data with encrypted measures. Furthermore, CTi uses its own token as a means of both data access and as a means of payment to investigators and third

parties. Working in partnership with Intellimed, ClinTex is seeking to promote the use of CTi in academia and has plans to engage with some of the world's largest pharmaceutical firms in order to do so [251]. TriNetX is a global federated network of EHR data that is developed to enhance clinical research and the efficiency of trials. It gives medicinal companies and healthcare organizations (HCOs) partners admittance to information-based study design and patient enrollment [252],[253]. TriNetX has grown steadily, being founded in 2017 with only 55 HCOs across 7 countries while operating with over 220 HCOs across 30 countries in 2022. The network has started more than 19 thousand sponsored clinical trial opportunities and has published more than 350 peer-reviewed articles [253]. West Virginia Clinical and Translational Science Institute (WVCTSI) researchers have real-world data from over 40 health organizations via the TriNetX platform that is built on blockchain. Members of the TriNetX network contribute data through a decentralized model, which provides monthly availability of new observation, discovery, and prescription order data. It comprises major academic medical centers and public/private hospitals that are located in four US census regions by attending to patients across the demographic spectrum. Also, this platform provides rich analytics tools that allows to determine the impact of the medical codes on patients and provide a statistical comparison of such outcomes. Innoplexus focuses on the research and development of life sciences with an incorporation of blockchain with artificial intelligence to provide advanced solutions in pharma and clinical research. The platform is made use of by 250 professionals and can accommodate multi-stage research designs, while the use of exclusive AI technologies and life sciences ontology makes work potential, offers real-time intelligence, and unveils new patterns at every stage of drug development. The demand for global clinical trial software is growing because the industry is now being digitized and adopting technology. Triall is using blockchain to build a decentralized clinical research network that can increase trust, data quality, accountability, and compatibility to improve the medical pipeline. It proposed a vision on how all the clinical research employees or associates could engage online and further proposed that blockchain technology could enhance data integrity, thereby enhancing quality and compliance. Another example is Embleema. Patient recruitment and study design are provided as a virtual research suite to ensure the accuracy and transparency of data. It allows patients to provide and sell their data safely, using wearable devices to gather additional data in the real world on the blockchain [251].

8.2 Revolutionizing Healthcare with Blockchain Technology

Blockchain technology is anticipated to play a revolutionary role in managing health data and to answer key issues with security and data sharing [254],[255]. Its property makes it more secure and private and provides ownership of health data to the patient [256],[254]. Blockchain makes healthcare systems of different formats interact through smart contracts and standardized formats [255]. It enhances the record-keeping of the medical practitioner to ease and enhance the validated patient record entry [257]. Some of use electronic health records, medical imaging, clinical trials, and drug supply chain management [256]. The subsequent discussion draws examples of innovative business and market entities leveraging blockchain in reshaping multiple capacities of the healthcare system and its functioning.

Table 9 Healthcare Industry Transformation via Blockchain [258].

Company/Platform	Industry	Applications
MEDREC	Big Data, Cybersecurity, Software	Through using blockchain technology, the MedRec shields electronic health records and medical research data. It controls the authentication, confidentiality, and data storage.
BURSTIQ	Big Data, Cybersecurity, Software	Optimizes the process of processing the medical data with the help of blockchain. It is a HIPPA compliant platform for blockchain-driven on-chain data management, multi-layered data ownership, and passive permission, which is being implemented by government agencies and big organizations.
FACTOM	Enterprise Software, Information Tech	Uses blockchain technology to assist the healthcare sector in managing the protection of digital records in the firm's blockchain system.
MEDICALCHAIN	Electronic Health Record, Medical	Uses a blockchain system of health and record keeping that ensures that records cannot be altered and the record has a record of having come into as well as keeping the identity of the patient safe.
GUARDTIME	Cybersecurity, Blockchain	Assists the healthcare corporations and governments to integrate blockchain into their security strategies.
ROBOMED	Blockchain, Medicine	Deploys the blockchain technology to more securely collect data pertaining to the patient and disseminate it to his/her care providers.

Company/Platform	Industry	Applications
PATIONTORY	Blockchain, Cybersecurity, Healthcare, Information Tech	For the safe storage and sharing of crucial medical records, it utilizes a blockchain platform.
BLOCKPHARMA	Blockchain, Pharmaceuticals, Supply Chain	Uses blockchain technology and has a solution to drug traceability and drug counterfeit products.
NANOVISION	Blockchain, Cybersecurity	Interconnects the advantages of the blockchain with AI to acquire information from traditional data repositories and incompatible record systems.
TIERION	Blockchain, SaaS	To retain an immutable record of ownership and history of the possession of documents, records, and medications, it employs blockchain to audit those within and across medical supply chains.
CONECTINGCARE	Cybersecurity, Blockchain	It deals with monitoring the progress of patients who move out of the hospital. It monitors the progress of patients who are discharged from the hospital.
NEBULA GENOMICS	Biotechnology, Genetics	Utilizes blockchain to cut through the redundant expenses and intermediaries required in the process of genetic studying.

8.3 Blockchain in Global Healthcare

The use of blockchain technology is likely to improve the key facets of medical data exchange in the healthcare systems throughout the world [259]. Some countries are looking at measures towards adopting blockchain in healthcare systems. Estonia, for instance, has recently earmarked itself in the league of the world's most advanced nations after it secured more than a million of its citizens' health records through blockchain technology through GovTech partnerships [260]. Sweden is already using CareChain, which is the national and connected blockchain health data. In the United States now, the healthcare industry is implementing blockchain in its companies [261]. Principal among them are initiatives meant to solve problems like EHR system dominance, issues of information security, and data interoperability. The use of blockchain has been proposed to enhance the credibility, protection, and confidentiality of the healthcare information even when there can be compromises in efficiency, space, and money [262]. The U.S. healthcare industry is only just beginning to introduce the blockchain into its system by solving the problem of the absence of an adequate base. In 2018, several market stakeholders, such as UnitedHealthcare, Optum,

Humana, Quest Diagnostics, and MultiPlan, began experimenting with using blockchain technology to manage data on healthcare providers with the goal of increasing accuracy and efficiency in sharing this information. Thus, the cooperation of the competitors is more typical with regard to the development of gross trends than blended attempts. That is why the project proves the effectiveness of blockchain in managing healthcare processes and calls for the expansion of cooperation in other areas to build a more extensive national blockchain network [261].

8.3.1 Europe Leads in Healthcare Blockchain

The section titled “Europe Takes the Lead” highlights the advancement made by Europe in implementing blockchain technology in the healthcare system. The EU is bringing out innovations such as the MyHealthMyData platform that undertakes the sharing of biomedical data through the use of blockchains and enables every individual to have their personal health data stored in a manner that the data can be accessed across all available devices. Such a transnational endeavor for electric vehicles can be backed by a consortium structure of private, academic and other forms, which may build the potential for emulation by US policymakers. On a national level, Sweden’s CareChain is best captured within the context of coordinated pluralist blockchain architecture governance across hospitals, insurance, start-ups, and governmental organizations. Estonia also exemplifies this leadership since it had forwarded more than 95% of its health information by the year 2012, including electronic billing and electronic prescriptions. These initiatives show that Europe is determined to change healthcare systems with the help of blockchain technologies and bring efficient collaboration by using various partnerships and holistic approaches. This model can be used to support any country that wants to achieve implementation of blockchain in health care [261].

8.4 Estonia’s Blockchain Healthcare Innovation

Estonia has taken the challenge to position itself as a global hub of blockchain in healthcare with the goal of mitigating increasing costs and ineffective processes. Since 2011, through cooperation with the company Guardtime, the authorities have used blockchain for sealing public records, and since 2016, they have expanded it to such a sphere as healthcare, where over one million people’s health records are now protected. Regarding priorities and

objectives of the Estonian e-health system, this initiative demonstrates Estonia's potential to leverage blockchain as not simply a subversive technical solution for the financial and legal sectors, but as a versatile technological breakthrough in general and a platform innovation in particular, which is capable of solving a number of fundamental problems facing the spheres of healthcare. Currently, Estonia has institutionalized the use of blockchain through partnerships with GovTech, which makes a strong, infallible environment that guarantees the integrity of data and access to the permitted individuals. It is anchored on the nation's strategic vision, technological infrastructure, and sound legal standards, which have included the Health Information System Act of 2007. Reflection of Estonia shows that innovative and improved public-private partnerships can become a powerful tool for change. In Estonia, when implementing blockchain-based solutions in healthcare, the experiences and lessons acquired were also practiced in other digital governance, like eTaxes, eElections, and eSchools. This is in some ways a deliberate application of the concept of 'value capture,' where the positive effects and efficiencies of one technology are carried over into other areas for the greatest overall return on investment. Nonetheless, like the overall life expectancy, there are many problems that we still face; Estonia's systematic approach to the innovation makes it a worthy example for nations that are striving to modernize the healthcare through the technologies [263].

8.4.1 KSI BLOCKCHAIN

- Origins and Deployment

KSI Blockchain was first created in 2008 for the government of Estonia as the first instance of improving the security of its valuable healthcare, law enforcement, and business data. Given the growing importance of implementing various secure and solution-based technology solutions, Estonia stepped forward as a pioneer of implementing this new technology for maintaining trustworthy information security processes by using blockchain technology. Many people assumed that KSI Blockchain was unique to Estonia, but over the past few years it has been adopted in numerous fields. Governments all around the world and companies in telecommunications, aerospace, defense, energy, financial institutions, and insurance industries have embraced this technology as their solution to their data security concerns. Widespread installation bears witness to the effectiveness of its application to satisfy the demands of the world's most voracious and cautionary data consumer and user organizations [264].

- eIDAS Compliance

Guardtime has developed KSI Blockchain Timestamping Service as its advanced product, which complies with eIDAS regulation to establish electronic identification and trust services for electronic transactions throughout the European Union. This compliance also means that KSI Blockchain is now on the European trusted list, which is major because it speaks for the reliability and creditability of KSI Blockchain. For instance, KSI is a unique blockchain-based technology that became the first one to gain an eIDAS accreditation, which paved the way for the advancement of digital trust technologies. Even though this syntax accreditation was done by TÜV Nord in Germany, it affirms the standard of security and trustworthiness of the technology. It puts KSI blockchain in a position of authority in the sector and creates a standard against which other blockchain-based solutions seeking to gain comparable degrees of compliance and credibility can be measured [264].

8.4.2 Methodology and Technology Overview

I have provided a technical analysis of the Keyless Signatures Infrastructure (KSI) in subsection 4.3.2. KSI employs cryptographic hash functions SHA-256 or SHA-3, and it provides unique digital signatures for files [265]. This particular digital signature technology is unique to Guardtime and called the Keyless Signature Infrastructure, or KSI for short. It embraces a cryptographic technique known as the hash tree, or Merkle tree, to reduce the risk of a data alteration. For every second, users upload the hash values of their data to the system, and the hash values are grouped in a bigger data structure called the global aggregation tree. The global root hash value, situated at the highest most level of this tree, is appended to another chain known as the Calendar Blockchain, which contains successively subsequent hash values for check purposes. At the time of submitting the data, the users get a signature token of their information that asserts it and its content. This token consists of several hash values that lead back to the global root hash value, facilitating a user who has to validate their data’s authenticity against the blockchain.

KSI is based on a permissioned private blockchain because users must identify themselves, and KSI is managed by Guardtime through a distributed network of servers around the globe. The system attains a theoretical throughput of 250 quadrillion signatures per second given by the fixed hash tree depth of fifty levels of the system, but in terms of practical channel throughput, it achieves approximately 1 trillion signatures per second given the overheads involved in such a system. It is also important to mention that KSI has a public verification

tool: the root hash of the Calendar Blockchain is disseminated by public means. This ensures that users can easily check on the data they have provided once the Guardtime company decides to close down [266].

The KSI infrastructure comprises distributed Black Lantern Security Appliances deployed in the roles of cores, aggregator, and gateway. These components accurately process and verify signatures, allowing for binary scalability to billions of transactions per second while occupying a storage space of no more than 2GB per year [265].

In comparison, KSI provides a much better mechanism for data identification. Unlike other blockchains, KSI scales temporally instead of transactionally and involves efficient computing of industrial data authentication. The use of cryptographic hashing instead of keys or public key infrastructure (PKI) reduces the issue of key compromise while data privacy is achieved without exposing the content of the original file. Credibility is evidenced by real-time capabilities for the processing of signatures as opposed to the unending minutes that blockchain systems take in safeguarding validation. Furthermore, as part of KSI operation, KSI signatures are inherently portable and consequently incorporated in digital assets to offer everlasting authorization of the value and the time of creation while keeping data integrity comprehensive [265].

8.4.3 KSI vs PKI Signature

Table 10 Comparison between KSI and PKI [266].

Feature	KSI	PKI
Core Mechanism	Relies on one-way cryptographic hash functions (for example, SHA-256 or SHA-3).	Uses public key cryptography (e.g., RSA, ECC).
Complexity	hash value + user ID + parent node hashes.	More complex includes public/private key pairs, certificates, timestamps, and metadata.
Signature Validity	Indefinite, not dependent on external validation.	Valid as long as the CA-issued certificate is valid.
Quantum Resistance	It is immune to quantum computational attacks.	Prone to quantum attacks because they depend on public key cryptography.
Trust Requirements	Reliance on the organization responsible for its credentials and Guardtime for authentication.	Trust pertains to the organization that handles the keys and the CA that issues certificates.

Feature	KSI	PKI
Signature Verification	It can be done independently utilizing the published Guardtime records or through the KSI access points.	It has to be verified with the help of the signer's public key and CA certificate.
Operational Mode	In order to create signatures, there must be a connection with Guardtime, and it's online.	Signatures can be created without an online connection.
Impact of Breach	Only the credentials of the organization in question are affected; other signatures remain legitimate.	Catastrophic; if there is a breach in CA or an organization, then it has an impact on all related certificates and signatures.
Revocation	It is not required that signatures remain valid indefinitely.	In order to revoke certificates, if keys or CAs are compromised, it totally depends upon revocation.
Use in Breach Detection	Not only can they validate access logs for determining breach timelines but also retain pre-breach signature integrity.	Offers no inherent mechanism for breach detection; compromised signatures lose validity.

8.4.4 Healthcare Applications of the KSI Blockchain

KSI is specifically designed to imbue authenticity and allow the attestation of the integrity and is therefore well-suited for health and healthcare applications. KSI guarantees that EHR is 100% accurate and non-fake, which is crucial in case of emergency decisions, and tracks the real-time status and safeguards personally identifiable information (PII), thereby meeting the letters and spirit of privacy acts. It also provides secure and easily auditable trails for telehealth communications as a means of enhancing public confidence in remote care solutions. In addition, it validates clinical trial data and clinical research information to ensure compliance with regulatory requirements; also, it provides the tracking and validation of health care transactions to minimize fraud and suspicious payments [265].

8.5 MediLedger

The MediLedger project, therefore, is an innovative solution being developed based on blockchain technology to counter the use of counterfeit drugs in the American markets. It employs zero-knowledge proofs in order to ensure that the belonging of the product is verified, but at the same time, preserve the privacy [267]. MediLedger implements blockchain technology to serve both industry supply chain enhancement and compliance purposes under

the Drug Supply Chain Security Act (DSCSA) US regulation. It uses Hyperledger Fabric to design a private blockchain infrastructure that would help track drugs and prevent counterfeit medicines [268]. MediLedger emphasizes the challenges that exist in the life science business on the distribution of manufactured pharmaceutical drugs to consumers. This ranges from regulatory issues that characterize the industry, complex pricing and contracting structures, and many exemptions to industry norms in business dealings among transacting parties. Overall, through the use of the blockchain technology that Mediledger uses, the buying and/or selling companies are able to retain control and have control over the data and information that they exchange with other partnered companies. It also allows the automation to go beyond the company's internal environment, providing increased value to the other players in the pharmaceutical supply chain in terms of collaboration, effectiveness, and obeyance to the rules [269].

8.6 My Health My Data (MHMD) (European Union)

MHMD (My Health, My Data) is a project supported by the European Union with a goal of changing the paradigm of biomedical data management, focusing on privacy of data, security, and primary ownership. It is designed to introduce blockchain technology and smart contracts in order to form the network to exchange health data safely and independently. At MHMD, have developed a data profiling system that categorizes data based on its informational and economic characteristics, where specialists use anonymization, pseudonymization, and homomorphic encryption for superior safety but with the potential to provide backup for analytics and artificial intelligence. Dynamic consent allows users to have choice over the use of their data and will help to build trust between patients, hospitals, researchers, and commerce. The project rests on GDPR principles to provide a safe platform for healthcare data and to create a culture of proper data utilization. The methodology consists of behavioral and ethical assessment of complex digital health services and uses hacking to stress check the system. MHMD proposes here a way of reaching this potential, as follows: Every one of these activities-recording, storing, analyzing, and sharing EHRs will ideally be run as a separate module [270].

8.7 PharmaLedger

PharmaLedger is a three-year project that started in January 2020 and is supported under the European Commission's Horizon 2020 Program and the Innovative Medicines Initiative 2 Joint Undertaking by Grant Agreement No. 853992. It plans to establish a decentralized solution grounded in blockchain that will allow stakeholders in the healthcare sector to collaborate securely and privately. On the fundamental principles including decentralization, transparency, and immutability, the platform follows protection of regulations and data privacy while solving use cases of supply chain, clinical trial, and health data. With the help of creating a favorable ecosystem for the use of blockchain solutions, such as PharmaLedger, the project aims to improve the functioning of the healthcare sector and minimize costs, risks, and compliance issues. Being spearheaded by a consortium of 29 partners, which include 12 big pharmaceutical firms and 17 public and private institutions, the project is working on a governance model to foster partnership and optimize the value of digital health, which would in turn have a benefit to patients [271]. Like in MyHealthMyData, PharmaLedger is an example of experiments with blockchain in maintaining the secure healthcare data flow and problems like the incompatible data formats and unauthorized data access [272]. These examples show how blockchains can be used to accomplish the collection and control of healthcare information without violating its privacy, to the credit of all members from manufacturers down to the patient [273].

The general architecture description of the PharmaLedger platform appears in the article written by Halid Kayhan. The structure of PharmaLedger becomes clearer through this explanation along with its essential role for OpenDSU. Here's an analysis:

- Methodology

The Pharmaledger platform uses a hierarchical blockchain system comprising several independent blockchains that can be integrated into the platform for specialty tasks such as identity management and specific applications of Pharmaledger. The Pharmaledger platform uses a hierarchical blockchain system comprising several independent blockchains that can be integrated into the platform for specialty tasks such as identity management and pharma applications. Its methodological approach is based on hierarchical anchoring in multiple tiers of blockchain, which guarantees the immutability and flexibility of data and code without changing the application code. One module, the OpenDSU (Open Data Sharing Unit),

controls encrypted files that are off-chain in blocks but anchored to dispersed ledgers using cryptographic hash, which helps decentralize the data storage for flexibility and compliance. Moreover, KeySSI (Key Self-Sovereign Identity) acts as cryptographic identifiers that are both decryption keys and self-sovereign identifiers for seamless and safe data management that is also compatible across applications.

- How OpenDSU Works in PharmaLedger

OpenDSU is the central element in PharmaLedger's architecture in handling data sharing and privacy, allowing encrypted off-chain solutions to mitigate blockchain utilization and maintain data privacy and potential scalability. It immutably fixes data into the blockchain by way of cryptographic hashes while making it possible to track data. OpenDSU works alongside the user-controlled digital wallet and helps personalize access to an individual's sensitive information, including health-related information, improving privacy and compliance. Also, its design is extensible; that means that there is no need for additional off-chain storage tools for each application and it is reusable.

- Key Features

OpenDSU disrupts the control of the user's data and supports GDPR and such regulations through an innovative approach. Its architectural design is also highly scalable, thereby providing an efficient means of data storage alongside the blockchain as well as supporting massively large programs without affecting the speed of execution. Being flexibly designed, it can work with almost any existing blockchain platform in order to address various use cases. In supporting PharmaLedger's endeavors in supply chains within the pharmaceutical industry, in clinical trials, and in managing data within the health domain, OpenDSU brings the fundamental ecosystem need for secure and open interoperability to these applications [273].

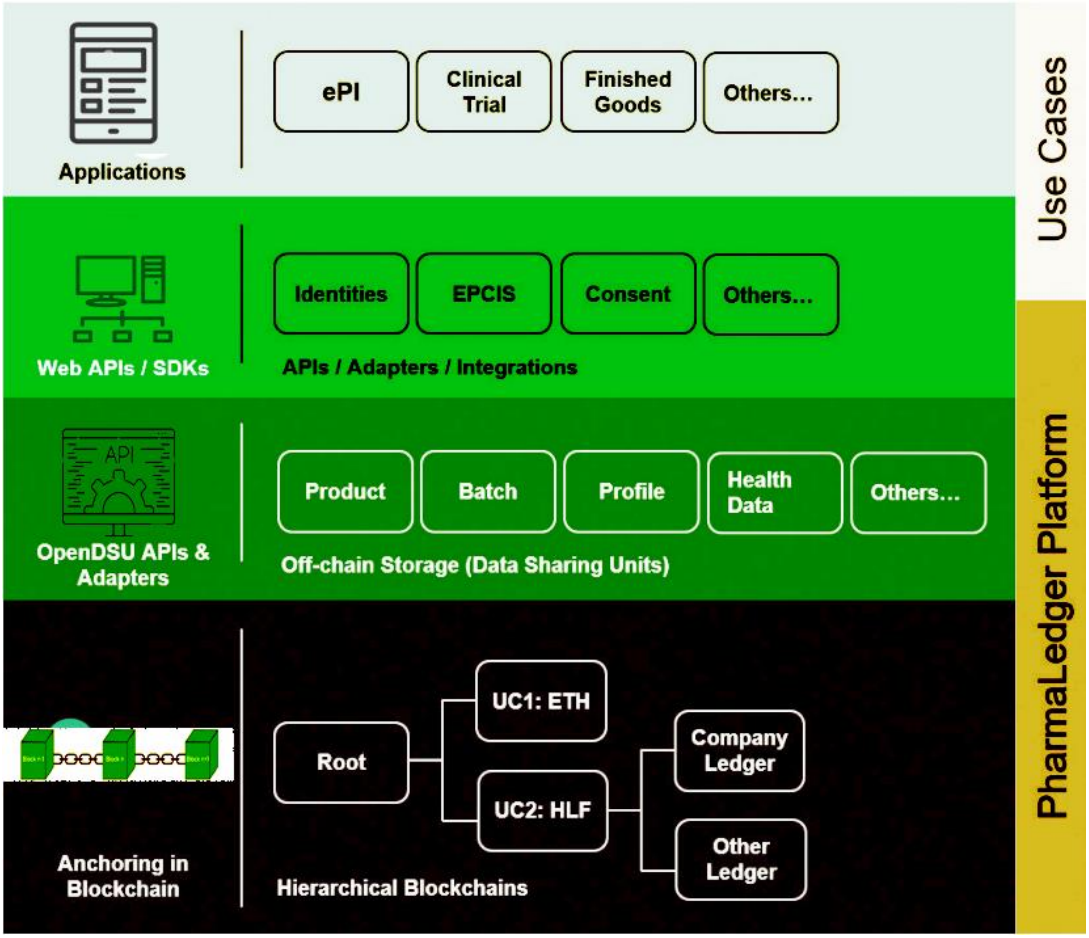

Figure 23 The intricate multilevel layout of the PharmaLedger [273].

8.8 MediBloc

MediBloc is a South Korean company based on the development of healthcare information systems through blockchain technology. Established by Allen Wookyun Kho and Dr. Eunsol Lee in 2017, MediBloc intends to create a patient-centric health data environment supported by highly valuable privacy and accuracy [274],[275]. The company's platform is based on its own blockchain solution known as Panacea; thus, the patients have the ability to be the owners of their health data and share it when necessary. This decentralized approach guarantees the data and makes it trustworthy; it also enhances patient and healthcare provider confidence. MediBloc Limited is developing 'Panacea,' a high-performance blockchain specifically designed for interoperable health data, to form a patient-centric health data network to protect patients' privacy and ensure the highest integrity of the health data.

Moreover, in the decentralized and immutable health data-sharing environment of blockchain, the data could be owned by the individual and utilized in a need-specific manner. Some of the key applications that have been created by MediBloc to support its blockchain-based health care include Dr. palette, an EHR software for medical establishments where they can build and share health information within the MediBloc system. This is accompanied by Medipass, a Personal Health Record (PHR) solution, which enables patients to control the medical data gathered from various healthcare providers in a patient-centric manner. [276].

8.8.1 Consensus Mechanism of Panacea

Panacea is the primary main chain of MediBloc, which is developed as a blockchain-based health information network that aims to solve the important issues that have emerged in the modern healthcare industry by providing personal, reliable, and accurate health information to patients. Since it is a public blockchain, Panacea guarantees the accuracy and ownership of health information by its major operations of hash value logging and verification. The Delegated Proof of Stake (DPoS) in synergy with the Practical Byzantine Fault Tolerance (PBFT) algorithm enables the efficient production of blocks with a one-block finality mechanism to preclude forks and to ensure high security. Other features, such as the slashing mechanism, affect dishonest validators negatively while encouraging voters to settle for genuine validators, thus creating a reliable voting circle. MED coins are paid to both validators and voters depending on contributions on votes and commission charges. Panacea uses Merkle trees to process health data; this allows the sharing of partial cleartext and preserving the entirety as the root hash stored within the blockchain. This approach enables data de-identification and validation of data integrity prior to data transfer, combined with the optionality of cryptographic key selection schemes and long-term data security. Patients are able to manage and modify their information while sharing it with others; institutions receive certain assurances about patient-controlled information. Through clear management of data and protection of patient identity, ensuring patients' consent, and allowing the use of the patient-approved data for patient care and research, Panacea seeks to revolutionize the experience of a patient and create a robust, stable, and secure system for health data [277].

Figure 24 Overview of Panacea's Simplified Architecture [277].

8.9 Patientory

Patientory Inc. is a healthcare data management and analytics company that focuses on using the blockchain to enhance population health. The company utilizes the following decentralized applications: NEITH is an enterprise software, and another one is the mobile application Patientory, which connects siloed healthcare data for analysis and reporting and opens the way for early interventions to decrease overall healthcare costs. Patientory thus adopts blockchain-based platforms as well as artificial intelligence, big data, and deep learning to enable accurate diagnosis of patients and enhance the health care delivery systems. Through the Patientory application for smartphones, patients can make personal, concise profiles to aggregate health data under a private and HIPPA-compliant environment. It involves individual health plans, promotes prevention, and helps support patient, carer, and multidisciplinary team working. Patientory fosters interactivity by developing clear healthcare goals that all stakeholders need to achieve, hence encouraging the active participation in enhancing human health and well-being. It also backs novel future solutions of caring for patients in digital healthcare, such as edge computing, IoT, and distributed deep learning for the improvement of both the reliability and availability of healthcare apps [278].

8.10 Medicalchain

Medicalchain is an environment built under the use of blockchain technology that facilitates the secure, fast, and transparent use of medical data [279]. Medicalchain is a medical data management project based on the blockchain for a successful provision of a high level of safety, decentralization, and full transparency of electronic health records or EHRs. Based on a bi-fractal technological framework using Hyperledger Fabric with patient privacy for Web Care Access and Ethereum for hosting decentralized apps, the patients hold sovereignty over their data and enable the propagation of this information under their terms to healthcare providers, researchers, and insurers. It allows interaction with EHRs while maintaining audibility and privacy for the patient, a revolutionary concept. It also includes additional features such as telemedicine for consultation through a distance and a merchant health data market for selling securely patient data back to patients and developing a healthy ecosystem of patients, doctors, and other stakeholders. The platform solves important issues in the current healthcare environment: existing silos, weak patient-centricity, and security concerns. With the incorporation of blockchain into the information and particular medical data systems, Medicalchain envisions a single-platform approach that will improve data portability, increase data transparency, and increase data security. It pays specific attention to the patient so that they are in a position to handle their data and augmented clinical decisions, thus eliminating unnecessary delays. The vision of the platform is “The Healthcare of Tomorrow”, and according to this vision for the platform, the solutions needed to bring about this vision are things like smart contracts, identity verification, and management of data [279].

This makes patient health interactions completely clear since the blockchain ledger creates transparency in all the interactions with the records. The ability to scale out Hyperledger Fabric is great due to the modularity of the platform, along with great control over permissions through the ACL built-in language, which is perfect for apps that need to align with HIPAA or GDPR. The platform also encourages the protection of data through a high level of encryption method used. Data encryption is employed by the use of symmetric keys for health record encryption, while the public or private key encryption guarantees restricted user access to the data. Dynamic key updates provide even further protection of the patient information in the event that permission is changed. Furthermore, through the API platform, it eases the creation of various interoperable communicative healthcare applications among the developers. Combined, these components result in a robust, patient-oriented, and easily

expandable framework that corresponds to present-day exigencies and contemporary medicine imperatives [279].

8.11 Comparative Analysis

Estonia's use of the blockchain in healthcare focuses on scalability by using the KSI blockchain, which can perform up to billions of transactions per second. This is done through cryptographic hashing and a permissioned private blockchain architecture, security, and efficiency. In the same way, there are initiatives like PharmaLedger that emphasize the applicability of hierarchical blockchain systems in supply chain management of pharmaceutical products together with an integration of data across different stakeholders to allow for consideration of compliance with the laws and regulations. And while Medicalchain and MediBloc focus on data ownership and putting patients in control of it while ensuring data security features the option to share the data safely with medical professionals. Medicalchain is an example of a private effort that lacks scalability and does not have a flexible response to such issues as coherence between subsystems, which Estonia solves structurally and with government support.

8.11.1 Thematic Insights

Those blockchain technologies that are impactful in the healthcare sector include the following: supply chain, patients' data protection, and administration. PharmaLedger & MediLedger initiatives improve drug traceability and fight counterfeiting in addition to compliance with such regulations as the DSCSA. Estonia, MediBloc, and Medicalchain all value the high importance of the data's privacy. Estonia accomplishes this through cryptographic hash functions, while Medicalchain does this with dynamic key updates and API platforms. Moreover, Estonia's application of blockchain in e-governance frameworks shows the sector's capability of optimizing the healthcare management, On the other hand, Patientory mixes blockchain with AI to improve its data analysis to comprehend latency to manage the population's health proactively.

9 Blockchain Innovation and Ethics in Healthcare

The application of blockchain can heavily contribute to the advancement of healthcare practices by reducing data vulnerability, setting increased transparency, and freeing patients [280],[281]. Some of the problems that it can solve include insurance fraud, management of electronic medical records, and connecting or system integration [282]. The use of blockchain in healthcare should consider some ethical issues such as use privacy, equality, and responsibility of using justice in professionalism [280]. Patient willingness to contribute data can be promoted by the technology offering better protection and data handling options. On the same note, secure computation techniques can support meta-analysis while still maintaining patient privacy. Smart contracts and transparent ledgers can provide system transparency and patients authority over their data [281]. Nonetheless, ethical debates on blockchain in healthcare are somewhat limited and require further development to address new emerging ethical issues raised by blockchain use [283].

In the section by the title “The Ethical Imperative in Blockchain Development” from the article Ethics of Blockchain by Design Guiding a Responsible Future for Healthcare Innovation by Muthu Ramachandran, the authors pinpoint the problem of the lack of ethical concerns implemented into blockchain technologies, especially in healthcare. Blockchain utilizes opportunities, which include abilities like unalterable patient records, decentered networks, and clinical trial transparency. Nevertheless, the perceived benefits accrue at the expense of data rights on privacy, governance, and accessibility. One major issue is how blockchain can be immutable while patients have the right to update or erase their data based on privacy regulations such as GDPR. The authors propose options like off-chain data management and the consent layer solution to avoid the aforementioned challenges to blockchain’s basic principles. The section also undertakes the ethical principles related to privacy, security, governance, data ownership, and openness. Proposed solutions include sound cryptographic techniques, distributed access control mechanisms, and conceivably open and punctilious systems such as smart contracts. Ethically developed blockchains can enhance the patients’ confidence in the health systems, besides compliance with relevant laws and orders, besides enhancing the facilities’ accessibility. In this way, blockchain can benefit from the idea of inclusiveness and equal access in order not to make the differences in the sphere of healthcare worse. This paper also discusses the Estonian national blockchain system in the context of secure healthcare by adopting off-chain data storage and blockchain access logging

to adhere to GDPR while maintaining patients' trust. Focusing on data sovereignty, disruption of data ownership regimes, and accountability, it stresses the ethical and policy-compliant features of blockchain in providing for secure, transparent, and fair future healthcare systems [280].

Marielle S. Gross, MD, MBE & Robert C. Miller Jr. propose a solution for the above problems through the use of blockchain technology alongside secure computations in ensuring that a learning healthcare system (LHCS) is implemented ethically. Blockchain guarantees the data integrity due to decentralization and high resistance to tampering and cryptographic controls based on zero-knowledge proof that allows for computations based on encrypted data without revealing the information. This approach improves the patient privacy act and makes it possible to learn from patient data. The ability of this ledger to be open to the public only enhances the possibility of patients' trust because patients can monitor how their data is being used. Say, for example, patients can check when it was accessed or even used to help modify clinical results. Private keys can be written off the chain while only pointers are kept on-chain to serve the purpose of achieving privacy and data security. The solution focuses on patient involvement and fairness through patient-centered decentralization of decision-making processes and by offering tokens or such direct benefits from the conclusion of the research as might benefit the patient. Smart contracts are useful in self-learning activities as well as the deployment of the findings of learning in a way that is both efficient and unbiased. Further, the framework recognizes diverse populations and addresses disparity by making blockchain-enabled solutions accessible to the excluded population, including those in vulnerable categories. In essence, this integrated model seeks to strike a utilitarian and rights-based approach to the optimal development of the LHCS [281].

Sami Hyrynsalmi, Sonja M. Hyrynsalmi, and Kai K. Kimppa wrote an article in the Finnish Journal of eHealth and eWelfare. The paper reviews the practical application of blockchain in healthcare and shows that this technology can transform many sectors, including operations related to patient records and medication distribution systems. Still, it notices a major problem: ethical research is not studied enough, stating that the majority of works mention ethics only in passing without further critique. Without practical ethical tools and frameworks at their disposal, developers are practically on their own, making mistakes when it comes to essentials like privacy, transparency, or equitable outcomes. Despite the desirable attributes such as security achieved through decentralized ledger, the use of blockchain technology

poses risks such as the permanent storage of health information that can be abused or misused due to disparity in legal jurisdictions across borders. The authors asked these questions and underscored the importance of the cross-disciplinary approach to solve the mentioned challenges, pointing out that ethical principles from other fields of ICTs could also be used in blockchain solutions. Several require improved obtainable ethical resources to use for evaluation of risks and implementing responsible practices. Furthermore, they stress privacy and transparency as the ethical, not merely legal, issues. Should the process not be actively managed with regard to ethical guidelines and proper representation of all stakeholders, blockchain has the potential to unwittingly create new skewed states in the healthcare sphere as well [284].

10 Conclusion

The application of cryptography and blockchain technology in solving the perennial problems of the health sector, such as data privacy and compliance, is a unique breakthrough. This thesis has reviewed the state of healthcare information (HI) security today, analyzed prevalent threats and risks, and appraised novel uses of technology but has not endorsed any approach. However, it focuses on the evaluation of conceptual developments of potential solutions and actual implementations. The study first explained how healthcare data is considered sensitive, as well as the growing threats facing healthcare information systems from cyber threats. Security became the primary area of focus for both structure and interoperability in order to ensure proper management and protection of what the report called electronic health records (EHRs) and other forms of sensitive medical data. Blockchain technology was presented as a revolutionary tool, as due to its decentralized, fixed, and clear structure, it can significantly improve the quality of data and trust.

In the cryptography sector, this thesis discussed the methods suggested by authors such as public key infrastructure, algorithms related to secure multi-party processing, and artificial neural network-based cryptographic methods. These methods were examined in terms of their ability to safeguard clinical data and big data analysis against global rules like HIPAA and GDPR. A detailed description based on the mathematical models and an analysis of consensus algorithms was a great example to examine the relevance of the topic to the healthcare blockchain systems. The proposed approaches discussed included Practical Byzantine Fault Tolerance (PBFT), Proof of Authority (PoA), and alterations of existing algorithms with how useful they were to attain security and scalability being compared. Likewise, within the smart contract segment, formulas and paradigms were discussed to analyze how they help decide functions, such as clinical trials, insurance claims, and supply chains.

Real-life applications were Aligned and illustrated through Estonia’s Blockchain, the healthcare innovation is an idea that implements the real-life application of blockchain technology in handling or managing patient data securely and transparently. It showed how blockchain could transform healthcare systems and serve as a guide for other countries and institutions. Despite the absence of any clear preference for any one method in the thesis, there is enough comparative analysis that will let the various stakeholders make informed choices that will not be constrained by the individual requirements and particularities of their organizations. The study also offered straightforward solutions to issues like scalability, the

adoption of the solutions, and regulatory issues to allow further research and innovation for the solutions presented. Altogether, this thesis offers a timely and comprehensive discussion on security by setting out an objective discussion of cryptographic and blockchain technologies. As well as the future advancement of healthcare technologies as a rapidly growing sector with significantly variable problems and issues. These insights can be beneficial for policymakers and industry practitioners as well as researchers for designing robust and protective as well as patient-centric healthcare environments.

List of Figures

List of Tables

References

[1] R. Bernard, G. Bowsher, and R. Sullivan, "Cyber security and the unexplored threat to global health: a call for global norms," *Glob. Secur. - Heal. Sci. Policy*, vol. 5, no. 1, pp. 134–141, 2020, doi: 10.1080/23779497.2020.1865182.

[2] R. Tertulino, N. Antunes, and H. Morais, "Privacy in electronic health records: a systematic mapping study," *J. Public Heal.*, vol. 32, no. 3, pp. 435–454, 2024, doi: 10.1007/s10389-022-01795-z.

[3] Gliklich RE, Leavy MB, and Dreyer NA (sr eds), "Registries for Evaluating Patient Outcomes: A User's Guide Fourth Edition Registries for Evaluating Patient Outcomes: A User's Guide," *AHRQ Publ.*, vol. 19(20)-EH, p. 360, 2020, [Online]. Available: https://doi.org/10.23970/AHRQEPCREGISTRIES4.

[4] S. Upadhyay and H. Hu, "A Qualitative Analysis of the Impact of Electronic Health Records (EHR) on Healthcare Quality and Safety: Clinicians' Lived Experiences," *Heal. Serv. Insights*, vol. 15, p. 11786329211070722, Jan. 2022, doi: 10.1177/11786329211070722.

[5] S. Jayousi *et al.*, "Scoping Review and Case Studies," *Sensors*, vol. 24, pp. 1–20, 2024.

[6] K. Kiania, S. M. Jameii, and A. M. Rahmani, "Blockchain-based privacy and security preserving in electronic health: a systematic review," *Multimed. Tools Appl.*, vol. 82, no. 18, pp. 28493–28519, 2023, doi: 10.1007/s11042-023-14488-w.

[7] C. M. DesRoches *et al.*, "Adoption Of Electronic Health Records Grows Rapidly, But Fewer Than Half Of US Hospitals Had At Least A Basic System In 2012," *https://doi.org/10.1377/hlthaff.2013.0308*, vol. 32, no. 8, pp. 1478–1485, Aug. 2017, doi: 10.1377/HLTHAFF.2013.0308.

[8] G. S. Birkhead, M. Klompas, and N. R. Shah, "Uses of electronic health records for public health surveillance to advance public health.," *Annu. Rev. Public Health*, vol. 36, pp. 345–359, Mar. 2015, doi: 10.1146/ANNUREV-PUBLHEALTH-031914-122747.

[9] R. Brighi and M. G. Virone, "EHR and Usability of Health Data to benefit Patient and Public Health," *Med. Informatics Eur.*, vol. 205, pp. 965–969, 2014, doi: 10.3233/978-1-61499-432-9-965.

[10] A. R. Watson, R. Wah, and R. Thamman, "The Value of Remote Monitoring for the COVID-19 Pandemic.," *Telemed. J. e-health*, vol. 26, no. 9, pp. 1110–1112, Sep. 2020, doi: 10.1089/TMJ.2020.0134.

[11] D. Roblyer, "Perspective on the increasing role of optical wearables and remote patient monitoring in the COVID-19 era and beyond," *J. Biomed. Opt.*, vol. 25, no. 10, Oct. 2020, doi: 10.1117/1.JBO.25.10.102703.

[12] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Comput.*

Secur., vol. 97, p. 101966, 2020, doi: https://doi.org/10.1016/j.cose.2020.101966.

[13] D. S. McDermott, J. L. Kamerer, and A. T. Birk, "Electronic Health Records," *Int. J. Cyber Res. Educ.*, vol. 1, no. 2, pp. 42–49, Jul. 2019, doi: 10.4018/IJCRE.2019070104.

[14] R. G. Wiatt, "The new management of recordkeeping," *J. Corp. Account. Financ.*, vol. 31, no. 2, pp. 13–20, Apr. 2020, doi: 10.1002/JCAF.22426.

[15] A. Ahmed, N. Ehsan, E. Mirza, S. A. Awan, and A. Ishaque, "Information technology: A means of quality in healthcare," *Proc. - 2010 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol. ICCSIT 2010*, vol. 9, pp. 26–30, 2010, doi: 10.1109/ICCSIT.2010.5564669.

[16] R. Tertulino, N. Antunes, and H. Morais, "Privacy in electronic health records: a systematic mapping study," *J. Public Health (Bangkok).*, vol. 32, no. 3, pp. 435–454, 2024, doi: 10.1007/s10389-022-01795-z.

[17] S. Balsari *et al.*, "Reimagining Health Data Exchange: An Application Programming Interface–Enabled Roadmap for India," *J. Med. Internet Res.*, vol. 20, no. 7, p. e10725, Jul. 2018, doi: 10.2196/10725.

[18] K. Joshi and Y. Yesha, "Workshop on Analytics for Big Data Generated by Healthcare and Personalized Medicine Domain," *Conf. Cent. Adv. Stud. Collab. Res.*, 2012.

[19] J. Luo, M. Wu, D. Gopukumar, and Y. Zhao, "Big Data Application in Biomedical Research and Health Care: A Literature Review," *Biomed. Inform. Insights*, vol. 8, p. BII.S31559, Jan. 2016, doi: 10.4137/BII.S31559.

[20] M. Mallappallil, J. Sabu, A. Gruessner, and M. Salifu, "A review of big data and medical research," *SAGE Open Med.*, vol. 8, 2020, doi: 10.1177/2050312120934839.

[21] J. Andreu-Perez, C. C. Y. Poon, R. D. Merrifield, S. T. C. Wong, and G. Z. Yang, "Big Data for Health," *IEEE J. Biomed. Heal. informatics*, vol. 19, no. 4, pp. 1193–1208, Jul. 2015, doi: 10.1109/JBHI.2015.2450362.

[22] L. O. Gostin, "National health information privacy: regulations under the Health Insurance Portability and Accountability Act.," *JAMA*, vol. 285, no. 23, pp. 3015–3021, Jun. 2001, doi: 10.1001/JAMA.285.23.3015.

[23] F. Akowuah, X. Yuan, J. Xu, and H. Wang, "A Survey of U.S. Laws for Health Information Security & Privacy," *Int. J. Inf. Secur. Priv.*, vol. 6, no. 4, pp. 40–54, 2012, doi: 10.4018/JISP.2012100102.

[24] S. Sadki, H. El Bakkali, and M. Akhattab, "Towards conflicts prevention among privacy policies: A comparative study of major privacy laws and regulations for healthcare," *Int. Conf. Cloud Comput. Technol. Appl.*, vol. 2018-January, pp. 1–7, Jul. 2017, doi: 10.1109/CLOUDTECH.2017.8284738.

[25] J. Goldman, "Protecting privacy to improve health care.," *Health Aff.*, vol. 17, no. 6, pp. 47–60, 1998, doi: 10.1377/HLTHAFF.17.6.47.

[26] U. D. of H. & H. Services, "OCR PRIVACY BRIEF SUMMARY OF THE HIPAA PRIVACY

RULE HIPAA Compliance Assistance," *Summ. HIPAA Priv. Rule*, p. 23, 2003, [Online]. Available: https://www.hhs.gov/sites/default/files/privacysummary.pdf

[27] J. Hiller, M. McMullen, W. M. Chumney, and D. Baumer, "Privacy and Security in the Implementation of Health Information Technology (Electronic Health Records): U.S. and EU Compared," 2011.

[28] G. Bincoletto, "Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union," *Data Policy*, vol. 2, no. 2, Mar. 2020, doi: 10.1017/DAP.2020.2.

[29] E. C. Schiza, G. J. Fakas, C. S. Pattichis, N. Petkov, and C. N. Schizas, "Data Protection Issues of Integrated Electronic Health Records (EHR)," *XIV Mediterr. Conf. Med. Biol. Eng. Comput. 2016*, vol. 57, pp. 787–790, 2016, doi: 10.1007/978-3-319-32703-7_153.

[30] M. Stauch, N. Forgó, and T. Krügel, "Using EHRs to design drug repositioning trials: A devolved approach to data protection," *Int. Rev. Law, Comput. Technol.*, vol. 28, no. 2, pp. 237–248, 2014, doi: 10.1080/13600869.2013.801582.

[31] G. Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records," *Annu. Priv. Forum*, vol. 11498 LNCS, pp. 161–181, 2019, doi: 10.1007/978-3-030-21752-5_11.

[32] M. Chawki and B. Schneier, "Security and Privacy in the Era of Electronic Health Records (EHRs)," 2021.

[33] D. Gonçalves-Ferreira *et al.*, "OpenEHR and General Data Protection Regulation: Evaluation of Principles and Requirements," *JMIR Med. Informatics*, vol. 7, no. 1, Jan. 2019, doi: 10.2196/MEDINFORM.9845.

[34] A. M. Udroiu, M. Dumitrache, and I. Sandu, "Improving the cybersecurity of medical systems by applying the NIST framework," *Eur. Conf. Artif. Intell.*, 2022, doi: 10.1109/ECAI54874.2022.9847498.

[35] M. P. Carello, A. M. Spaccamela, L. Querzoni, and M. Angelini, "A Systematization of Cybersecurity Regulations, Standards and Guidelines for the Healthcare Sector," *arXiv.org*, 2023, doi: 10.48550/ARXIV.2304.14955.

[36] D. Parmeggiani *et al.*, "The adoption of a Cyber Security Framework in a health care environment (Preprint)," Mar. 2021, doi: 10.2196/PREPRINTS.29177.

[37] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "Digital Healthcare - Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST perspectives, and Recommendations," *IEEE Access*, vol. 10, pp. 12345–12364, 2022, doi: 10.1109/ACCESS.2022.3145372.

[38] T. Granlund, J. Vedenpaa, V. Stirbu, and T. Mikkonen, "On Medical Device Cybersecurity Compliance in EU," *Int. Work. Softw. Eng. Healthc.*, pp. 20–23, Jun. 2021, doi: 10.1109/SEH52539.2021.00011.

[39] S. Chandra, S. Ray, and R. T. Goswami, “Big Data Security in Healthcare: Survey on Frameworks and Algorithms,” *IEEE Int. Adv. Comput. Conf.*, pp. 89–94, Jul. 2017, doi: 10.1109/IACC.2017.0033.

[40] M. J. Harvey and M. G. Harvey, “Privacy and security issues for mobile health platforms,” *J. Assoc. Inf. Sci. Technol.*, vol. 65, no. 7, pp. 1305–1318, Jul. 2014, doi: 10.1002/ASI.23066.

[41] R. DRAKE and E. RIDDER, “Healthcare Cybersecurity Vulnerabilities,” *Int. Conf. Cybersecurity Cybercrime*, vol. 9, pp. 49–56, Apr. 2022, doi: 10.19107/CYBERCON.2022.06.

[42] A. H. Seh *et al.*, “Healthcare Data Breaches: Insights and Implications,” *Healthc. 2020, Vol. 8, Page 133*, vol. 8, no. 2, p. 133, May 2020, doi: 10.3390/HEALTHCARE8020133.

[43] N. Gupta, A. Rawal, V. L. Narasimhan, and S. Shiwani, “Accuracy, Sensitivity and Specificity Measurement of Various Classification Techniques on Healthcare Data,” *IOSR J. Comput. Eng.*, vol. 11, no. 5, pp. 70–73, 2013, doi: 10.9790/0661-1157073.

[44] W. Hu, “Review of the data science in the field of healthcare,” *Appl. Comput. Eng.*, vol. 74, no. 1, pp. 154–158, Jul. 2024, doi: 10.54254/2755-2721/74/20240458.

[45] S. G. Janani Ratthna, K. Jothikumar, and P. Priyadharshini, “Advancing Healthcare Through Data Science Techniques for Comprehensive Analysis and Visualization of Healthcare Data,” *Adv. Healthc. Inf. Syst. Adm. B. Ser.*, pp. 1–15, Jul. 2024, doi: 10.4018/979-8-3693-7457-3.CH001.

[46] Chidera Victoria Ibeh, Oluwafunmi Adijat Elufioye, Temidayo Olorunsogo, Onyeka Franca Asuzu, Ndubuisi Leonard Nduubuisi, and Andrew Ifesinachi Daraojimba, “Data analytics in healthcare: A review of patient-centric approaches and healthcare delivery,” *World J. Adv. Res. Rev.*, vol. 21, no. 2, pp. 1750–1760, Feb. 2024, doi: 10.30574/WJARR.2024.21.2.0246.

[47] Arenike Patricia Adekugbe and Chidera Victoria Ibeh, “Advancing healthcare data solutions: comparative analysis of business and research models in the u.s,” *Int. Med. Sci. Res. J.*, vol. 4, no. 4, pp. 373–390, Apr. 2024, doi: 10.51594/IMSRJ.V4I4.997.

[48] Y. C. Yau, P. Khethavath, and J. A. Figueroa, “Secure Pattern-Based Data Sensitivity Framework for Big Data in Healthcare,” *Int. Conf. Big Data, Cloud Comput. Data Sci. Eng.*, pp. 65–70, May 2019, doi: 10.1109/BCD.2019.8885114.

[49] I. E. Olatunji, J. Rauch, M. Katzensteiner, and M. Khosla, “A Review of Anonymization for Healthcare Data,” *Big Data*, Dec. 2021, doi: 10.1089/BIG.2021.0169.

[50] J. M. M. Rumbold and B. K. Pierscionek, “What Are Data? A Categorization of the Data Sensitivity Spectrum,” *Big Data Res.*, vol. 12, pp. 49–59, Jul. 2017, doi: 10.1016/J.BDR.2017.11.001.

[51] M. Katarahweire, E. Bainomugisha, and K. A. Mughal, “A Multi-level Data Sensitivity Model for Mobile Health Data Collection Systems,” *WorldCIST*, vol. 932, pp. 547–556, 2019, doi: 10.1007/978-3-030-16187-3_53.

[52] J. Priya and C. Palanisamy, “Novel Block Chain Technique for Data Privacy and Access

Anonymity in Smart Healthcare," *Intell. Autom. Soft Comput.*, vol. 35, no. 1, pp. 243–259, 2023, doi: 10.32604/IASC.2023.025719.

[53] M. Langarizadeh, A. Orooji, and A. Sheikhtaheri, "Effectiveness of Anonymization Methods in Preserving Patients' Privacy: A Systematic Literature Review," *eHealth Conf.*, vol. 248, pp. 80–87, 2018, doi: 10.3233/978-1-61499-858-7-80.

[54] N. Khan and M. Nassar, "A Look into Privacy-Preserving Blockchains," *ACS/IEEE Int. Conf. Comput. Syst. Appl.*, vol. 2019-November, Nov. 2019, doi: 10.1109/AICCSA47632.2019.9035235.

[55] F. J. de Haro-Olmo, Á. J. Varela-Vaca, and J. A. Álvarez-Bermejo, "Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review," *Ital. Natl. Conf. Sensors*, vol. 20, no. 24, pp. 1–21, Dec. 2020, doi: 10.3390/S20247171.

[56] W. F. Mukhtar and E. S. Abuelyaman, "Opportunities and Challenges of Big Data in Healthcare," *Data Anal. Med.*, pp. 47–58, Aug. 2020, doi: 10.4018/978-1-5225-0920-2.CH004.

[57] P. S. Mathew and A. S. Pillai, "Big Data Challenges and Solutions in Healthcare: A Survey," *Int. Conf. Innov. Bio-inspired Comput. Appl.*, vol. 424, pp. 543–553, 2015, doi: 10.1007/978-3-319-28031-8_48.

[58] M. R. C. de Gomez, "A Comprehensive Introduction to Healthcare Data Analytics," *J. Biomed. Sustain. Healthc. Appl.*, pp. 73–82, Jan. 2024, doi: 10.53759/0088/JBSHA202404007.

[59] K. Ng *et al.*, "Curating and Integrating Data from Multiple Sources to Support Healthcare Analytics," *Medinfo*, vol. 216, p. 1056, 2015, doi: 10.3233/978-1-61499-564-7-1056.

[60] P. Khan, P. Ranjan, and S. Kumar, "Data heterogeneity mitigation in healthcare robotic systems leveraging the Nelder–Mead method," *Artif. Intell. Futur. Gener. Robot.*, pp. 71–82, Jan. 2021, doi: 10.1016/B978-0-323-85498-6.00012-5.

[61] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment," *J. Med. Syst.*, vol. 42, no. 8, Aug. 2018, doi: 10.1007/S10916-018-1007-5.

[62] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward.," *Maturitas*, vol. 113, pp. 48–52, Jul. 2018, doi: 10.1016/J.MATURITAS.2018.04.008.

[63] R. DRAKE and E. RIDDER, "Healthcare Cybersecurity Vulnerabilities," *Int. Conf. Cybersecurity Cybercrime*, vol. 9, pp. 49–56, Apr. 2022, doi: 10.19107/CYBERCON.2022.06.

[64] R. W. Anwar, T. Abdullah, and F. Pastore, "Firewall Best Practices for Securing Smart Healthcare Environment: A Review," *Appl. Sci. 2021, Vol. 11, Page 9183*, vol. 11, no. 19, p. 9183, Oct. 2021, doi: 10.3390/APP11199183.

[65] Y. He, A. Aliyu, M. Evans, and C. Luo, "Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review," *J. Med. Internet Res.*, vol. 23, no. 4, p. e21747, Apr. 2021, doi: 10.2196/21747.

[66] L. Wasserman and Y. Wasserman, “Hospital cybersecurity risks and gaps: Review (for the non-cyber professional),” *Front. Digit. Heal.*, vol. 4, Aug. 2022, doi: 10.3389/FDGTH.2022.862221/PDF.

[67] M. Clarke and K. Martin, “Managing cybersecurity risk in healthcare settings,” *Healthc. Manag. Forum*, vol. 37, no. 1, pp. 17–20, Jan. 2023, doi: 10.1177/08404704231195804.

[68] A. J. Coronado and T. L. Wong, “Healthcare cybersecurity risk management: keys to an effective plan.,” *Biomed. Instrum. Technol.*, vol. 48, no. HORIZONS SPRING, pp. 26–30, 2014, doi: 10.2345/0899-8205-48.S1.26.

[69] N. Jerry-Egemba, “Safe and sound: Strengthening cybersecurity in healthcare through robust staff educational programs,” *Healthc. Manag. Forum*, vol. 37, no. 1, pp. 21–25, Jan. 2023, doi: 10.1177/08404704231194577.

[70] V. Radhakrishnan, “Review Analysis of Cyber Security in Healthcare System: A Systematic Approach of Modern Development,” *Int. J. Innov. Res. Comput. Sci. Technol.*, vol. 11, no. 3, pp. 38–42, May 2023, doi: 10.55524/IJIRCST.2023.11.3.7.

[71] J. Kwon and M. E. Johnson, “Proactive versus reactive security investments in the healthcare sector,” *MIS Q. Manag. Inf. Syst.*, vol. 38, no. 2, pp. 451–471, Jun. 2014, doi: 10.25300/MISQ/2014/38.2.06.

[72] D. Parmeggiani *et al.*, “The adoption of a Cyber Security Framework in a health care environment (Preprint),” Mar. 2021, doi: 10.2196/PREPRINTS.29177.

[73] A. H. Seh *et al.*, “Healthcare Data Breaches: Insights and Implications,” *Healthcare*, vol. 8, no. 2, Jun. 2020, doi: 10.3390/HEALTHCARE8020133.

[74] M. Al Kinoon, M. Omar, M. Mohaisen, and D. Mohaisen, “Security Breaches in the Healthcare Domain: A Spatiotemporal Analysis,” *Int. Conf. Comput. Soc. Networks*, vol. 13116 LNCS, pp. 171–183, 2021, doi: 10.1007/978-3-030-91434-9_16.

[75] M. Hossain and Y. Hong, “Trends and characteristics of protected health information breaches in the United States,” *Am. Med. Informatics Assoc. Annu. Symp.*, 2020.

[76] S. C. Litton, “What’s Causing Our Healthcare Breaches? A Comparison of Data from 2013 to 2020,” May 2022, doi: 10.1037/TMS0000149.

[77] D. J. Ferreira and N. Mateus-Coelho, “Cybersecurity Risks in Health Data and Measures to Take,” *Adv. Digit. crime, forensics, cyber Terror. B. Ser.*, pp. 1–18, Sep. 2023, doi: 10.4018/978-1-6684-8422-7.CH001.

[78] A. Abdi, H. Bennouri, and A. Keane, “Emerging Cyber Risks & Threats in Healthcare Systems: A Case Study in Resilient Cybersecurity Solutions,” *2024 13th Mediterr. Conf. Embed. Comput. MECO 2024*, Jun. 2024, doi: 10.1109/MECO62516.2024.10577790.

[79] M. D. Espinoza, “Cybercrime and Insider Threats in Healthcare Organizations,” *Adv. Bus. Strateg. Compet. Advant. B. Ser.*, pp. 1–15, Oct. 2023, doi: 10.4018/979-8-3693-1634-4.CH001.

[80] P. DYMORA, M. MAZUREK, and M. NYCZ, “Modeling and Statistical Analysis of Data Breach Problems in Python,” *J. Educ. Technol. Comput. Sci.*, vol. 4, no. 34, pp. 223–233, Dec. 2023, doi: 10.15584/JETACOMPS.2023.4.22.

[81] J. Reddy, N. Elsayed, Z. ElSayed, and M. Ozer, “A Review on Data Breaches in Healthcare Security Systems,” *Int. J. Comput. Appl.*, vol. 184, no. 45, pp. 1–7, 2023, doi: 10.5120/ijca2023922333.

[82] “UVM Health Continues to Feel Effects of Ransomware Attack | TechTarget.” Accessed: Jan. 09, 2025. [Online]. Available: https://www.techtarget.com/healthtechsecurity/news/366595241/UVM-Health-Continues-to-Feel-Effects-of-Ransomware-Attack

[83] “Vermont Hospital confirmed the ransomware attack.” Accessed: Jan. 09, 2025. [Online]. Available: https://www.felipeprado1975.com/single-post/vermont-hospital-confirmed-the-ransomware-attack

[84] “Ransomware Attack on the University of Vermont Health Network – Westoahu Cybersecurity.” Accessed: Jan. 09, 2025. [Online]. Available: https://westoahu.hawaii.edu/cyber/ics-cybersecurity/ics-weekly-summaries/ransomware-attack-on-the-university-of-vermont-health-network/

[85] J. C. L. Looi *et al.*, “Cybersecurity lessons from the Vastaamo psychotherapy data breach for psychiatrists and other mental healthcare providers.,” *Australas. Psychiatry*, vol. 0, no. 0, pp. 1–5, 2024, doi: 10.1177/10398562241291340.

[86] H. Ghanbari and K. Koskinen, “When data breach hits a psychotherapy clinic: The Vastaamo case,” *J. Inf. Technol. Teach. Cases*, vol. 0, no. 0, pp. 1–9, 2024, doi: 10.1177/20438869241258235.

[87] M. Kortesoja, “A Symptomatic Reading of the Vastaamo Case,” *Tutk. Krit.*, vol. 2, no. 1, p. 139, Nov. 2022, doi: 10.55294/TK.124653.

[88] D. Sahu, N. Tiwari, and M. Chawla, “Blockchain as a Solution for Electronic Health Record Management : A Comprehensive Review,” *2024 IEEE Int. Students’ Conf. Electr. Electron. Comput. Sci. SCEECS 2024*, 2024, doi: 10.1109/SCEECS61402.2024.10482149.

[89] M. F. Ansari, B. Dash, S. Swayamsiddha, and G. Panda, “Use of Blockchain Technology to Protect Privacy in Electronic Health Records- A Review,” *2023 Int. Conf. Intell. Data Commun. Technol. Internet Things*, pp. 144–149, 2023, doi: 10.1109/IDCIOT56793.2023.10053417.

[90] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, “Blockchain technology applications in healthcare: An overview,” *Int. J. Intell. Networks*, vol. 2, pp. 130–139, Jan. 2021, doi: 10.1016/J.IJIN.2021.09.005.

[91] M. Miah, “A Comprehensive Study on the Use of Blockchain Technology in Healthcare,” *Inf. Technol. Manag. Sci.*, vol. 26, pp. 1–9, Nov. 2023, doi: 10.7250/ITMS-2023-0001.

[92] S. Dash, P. K. Gantayat, and R. K. Das, “Blockchain Technology in Healthcare: Opportunities and Challenges,” *Intell. Syst. Ref. Libr.*, vol. 203, pp. 97–111, 2021, doi: 10.1007/978-3-030-69395-4_6.

[93] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, “A Systematic Review of the Use of Blockchain in Healthcare,” *Symmetry (Basel).*, vol. 10, no. 10, 2018, doi: 10.3390/SYM10100470.

[94] H. D. Zubaydi, Y. W. Chong, K. Ko, S. M. Hanshi, and S. Karuppayah, “A Review on the Role of Blockchain Technology in the Healthcare Domain,” *Electronics*, vol. 8, no. 6, Jun. 2019, doi: 10.3390/ELECTRONICS8060679.

[95] N. R. S. Narikimilli, A. Kumar, A. D. Antu, and B. Xie, “Blockchain Applications in Healthcare - A Review and Future Perspective,” *Int. Conf. Blockchain*, vol. 12404 LNCS, pp. 198–218, 2020, doi: 10.1007/978-3-030-59638-5_14.

[96] K. Murugeswari, G. Ganesan, and S. K. Ga, “Introduction to Blockchain Technology for Securing Healthcare,” *Adv. Healthc. Inf. Syst. Adm. B. Ser.*, pp. 197–210, Jul. 2024, doi: 10.4018/979-8-3693-7457-3.CH009.

[97] A. Agbeyangi, O. Oki, and A. Mgidi, “Blockchain in Healthcare: Implementing Hyperledger Fabric for Electronic Health Records at Frere Provincial Hospital,” Jul. 2024, Accessed: Nov. 09, 2024. [Online]. Available: https://arxiv.org/abs/2407.15876v1

[98] M. Sagiv *et al.*, “The blockchain technology,” *Harnessing Blockchain Sustain. Dev.*, pp. 2–9, Nov. 2021, doi: 10.18356/9789214030430C004.

[99] M. Attaran and A. Gunasekaran, “Blockchain Principles, Qualities, and Business Applications,” *SpringerBriefs Oper. Manag.*, pp. 13–20, 2019, doi: 10.1007/978-3-030-27798-7_3.

[100] W. Nowiński and M. Kozma, “How Can Blockchain Technology Disrupt the Existing Business Models,” *Entrep. Bus. Econ. Rev.*, vol. 5, no. 3, pp. 173–188, 2017, doi: 10.15678/EBER.2017.050309.

[101] A. Chen and A. Jacob-sen, “Distributed ledgers and blockchain: concepts and applications,” *Conf. Cent. Adv. Stud. Collab. Res.*, 2018.

[102] V. Trivedi, “The Blockchain,” *How to Speak Tech*, pp. 139–156, 2019, doi: 10.1007/978-1-4842-4324-4_16.

[103] K. C, “An Overview of Blockchain Technology,” *Int. Res. J. Electron. Comput. Eng.*, vol. 4, no. 4, p. 1, Dec. 2018, doi: 10.24178/IRJECE.2018.4.4.01.

[104] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K. K. R. Choo, “Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey,” *Comput. Secur.*, vol. 97, Oct. 2020, doi: 10.1016/J.COSE.2020.101966.

[105] M. A. Acquah, N. Chen, J. S. Pan, H. M. Yang, and B. Yan, “Securing Fingerprint Template Using Blockchain and Distributed Storage System,” *Symmetry (Basel).*, vol. 12, no. 6, Jun.

2020, doi: 10.3390/SYM12060951.

[106] C. Ehmke, F. Blum, and V. Gruhn, “Properties of Decentralized Consensus Technology - Why not every Blockchain is a Blockchain,” *arXiv.org*, Jul. 2019, doi: 10.13140/RG.2.2.35506.45765.

[107] R. S. Gopalan, “Blockchain and Cybersecurity,” *Secur. IoT Ind. 4.0 Appl. with Blockchain*, pp. 221–245, Sep. 2021, doi: 10.1201/9781003175872-9.

[108] R. Impagliazzo and M. Luby, “One-way functions are essential for complexity based cryptography,” *30th Annu. Symp. Found. Comput. Sci.*, pp. 230–235, 1989, doi: 10.1109/SFCS.1989.63483.

[109] M. Naor and M. Yung, “Universal one-way hash functions and their cryptographic applications,” *Symp. Theory Comput.*, pp. 33–43, 1989, doi: 10.1145/73007.73011.

[110] C. King, “Some mathematical topics in blockchain and digital ledger technology,” 2022.

[111] C. M. Nalayini, Jeevaakatiravan, P. V. Imogen, and J. M. Sahana, “A Study on Digital Signature in Blockchain Technology,” *Int. Conf. Adapt. Intell. Syst.*, pp. 398–403, 2023, doi: 10.1109/ICAIS56108.2023.10073680.

[112] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang, “Digital signature scheme for information non-repudiation in blockchain: a state of the art review,” *EURASIP J. Wirel. Commun. Netw.*, vol. 2020, no. 1, Dec. 2020, doi: 10.1186/S13638-020-01665-W.

[113] Z. Xu, “The Advance of Digital Signature with Quantum Computing,” *Highlights Sci. Eng. Technol.*, vol. 39, pp. 1111–1121, Apr. 2023, doi: 10.54097/HSET.V39I.6716.

[114] D. Johnson, A. Menezes, and S. Vanstone, “The Elliptic Curve Digital Signature Algorithm (ECDSA),” *Int. J. Inf. Secur. 2001 11*, vol. 1, no. 1, pp. 36–63, Jan. 2014, doi: 10.1007/S102070100002.

[115] A. K. Rai, M. Singh, H. C. Sudheendramouli, V. Panwar, N. A. Balaji, and R. Kukreti, “Digital Signature for Content Authentication,” *2023 Int. Conf. Adv. Comput. Commun. Appl. Informatics*, 2023, doi: 10.1109/ACCAI58221.2023.10200472.

[116] C. Nist, “The digital signature standard,” *Commun. ACM*, vol. 35, no. 7, pp. 36–40, Jan. 1992, doi: 10.1145/129902.129904.

[117] R. Musale, “Application of Digital Signature to Achieve Secure Transmission,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 7, no. 2, pp. 150–153, Feb. 2019, doi: 10.22214/IJRASET.2019.2022.

[118] S. Ghoshal, P. Bandyopadhyay, S. Roy, and M. Baneree, “A Journey from MD5 to SHA-3,” *Lect. Notes Networks Syst.*, vol. 99, pp. 107–112, 2020, doi: 10.1007/978-981-15-1624-5_11.

[119] S. Aggarwal and N. Kumar, “Chapter Four - Digital signatures,” *Adv. Comput.*, vol. 121, pp. 95–107, Jan. 2021, doi: 10.1016/BS.ADCOM.2020.08.004.

[120] N. Hasyim, “PEMBUATAN TANDA TANGAN DIGITAL DENGAN DIGITAL SIGNATURE ALGORITHM (DSA),” 2010.

[121] A. Saepulrohman and A. Ismangil, “Data integrity and security of digital signatures on electronic systems using the digital signature algorithm (DSA),” *Int. J. Electron. Commun. Syst.*, vol. 1, no. 1, pp. 11–15, Jun. 2021, doi: 10.24042/IJECS.V1I1.7923.

[122] M. Fartitchou, H. El Marraki, L. Lafkir, A. Azzouz, K. El Makkaoui, and Z. El Allali, “Public-Key Cryptography behind Blockchain Security,” *Int. Conf. Networking, Inf. Syst. Secur.*, 2022, doi: 10.1109/NISS55057.2022.10085236.

[123] B. Tulu, H. Li, S. Chatterjee, B. N. Hilton, D. Lafky, and T. Horan, “Design and Implementation of a Digital Signature Solution for a Healthcare Enterprise,” *Am. Conf. Inf. Syst.*, 2004.

[124] G. D. de Moor, B. Claerhout, and F. De Meyer, “Implementation framework for digital signatures for electronic data interchange in healthcare.,” *Stud. Health Technol. Inform.*, 2004.

[125] Y. Fang, “A research on different digital signature schemes,” *Appl. Comput. Eng.*, vol. 16, no. 1, pp. 27–35, Oct. 2023, doi: 10.54254/2755-2721/16/20230855.

[126] M. D. Kelly, “The RSA Algorithm : A Mathematical History of the Ubiquitous Cryptological Algorithm,” 2009.

[127] Z. Arifin, “Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman,” 2016, doi: 10.30872/JIM.V4I3.43.

[128] X. Zhou and X. Tang, “Research and implementation of RSA algorithm for encryption and decryption,” *Proc. 6th Int. Forum Strateg. Technol. IFOST 2011*, vol. 2, pp. 1118–1121, 2011, doi: 10.1109/IFOST.2011.6021216.

[129] A. Negi, P. Sharma, P. Chaudhary, and H. Gupta, “New Method for Obtaining Digital Signature Certificate using Proposed RSA Algorithm,” *Int. J. Comput. Appl.*, vol. 121, no. 23, pp. 24–29, Jul. 2015, doi: 10.5120/21841-5084.

[130] Y. Sun, R. Zhang, X. Wang, K. Gao, and L. Liu, “A Decentralizing Attribute-Based Signature for Healthcare Blockchain,” *Int. Conf. Comput. Commun. Networks*, vol. 2018-July, Oct. 2018, doi: 10.1109/ICCCN.2018.8487349.

[131] J. Li, Y. Chen, J. Han, C. Liu, Y. Zhang, and H. Wang, “Decentralized Attribute-Based Server-Aid Signature in the Internet of Things,” *IEEE Internet Things J.*, vol. 9, no. 6, pp. 4573–4583, Mar. 2021, doi: 10.1109/JIOT.2021.3104585.

[132] Q. Su, R. Zhang, R. Xue, Y. Sun, and S. Gao, “Distributed Attribute-Based Signature With Attribute Dynamic Update for Smart Grid,” *IEEE Trans. Ind. Informatics*, vol. 19, no. 9, pp. 9424–9435, Sep. 2023, doi: 10.1109/TII.2022.3228688.

[133] D. Toradmalle, R. Singh, H. Shastri, N. Naik, and V. Panchidi, “Prominence Of ECDSA Over RSA Digital Signature Algorithm,” *2018 2nd Int. Conf. I-SMAC (IoT Soc. Mobile, Anal. Cloud) (I-SMAC)I-SMAC (IoT Soc. Mobile, Anal. Cloud) (I-SMAC), 2018 2nd Int. Conf.*, pp. 253–257, Jul. 2018, doi: 10.1109/I-SMAC.2018.8653689.

[134] P. Kurariya *et al.*, “LTV-Backed E-Signatures Using Post-Quantum Cryptography,” *2023 Int.*

Conf. Quantum Technol. Commun. Comput. Hardw. Embed. Syst. Secur., 2023, doi: 10.1109/IQ-CCHESS56596.2023.10391601.

[135] K. Longmate, E. M. Ball, E. Dable-Heath, and R. J. Young, "Signing Information in the Quantum Era," *AVS Quantum Sci.*, vol. 2, no. 4, Dec. 2020, doi: 10.1116/5.0022519.

[136] T. Christian and T. Christoph, "Quantum Computer Resistant Cryptographic Methods and Their Suitability for Long-Term Preservation of Evidential Value," *Bled eConference*, pp. 481–493, 2021, doi: 10.18690/978-961-286-485-9.35.

[137] T. G. Tan and J. Zhou, "Layering Quantum-Resistance into Classical Digital Signature Algorithms," *Inf. Secur. Conf.*, vol. 13118 LNCS, pp. 26–41, 2021, doi: 10.1007/978-3-030-91356-4_2.

[138] A. Buldas, R. Laanoja, and A. Truu, "Efficient Quantum-Immune Keyless Signatures with Identity," *IACR Cryptol. ePrint Arch.*, 2014.

[139] S. Kaur, S. Chaturvedi, A. Sharma, and J. Kar, "A Research Survey on Applications of Consensus Protocols in Blockchain," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/6693731.

[140] S. Hattab and I. F. Taha Alyaseen, "Consensus Algorithms Blockchain: A comparative study," *Int. J. Perceptive Cogn. Comput.*, vol. 5, no. 2, pp. 66–71, Dec. 2019, doi: 10.31436/IJPCC.V5I2.103.

[141] O. A. Safaryan, K. S. Lemeshko, A. N. Beskopylny, L. V. Cherckesova, and D. A. Korochentsev, "Mathematical Analysis of Parametric Characteristics of the Consensus Algorithms Operation with the Choice of the Most Priority One for Implementation in the Financial Sphere," *Electronics*, vol. 10, no. 21, Nov. 2021, doi: 10.3390/ELECTRONICS10212659.

[142] F. Hashim, K. Shuaib, and F. Sallabi, "Performance Evaluation of Blockchain Consensus Algorithms for Electronic Health Record Sharing," *2021 Glob. Congr. Electr. Eng.*, pp. 136–143, 2021, doi: 10.1109/GC-ELECENG52322.2021.9788285.

[143] P. Prabha and K. Chatterjee, "Design and implementation of hybrid consensus mechanism for IoT based healthcare system security," *Int. J. Inf. Technol.*, vol. 14, no. 3, pp. 1381–1396, May 2022, doi: 10.1007/S41870-022-00880-6.

[144] S. Kanagasankari and V. Vallinayagi, "comparative analysis of consensus algorithms in the health care sector using block chain technology," *Int. J. Health Sci. (Qassim).*, May 2022, doi: 10.53730/IJHS.V6NS1.7863.

[145] K. Domdouzis, P. Lake, and P. Crowther, "Blockchain," *Undergrad. Top. Comput. Sci.*, pp. 359–373, 2021, doi: 10.1007/978-3-030-42224-0_17.

[146] B. Ramdasu and K. K. Prakash, "A Review on Blockchain and Its Security," *Int. J. Electron. Eng. Appl.*, vol. 10, no. 2, pp. 13–22, Sep. 2021, doi: 10.30696/IJEEA.X.II.2022.13-22.

[147] B. Shrimali and H. B. Patel, "Blockchain state-of-the-art: architecture, use cases, consensus,

challenges and opportunities," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6793–6807, Oct. 2021, doi: 10.1016/J.JKSUCI.2021.08.005.

[148] R. A. Andreev, P. Andreeva, L. N. Krotov, and E. Krotova, "Review of Blockchain Technology: Types of Blockchain and Their Application," *Intellekt. Sist. Proizv.*, vol. 16, no. 1, p. 11, Apr. 2018, doi: 10.22213/2410-9304-2018-1-11-14.

[149] X. Zheng and W. Feng, "Research on Practical Byzantine Fault Tolerant Consensus Algorithm Based on Blockchain," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 1802, no. 3, Mar. 2021, doi: 10.1088/1742-6596/1802/3/032022.

[150] L. Ismail and H. Materwala, "Article A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions," *Symmetry (Basel).*, vol. 11, no. 10, Oct. 2019, doi: 10.3390/SYM11101198.

[151] A. Gautama, A. F. Rochim, and L. Bayuaji, "Privacy Preserving Electronic Health Record with Consortium Blockchain," *2022 6th Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng.*, pp. 303–308, 2022, doi: 10.1109/ICITISEE57756.2022.10057649.

[152] C. Kombe, M. Ally, and A. Sam, "A review on healthcare information systems and consensus protocols in blockchain technology," *Int. J. Adv. Technol. Eng. Explor.*, vol. 5, no. 49, pp. 473–483, Dec. 2018, doi: 10.19101/IJATEE.2018.547023.

[153] G. Subramanian and A. Sreekantan Thampy, "Implementation of Blockchain Consortium to Prioritize Diabetes Patients' Healthcare in Pandemic Situations," *IEEE Access*, vol. 9, pp. 162459–162475, 2021, doi: 10.1109/ACCESS.2021.3132302.

[154] A. Ferenczi and C. Bădică, "An Experimental Validation of the Practical Byzantine Fault Tolerant Algorithm," *Int. Conf. Interact. Des. Child.*, vol. 1089 SCI, pp. 244–253, 2022, doi: 10.1007/978-3-031-29104-3_27.

[155] H. Tang, Y. Sun, and J. Ouyang, "Excellent Practical Byzantine Fault Tolerance," *J. Cyber Secur.*, vol. 2, no. 4, pp. 167–182, 2020, doi: 10.32604/JCS.2020.011341.

[156] H. P. H. Pang, Y. L. H. Pang, X. W. Y. Liu, and Y. M. X. Wen, "Research on Practical Byzantine Fault Tolerant Algorithm Based on Trust Mechanism," 電腦學刊, vol. 33, no. 2, pp. 011–023, Apr. 2022, doi: 10.53106/199115992022043302002.

[157] X. Gu, T. Kang, A. Zhou, and L. Guo, "Consensus Node Group Selection and Adjustment Algorithm Based on Dual Random Selection Mechanism," *Int. Conf. Crit. Infrastruct. Prot.*, pp. 407–414, Dec. 2023, doi: 10.1145/3638884.3638947.

[158] G. Yuan, L. Feng, J. Ning, and X. Yang, "Improvement of Practical Byzantine Fault Tolerant Consensus Algorithm for Blockchain," *2021 IEEE 3rd Int. Conf. Front. Technol. Inf. Comput.*, pp. 182–187, 2021, doi: 10.1109/ICFTIC54370.2021.9647347.

[159] Z. Pang, Y. Yao, Q. Li, X. Zhang, and J. Zhang, "Electronic Health Records Sharing Model Based on Blockchain With Checkable State PBFT Consensus Algorithm," *IEEE Access*, vol. 10, pp. 87803–87815, 2022, doi: 10.1109/ACCESS.2022.3186682.

[160] P. Hegde and P. K. R. Maddikunta, “Secure PBFT Consensus-Based Lightweight Blockchain for Healthcare Application,” *Appl. Sci.*, vol. 13, no. 6, Mar. 2023, doi: 10.3390/APP13063757.

[161] Y. Meshcheryakov, A. Melman, O. Evsutin, V. Morozov, and Y. Koucheryavy, “On Performance of PBFT Blockchain Consensus Algorithm for IoT-Applications With Constrained Devices,” *IEEE Access*, vol. 9, pp. 80559–80570, 2021, doi: 10.1109/ACCESS.2021.3085405.

[162] K. Lei, Q. Zhang, L. Xu, and Z. Qi, “Reputation-Based Byzantine Fault-Tolerance for Consortium Blockchain,” *Int. Conf. Parallel Distrib. Syst.*, vol. 2018-December, pp. 604–611, Jul. 2018, doi: 10.1109/PADSW.2018.8644933.

[163] A. D. Dwivedi, L. Malina, P. Dzurenda, and G. Srivastava, “Optimized Blockchain Model for Internet of Things based Healthcare Applications,” *Int. Conf. Telecommun. Signal Process.*, pp. 135–139, Jul. 2019, doi: 10.1109/TSP.2019.8769060.

[164] Z. Mahmood, “On the Scalability of a Blockchain Network based on the Practical Byzantine Fault Tolerance Consensus Method,” 2020.

[165] S. Sakho, J. Zhang, F. Essaf, K. Badiss, T. Abide, and J. K. Kiprop, “Research on an improved practical byzantine fault tolerance algorithm,” *2020 2nd Int. Conf. Adv. Comput. Technol. Inf. Sci. Commun.*, pp. 176–181, Mar. 2020, doi: 10.1109/CTISC49998.2020.00035.

[166] Y. A. Min, “The Modification of pBFT Algorithm to Increase Network Operations Efficiency in Private Blockchains,” *Appl. Sci.*, vol. 11, no. 14, Jul. 2021, doi: 10.3390/APP11146313.

[167] V. N. Patil and V. H. Kalmani, “Enhancing security and ensuring secure performance: A performance evaluation of consensus algorithms in a distributed healthcare blockchain system,” *J. Stat. Manag. Syst.*, vol. 26, no. 6, pp. 1391–1406, 2023, doi: 10.47974/JSMS-1079.

[168] A. Giordanengo, “Possible Usages of Smart Contracts (Blockchain) in Healthcare and Why No One Is Using Them,” *Medinfo*, vol. 264, pp. 596–600, Aug. 2019, doi: 10.3233/SHTI190292.

[169] M. Schnitzbauer, “Smart Contracts in Healthcare,” *Digit. Healthc.*, pp. 211–223, 2021, doi: 10.1007/978-3-030-65896-0_19.

[170] M. N. O. Sadiku, K. G. Eze, and S. M. Musa, “Smart Contracts: A Primer,” 2018.

[171] G. MATEI, “Smart Contracts – Support for Successful Businesses,” *Inform. Econ.*, vol. 26, no. 4/2022, pp. 28–39, Dec. 2022, doi: 10.24818/ISSN14531305/26.4.2022.03.

[172] S. Rouhani and R. Deters, “Security, Performance, and Applications of Smart Contracts: A Systematic Survey,” *IEEE Access*, vol. 7, pp. 50759–50779, 2019, doi: 10.1109/ACCESS.2019.2911031.

[173] K. Hu, J. Zhu, Y. Ding, X. Bai, and J. Huang, “Smart Contract Engineering,” *Electronics*, vol. 9, no. 12, pp. 1–26, Dec. 2020, doi: 10.3390/ELECTRONICS9122042.

[174] P. Tolmach, Y. Li, S. W. Lin, Y. Liu, and Z. Li, “A Survey of Smart Contract Formal Specification and Verification,” *ACM Comput. Surv.*, vol. 54, no. 7, Jan. 2020, doi: 10.1145/3464421.

[175] A. Singh, R. M. Parizi, Q. Zhang, K. K. R. Choo, and A. Dehghantanha, “Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities,” *Comput. Secur.*, vol. 88, Jan. 2020, doi: 10.1016/J.COSE.2019.101654.

[176] M. Krichen, M. Lahami, and Q. A. Al-Haija, “Formal Methods for the Verification of Smart Contracts: A Review,” *Int. Conf. Secur. Inf. Networks*, 2022, doi: 10.1109/SIN56466.2022.9970534.

[177] K. Chatterjee, A. K. Goharshady, and Y. Velner, “Quantitative Analysis of Smart Contracts,” *Eur. Symp. Program.*, vol. 10801 LNCS, pp. 739–767, 2018, doi: 10.1007/978-3-319-89884-1_26.

[178] T. Durieux, J. F. Ferreira, R. Abreu, and P. Cruz, “Empirical Review of Automated Analysis Tools on 47,587 Ethereum Smart Contracts,” *Int. Conf. Softw. Eng.*, pp. 530–541, Jun. 2019, doi: 10.1145/3377811.3380364.

[179] L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making Smart Contracts Smarter,” *IACR Cryptol. ePrint Arch.*, vol. 24-28-October-2016, pp. 254–269, Oct. 2016, doi: 10.1145/2976749.2978309.

[180] T. D. Nguyen, L. H. Pham, and J. Sun, “SGUARD: Towards Fixing Vulnerable Smart Contracts Automatically,” *IEEE Symp. Secur. Priv.*, vol. 2021-May, pp. 1215–1229, May 2021, doi: 10.1109/SP40001.2021.00057.

[181] P. Tantikul and S. Ngamsuriyaroj, “Exploring Vulnerabilities in Solidity Smart Contract,” *Int. Conf. Inf. Syst. Secur. Priv.*, pp. 317–324, 2020, doi: 10.5220/0008909803170324.

[182] W. Ahrendt, G. Pace, and G. Schneider, “Smart Contracts – A Killer Application for Deductive Source Code Verification,” 2018.

[183] R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and A. Singh, “Empirical Vulnerability Analysis of Automated Smart Contracts Security Testing on Blockchains,” *Conf. Cent. Adv. Stud. Collab. Res.*, Sep. 2018, doi: 10.5555/3291291.3291303.

[184] G. Bigi, A. Bracciali, G. Meacci, and E. Tuosto, “Validation of Decentralised Smart Contracts Through Game Theory and Formal Methods,” *Program. Lang. with Appl. to Biol. Secur.*, vol. 9465, pp. 142–161, 2015, doi: 10.1007/978-3-319-25527-9_11.

[185] D. Palanikkumar, A. F. Alrasheedi, P. Parthasarathi, S. S. Askar, and M. Abouhawwash, “Hybrid Smart Contracts for Securing IoMT Data,” *Comput. Syst. Sci. Eng.*, vol. 44, no. 1, pp. 457–469, 2022, doi: 10.32604/CSSE.2023.024884.

[186] R. D. Garcia, G. Ramachandran, and J. Ueyama, “Exploiting smart contracts in PBFT-based blockchains: A case study in medical prescription system,” *Comput. Networks*, vol. 211, Jul. 2022, doi: 10.1016/J.COMNET.2022.109003.

[187] R. Phanse and J. Stingel, “Designing a Unified Healthcare Data System with Blockchain and Cryptography,” *J. student-scientists’ Res.*, vol. 11, no. 3, Aug. 2022, doi: 10.47611/JSRHS.V11I3.3951.

[188] R. Kumar and R. Tripathi, “Secure Healthcare Framework Using Blockchain and Public Key Cryptography,” *Blockchain Cybersecurity, Trust Priv.*, vol. 79, pp. 185–202, 2020, doi: 10.1007/978-3-030-38181-3_10.

[189] S. A and K. G, “Advanced Cryptography & Block Chain Based Cloud Environment for Secured E-Health Record,” Jun. 2021, doi: 10.21203/RS.3.RS-633622/V1.

[190] A. Odeh, I. Keshta, and Q. A. Al-Haija, “Analysis of Blockchain in the Healthcare Sector: Application and Issues,” *Symmetry (Basel).*, vol. 14, no. 9, Sep. 2022, doi: 10.3390/SYM14091760.

[191] F. Abbasi and P. Singh, “Cryptography: Security and Integrity of Data Management,” *J. Manag. Serv. Sci.*, vol. 1, no. 2, pp. 1–9, May 2021, doi: 10.54060/JMSS/001.02.004.

[192] B. Ghosh, R. Aich, A. Khag, S. Nayak, and P. Kumar, “CRYPTOGRAPHY,” *J. Math. Sci. Comput. Math.*, vol. 1, no. 2, pp. 225–228, Feb. 2020, doi: 10.15864/JMSCM.1207.

[193] M. Farajallah, R. Tahboub, M. Odeh, M. AbuTaha, and P. M. Farajallah, “Survey Paper: Cryptography Is The Science Of Information Security,” *Math. Gaz.*, vol. 86, p. 560, 2011.

[194] K. Raut, “A Comprehensive Review of Cryptographic Algorithms,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 9, no. 12, pp. 1750–1756, Dec. 2021, doi: 10.22214/IJRASET.2021.39581.

[195] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, “A comparative survey of Symmetric and Asymmetric Key Cryptography,” *2014 Int. Conf. Electron. Commun. Comput. Eng.*, pp. 83–93, Apr. 2014, doi: 10.1109/ICECCE.2014.7086640.

[196] A. Jeeva, D. V. Palanisamy, and K. Kanagaram, “COMPARATIVE ANALYSIS OF PERFORMANCE EFFICIENCY AND SECURITY MEASURES OF SOME ENCRYPTION ALGORITHMS,” 2012.

[197] Y. Kumar, R. Munjal, and H. Sharma, “Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures,” 2011.

[198] M. A. Al-Shabi, “A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security,” *Int. J. Sci. Res. Publ.*, vol. 9, no. 3, p. p8779, Mar. 2019, doi: 10.29322/IJSRP.9.03.2019.P8779.

[199] H. B. Ul Haq *et al.*, “E-Healthcare Using Block Chain Technology and Cryptographic Techniques: A Review,” *Pakistan J. Eng. Technol.*, vol. 5, no. 4, pp. 21–28, Dec. 2022, doi: 10.51846/VOL5ISS4PP21-28.

[200] R. Thabit, “Review of Cryptography Applications in eHealth Security Systems,” 2019.

[201] H. B. Mahajan and A. A. Junnarkar, “Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing,” *Multimed. Tools Appl.*, vol. 82, no. 28, pp. 44335–44358, Nov. 2023, doi: 10.1007/S11042-023-15204-4.

[202] K. Raju and N. Prabha, “A REVIEW OF REVERSIBLE DATA HIDING TECHNIQUE BASED ON STEGANOGRAPHY,” 2018.

[203] Y. Zhaoxia, W. Huabin, Z. Haifeng, L. Bin, and Z. Xinpeng, “Complete Separable Reversible

Data Hiding in Encrypted Image," *Int. Conf. Commun. Comput. Secur.*, vol. 9483, pp. 101–110, 2015, doi: 10.1007/978-3-319-27051-7_9.

[204] J. H. Horng, C. C. Chang, G. L. Li, W. K. Lee, and S. O. Hwang, "Blockchain-Based Reversible Data Hiding for Securing Medical Images," *J. Healthc. Eng.*, vol. 2021, 2021, doi: 10.1155/2021/9943402.

[205] M. Wack and B. Rance, "Clinical Data Warehouses," *Biol. Data Integr. Comput. Stat. Approaches*, pp. 1–23, Dec. 2023, doi: 10.1002/9781394257317.CH1.

[206] N. Power, N. R. Plummer, J. Baldwin, F. R. James, and S. Laha, "Intensive care decision-making: Identifying the challenges and generating solutions to improve inter-specialty referrals to critical care," *J. Intensive Care Soc.*, vol. 19, no. 4, pp. 287–298, Nov. 2018, doi: 10.1177/1751143718758933.

[207] H. Jin, C. Xu, Y. Luo, and P. Li, "Blockchain-Based Secure and Privacy-Preserving Clinical Data Sharing and Integration," *Int. Conf. Algorithms Archit. Parallel Process.*, vol. 12454 LNCS, pp. 93–109, 2020, doi: 10.1007/978-3-030-60248-2_7.

[208] C. Nayak, "A Monthly Double-blind Peer Reviewed Refereed Open Access International E-journal -included in the International Serial Directories International Journal of Management, It and Engineering Performance of Various Algorithms Used in Cryptography Ijmie _____".

[209] K. Ali, F. Akhtar, S. A. Memon, A. Shakeel, A. Ali, and A. Raheem, "Performance of Cryptographic Algorithms based on Time Complexity," *2020 3rd Int. Conf. Comput. Math. Eng. Technol.*, Jan. 2020, doi: 10.1109/ICOMET48670.2020.9073930.

[210] S. Gracious, G. Nandanan, K. R. Dagma, and A. G. Hari Narayana, "Big data security analytics in clinical data using cryptographic algorithms," *Int. J. Recent Technol. Eng.*, vol. 8, no. 2, pp. 107–110, Jul. 2019, doi: 10.35940/IJRTE.A1819.078219.

[211] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. R. S. Tavares, and V. H. C. de Albuquerque, "A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform," *Cogn. Syst. Res.*, vol. 52, pp. 1–11, Dec. 2018, doi: 10.1016/j.cogsys.2018.05.004.

[212] M. M. Alani, "Applications of machine learning in cryptography: a survey," *Int. Conf. Cryptogr. Secur. Priv.*, pp. 23–27, Jan. 2019, doi: 10.1145/3309074.3309092.

[213] J. Blackledge and N. Mosola, "Applications of Artificial Intelligence to Cryptography," *Trans. Mach. Learn. Artif. Intell.*, vol. 8, no. 3, pp. 21–60, Jun. 2020, doi: 10.14738/TMLAI.83.8219.

[214] A. Nitaj and T. Rachidi, "Applications of Neural Network-Based AI in Cryptography," *IACR Cryptol. ePrint Arch.*, vol. 7, no. 3, Sep. 2023, doi: 10.3390/CRYPTOGRAPHY7030039.

[215] K. Sooksatra and P. Rivas, "A Review of Machine Learning and Cryptography Applications," *2020 Int. Conf. Comput. Sci. Comput. Intell.*, pp. 591–597, Dec. 2020, doi: 10.1109/CSCI51800.2020.00105.

[216] Y. Long, Y. Gong, W. Huang, J. Cai, N. Xu, and K. ching Li, “Cryptography of Blockchain,” *Int. Conf. Smart Comput. Commun.*, vol. 13828 LNCS, pp. 340–349, 2022, doi: 10.1007/978-3-031-28124-2_32.

[217] S. Ahmad, S. K. Arya, S. Gupta, P. Singh, and S. K. Dwivedi, “Study of Cryptographic Techniques Adopted in Blockchain,” *2023 4th Int. Conf. Intell. Eng. Manag.*, 2023, doi: 10.1109/ICIEM59379.2023.10166591.

[218] І. В. Миронець and А. В. Шкребтій, “Cryptographic algorithms and features of their use in blockchain systems,” *Ukr. Sci. J. Inf. Secur.*, vol. 25, no. 2, Aug. 2019, doi: 10.18372/2225-5036.25.13745.

[219] M. Raikwar, D. Gligoroski, and K. Kralevska, “SoK of Used Cryptography in Blockchain,” *IEEE Access*, vol. 7, pp. 148550–148575, 2019, doi: 10.1109/ACCESS.2019.2946983.

[220] G. J. Katuwal, S. Pandey, M. Hennessey, and B. Lamichhane, “Applications of Blockchain in Healthcare: Current Landscape & Challenges,” *arXiv.org*, 2018.

[221] L. Bell, W. J. Buchanan, J. Cameron, and O. Lo, “Applications of Blockchain Within Healthcare,” *Blockchain Healthc. Today*, vol. 1, Jul. 2018, doi: 10.30953/BHTY.V1.8.

[222] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, “Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives,” *Cryptogr.*, vol. 3, no. 1, pp. 1–16, Mar. 2019, doi: 10.3390/CRYPTOGRAPHY3010003.

[223] A. S. Shete, S. Bhutada, M. B. Patil, P. H. Sen, N. Jain, and P. Khobragade, “Blockchain technology in pharmaceutical supply chain : Ensuring transparency, traceability, and security,” *J. Stat. Manag. Syst.*, vol. 27, no. 2, pp. 417–428, 2024, doi: 10.47974/JSMS-1266.

[224] G. Tiwari, P. Channakkalavara, G. Singh, and P. N. K. Sarella, “Enhancing Security, Transparency, and Efficiency of Blockchain Technology in Pharmaceutical Supply Chain,” *Int. J. Pharm. Qual. Assur.*, vol. 15, no. 02, pp. 1009–1016, Jun. 2024, doi: 10.25258/IJPQA.15.2.71.

[225] I. Haq and O. Muselemu, “Blockchain Technology in Pharmaceutical Industry to Prevent Counterfeit Drugs,” *Int. J. Comput. Appl.*, vol. 180, no. 25, pp. 8–12, Mar. 2018, doi: 10.5120/IJCA2018916579.

[226] S. K., P. Pandey, and R. Dhanalakshmi, “A Counterfeit Solution for Pharma Supply Chain,” *EAI Endorsed Trans. Cloud Syst.*, vol. 3, no. 11, p. 154550, Apr. 2018, doi: 10.4108/EAI.11-4-2018.154550.

[227] L. Hang, B. H. Kim, K. H. Kim, and D. H. Kim, “A Permissioned Blockchain-Based Clinical Trial Service Platform to Improve Trial Data Transparency,” *Biomed Res. Int.*, vol. 2021, 2021, doi: 10.1155/2021/5554487.

[228] A. Moatari-Kazerouni, D. R. Pai, A. E. Chicas, and A. Keramati, “How blockchain technology supports the business processes of clinical trials: a systematic review,” *Bus. Process Manag. J.*, vol. 30, no. 2, pp. 388–410, Apr. 2023, doi: 10.1108/BPMJ-04-2023-0301.

[229] W. Zhang, “Blockchain-based solutions for clinical trial data management: a systematic review,” *Metaverse Basic Appl. Res.*, vol. 1, p. 17, Dec. 2023, doi: 10.56294/MR202217.

[230] M. Benchoufi and P. Ravaud, “Blockchain technology for improving clinical research quality,” *Trials*, vol. 18, no. 1, Jul. 2017, doi: 10.1186/S13063-017-2035-Z.

[231] M. de-Melo-Diogo, J. Tavares, and Â. N. Luís, “Data Security in Clinical Trials Using Blockchain Technology,” *Polit. Econ. Implic. Blockchain Technol. Bus. Healthc.*, pp. 250–268, Jun. 2021, doi: 10.4018/978-1-7998-7363-1.CH010.

[232] M. Benchoufi, D. Altman, and P. Ravaud, “From Clinical Trials to Highly Trustable Clinical Trials: Blockchain in Clinical Trials, a Game Changer for Improving Transparency?,” *Front. Blockchain*, vol. 2, 2019, doi: 10.3389/FBLOC.2019.00023/PDF.

[233] I. P. Odilibe, A. Atadoga, O. A. Elufioye, T. T. Omaghomi, O. Akomolafe, and R. Owolabi, “Blockchain in healthcare: A comprehensive review of applications and security concerns,” *Int. J. Sci. Res. Arch.*, vol. 11, no. 1, pp. 1605–1613, Feb. 2024, doi: 10.30574/IJSRA.2024.11.1.0244.

[234] M. N. Alruwaill, S. P. Mohanty, and E. Kougianos, “Forti-Ins: A Blockchain Based Framework to Automate Healthcare Insurance Processing in Smart Cities,” *Int. Symp. Smart Electron. Syst.*, pp. 353–358, 2023, doi: 10.1109/ISES58672.2023.00078.

[235] J. C. Mendoza-Tello, T. Mendoza-Tello, and H. Mora, “Blockchain as a Healthcare Insurance Fraud Detection Tool,” *Res. Innov. Forum*, pp. 545–552, 2020, doi: 10.1007/978-3-030-62066-0_41.

[236] S. Wakekar, P. R. A. Meshram, S. Jadhao, V. Pachpol, and V. Umbarkar, “Revolutionizing the Insurance Industry: A Blockchain based Claims Management System,” *IJARCCE*, vol. 12, no. 4, Apr. 2023, doi: 10.17148/IJARCCE.2023.124123.

[237] V. Sharma, A. Gupta, N. U. Hasan, M. Shabaz, and I. Ofori, “Blockchain in Secure Healthcare Systems: State of the Art, Limitations, and Future Directions,” *Secur. Commun. Networks*, vol. 2022, 2022, doi: 10.1155/2022/9697545.

[238] A. A. Mazlan, S. M. Daud, S. M. Sam, H. Abas, S. Z. A. Rasid, and M. F. Yusof, “Scalability Challenges in Healthcare Blockchain System—A Systematic Review,” *IEEE Access*, vol. 8, pp. 23663–23673, 2020, doi: 10.1109/ACCESS.2020.2969230.

[239] M. Miah, “A Comprehensive Study on the Use of Blockchain Technology in Healthcare,” *Inf. Technol. Manag. Sci.*, vol. 26, pp. 1–9, Nov. 2023, doi: 10.7250/ITMS-2023-0001.

[240] A. Atadoga, O. Adijat Elufioye, T. T. Omaghomi, O. Akomolafe, I. P. Odilibe, and O. R. Owolabi, “Blockchain in healthcare: A comprehensive review of applications and security concerns,” *Int. J. Sci. Res. Arch.*, vol. 11, no. 1, pp. 1605–1613, Feb. 2024, doi: 10.30574/IJSRA.2024.11.1.0244.

[241] A. AbuHalimeh and O. Ali, “Comprehensive review for healthcare data quality challenges in blockchain technology,” *Front. Big Data*, vol. 6, 2023, doi:

10.3389/FDATA.2023.1173620/PDF.

[242] R. D. Garcia, G. S. Ramachandran, R. Jurdak, and J. Ueyama, “Blockchain-Aided and Privacy-Preserving Data Governance in Multi-Stakeholder Applications,” *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 4, pp. 3781–3793, Dec. 2022, doi: 10.1109/TNSM.2022.3225254.

[243] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” *IEEE Int. Symp. Pers. Indoor Mob. Radio Commun.*, vol. 2017-October, pp. 1–5, Jul. 2017, doi: 10.1109/PIMRC.2017.8292361.

[244] A. Vernekar, A. Kshirsagar, and V. K. Pachghare, “Sharding-Based Scalability Enhancement of Blockchain-Based Health Application,” *Int. Conf. Circuit, Power Comput. Technol.*, pp. 901–906, 2023, doi: 10.1109/ICCPCT58313.2023.10245363.

[245] C. Pandey, “Scalability Challenges and Opportunities in Blockchain-based Systems: A Systematic Review,” *Turkish J. Comput. Math. Educ.*, vol. 11, no. 3, pp. 2022–2031, Dec. 2020, doi: 10.17762/TURCOMAT.V11I3.13599.

[246] G. Farouk and T. Alsamara, “Legal View on Blockchain Technologies in Healthcare: A European States Case Study,” *Int. J. Sociotechnology Knowl. Dev.*, vol. 15, no. 1, 2023, doi: 10.4018/IJSKD.333154.

[247] A. Corte-Real, T. Nunes, and P. R. da Cunha, “Reflections about Blockchain in Health Data Sharing: Navigating a Disruptive Technology,” *Int. J. Environ. Res. Public Health*, vol. 21, no. 2, Feb. 2024, doi: 10.3390/IJERPH21020230.

[248] K. Paranjape, M. Parker, D. Houlding, and J. Car, “Implementation Considerations for Blockchain in Healthcare Institutions,” *Blockchain Healthc. Today*, vol. 2, Jan. 2019, doi: 10.30953/BHTY.V2.114.

[249] S. A. Wright, “Technical and Legal Challenges for Heal Thcare Blockchains and Smart Contracts,” *2019 ITU Kaleidosc. ICT Heal. Networks, Stand. Innov. (ITU K)*, Dec. 2019, doi: 10.23919/ITUK48006.2019.8996146.

[250] T. Justinia, “Blockchain Technologies: Opportunities for Solving Real-World Problems in Healthcare and Biomedical Sciences,” *Acta Inform. Medica*, vol. 27, no. 4, pp. 284–291, 2019, doi: 10.5455/AIM.2019.27.284-291.

[251] L. Hang, C. Chen, L. Zhang, and J. Yang, “Blockchain for applications of clinical trials: Taxonomy, challenges, and future directions,” *IET Commun.*, vol. 16, no. 20, pp. 2371–2393, Dec. 2022, doi: 10.1049/CMU2.12488.

[252] U. Topaloglu and M. B. Palchuk, “Using a Federated Network of Real-World Data to Optimize Clinical Trials Operations.,” *JCO Clin. Cancer Informatics*, no. 2, pp. 1–10, Dec. 2018, doi: 10.1200/CCI.17.00067.

[253] M. B. Palchuk *et al.*, “A global federated real-world data and analytics platform for research,” *JAMIA Open*, vol. 6, no. 2, Jul. 2023, doi: 10.1093/JAMIAOPEN/OOAD035.

[254] E. P. Adeghe, C. A. Okolo, and O. T. Ojeyinka, “Evaluating the impact of blockchain

technology in healthcare data management: A review of security, privacy, and patient outcomes," *Open Access Res. J. Sci. Technol.*, vol. 10, no. 2, pp. 013–020, Mar. 2024, doi: 10.53022/OARJST.2024.10.2.0044.

[255] R. P. Gowri, S. Muralitharan, G. Nivin, and M. S. Aravindh, "Decentralizing Healthcare and Securing with Blockchain Technology," *March 2024*, vol. 6, no. 1, pp. 12–26, Mar. 2024, doi: 10.36548/JITDW.2024.1.002.

[256] Z. A. Shaikh, A. A. Memon, A. M. Shaikh, S. Soomro, and M. Sayed, "BLOCKCHAIN IN HEALTHCARE: UNLOCKING THE POTENTIAL OF BLOCKCHAIN FOR SECURE AND EFFICIENT APPLICATIONS FOR MEDICAL DATA MANAGEMENT- A PRESENTATION OF BASIC CONCEPTS," *Liaquat Med. Res. J.*, vol. 5, no. 2, Jun. 2023, doi: 10.38106/LMRJ.2023.5.2-08.

[257] S. Singh, S. Kumar Sharma, P. Mehrotra, P. Bhatt, and M. Kaurav, "Blockchain technology for efficient data management in healthcare system: Opportunity, challenges and future perspectives," *Mater. Today Proc.*, vol. 62, pp. 5042–5046, Jan. 2022, doi: 10.1016/J.MATPR.2022.04.998.

[258] M. Attaran, "Blockchain technology in healthcare: Challenges and opportunities," *Int. J. Healthc. Manag.*, vol. 15, no. 1, pp. 70–83, 2020, doi: 10.1080/20479700.2020.1843887.

[259] V. P. K. Juturi, "Utilizing Blockchain Technology in the Pharmaceutical Enterprise Business," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 10, no. 3, pp. 612–618, Jun. 2024, doi: 10.32628/CSEIT2410342.

[260] T. F. Heston, "A Case Study in Blockchain Healthcare Innovation," *Energy Eng. eJournal*, 2017, doi: 10.22541/AU.151060471.10755953.

[261] A. S. Rutschman, "Healthcare Blockchain Infrastructure: A Comparative Approach," *IO Product.*, 2018.

[262] E. Chukwu and L. Garg, "A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations," *IEEE Access*, vol. 8, pp. 21196–21214, 2020, doi: 10.1109/ACCESS.2020.2969881.

[263] T. F. Heston, "A Case Study in Blockchain Healthcare Innovation," *Energy Eng. eJournal*, 2017, doi: 10.22541/AU.151060471.10755953.

[264] "KSI Blockchain Timestamping — Guardtime." Accessed: Jan. 03, 2025. [Online]. Available: https://guardtime.com/timestamping

[265] "Keyless Signature Infrastructure® (KSI™) Technology An Introduction to KSI Blockchain Technology and Its Benefits," 2016.

[266] "Evaluating the practicality of using blockchain technology in different use cases in the healthcare sector," 2020.

[267] J. Mattke, A. Hund, C. Maier, and T. Weitzel, "How an Enterprise Blockchain Applicationin the U.S. Pharmaceuticals Supply Chain isSaving Lives," *MIS Q. Exec.*, vol. 18, no. 4, pp. 245–

261, 2019, doi: 10.17705/2MSQE.00019.

[268] M. Uddin, “Blockchain Medledger: A Hyperledger Fabric Enabled Drug Traceability System for Counterfeit Drugs in Pharmaceutical Industry.,” *Int. J. Pharm.*, vol. 597, Mar. 2021, doi: 10.1016/J.IJPHARM.2021.120235.

[269] “About Us.” Accessed: Jan. 04, 2025. [Online]. Available: https://www.chronicled.com/about-us

[270] E. Morley-Fletcher, “MHMD: My Health, My Data,” *EDBT/ICDT Work.*, 2017.

[271] “PharmaLedger - LifeSTech.” Accessed: Jan. 05, 2025. [Online]. Available: https://www.lst.tfo.upm.es/pharmaledger/

[272] G. Kondova and A. Arockia, “Healthcare Data Management Using Blockchain: MyHealthMyData (MHMD) and PharmaLedger,” *Hum. Interact. Emerg. Technol. (IHIET-AI 2022) Artif. Intell. Futur. Appl.* , vol. 23, no. 23, 2022, doi: 10.54941/AHFE100897.

[273] H. Kayhan, “Ensuring Trust in Pharmaceutical Supply Chains by Data Protection by Design Approach to Blockchains,” *Blockchain Healthc. Today*, vol. 5, Oct. 2022, doi: 10.30953/BHTY.V5.232.

[274] “MediBloc Company Profile 2025: Valuation, Funding & Investors | PitchBook.” Accessed: Jan. 06, 2025. [Online]. Available: https://pitchbook.com/profiles/company/228939-31#overview

[275] “MediBloc, a blockchain-based PHR(personal health records) platform - 바이오스펙테이터.” Accessed: Jan. 06, 2025. [Online]. Available: https://www.biospectator.com/news/view/6509

[276] “MediBloc Limited - Own your health data. It’s rightfully yours.” Accessed: Jan. 06, 2025. [Online]. Available: https://medibloc.com/

[277] “whitepaper/TechinicalWhitepaper_ENG.md at master · medibloc/whitepaper · GitHub.” Accessed: Jan. 06, 2025. [Online]. Available: https://github.com/medibloc/whitepaper/blob/master/TechinicalWhitepaper_ENG.md

[278] “Patientory | Your Health At Your Fingertips.” Accessed: Jan. 06, 2025. [Online]. Available: https://patientory.com/faq

[279] “Whitepaper | Medicalchain.” Accessed: Jan. 06, 2025. [Online]. Available: https://medicalchain.com/en/whitepaper/

[280] M. Ramachandran, “Ethics of Blockchain by Design: Guiding a Responsible Future for Healthcare Innovation,” *Blockchain Healthc. Today*, vol. 7, no. 3, Dec. 2024, doi: 10.30953/BHTY.V7.362.

[281] M. S. Gross and R. Miller, Jr., “Ethical Implementation of the Learning Healthcare System with Blockchain Technology,” *Blockchain Healthc. Today*, Jun. 2019, doi: 10.2139/SSRN.3391034.

[282] K. Singh, C. Krishna, and D. Kumar, “Professional Ethics, Challenges and Opportunities for

BlockchainTechnology in Healthcare Sector: A Systematic Review," *Recent Adv. Comput. Sci. Commun.*, vol. 17, no. 1, Nov. 2023, doi: 10.2174/0126662558263462231020111428.

[283] S. Hyrynsalmi, S. M. Hyrynsalmi, and K. K. Kimppa, "The state of the art of the blockchain ethics in healthcare: A systematic literature review," *Finnish J. eHealth eWelfare*, vol. 13, no. 3, p. 193, Oct. 2021, doi: 10.23996/FJHW.102906.

[284] S. Hyrynsalmi, S. M. Hyrynsalmi, and K. K. Kimppa, "The state of the art of the blockchain ethics in healthcare: A systematic literature review," *Finnish J. eHealth eWelfare*, vol. 13, no. 3, Oct. 2021, doi: 10.23996/FJHW.102906.