ISSN E: 3006-1466
ISSN P: 3006-1458

CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR

CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW

Vol.03 No.03 (2025)

An Evaluation on the Use of Blockchain Technology in Healthcare Systems

1. ***Shahzad Ali Khaskheli (Corresponding Author)***
   Lecturer IT, Shaheed Benazir Bhutto University, Sanghar Campus, Pakistan.
   Email: shahzadali@sbbusba.edu.pk
2. ***Mazhar Basheer Arain***
   Computer Science, Faculty of Computing & IT, Government College University, Hyderabad, Sindh, Pakistan.
   Email: mazhar.arain@gcuh.edu.pk
3. ***Imran Ali Memon***
   Lecturer IT, Shaheed Benazir Bhutto University, Sanghar Campus, Pakistan.
   Email: imranmemon@sbbusba.edu.pk
4. ***Manzar Bashir Arain***
   Lecturer, Department of Information Technology, Shaheed Benazir Bhutto University, Sanghar Campus, Pakistan.
   Email: manzar.arain_sng@sbbusba.edu.pk

Abstract

Recently, the emergence of blockchain techniques—and their corresponding capabilities—have been heavily discussed—particularly—within the purview of the healthcare sector. Certainly, blockchain technology could remedy a number of fundamental challenges pertaining to the electronic health record system. This paper attempts to address this gap by assessing the body of research pertaining to blockchain technology and health with a special focus on the challenges that blockchain poses. Adopting a systematic funnel approach, this paper seeks to analyze 144 articles on the challenges and importance of the technology. The aim is to reconcile the possible adverse outcomes of the health sector with the outcomes of such technologies by speculating on possible domains of blockchain technology that can be further researched in healthcare. The paper provides a thorough examination on the defining characteristics of blockchain and blockchain technology in all available literature. This background helps frame the growing body of literature on blockchain and health—approached by defining the current focus areas of research in blockchain and healthcare systems. From there, it narrows down on specific issues and pinpoints the associated blockchain solutions to healthcare systems. Ultimately, the author reflects on the looming issues of research gaps and prospective challenges of the health sector in the concluding section.

Keywords: *healthcare_environment; distributed_ledger_technology; patient-chart; physiological-surveillance; clinical-dataset_confidentialit*

1. Introduction

Soaring operational expenditures and protracted management cycles rank among the most urgent challenges confronting contemporary health-care systems [1]. Characterized by intricate interdependencies, the ecosystem encompasses a diverse constellation of actors—physicians, researchers, allied health personnel, managerial staff, and the patients themselves—operating across heterogeneous administrative and clinical domains [2]. Within this context, the systematic classification, stewardship, and dissemination of patient data escalate into a formidable task [3,4]. Variability in data schemata and work processes across different clinical and administrative silos compounds the difficulty, resulting in severely fragmented information flows. Therefore, the inability to exchange patient-related data effectively among heterogeneous health-care domains constitutes a pervasive and deleterious bottleneck [5].

To remediate the fragmentation of health information records and facilitate robust data exchange, a sustained investment in design, governance, and operational stewardship is indispensable. Legacy approaches assign the creation and upkeep of personal health record and electronic health record systems to centralized third parties, leaving issues of trust, confidentiality, and data integrity inadequately addressed [6]. These traditional, vendor-controlled architectures have proven incapable of aligning the privacy expectations of multiple stakeholders—patients, clinicians, and regulators alike [7]. Consequently, current electronic health-care frameworks suffer from an opacity that acts as a constraint, essentially delegating the stewardship of sensitive health information to intermediaries and obscuring the granularity of user consent and data provenance.

To address pressing security issues and the considerable challenge posed by both the volume and heterogeneity of data in the healthcare domain, the potential of blockchain technology is increasingly acknowledged. Fundamentally, blockchain operates as a decentralized, distributed digital ledger, employing a peer-to-peer networking model. Within this architecture, a network of nodes cooperates to verify and append new blocks to the chain, thereby enabling the secure transmission of medical information without requiring the endorsement of a central authority. End users, once authenticated through secure cryptographic credentials, retain immediate and comprehensive visibility of all data to which they have been granted legitimate and verifiable access. Transactions may be initiated by any permitted actor, and subsequent blocks can therefore be successively concatenated by augmenting the existing chain in a manner that preserves integrity. The continuous chain is anchored through a cryptographic hash that distills each block into a fixed-size, immutable fingerprint; this hash serves as the unique key permitting the safe inscription of records and, in cryptocurrency contexts, the validation of monetary exchanges.

Marginal confidence in proprietary electronic health record– and personal health record–based health-information-exchange networks with respect to privacy and security has consistently stalled multilateral engagement among stakeholders required to share health information effectively. Consequently, aggregate system-on-board failure has inflated health-care expenditure, burdening both patients and providers alike. To address the attendant trust deficits, attention is now pivoting toward blockchain protocols. According to IBM, leading health-care organizations anticipate that blockchain will markedly transform system architecture by migrating health-management infrastructure to a permissioned, decentralized ledger that atomically exchanges electronic health-data parcels. Recent forecasts indicate that the dedicated blockchain health-care services market will exceed USD 500 million by 2022. Although the academic and professional literature has produced a substantive, if partial, body of blockchain-health-case studies, a fragmentary picture of plausible application domains persists. Consequently, systematic reviews must now be commissioned to thoroughly delineate architectural, administrative, and operational use cases of blockchain within the health-care industry. Concomitant infrastructural programmes continue to aggregate cloud-hosted ledger nodes capable of provisioning service to geographically dispersed mobile clients.

Today’s pervasive Internet infrastructure enables mobile devices and integrated applications to generate and transfer vast volumes of medical information on a weekly, and frequently a daily, basis. This surging capability suggests that prevailing healthcare delivery frameworks could, in principle, alleviate constraints tied to expenditure, tactical procurement, standardization, and patient adherence to care pathways. Nonetheless, healthcare producers do not uniformly exploit contemporary technological capabilities across supply chains. An observable gap persists, for instance, in the procurement and inventory redistribution of the core medical stock, which remains misaligned with real-time demand signals. Healthcare Finance, in one authoritative account, quantified the recurring, superfluous fiscal burden at approximately $25.7 billion annually, attributed to outdated or fragmented material-management processes. Substantial realignment is, therefore, obligatory; a concerted, intelligent healthcare system must absorb this disparity. Attention must, therefore, be devoted to methodical optimization of design and engineering, anchored in interconnected smart devices, purpose-optimized infrastructure, interoperable workflows, and a reconfigured institutional architecture that is digitally rotted.

The deployment of intelligent healthcare could similarly leverage patient-linked applications, next-generation biosensors, and enhanced emergency management platforms [14]. Consequently, the design of a more resilient network mandates the evaluation of consensus mechanisms presently adopted by varied blockchain systems, followed by the selection of those most congruous with a healthcare-focused, IoT-oriented architecture [15]. An alternative extension of blockchain's data-criticality lies in the Distributed Data Storage System (DDSS), which accelerates information dispersion by leveraging a mediated caching architecture and file transformation protocols [16]. This framework reconciles the indexing of identically titled files ubiquitous in clinical directories; upon receipt of an oversized dataset, the DDSS deconstructs it into smaller, re-constitutable segments—256 kilobyte shards, for illustrative purposes—each aggregated into a vacant logical holder and subsequently retrievable through Distributed Hash Table (DHT) referents [17]. A converging set of sensor modules is capable of suspensory proximal actuations: automatic subject interrogations and proximal transmission to federated depositories or cloud shelters, facilitating subsequent review by attending physicians, nursing teams, or supporting agents [18]. To reinforce patient-centered sovereignty, an array of legislative and normative safeguards is concurrently Table-19 proposed, each calibrated to fund proscriptive protective lenses.

Compliance frameworks mandate robust security management measures governing the observation, dissemination, and transmission of patient health information, and nonadherence to these stipulations is met with stringent prosecution, drawing exorbitant financial and operational penalties against electronic health record (EHR) platforms . An analysis commissioned by IBM indicates that approximately 70% of healthcare executives anticipate that blockchain technology will profoundly transform multiple domains within the health sector, notably by enhancing the conduct of clinical trials, by facilitating adherence to regulatory standards, and by enabling the establishment of a decentralized architecture for the secure exchange of electronic health records. Increased access to lower-cost data security and management is driving rising interest in blockchain-powered healthcare platforms among both practitioners and researchers. Over the past decade, the corpus of investigations into blockchain in healthcare has expanded dramatically. A systematic synthesis of the field, however, is undermined by the absence of centralized, enduring documentation that collates and interprets earlier contributions. Present meta-analyses provide concise snapshots of recent innovations and critically annotate the merits and limitations of specific scholarly proposals, yet omit detailed comparative evaluation of the architecture. An integrated appraisal is still lacking of core dimensions such as recurrent and emergent research themes, the clinical domains where blockchain pilots and prototypes are concentrated, function categories, and the performance of available deployed systems. Thus, strategic agendas for continued inquiry confront a fragmented baseline that hampers identification of knowledge gaps, evaluation of accumulated evidence, and systematic planning of incremental or transformative elaborations of blockchain in the healthcare landscape.

The objective of the present investigation is to survey comprehensively the corpus of extant literature in order to delineate the substantive and prospective modalities for blockchain deployment across diverse domains of healthcare practice. Supplementary to the survey, the inquiry addresses the emerging trajectories of inquiry, the prevailing impediments, and the prospective itinerary for subsequent investigation within blockchain-enabled healthcare architectures. The decisive contribution of this work resides in the systematic synthesis of the assembled literature, designed to organize and consolidate the conceptual and empirical knowledge appertaining to blockchain applications in the healthcare setting.

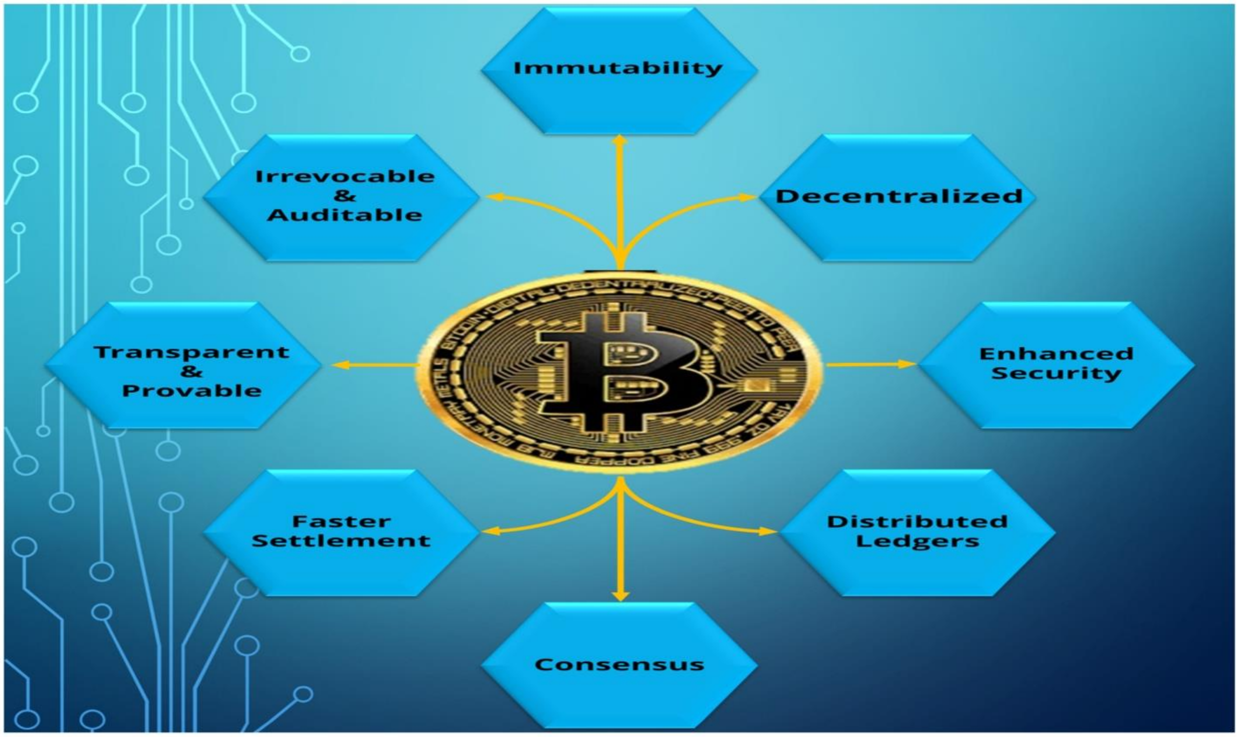
2. Background Study of Blockchain

2.1. Definition of Blockchain

Blockchain refers to a distributed, tamper-resistant ledger that enables organizations to track assets and log transactions in a network without a central authority. The structure consists of an increasing series of discrete files, called blocks, that are linked through cryptography to form a secure chain. Each block contains transaction records, a timestamp, and a cryptographic hash that identifies and authenticates the immediately preceding block. The timestamp attests to the presence of the transaction data at the instant the block was generated. Because each new block contains a reference to the block that came before, the records are inherently interconnected, producing a continuous chain. Consequently, when a transaction is inscribed in a block and that block is added to the chain, the record becomes permanent. Later modification of that record would necessitate alteration of all subsequent blocks, a task that is computationally infeasible, thus safeguarding the irreversibility of blockchain transactions.

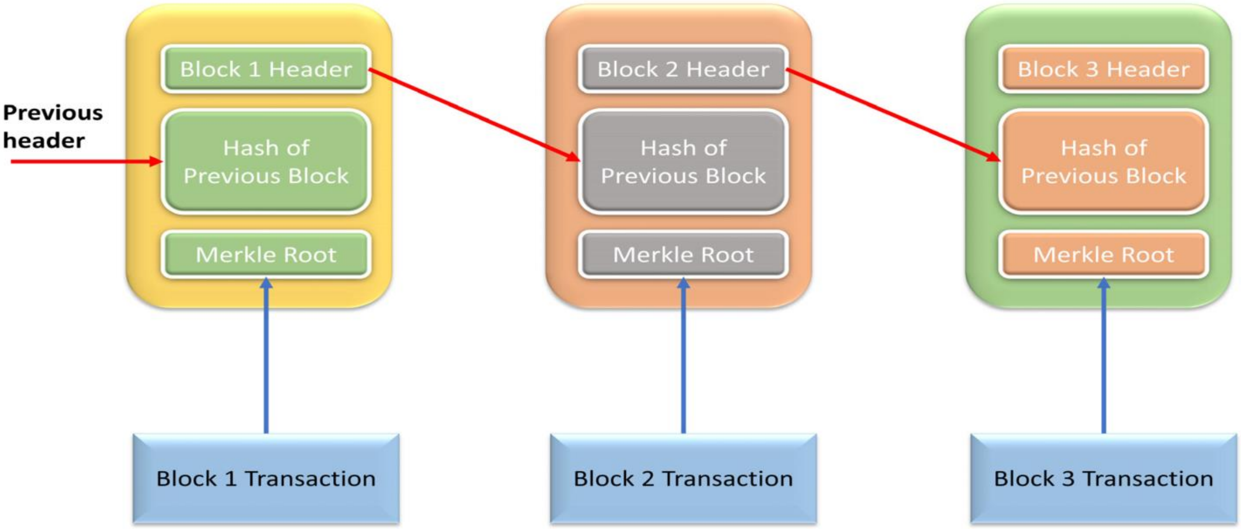
2.1.1. Key Features

Decentralization represents one of the foundational attributes of blockchain systems. By design, no single authority presides over the validity of information posted to the chain; instead, the data is validated through distributed consensus mechanisms that engage all nodes in the peer-to-peer architecture. A comprehensive treatment of these mechanisms may be found in Section 2.1.4. The design architecture prioritizes data security such that transactions occur without intermediaries, thereby minimizing exposure to data breaches, tampering, or unauthorized interception. An additional defining quality is permanence: once a record is validated and appended to the chain, its footprint is replicated across a wide array of independent nodes, rendering erasure infeasible. Furthermore, many blockchain implementations incorporate a level of pseudonymity, permitting participants to mask their identities while still enforcing accountability through cryptographic proofs. Figure 1 synthesizes these principal attributes and illustrates their interplay at a high level.



A blockchain permits auditing and traceability through the batch-wise linkage of successive blocks, thereby establishing a continuous chain. For each block, a Merkle tree is constructed, synthesizing a digest of the contained transactions. The transactions themselves are hashed into leaf nodes, and these nodes are recursively hashed to form a single summary, the Merkle root, which is embodied within the block header. This design confines the responsibility for retaining and endorsing the integrity of the root to the blockchain itself, which periodically re-includes this root when appending new blocks. The graphic representation given in Figure 2 elucidates the layered architecture of the blockchain and the interfacing Merkle tree.

2.1.2. Different Kinds of Blockchain



As summarized in Table 1, blockchain architectures can be broadly categorized into three types: private, public, and consortium [21]. The distinguishing attributes of each type relate directly to permissions governing who may write, read, and transact on the ledger. A public blockchain is characterized by unrestricted access: any user may inspect the ledger, and their permissionless model enables individuals to join the network, contribute to data storage, and—in some cases—modify the governing software [21]. This framework is prevalent in cryptocurrency applications, most notably in the two largest digital currencies, Bitcoin, analyzed in [23], and Ethereum, examined in [24]. Conversely, consortium blockchains limit participation to a predefined set of organizations, thereby creating a shared ledger whose governance and validation nodes are controlled by an allocated alliance. Private blockchains restrict operations to a single organization, resulting in a ledger that is invisibly maintained and definitively controlled from a central node, with no allowance for external access or validation [21]. Beyond these functional descriptions, the academic community continues to debate the need for a more comprehensive taxonomy of blockchain systems [25].

2.1.3. Difference between Blockchain in Healthcare and General Sectors

From its launch as the underlying architecture of Bitcoin, blockchain was overwhelmingly oriented towards facilitating electronic monetary transactions. This foundational paradigm subsequently expanded in the past decade with the emergence of numerous blockchain-derived cryptocurrencies such as Ethereum, Tether, BNB, and Dogecoin. Endowed with characteristics of decentralization, immutability, and cryptographic security, these currencies have proven to be advantageous vehicles for diverse financial operations, including the provision of loans and the underwriting of insurance risks.

In contrast to this predominant monetary focus, the health-care application of blockchain centres principally on the construction of federated, trustless architectures for the governance of sensitive patient-identifiable data. By performing this central function, health care possesses a secondary module for conducting cryptographic monetary transactions, which complements its dominant mandate of medical record security without supplanting the original financial logic of the underlying technology.

The expansion of blockchain technology has advanced at an extraordinary pace since its initial conception. Originally designed to facilitate cryptocurrency transactions, the ledger template is now being repurposed to secure the electoral process, capitalizing on its immutability. Deploying immutable smart contracts compounds the benefit by mandating transparency, thereby binding all actors to predefined obligations, while preserving the transaction history. Parallel progress has addressed the inherent vulnerability of the Internet of Things (IoT) architectures by substituting conventional communication and archival mechanisms with blockchain-anchored infrastructures that assure confidentiality, provenance, and integrity. Conceptually, the diffusion of technology is constrained solely by the creative projection of its operators. Within the present research, attention is concentrated on quantifying the repercussions of distributed ledgers within the healthcare domain; however, the technology provides identical generic advantages across all industries. Hence, the vertical, subject-agnostic blocks of financial settlement, personal information circumscription, material traceability, and consolidated data sovereignty continue to be equally available to the healthcare ecosystem.

2.1.4. Frameworks for Decentralized Development

A wide assemblage of pre-engineered blockchain stacks is now accessible for fabricating decentralized software ecosystems. Prominent among these ecosystems are Hyperledger and Ethereum. Both infrastructures furnish engineers with programmable scripting and mining alternatives for incubating innovative distributed ledgers while permitting the formal deployment of ephemeral test nets that imitate genesis protocols.

2.1.5. Mechanisms for Consensus

Consensus on insertion of new entries into a blockchain is achieved through the operation of distributed ledgers governed by a distributed agreement protocol. The three predominant consensus protocols are catalogued in Table 2.

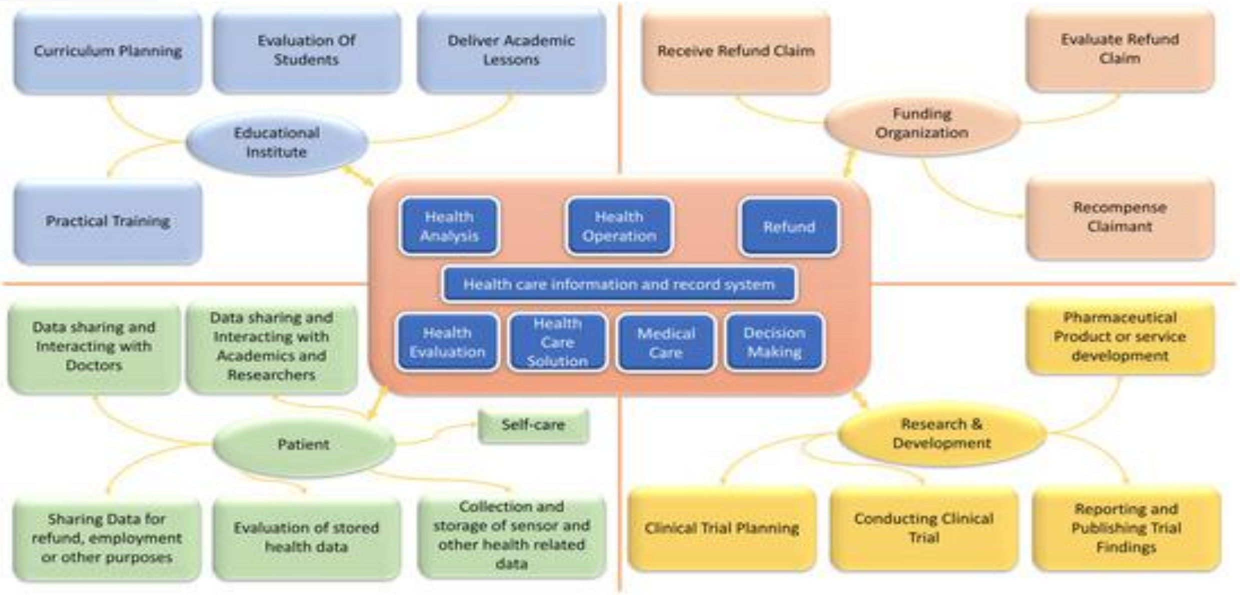
The proof-of-work (PoW) protocol is the mechanism upon which the Bitcoin network operates, thereby inextricably linking its operation to the blockchain architecture. Under PoW, miners compete to solve a cryptographically challenging puzzle. Each miner strives to produce a hash of the proposed block such that the hash possesses a numeric value lower than a designated threshold. The miner that successfully generates a qualifying hash is deemed to have solved the puzzle and is granted a block reward, provided that the transactions within the block are valid. Despite its widespread adoption, PoW exhibits a significant limitation: when employed in a large-scale blockchain, it imposes exceedingly high energy demands, as enumerated in reference [27].

In the proof-of-stake blockchain paradigm, node selection is derived from a deterministic criterion that leverages the state of the blockchain itself. In this context, the term "stake" is equivalent to the quantity of a specific cryptocurrency held by the participant. This mechanism inherently favours economically advantaged nodes, since larger holdings confer disproportionate influence over consensus. To mitigate this property, several proof-of-stake variants parasitically incorporate randomized functions into the validation process, delegating some influence to unpredictability that is independent of mere capitalisation. The Ethereum development team is in the process of transitioning from a proof-of-work to a proof-of-stake validation model [21]. An examination of consensus assemblies reveals that the fault tolerance of the Byzantine model is sustained through Byzantine agreements [28]. Under practical Byzantine fault tolerance (PBFT), the participating nodes are implicitly identified in advance, thus cubic expansiveness in node connectivity precludes the direct application of this methodology in open-admission blockchain networks. PBFT is modular, being instantiated in committed, pre-prepared, and prepared variations. In each case, a super-majority of two-thirds of the total node set is requisite to advance the system from one state to the next. Currently, the PQBFT architecture is operational in the Hyperledger Fabric instantiation of the modular blockchain framework [29].

2.1.6. Smart Contracts Elevated as Codified Commitments

Ethereum furnishes a programmable blockchain wherein the premier innovation extends beyond a mere distributed ledger to encompass self-executing smart contracts [24]. These instruments embody contractual arrangements encoded in deterministic source code, yielding contractual performance that is triggered purely by the observance of programmatic conditions. Once inscribed onto the ledger, such agreements are mediated by cryptography, thereby obviating the necessity of intermediate authorities. The inherent autonomy of Ethereum’s smart contracts has catalyzed a growing penetrance within the biomedical environment [24].

2.2. Blockchain Potential in Healthcare


Curriculum Planning
Evaluation Of Students
Deliver Academic Lessons
Educational Institute
Practical Training
Receive Refund Claim
Evaluate Refund Claim
Funding Organization
Recompense Claimant
Health Analysis
Health Operation
Refund
Health care information and record system
Health Evaluation
Health Care Solution
Medical Care
Decision Making
Data sharing and Interacting with Doctors
Data sharing and Interacting with Academics and Researchers
Patient
Self-care
Sharing Data for refund, employment or other purposes
Evaluation of stored health data
Collection and storage of sensor and other health related data
Pharmaceutical Product or service development
Research & Development
Clinical Trial Planning
Conducting Clinical Trial
Reporting and Publishing Trial Findings

The fragmentation of patient records across diverse systems, compounded by frequent personnel turnover and limited asset-sharing mechanisms, diminishes trust in healthcare transactions. Such vulnerabilities stretch the capacity of health delivery, governance, research, and education. We may therefore decompose integrated care into the stage tasks of diagnosis, decision support, triage, care delivery, and outcome assessment (Figure 3). Each of these handles dynamic knowledge, requires diverse agents, and may harbor conflicting incentives. For optimal patient access, guided administrative, technical, and cognitive pathways must synchronize in real time. Degree programs must be jointly instantiated to summon up-to-date curricula and, consequently, to expose students to living patient material, quality metrics, and reflective practice. Conversely, hospitals, foundations, and regulatory sponsors must furnish realistic caseloads, consent workflows, biospecimens, and observational notes, while training programs second credentialed profiles approved by practice and research IRBs. Research sponsors do not only reciprocally influence regimen design, delta, but casually supply the infrastructure of protocol, consent instrument, data dictionary, and visualization, iterating these artifacts across empathy coalitions anchored seven environments. The cooperation reduces effectiveness and datum latency time, and diminishes relatives and design rate while amassing knowledge, talent and trust across the stakeholder networks central to sustainable healthcare experiments.

Health organizations engage in the instruction and biomedical investigation of the health workforce, as depicted in Figure 3. Such efforts necessitate the transmission of consent, clinical data, findings, and financial transactions, tasks governed by established data-exchange protocols. Regulatory stipulations mandate that these entities rigorously safeguard all information disclosed by patients during care episodes.

Figure 3: Map of the health sector

Access control and data integrity are foundational elements for safeguarding patient confidentiality and for secure data sharing among authorized partners. By carefully regulating who may view or modify patient records, confidence is fostered between information custodians and their service providers. Server components remain exclusively accountable for the formation and enforcement of access-control directives. Interactivity, in this context, refers to the capacity for heterogeneous information systems and devices—operating within the collaborative ecosystem defined by various stakeholders—to exchange data efficiently, thereby advancing the health of both individuals and the population at large. Data provenance traces its relevance to the originating data source, and within the healthcare environment, it permits continuous oversight of electronic health records, enhancing the verifiability and, consequently, the trustworthiness of such records. As articulated by Courtney and Ware, data integrity arises when the system is able to meet pre-defined quality standards. Fulfillment of specified quality objectives is therefore the definitive measure of data integrity within health information systems.

Presently, healthcare institutions are experiencing significant demand for data from research organizations [32]. Incidents of unauthorized disclosure and data exfiltration erode public trust in healthcare providers, while other breaches of practice undermine confidence in the entire healthcare system. To address these vulnerabilities, an alternative framework is warranted. The inherent decentralization characteristic of blockchain technology enables secure sharing of data, ensures data integrity, and facilitates distributed access control among the relevant stakeholders without the mediation of central intermediaries, thus preserving the public's trust in the integrity and confidentiality of the ecosystem.

2.3. Types of Blockchain in Healthcare Systems: Public, Private, and Consortium

At its core, blockchain comprises a distributed ledger that interlinks a set of nodes, each of which participates in the consensus process that authenticates the entire network. Such nodes may be classified according to their degree of openness to participant verification. In the case of permissioned, or authorized, blockchains, access and transaction validation are restricted to pre-approved members; well-known instances include Ripple [33] and Hyperledger Fabric [34]. Conversely, public blockchains such as Bitcoin [35] and Ethereum [36] concede full visibility and participatory rights to any user who chooses to join, having cryptographic credentials verified by the network. Across both types, the value proposition resides in the ability to instantiate and update cryptographically secured, distributed ledgers in a direct peer-to-peer (P2P) fashion. Figure 4 illustrates the architectural layout of a generic blockchain application in a healthcare context. Participants independently verify and cryptographically submit transactions, expunging the need for an intermediary authority. This decentralised mechanism significantly curtails expenditures related to arbitration, ad hoc modifications, network configuration, and ongoing operational maintenance that would accrue in a centralized transmission model. Critically, while these efficiencies are substantial, the architectures may still be hampered by scalability limitations as transaction volumes or network expansion intensify [37].

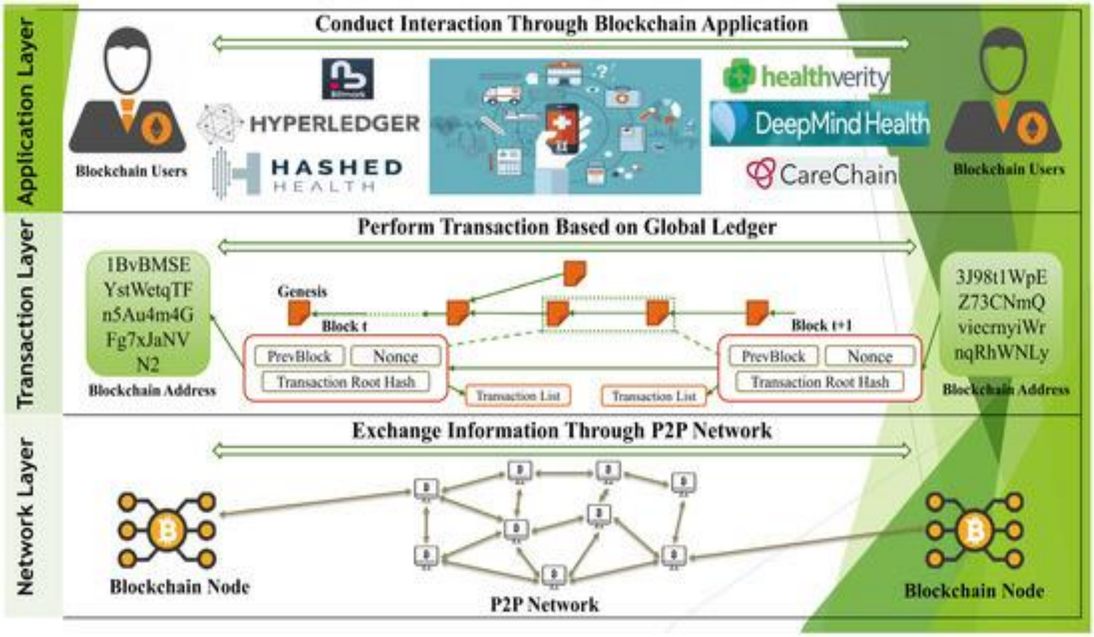
Figure 4 Blockchain Architecture

2.3.1. Public Blockchain

Public blockchains afford unrestricted entry to any participant, obviating the need for prior authorization and enabling instantaneous membership. Contributors take part in consensus via a proof-of-work smart contract. Conceived to obrogate centralized control, the architecture employs peer-to-peer propagation of blocks to verify the desired level of decentralization. Each transaction is hashed within a Merkle tree, generating a compact proof appended to the new block, which is then cross-validated against a historical ledger. Updates propagate in real time to all operative nodes, and any individual may subscribe to the network, replicating the blockchain's state on their local instance. The reliability of the ledger is underpinned by identical copies maintained by the distributed consensus environment. Public blockchains have demonstrated the capacity to streamline secure transaction processing; nevertheless, the validation process imposes considerable computational overhead, the exigency of which scales with the number of active miners. As documented, the escalating difficulty of mining directly correlates to a marked rise in cumulative energy consumption across the network [38].

2.3.2. Restricted Blockchain

Restricted blockchains impose strict access controls; only authorized nodes may observe and append the chain. Every prospective participant must present verified permissions prior to engaging in block formation and consensus, effectively prohibiting anonymous users. When firms operate such systems, transaction endorsement may be performed through credentialled validators who need not additionally obtain external permission, provided their technical competence is verified. Although transaction finality and integrity are preserved, the absence of a publicly accounting infrastructure characteristic of decentralized architectures remains a conspicuous



limitation of the model, and the overall consensus authority of the network is consequently more concentrated.

2.3.3. Federated Blockchain

Federated ledgers occupy a middle ground, exhibiting a hybrid of decentralized and centralized principles. Network nodes are not publicly discoverable; instead, their identities are predefined within a governing council or consortium. This characteristic permits the selective admission of actors who are neither wholly trusted nor wholly distrustful, reconceptualizing the public-private dichotomy of classic designs. Technical controls, especially robust cryptography, abrogate the transcription and storage risks typically posed by incomplete isolation, yet the ledger assumes ultimate consistency only to the extent that the governing protocol precludes collusion and fault. Because the invalidation of consensus augments further systemic hazards, the integrity, authenticity, and ex-ante determinism of federated blockchains continue to necessitate diligent and consistent third-party audits and governance monitoring.

3.1. Research Questions

During the initial phase of the literature review, a series of focused research questions were articulated to conform to the overarching objective of the study: to synthesise the contemporary landscape of blockchain applications within the healthcare sector and to delineate foreseeable trajectories in the domain. Accordingly, the questions served as systemic filters to curate high-quality articles emanating from eminent academic outlets. The queries are as follows:

What is the contemporary bibliometric and methodological profile of blockchain applications within the healthcare literature?

Which operational domains of the healthcare sector have adopted blockchain-based solutions?

What technical, regulatory, or organisational barriers constrain the advancement of blockchain applications in healthcare?

Which healthcare functions and decision-making processes have the potential to achieve measurable improvements through future blockchain integration?

3.2. Search Strategy and Databases

Construction of a rigorous and evidence-informed systematic review necessitates a well-defined search protocol, inclusive of a bounded lexicon that maximally extracts pertinent data. Accordingly, search terms were articulated to encompass the dual vectors of blockchain technology and healthcare processes, while still permitting a broad representation of variations in terminological and conceptual framings. Prior to the formulation of exhaustive search strategies and the delineation of paper screening criteria, a comprehensive evaluation of unresolved deficiencies within the healthcare system, amenable to remediation through blockchain, was undertaken. A variety of domains were pinpointed as the most opportune loci for blockchain implementation. Central to the architecture of blockchain is the assured transport of data and the immutable log of every transaction, attributes of conspicuous utility within healthcare, where safeguarding of patient records and verifiable documentation of financial exchanges rank as critical imperatives. Beyond confidentiality, blockchain can underpin a secure architecture for remote patient surveillance within telemedicine and expedite data propagation. The technology safeguards both the aggregation and archival of data generated by wearables. Because blockchain facilitates concurrent, real-time observation of data by a cohort of authorized users, it enhances clinical judgement by enabling simultaneous access for multiple clinicians. Furthermore, the technology's decentralized design mitigates the risk of data corruption. The foregoing represent illustrative deficiencies amenable to redress through the strategic application of blockchain. Optimal search strings can be constructed by deconstructing research queries in a systematic manner, as outlined in several studies, notably [40, 41–43]. The authors recommend segmenting queries by research focus, stakeholder group, and abbreviations while gathering associated variants—synonymous terms, acronyms, and alternative spellings—across the Boolean operators set.

The procedure leading to the final search string can be summarized in three incremental steps:

1. Collect all abstract and auxiliary lexemes encountered in the preliminary article review.
2. Employ Boolean operators, primarily OR, to connect synonymous units, while using AND, NOT, and proximity operators as appropriate.
3. Ascertain and collate abbreviations, tantamount variants, and synonymous phrases in a consolidated list.

Applying these three phases yields the following prototype search string: (“blockchain”) AND (“healthcare”) (“health”) OR (“health record”) OR (“EHR”) OR (“PHR”) OR (“medical record”) OR (“EMR”).

Executing the string, the authors interrogated the principal repositories for biomedical and computing research: IEEE XPLORE, ScienceDirect, Springer, ACM Digital Library, Sage Publications, MDPI, and Taylor & Francis. The search retrieved a primary set of 712 articles meeting the criteria.

3.3. Quality Assessment

An evaluation of the quality of the included articles is critical to the assurance that the final review will be both informative and useful. For that purpose, the manuscripts were examined with respect to research objectives, contextual framing, prior literature, salient empirical studies, applied methodology, reported results, and proposed or prospective research trajectories. Prior to the formal inclusion of studies, each article was juxtaposed with the following deliberative queries, aiming to discern conformity with the prescribed quality benchmarks:

1. What is the declared purpose of the investigation, and is that purpose explicitly addressed within the text?
2. Is the article informed by relevant reviews, historical accounts, or contextual analyses?
3. Is the manuscript pertinent to the present inquiry?
4. Is a clearly delineated research methodology articulated?
5. Is empirical or theoretical analysis undertaken?
6. Does the article advance a concise conclusion?

3.4. Article Selection

The article selection procedure commenced with a harvest of 712 manuscripts retrieved through multiple online repositories, following initial selection criteria. The process was subsequently partitioned into four discrete phases, each designed to progressively refine the corpus towards studies of maximum relevance and quality.

Phase 1: A comprehensive gathering of recent research materials was conducted, emphasizing studies published after 2018. Notably, a limited number of earlier works were retained solely for their exceptional research contributions.

Phase 2: The initial set of papers was subjected to a critical appraisal against predetermined selection criteria, resulting in the exclusion of 321 works deemed not pertinent to the current inquiry.

Phase 3: Instances of duplicate records were rectified in this phase. Following deduplication of 391 documents, the corpus was reduced to 294 unique studies.

Phase 4: A stringent qualitative assessment was performed to confirm that each paper coherently aligned with the research dilemmas under investigation. Only studies demonstrating methodological rigor and substantive relevance were retained, leading to the removal of an additional 150 papers.

Ultimately, a final assembly of 144 studies was constituted. The entire selection and appraisal process was systematically documented in accordance with the CASP Systematic Review Checklist [44].

5. Research Themes of Blockchain-Based Healthcare Systems

This section sheds lights on the former researches and analyzes their limitations, research themes and future research directions.

5.1. Research Themes

The four thematic fields that represent the focal issues that are addressed in this literature are conceptual evolution, performance improvement, technological development, and data management. From the previous results, we observe a continuing scholarly endeavor applied to improve intellectual and technological knowledge to maximize the productivity of the systems for healthcare and data management by means of blockchain.

5.1.1. Evolution of Concept

Analysis of present research materials reveals that research is being conducted on blockchain in healthcare for the development of concepts that help scholars achieve multi-domain efficiency [46]. Application feasibility is divided into three categories, as illustrated in Figure 5. These categories are further discussed in the following section.

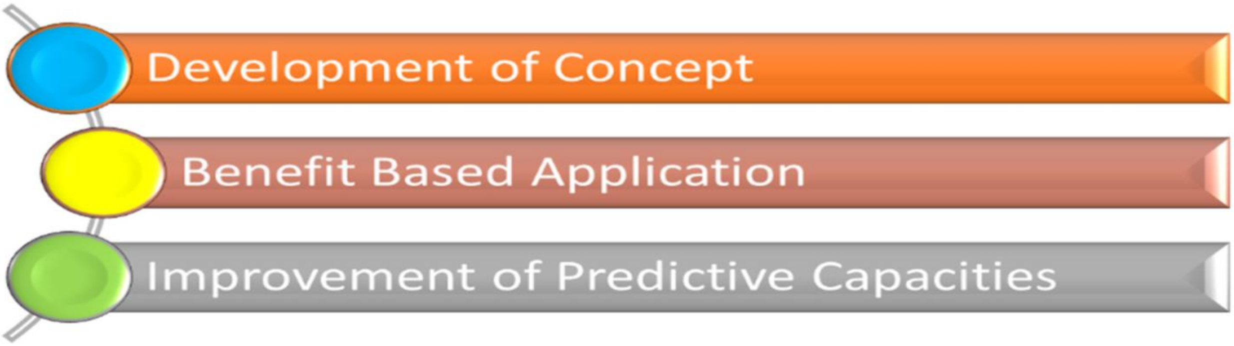

Development of Concept
Benefit Based Application
Improvement of Predictive Capacities

Figure 5: Evaluation of concept in blockchain-based healthcare system

The evolving literature illustrates how blockchain technology can yield measurable opportunities beyond theoretical models. One approach involves a proof-of-work (PoW) architecture whereby the network imposes a computational cost proportional to the resource footprint of a malicious operation—say, generating impersonated frames in an email address or orchestrating a distributed denial-of-service attack—hence rendering such activities economically unattractive for strategic adversaries. Complementarily, the proof-of-identity (PoID) paradigm, oriented to public permissionless settings, entitles each authenticated entity to a strictly fixed slice of both governance and reward, thereby neutralising wealth concentration while multiplexing participation. Design strategies also integrate tokens of source veracity, or primitive referenda, which quantify how many corroborating timestamps a datum can muster before reaching a protocol. Collectively, the recent scholarship concentrates on algorithmic and procedural lyric refinements that optimise blockchain scalability while offering modular contexts for experimental architecture—each hosting varying constructs, verifiable in situ, and logically expandable upwards. Within recent discourse on enhancing efficiency, several paradigms have been employed, including homomorphic encryption tailored to calculations [51], Stackelberg-like strategic games [52], feature-addressable cryptosystems [53], and architectural pursuits focused on infeasible sibling characteristics [54]. A leading instance is the articulation of permissionless, blockchain-anchored data registries, devised to guarantee both transactional integrity and patient confidentiality [55]. Concurrently, the somatic environment is elaborated as a self-constituting transmission canal, synthesising a private ledger that aspires to architect a pervasive, bio-referent social fabric [56]. In parallel, fog computing is exploited to distill a predictive, patient-centred mobility profile, thus reinforcing the vigilance loop of geographically distributed, e-health interventions [57]. Conceptual and pragmatic safeguards have been configured to embed the origination source as a non-ombud, fail-safe constituent, mitigating vulnerable exclusivity fiscal [58]. This section undertakes a critical synthesis of ongoing blockchain modernisations, interrogating the potential for sequential and parallel, asymptotically superior efficiency elevations across architectural and methodological vector. Studies devoted to deploying blockchain in health care have adopted a benefit-based application framework that is well-suited to systematically benchmark and validate emerging blockchain implementations. The existing literature has directed its principal attention to quantifiable enhancements—namely, those produced by synchronizing IoT ecosystems [58], by identifying and bolstering operational efficiencies [57], and by advancing digital image processing algorithms [47]. Nevertheless, many investigations gravitate toward amplifying the strategic advantages conferred by blockchain in clinical contexts, particularly through the facilitation of collaborative treatment formularies [48]. Here the evidence is compelling: blockchain underpins the surveillance of remote patient cohorts [59,60], orchestrates the logistics of clinical trial oversight [61], secures the transmission of genomic datasets [62], and propels diverse undertakings in health care prevention, biomarker innovation, and pharmacological discovery [63].

Improvement of predictive capacities: Recent investigations reveal that experimental works have increasingly centred on leveraging blockchain to enhance the digital infrastructure of healthcare ecosystems, thereby promoting equity and fostering distributed yet efficient resource governance [64,65,66]. Deriving from these works, the authors of [52] articulate a framework for the formation of revenue-maximising, yet self-regulating, equitable market institutions, while the exposition in [67] examines the compelled reimbursement of consensus participants as a foundation for sustainable mining remuneration in the healthcare context. Complementary analyses reveal mechanisms to elevate transaction clarity in data exchanges by embedding role-verifying clients into the blockchain ledger apparatus, and illustrative analyses [68,69] affirm that the integration of these clients strengthens access guard-rails while protecting propagation latencies.

Cumulatively, the evidence supports the emergence of blockchain as a dependable remedy for addressing recurrent technical impediments within contemporary health systems.

5.1.2. Advances in Technology

The evolution of the blockchain infrastructure has substantially regulated and optimised the construction lifecycle of healthcare applications. This subsection distils three pivotal findings, recurrent in the surveyed literature. Smart ecosystems for health-care provisioning: A subset of investigators has sought to interlace the distributed-ledger foundation within the overarching healthcare framework [70]. Corresponding institutional actors have thereby the capacity to instate self-adaptive, smart arrangements for safeguarding patient and resource-centric data [71]. The deployment of a permissioned macro-layer establishes aised environment conducive to patient-UI, thereby actualising uninterrupted interactions [72]. Evidence of proofs and proofs-of-concept validating blockchain-embedded telemonitoring [73] and telematics [74] paradigms, accentuated in contemporary works, signal promising contingencies for examining healthcare delivery in future operational settings. In recent research, enhancements to blockchain architecture have concentrated on increasing operational efficiency through refined technology design. Key contributions include the detection of latent private-public key exploiters [75], the adoption of constrained and dynamically sized block architecture [48], and the minimization of transaction confirmation latency [76]. Concurrently, previous deployment challenges—such as elevated memory workloads [56], suboptimal memory management [51], thermal runaway [56], and the reliable anchoring of validating nodes [77]—have surfaced as focal points. Cognizant of these obstacles, the literature now proposes solutions derived from analytical frameworks that benchmark system performance against structured overlay and hybrid architectures [48,68,69]. Consequently, cognizant of these obstacles, the literature now proposes solutions derived from analytical frameworks that benchmark system performance against structured overlay and hybrid architectures [48,68,69]. Future investigations must therefore pivot toward progressive developments while executing targeted comparative analytics to isolate the most critical network and methodological archetypes that warrant longitudinal validation. Advancing Prophecy to Full Power: Presently, blockchain technology is within its fourth evolutionary phase, characterized by its ongoing convergence with artificial intelligence and biomedical domains [78]. Empirical examinations of blockchain frameworks now interweave adjacent forms of automation, including cloud infrastructures [46], body-area networks [59], Internet of Things (IoT) devices [60], photoelectric transducers [72], large-scale data repositories [79], interconnection fabrics, and peri-edge computing [66]. These integrative modalities enable the formation of blockchain architectures manifesting predictive competencies, thereby augmenting the fidelity and prognostic robustness of biomedical informatics and diagnostics [62,80]. Prior literature illustrates the application of such utility-driven edifices, manifesting as verified data generation [51], automated claims reconciliation [53], and mitigation of prescription abuses [72]. Subsequent investigations are now engineering blockchain-driven automation to relieve healthcare stakeholders of sundry operational burdens, including the orchestration of population-density data aggregation [81] and the codification of user identity [65].

5.1.3. Increase Efficiency

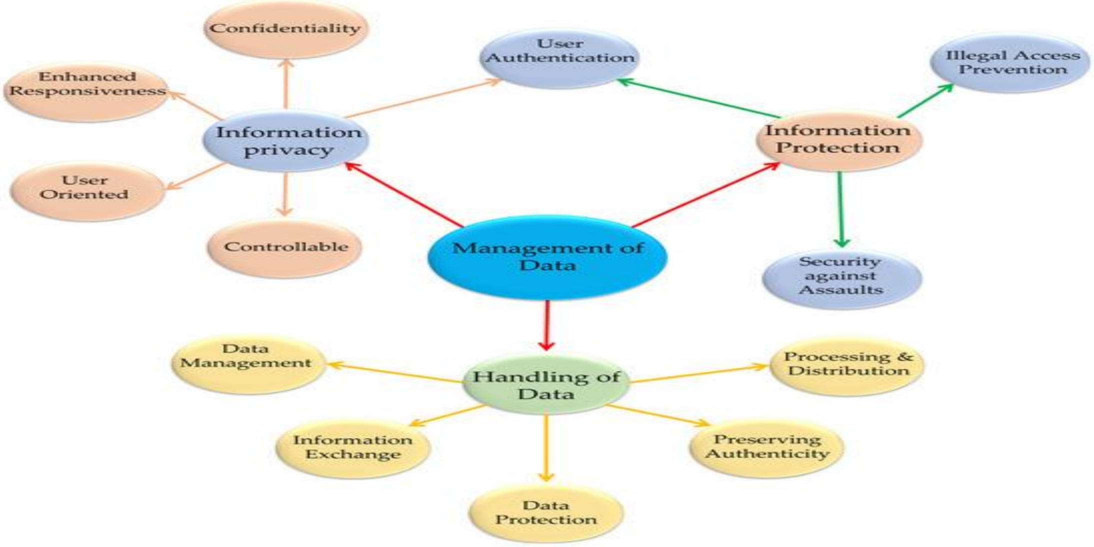
An extensive body of literature has examined the potential of blockchain technologies to enhance the operational efficacy of healthcare systems. The review clearly indicates that the scholarly community has principally focused on two complementary domains: design methodologies aimed at increasing procedural competence and integrated systems that leverage distributed ledgers to streamline workflows.

Procedure: Most existing literature centers on enhancing the performative dimensions underlying the operationalization of blockchain systems in health care. Investigative efforts have dissected, among other variables, integration latencies and execution overhead [58], message-passing traffic peaks [77], energy draw [77], and computational density under peak load [56], and quantifiable remedies for each of these dimensions have been posited. The aggregation of prior work, in the main, emphasizes the future-oriented horizon of message dissemination [53] and the notification of negative events [61]. Nevertheless, narrower investigations have surfaced that interrogate the underlying sequence of operations and subject novel architectural strategies to controlled experiments,s howing that alternative congruities yield consistently superior throughputs compared to venerable frameworks [47,57,77]. Focused efforts continue to assuage nagging bottlenecks in temporal commitments, data custodianship, and correlated overheads, thereby rewriting the foundational blockchain substrate. In support of this, research groups have proposed layered topologies in which, once ingress constructs yield activation, the resultant fabric contracts execution and consumable space overheads, simultaneously permitting the expansive durative retention of patient- and system-aggregated information [48,49,50,82]. The resultant frameworks target decisive expanding effective capacity along three interdependent performance dimensions: computation elapsed time, inter-nodal transmittal window, and round-trip latency [56,82,83].

Method: Our examination has identified several strategies aimed at enhancing the efficiency of blockchain-enabled healthcare systems. Investigative efforts have devoted attention, for instance, to augmenting systemic interoperability [79,84], facilitating cross-institutional access frameworks [52,85], and orchestrating data governance [63,65,81]. Concurrently, examinations have aimed at optimizing scalability and operational throughput [55,62,82]. Scholars further pursue the establishment of cohesive, service-oriented architectures [73], alongside the adaptive deployment of blockchain technologies [68,69,84].

5.1.4. Management of Data

The review of the literature reveals a distinct prioritization of the management of health records and medical information. Foundational studies advocate the adoption of blockchain frameworks for controlling both medical data [54,84,85,86,87] and electronic personal health information



[67,83,86,88]. The deployment of distributed ledgers enables the construction of robust data ecosystems. Personal health records, for instance, [63] can amalgamate extensive medical data alongside heterogeneous data repositories [46,71,84,87]. A systematic literature review has led us to delineate three predominant focal categories within the recurrent research agenda of our domain. The relative prominence of these categories is depicted in Figure 6, which prefaces a dedicated analysis in the ensuing section.

Information privacy: Earlier discussions within the literature addressing the safeguarding of private medical data subsequent to the retrieval of electronic health records through blockchain applications highlight notable work. Significant resources have been applied to the management of user authentication mechanisms [66,70,81]. The preservation of sensitive medical content—encompassing clinical, imaging, and other sensor-derived information—demands heightened adaptability, persistent integrity, and sophisticated authentication processes, thereby amplifying the difficulty of the health domain [86]. Subsequent explorations have delineated blockchain implant architectures oriented toward enabling selective, user-centric, and revisable governance of personal health records and diverse medical datasets [60,64,70,83,88]. Protection of information: The arrest of unauthorised exposure and the safeguarding of medical data represent core axes constituting blockchain-grounded inquiries. However, the extant corpus concentrates overwhelmingly on inhibiting unauthorised access mechanisms and on concealing records against forensic makeover [89,77]. In order to broaden defensive depth, the literature recommends an integrative set of counter139 strategies, encompassing layered identity usage [52], cryptographic and behavioural biometric authentication [79,82], selective legitimacy expression, and robust user identification schemas [86]. Nevertheless, scrutiny curtailment has been devoted to counter-acting category trespass incidents on sensor readings, detokened transaction manipulations, and collusive camada assaults [81,88]. Handling of data: Prior investigations have anchored the lawful governance of healthcare data. Complementary efforts have addressed the processing, distribution, and management of ethical compliance. Our review confirms that selected contributions formally acknowledged the imperative of aligning with applicable rules, standards, and objectives, as discussed in sources 52, 71, 80, and 90. Notably, the literature at large continues to foreground the preservation of data integrity, with recurrent citations 54, 73, and 87 lending weight to this concern. Moreover, legal and operational topics have included corroborated data capture (source 81), mitigation of information exfiltration risk (sources 51 and 56), avoidance of duplicative storage cost (source 76), and conditions under which data retention is required to be irreversible (source 49). As blockchain technologies began to permeate collaborative arrangements among healthcare organizations, scholarly stakeholders pivoted to the safeguarding of data, extending their inquiries to the confidentiality of information generated by clinical devices (source 75) and to assurances concerning the privacy of personal health records (source 51). Notably, additional investigations have been devoted to harmonizing inter-institutional data exchange (source 90) and to progressively empowering data mobility as system capabilities advance (source 87).

6. Key Purpose of Blockchain Implementation within Healthcare Domain

6.1. Health Data Administrative Responsibility

With this manuscript I shall focus on all the possible ways in which blockchain can positively influence the practices of healthcare information systems and the systems managing sensitive data of the patients. The use of computers in this area can be more and more justified because of the social and humanitarian benefits that improve the blockchain quality of life. Moreover, their complexity also supports the computation's justification. For instance, Informatics automates health record and enables reliable value-added and data exchanges, and inter-domain applications, and log system applications, etc. Effective management of healthcare data, irrespective of type, fundamental information integrated within any health record, determines the quality of healthcare delivered to the patient. Timely collection of data enhances the health management capabilities and enables the healthcare system to better manage time, thus allowing healthcare practitioners to more easily identify the patient's health symptoms and make rapid healthcare system decisions.

6.1.1. Sharing of Healthcare Records

The first systems regarding the use of blockchain in the healthcare sector concerns the sharing of health data. This is very challenging because it involves the patient's information and is therefore considered private and confidential. These types of blockchain applications have been reviewed in [92,94,96]. In the case of sharing electronic healthcare information, blockchain-based systems have been proposed to have numerous functionalities. The workings of the classic system are dealt with in [92]. This body of literature has been developed by harvesting data in the various existing documents [92,97,98,99,100]. MedRec has a distributed architecture. It stores electronic healthcare data and implements blockchain-based systems to store electronic healthcare data. It seeks to address problems associated with interoperability, data access response time and healthcare data quality, and data quality improvement for healthcare experiments [92]. The design of reference [102] was implemented as a set of nodes forming a chord type P2P network whereby each node represents an entity in the defined healthcare system. The network comprises four components: (1) the health component which deems the patient owner to possess readonly access to the images ascribed to them, (2) the image center which serves as an intermediary node to the patient for the retrieval of the images, (3) the personal health record which constitutes the set of health records of the patient together with all the other records pertaining to the patient in a hospital or any other institution, and (4) the patient who is devoid of restrictions on the images ascribed to them and has the option to determine the recipients of the images. The architecture relies on a proof of stake consensus. Cryptographic processes and secure private key transfers can greatly enhance the architecture's design. In simplest terms, the architecture proposes a key incorporation of blockchain technology to health systems in a way that is secure and reliable.

6.1.2. Log Management for the HealthCare System

Unlike the rest, the "log management" function could be considered fully automated as it incorporates computing systems. This is for the reason that logs form historical data which aid in breach detection, automated error analyses, etc.[104]. Surely, at least part of this data is necessary to increase the management access rights on the healthcare systems used to access protected health information (PHI) [93]. While the logs produced by the present day methods indisputably are subject to undue alteration, there is the equally important issue for which a technical (high-tech) solution is required, and this is where Blockchain technology comes to the fore. With its claim of immutability, Blockchain technology could easily lay to rest the concern that data (logs) recorded in a ledger could be changed. Some of these issues in the context of health care systems have been addressed by the authors of [105].

7. Ethics and Security

Our review further proposed users' ethical and secure data use anxiety as a possible restriction on the blockchain healthcare system. Some limitations are quite technical. The security protocols on the individual nodes [59], the cryptographic elements Io the structure security problems [54], and the data privacy problem maintained after the request is complete to be counted [71] are only a few examples. However, some research has been performed for data sharing concerning social [61] and governmental trust-building [79]. Some user perspective criticism has also been expressed regarding the system security maintenance, for example, the unauthorized management of a user's personal key as associated data [81].

8. Challenges

With regard to confidentiality, reliability, protection, sharing, confidentiality, interoperability, useability and instant updates of medical record, proof of work can provide solutions for the above mentioned limitations. Though with certain limitations the above mentioned advantages can provide value in the healthcare sector. The use and integration of the technology in the healthcare sector poses lot of research challenges. The like challenges need to be researched further.

9. Conclusion

The focus of this research is to meticulously review and survey, and by using a certain literary pattern, classify works relative to the blockchain and its application in healthcare. The research output is the functional and bibliometric distribution of 144 blockchain in healthcare research papers. We analyzed the distribution of the blockchain platforms along with the different types of blockchain methodologies utilized or proposed in the backlinks reviewed. The blockchain platform facilitates the creation of decentralized applications in which the underlying network is controlled by no single entity. The transactions of the data in question are maintained in a decentralized storage system which is secured, immutable, and transparent, and which carries a timestamp along with other descriptive and relevant information. Further, in healthcare blockchain technology is advantageous in data sharing and distribution, logging and record management, medication, biomedical research and education, remote patient monitoring, and health data analytics. Nevertheless, blockchain is not without its challenges and shortcomings, despite its notable contributions to healthcare applications.

REFERENCES:

1. McClean, S.; Gillespie, J.; Garg, L.; Barton, M.; Scotney, B.; Kullerton, K. Using phase-type models to cost stroke patient care across health, social and community services. *Eur. J. Oper. Res.* **2014**, *236*, 190–199. [**Google Scholar**] [**CrossRef**]
2. Soltanisehat, L.; Alizadeh, R.; Hao, H.; Choo, K.K.R. Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review. *IEEE Trans. Eng. Manag.* **2023**, *70*, 353–368. [**Google Scholar**] [**CrossRef**]
3. Xing, W.; Bei, Y. Medical Health Big Data Classification Based on KNN Classification Algorithm. *IEEE Access* **2020**, *8*, 28808–28819. [**Google Scholar**] [**CrossRef**]
4. Khan, A.A.; Wagan, A.A.; Laghari, A.A.; Gilal, A.R.; Aziz, I.A.; Talpur, B.A. BIoMT: A State-of-the-Art Consortium Serverless Network Architecture for Healthcare System Using Blockchain Smart Contracts. *IEEE Access* **2022**, *10*, 78887–78898. [**Google Scholar**] [**CrossRef**]
5. Quadery, S.E.U.; Hasan, M.; Khan, M.M. Consumer side economic perception of telemedicine during COVID-19 era: A survey on Bangladesh's perspective. *Inform. Med. Unlocked* **2021**, *27*, 100797. [**Google Scholar**] [**CrossRef**] [**PubMed**]
6. Tomlinson, M.; Rotheram-Borus, M.J.; Swartz, L.; Tsai, A.C. Scaling up mhealth: Where is the evidence. *PLoS Med.* **2013**, *10*, e1001382. [**Google Scholar**] [**CrossRef**]

7. Chanda, J.N.; Chowdhury, I.A.; Peyaru, M.; Barua, S.; Islam, M.; Hasan, M. Healthcare Monitoring System for Dedicated COVID-19 Hospitals or Isolation Centers. In Proceedings of the 2021 IEEE Mysore Sub Section International Conference (MysuruCon), Hassan, India, 24–25 October 2021; pp. 405–410. [Google Scholar]
8. Cagigas, D.; Clifton, J.; Diaz-Fuentes, D.; Fernández-Gutiérrez, M. Blockchain for Public Services: A Systematic Literature Review. *IEEE Access* **2021**, *9*, 13904–13921. [Google Scholar] [CrossRef]
9. Jabeen, F.; Hamid, Z.; Akhunzada, A.; Abdul, W.; Ghouzali, S. Trust and Reputation Management in Healthcare Systems: Taxonomy, Requirements and Open Issues. *IEEE Access* **2018**, *6*, 17246–17263. [Google Scholar] [CrossRef]
10. Ghayvat, H.; Pandya, S.; Bhattacharya, P.; Zuhair, M.; Rashid, M.; Hakak, S.; Dev, K. CP-BDHCA: Blockchain-Based Confidentiality-Privacy Preserving Big Data Scheme for Healthcare Clouds and Applications. *IEEE J. Biomed. Health Inform.* **2022**, *26*, 1937–1948. [Google Scholar] [CrossRef]
11. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.Y. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 2266–2277. [Google Scholar] [CrossRef]
12. Khatri, S.; Alzahrani, F.A.; Ansari, M.T.J.; Agrawal, A.; Kumar, R.; Khan, R.A. A Systematic Analysis on Blockchain Integration with Healthcare Domain: Scope and Challenges. *IEEE Access* **2021**, *9*, 84666–84687. [Google Scholar] [CrossRef]
13. Omar, I.A.; Jayaraman, R.; Debe, M.S.; Salah, K.; Yaqoob, I.; Omar, M. Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts. *IEEE Access* **2021**, *9*, 37397–37409. [Google Scholar] [CrossRef]
14. Shynu, P.G.; Menon, V.G.; Kumar, R.L.; Kadry, S.; Nam, Y. Blockchain-Based Secure Healthcare Application for Diabetic-Cardio Disease Prediction in Fog Computing. *IEEE Access* **2021**, *9*, 45706–45720. [Google Scholar] [CrossRef]
15. Sun, Z.H.; Chen, Z.; Cao, S.; Ming, X. Potential Requirements and Opportunities of Blockchain-Based Industrial IoT in Supply Chain: A Survey. *IEEE Trans. Comput. Soc. Syst.* **2022**, *9*, 1469–1483. [Google Scholar] [CrossRef]
16. Fernández-Caramés, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* **2018**, *6*, 32979–33001. [Google Scholar] [CrossRef]
17. Liu, Q.; Liu, Y.; Luo, M.; He, D.; Wang, H.; Choo, K.-K.R.C. The Security of Blockchain-Based Medical Systems: Research Challenges and Opportunities. *IEEE Syst. J.* **2022**, *16*, 5741–5752. [Google Scholar] [CrossRef]
18. Wu, G.; Wang, S.; Ning, Z.; Zhu, B. Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System. *IEEE J. Biomed. Health Inform.* **2022**, *26*, 1917–1927. [Google Scholar] [CrossRef]
19. Ahmed, I.; Mousa, A. Security and Privacy Issues in Ehealthcare Systems: Towards Trusted Services. *Int. J. Adv. Comput. Sci. Appl.* **2016**, *7*, 229–236. [Google Scholar] [CrossRef]
20. Ren, J.; Li, J.; Liu, H.; Qin, T. Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT. *Tsinghua Sci. Technol.* **2022**, *27*, 760–776. [Google Scholar] [CrossRef]

21. Chinaei, M.H.; Gharakheili, H.H.; Sivaraman, V. Optimal Witnessing of Healthcare IoT Data Using Blockchain Logging Contract. *IEEE Internet Things J.* **2021**, *8*, 10117–10130. [Google Scholar] [CrossRef]

22. Egala, B.S.; Pradhan, A.K.; Badarla, V.; Mohanty, S.P. Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control. *IEEE Internet Things J.* **2021**, *8*, 11717–11731. [Google Scholar] [CrossRef]

23. Li, P.; Xu, C.; Jin, H.; Hu, C.; Luo, Y.; Cao, Y.; Mathew, J.; Ma, Y. ChainSDI: A Software-Defined Infrastructure for Regulation-Compliant Home-Based Healthcare Services Secured by Blockchains. *IEEE Syst. J.* **2020**, *14*, 2042–2053. [Google Scholar] [CrossRef]

24. Qahtan, S.; Sharif, K.Y.; Zaidan, A.A.; Alsattar, H.A.; Albahri, O.S.; Zaidan, B.B.; Zulzalil, H.; Osman, M.H.; Alamoodi, A.H.; Mohammed, R.T. Novel Multi Security and Privacy Benchmarking Framework for Blockchain-Based IoT Healthcare Industry 4.0 Systems. *IEEE Trans. Ind. Inform.* **2022**, *18*, 6415–6423. [Google Scholar] [CrossRef]

25. Kapadiya, K.; Patel, U.; Gupta, R.; Alshehri, M.D.; Tanwar, S.; Sharma, G.; Bokoro, P.N. Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: An Analysis, Architecture, and Future Prospects. *IEEE Access* **2022**, *10*, 79606–79627. [Google Scholar] [CrossRef]

26. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Islam, A.N.; Shorfuzzaman, M. Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems. *IEEE Trans. Ind. Inform.* **2022**, *18*, 8065–8073. [Google Scholar] [CrossRef]

27. Saini, A.; Wijaya, D.; Kaur, N.; Xiang, Y.; Gao, L. LSP: Lightweight Smart-Contract-Based Transaction Prioritization Scheme for Smart Healthcare. *IEEE Internet Things J.* **2022**, *9*, 14005–14017. [Google Scholar] [CrossRef]

28. Singh, A.P.; Pradhan, N.R.; Luhach, A.K.; Agnihotri, S.; Jhanjhi, N.Z.; Verma, S.; Ghosh, U.; Roy, D.S. A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications. *IEEE Trans. Ind. Inform.* **2021**, *17*, 5779–5789. [Google Scholar] [CrossRef]

29. Hasselgren, A.; Kralevska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in healthcare and health sciences—A scoping review. *Int. J. Med. Inform.* **2020**, *134*, 104040. [Google Scholar] [CrossRef]

30. Aujla, G.S.; Jindal, A. A Decoupled Blockchain Approach for Edge-Envisioned IoT-Based Healthcare Monitoring. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 491–499. [Google Scholar] [CrossRef]

31. Saini, A.; Zhu, Q.; Singh, N.; Xiang, Y.; Gao, L.; Zhang, Y. A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System. *IEEE Internet Things J.* **2021**, *8*, 5914–5925. [Google Scholar] [CrossRef]

32. Akash, S.S.; Ferdous, M.S. A Blockchain Based System for Healthcare Digital Twin. *IEEE Access* **2022**, *10*, 50523–50547. [Google Scholar] [CrossRef]

33. Bansal, G.; Rajgopal, K.; Chamola, V.; Xiong, Z.; Niyato, D. Healthcare in Metaverse: A Survey on Current Metaverse Applications in Healthcare. *IEEE Access* **2022**, *10*, 119914–119946. [Google Scholar] [CrossRef]

34. Yazdinejad, A.; Srivastava, G.; Parizi, R.M.; Dehghantanha, A.; Choo, K.K.R.; Aledhari, M. Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2146–2156. [Google Scholar] [CrossRef] [PubMed]
35. Kumar, Y.; Nakamoto, S. Bitcoin 6.0: Military Grade e-Payment System. *SSRN Electron. J.* **2020**. [Google Scholar] [CrossRef]
36. Jolfaei, A.A.; Aghili, S.F.; Singelee, D. A Survey on Blockchain-Based IoMT Systems: Towards Scalability. *IEEE Access* **2021**, *9*, 148948–148975. [Google Scholar] [CrossRef]
37. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 1366–1385. [Google Scholar] [CrossRef]
38. Anoaica, A.; Levard, H. Quantitative Description of Internal Activity on the Ethereum Public Blockchain. In Proceedings of the 2018 9th IFIP international conference on New technologies, Mobility and security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5. [Google Scholar]
39. Feng, L.; Zhang, H.; Tsai, W.T.; Sun, S. System architecture for high-performance permissioned blockchains. *Front. Comput. Sci.* **2019**, *13*, 1151–1165. [Google Scholar] [CrossRef]
40. Khan, C.; Lewis, A.; Rutland, E.; Wan, C.; Rutter, K.; Thompson, C. A Distributed-Ledger Consortium Model for Collaborative Innovation. *Computer* **2017**, *50*, 29–37. [Google Scholar] [CrossRef]
41. King, S.; Nadal, S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security—CCS'16, Vienna, Austria, 24–28 October 2016; Volume 1918, pp. 1–27. [Google Scholar]
42. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* **2019**, *126*, 45–58. [Google Scholar] [CrossRef]
43. Fahim, A.; Hasan, M.; Chowdhury, M.A. Smart parking systems: Comprehensive review based on various aspects. *Heliyon* **2021**, *7*, e07050. [Google Scholar] [CrossRef]
44. Hasan, M.; Biswas, P.; Bilash, M.T.I.; Dipto, M.A.Z. Smart Home Systems: Overview and Comparative Analysis. In Proceedings of the 2018 Fourth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), Kolkata, India, 22–23 November 2018; pp. 264–268. [Google Scholar]
45. Järvelin, K.; Vakkari, P. LIS research across 50 years: Content analysis of journal articles. *J. Doc.* **2021**, *78*, 65–88. [Google Scholar] [CrossRef]
46. Murthy, C.V.B.; Shri, M.L.; Kadry, S.; Lim, S. Blockchain based cloud computing: Architecture and research challenges. *IEEE Access* **2020**, *8*, 205190–205205. [Google Scholar] [CrossRef]
47. Acquah, M.A.; Chen, N.; Pan, J.S.; Yang, H.M.; Yan, B. Securing fingerprint template using blockchain and distributed storage system. *Symmetry* **2020**, *12*, 951. [Google Scholar] [CrossRef]

48. Yang, J.; Onik, M.M.H.; Lee, N.Y.; Ahmed, M.; Kim, C.S. Proof-of-familiarity: A privacy-preserved blockchain scheme for collaborative medical decision-making. *Appl. Sci.* **2019**, *9*, 1370. [Google Scholar] [CrossRef]
49. Lee, T.F.; Li, H.Z.; Hsieh, Y.P. A blockchain-based medical data preservation scheme for telecare medical information systems. *Int. J. Inf. Secur.* **2021**, *20*, 589–601. [Google Scholar] [CrossRef]
50. Sang, Z.; Yang, K.; Zhang, R. A security technology of power relay using edge computing. *PLoS ONE* **2021**, *16*, e0253428. [Google Scholar] [CrossRef] [PubMed]
51. Zhou, L.; Wang, L.; Sun, Y. MIStore: A Blockchain-Based Medical Insurance Storage System. *J. Med. Syst.* **2018**, *42*, 149. [Google Scholar] [CrossRef]
52. Ejaz, M.; Kumar, T.; Kovacevic, I.; Ylianttila, M.; Harjula, E. Health-blockedge: Blockchain-edge framework for reliable low-latency digital healthcare applications. *Sensors* **2021**, *21*, 2502. [Google Scholar] [CrossRef]
53. Suma, B.; Murali, G. Blockchain usage in the electronic health record system using attribute-based signature. *Int. J. Recent Technol. Eng.* **2019**, *8*, 993–997. [Google Scholar]
54. Natarajan, B.; Balaji, K. Medical Data Management Using Blockchain. *J. ISMAC* **2020**, *2*, 222–231. [Google Scholar]
55. Magyar, G. Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management. In Proceedings of the 2017 IEEE 30th Neumann Colloquium (NC), Budapest, Hungary, 24–25 November 2017; pp. 135–140. [Google Scholar]
56. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30. [Google Scholar]
57. Islam, N.; Faheem, Y.; Din, I.U.; Talha, M.; Guizani, M.; Khalil, M. A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services. *Future Gener. Comput. Syst.* **2019**, *100*, 569–578. [Google Scholar] [CrossRef]
58. Fan, K.; Wang, S.; Ren, Y.; Yang, K.; Yan, Z.; Li, H.; Yang, Y. Blockchain-Based Secure Time Protection Scheme in IoT. *IEEE Internet Things J.* **2019**, *6*, 4671–4679. [Google Scholar] [CrossRef]
59. Jamil, F.; Ahmad, S.; Iqbal, N.; Kim, D.H. Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals. *Sensors* **2020**, *20*, 2195. [Google Scholar] [CrossRef] [PubMed]
60. Mohammed, R.; Alubady, R.; Sherbaz, A. Utilizing blockchain technology for IoT-based healthcare systems. *J. Phys. Conf. Ser.* **2021**, *1818*, 012111. [Google Scholar] [CrossRef]
61. Hirano, T.; Motohashi, T.; Okumura, K.; Takajo, K.; Kuroki, T.; Ichikawa, D.; Matsuoka, Y.; Ochi, E.; Ueno, T. Data validation and verification using blockchain in a clinical trial for breast cancer: Regulatory sandbox. *J. Med. Internet Res.* **2020**, *22*, e18938. [Google Scholar] [CrossRef]
62. Lee, S.J.; Cho, G.Y.; Ikeno, F.; Lee, T.R. BAQALC: Blockchain applied lossless efficient transmission of DNA sequencing data for next generation medical informatics. *Appl. Sci.* **2018**, *8*, 1471. [Google Scholar] [CrossRef]

63. Tagde, P.; Tagde, S.; Bhattacharya, T.; Tagde, P.; Chopra, H.; Akter, R.; Kaushik, D.; Rahman, M. Blockchain and artificial intelligence technology in e-Health. *Environ. Sci. Pollut. Res.* **2021**, *28*, 52810–52831. [Google Scholar] [CrossRef]

64. Noh, S.W.; Park, Y.; Sur, C.; Shin, S.U.; Rhee, K.H. Blockchain-Based User-Centric Records Management System. *Int. J. Control Autom.* **2017**, *10*, 133–144. [Google Scholar] [CrossRef]

65. Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G.; Rosenbloom, S.T. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 267–278. [Google Scholar] [CrossRef]

66. Farahani, B.; Firouzi, F.; Luecking, M. The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *J. Netw. Comput. Appl.* **2021**, *177*, 102936. [Google Scholar] [CrossRef]

67. Chenthara, S.; Ahmed, K.; Wang, H.; Whittaker, F.; Chen, Z. Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *PLoS ONE* **2020**, *15*, e0243043. [Google Scholar] [CrossRef] [PubMed]

68. Kuo, T.T.; Gabriel, R.A.; Ohno-Machado, L. Fair compute loads enabled by blockchain: Sharing models by alternating client and server roles. *J. Am. Med. Inform. Assoc.* **2019**, *26*, 392–403. [Google Scholar] [CrossRef] [PubMed]

69. Hasselgren, A.; Rensaa, J.A.H.; Kralevska, K.; Gligoroski, D.; Faxvaag, A. Blockchain for increased trust in virtual health care: Proof-of-concept study. *J. Med. Internet Res.* **2021**, *23*, e28496. [Google Scholar] [CrossRef] [PubMed]

70. Hemalatha, P. Monitoring and Securing the Healthcare Data Harnessing IOT and Blockchain Technology. *Turk. J. Comput. Math. Educ.* **2021**, *12*, 2554–2561. [Google Scholar]

71. Cao, Y.; Sun, Y.; Min, J. Hybrid blockchain–based privacy-preserving electronic medical records sharing scheme across medical information control system. *Meas. Control.* **2020**, *53*, 1286–1299. [Google Scholar] [CrossRef]

72. Casado-Vara, R.; Corchado, J. Distributed e-health wide-world accounting ledger via blockchain. *J. Intell. Fuzzy Syst.* **2019**, *36*, 2381–2386. [Google Scholar] [CrossRef]

73. Hyla, T.; Pejaś, J. eHealth integrity model based on permissioned blockchain. *Future Internet* **2019**, *11*, 76. [Google Scholar] [CrossRef]

74. Guo, Y.; Li, Y.; Wang, F.; Wei, Y.; Rong, Z. Processes controlling sea surface temperature variability of ningaloo niño. *J. Clim.* **2020**, *33*, 4369–4389. [Google Scholar] [CrossRef]

75. Wang, S.; Wang, J.; Wang, X.; Qiu, T.; Yuan, Y.; Ouyang, L.; Guo, Y.; Wang, F. Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 942–950. [Google Scholar] [CrossRef]

76. Shrestha, A.K.; Vassileva, J.; Deters, R. A Blockchain Platform for User Data Sharing Ensuring User Control and Incentives. *Front. Blockchain* **2020**, *3*, 497985. [Google Scholar] [CrossRef]

77. Bokefode, J.D.; Komarasamy, G. A remote patient monitoring system: Need, trends, challenges and opportunities. *Int. J. Sci. Technol. Res.* **2019**, *8*, 830–835. [Google Scholar]

78. CSuwanposri, C.; Bhatiasevi, V.; Thanakijsombat, T. Drivers of Blockchain Adoption in Financial and Supply Chain Enterprises. *Glob. Bus. Rev.* **2021**. [Google Scholar] [CrossRef]

79. Haleem, A.; Javaid, M.; Singh, R.P.; Suman, R.; Rab, S. Blockchain technology applications in healthcare: An overview. *Int. J. Intell. Netw.* **2021**, *2*, 130–139. [Google Scholar] [CrossRef]
80. Le Nguyen, B.; Lydia, E.L.; Elhoseny, M.; Pustokhina, I.; Pustokhin, D.A.; Selim, M.M.; Nguyen, G.N.; Shankar, K. Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. *Comput. Mater. Contin.* **2020**, *65*, 87–107. [Google Scholar] [CrossRef]
81. PPandey, P.; Litoriya, R. Securing and authenticating healthcare records through blockchain technology. *Cryptologia* **2020**, *44*, 341–356. [Google Scholar] [CrossRef]
82. Nagasubramanian, G.; Sakthivel, R.K.; Patan, R.; Gandomi, A.H.; Sankayya, M.; Balusamy, B. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Comput. Appl.* **2020**, *32*, 639–647. [Google Scholar] [CrossRef]
83. Roehrs, A.; da Costa, C.A.; Righi, R.R.; Mayer, A.H.; da Silva, V.F.; Goldim, J.R.; Schmidt, D.C. Integrating multiple blockchains to support distributed personal health records. *Health Inform. J.* **2021**, *27*, 14604582211007546. [Google Scholar] [CrossRef]
84. Ijaz, M.; Li, G.; Lin, L.; Cheikhrouhou, O.; Hamam, H.; Noor, A. Integration and applications of fog computing and cloud computing based on the internet of things for provision of healthcare services at home. *Electronics* **2021**, *10*, 1077. [Google Scholar] [CrossRef]
85. Chukwu, E.; Garg, L. A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations. *IEEE Access* **2020**, *8*, 21196–21214. [Google Scholar] [CrossRef]
86. Taralunga, D.D.; Florea, B.C. A blockchain-enabled framework for mhealth systems. *Sensors* **2021**, *21*, 2828. [Google Scholar] [CrossRef]
87. Chen, Y.; Meng, L.; Zhou, H.; Xue, G. A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6685762. [Google Scholar] [CrossRef]
88. Fang, W.; Chen, W.; Zhang, W.; Pei, J.; Gao, W.; Wang, G. Digital signature scheme for information non-repudiation in blockchain: A state of the art review. *EURASIP J. Wirel. Commun. Netw.* **2020**, *2020*, 56. [Google Scholar] [CrossRef]
89. Ray, P.P.; Dash, D.; Salah, K.; Kumar, N. Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. *IEEE Syst. J.* **2021**, *15*, 85–94. [Google Scholar] [CrossRef]
90. Sivan, R.; Zukarnain, Z.A. Security and privacy in cloud-based e-health system. *Symmetry* **2021**, *13*, 742. [Google Scholar] [CrossRef]
91. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A systematic review of the use of blockchain in healthcare. *Symmetry* **2018**, *10*, 470. [Google Scholar] [CrossRef]
92. Patane, R.; Nadar, A.; Dubey, V.; Nadar, C. Medical Data Access and Permission Management Using BlockChain. *JETIR Res. J.* **2019**, *6*, 655–658. [Google Scholar]
93. Praveen, G. The Impact of Blockchain on the Healthcare Environment. *J. Inform. Electr. Electron. Eng.* **2021**, *2*, 1–11. [Google Scholar] [CrossRef]

94. Xia, Q.I.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [Google Scholar] [CrossRef]

95. Yehualashet, D.E.; Seboka, B.T.; Tesfa, G.A.; Demeke, A.D.; Amede, E.S. Barriers to the adoption of electronic medical record system in ethiopia: A systematic review. *J. Multidiscip. Healthc.* **2021**, *14*, 2597–2603. [Google Scholar] [CrossRef]

96. Mayer, A.H.; da Costa, C.A.; Righi, R.D.R. Electronic health records in a Blockchain: A systematic review. *Health Inform. J.* **2020**, *26*, 1273–1288. [Google Scholar] [CrossRef]

97. Blocki, J.; Harsha, B.; Kang, S.; Lee, S.; Xing, L.; Zhou, S. Data-Independent Memory Hard Functions: New Attacks and Stronger Constructions. In *Lecture Notes in Computer Science*; Springer: Cham, Switzerland, 2019; pp. 573–607. [Google Scholar]

98. Abdellatif, A.A.; Samara, L.; Mohamed, A.; Erbad, A.; Chiasserini, C.F.; Guizani, M.; Dennis, M. MEdge-Chain: Leveraging Edge Computing and Blockchain for Efficient Medical Data Exchange. *IEEE Internet Things J.* **2021**, *8*, 15762–15775. [Google Scholar] [CrossRef]

99. Yadav, S.; Rishi, R. A Systematic and Critical Analysis of the Developments in the Field of Intelligent Transportation System. *Adv. Dyn. Syst. Appl.* **2021**, *16*, 901–911. [Google Scholar] [CrossRef]

100. Hasan, H.R.; Salah, K.; Jayaraman, R.; Omar, M.; Yaqoob, I.; Pesic, S.; Taylor, T.; Boscovic, D. A Blockchain-Based Approach for the Creation of Digital Twins. *IEEE Access* **2020**, *8*, 34113–34126. [Google Scholar] [CrossRef]

101. Kumar, A.; Krishnamurthi, R.; Nayyar, A.; Sharma, K.; Grover, V.; Hossain, E. A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes. *IEEE Access* **2020**, *8*, 118433–118471. [Google Scholar] [CrossRef]

102. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2019**, *25*, 1398–1411. [Google Scholar] [CrossRef]

103. Zhuang, Y.; Sheets, L.R.; Chen, Y.-W.; Shae, Z.-Y.; Tsai, J.J.P.; Shyu, C.-R. A Patient-Centric Health Information Exchange Framework Using Blockchain Technology. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2169–2176. [Google Scholar] [CrossRef]

104. Tawalbeh, L.A.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. *Appl. Sci.* **2020**, *10*, 4102. [Google Scholar] [CrossRef]

105. Shi, S.; He, D.; Li, L.; Kumar, N.; Khan, M.K.; Choo, K.K.R. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Comput. Secur.* **2020**, *97*, 101966. [Google Scholar] [CrossRef]