frontiers | Frontiers in Blockchain

TYPE Systematic Review
PUBLISHED 27 October 2025
DOI 10.3389/fbloc.2025.1699290

OPEN ACCESS

EDITED BY
Yang Lu,
Beijing Technology and Business University, China

REVIEWED BY
Lei Yang,
Shenyang University of Technology, China
Fengyi Wang,
Beijing Technology and Business University, China

*CORRESPONDENCE
Yisong Chen,
yisongchen97@gmail.com

RECEIVED 04 September 2025
ACCEPTED 12 September 2025
PUBLISHED 27 October 2025

CITATION
Chen Y, Zhao C and Gao Y (2025) Blockchain applications in health insurance: a review of applications, challenges, and prospects. *Front. Blockchain* 8:1699290. doi: 10.3389/fbloc.2025.1699290

Blockchain applications in health insurance: a review of applications, challenges, and prospects

Yisong Chen[1]*, Chuqing Zhao[2] and Yifan Gao[3]

[1]College of Computing, Georgia Institute of Technology, Atlanta, GA, United States, [2]School of Engineering and Applied Sciences, Harvard University, Cambridge, MA, United States, [3]Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX, United States

Introduction: This systematic review comprehensively examines the application of blockchain in health insurance, highlighting the current state of research, inherent challenges, and future trends. Blockchains have demonstrated excellent potential in health insurance, especially in fraud prevention, claims processing, and data security. Moreover, this study also aims to identify several critical challenges that hinder their broader adoption and effectiveness, including data heterogeneity, individual task requirements, scalability and regulatory alignment.
Methods: System Review
Results and Discussion: Through comprehensive analysis, this study discusses some actionable solutions and strategies. Conclusively, this review underscores blockchain's transformative impact on building a secure, efficient, and patient-centric health insurance system.

KEYWORDS

blockchain, health insurance, fraud detection, claims processing, data security, automation, interoperability, smart contracts

1 Introduction

Effective coordination among patients, healthcare providers, and insurers remains a cornerstone of the health insurance industry, yet the sector continues to face persistent operational bottlenecks. Claims submission, adjudication, and payment are often slowed by fragmented data systems, duplicated records, and fraud risks, contributing to high administrative costs and delayed reimbursements (He et al., 2023; Omoseebi et al., 2023). Fraud alone has been estimated to cost global healthcare systems billions annually, placing financial strain on insurers and indirectly burdening patients with higher premiums. Moreover, compliance with regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) adds further complexity to ensuring secure and transparent data management. These challenges underscore the urgent need for innovative solutions that balance efficiency, fraud prevention, and patient-centric care.

Blockchain technology has emerged as a promising response to these challenges. Its decentralized, immutable, and tamper-proof architecture enhances trust and transparency by eliminating reliance on centralized intermediaries and enabling secure, consensus-driven validation of transactions. Within the health insurance domain, blockchain supports a range of applications, including fraud detection, secure claims management, and interoperable health data exchange (Abdelhamid et al., 2024; Arbabi et al., 2023; Singh

et al., 2023). Key innovations such as smart contracts can automate claims adjudication and payments, reducing human error, administrative delays, and disputes between stakeholders. Furthermore, when integrated with complementary technologies like artificial intelligence (AI) and the Internet of Things (IoT), blockchain can enable real-time fraud analytics, continuous patient monitoring, and data-driven decision-making, thereby advancing the efficiency and resilience of insurance systems.

Despite these advantages, significant barriers hinder widespread adoption. Technical issues such as scalability, latency, and energy efficiency remain unresolved in many blockchain implementations, while interoperability with legacy systems poses integration difficulties (Kasyapa and Vanmathi, 2024; Atadoga et al., 2024). Additionally, regulatory alignment and compliance introduce uncertainty, as existing laws often lag behind emerging blockchain applications in healthcare. Overcoming these barriers will require not only technological innovation but also collaboration among policymakers, industry leaders, and healthcare stakeholders to create standardized frameworks and sustainable models of adoption.

While several surveys have reviewed blockchain in healthcare broadly (Abdelhamid et al., 2024; de Aguiar et al., 2020; Arbabi et al., 2023), they often treat health insurance only peripherally, overlooking domain-specific challenges such as claims adjudication, regulatory compliance, and fraud prevention. Moreover, few prior works adopt a systematic PRISMA methodology, and many fail to differentiate between theoretical proposals and real-world implementations, which limits practical applicability. This study addresses these gaps by conducting a PRISMA-guided review of 74 peer-reviewed works published in the last decade, focusing specifically on blockchain's role across the health insurance lifecycle. Our contributions are threefold: (1) we provide a structured mapping of blockchain applications in registration, claims submission, adjudication, payment, and data management; (2) we integrate bibliometric keyword analysis to uncover research trends and thematic clusters; and (3) we synthesize actionable insights on emerging innovations such as parametric insurance, hybrid blockchain models, and AI-driven fraud detection. Together, these contributions position this study as the first comprehensive, health-insurance–focused systematic review of blockchain applications.

To address these issues, this paper provides a systematic review of blockchain applications in health insurance, focusing on their role in fraud prevention, claims processing, data management, and emerging patient-centric models. By synthesizing findings from peer-reviewed studies and real-world implementations, the study highlights blockchain's transformative potential while critically examining its limitations. The review also identifies open challenges and future research directions, offering actionable insights for researchers, practitioners, and policymakers seeking to modernize the health insurance ecosystem. This paper provides a comprehensive analysis of blockchain applications in health insurance, focusing on its role in fraud prevention, data management, claims processing, and payment reconciliation. Additionally, it explores emerging trends and challenges, offering insights into blockchain's potential to create a secure, efficient, and patient-focused healthcare ecosystem.

The paper is structured as follows. Section 2 introduces the background and preliminary concepts, providing an overview of the health insurance ecosystem and the foundational principles of blockchain technology, with emphasis on processes such as claims submission, adjudication, and data security. Section 3 outlines the research methodology, describing the systematic review process, inclusion and exclusion criteria, and the PRISMA-guided selection of studies. Section 4 synthesizes the results, mapping blockchain's role across the health insurance lifecycle through visual analysis and case-based comparisons. Section 5 highlights practical applications, focusing on secure interoperability, process automation, and fraud prevention, supported by real-world implementations. Section 6 discusses the transformative potential of blockchain, emphasizing five key enablers—data security, interoperability, scalability, cost efficiency, and real-time processing—while acknowledging integration and regulatory challenges. Section 7 identifies trends and open challenges, including clinical trial management, patient-centric models, disaster recovery, and fraud analytics, situating them within the broader trajectory of blockchain adoption in healthcare. Finally, Section 8 concludes the study by summarizing the core insights and presenting implications for both academic research and industry practice in health insurance.

2 Background and preliminary concepts

2.1 Health insurance processes

Health insurance operates within a complex ecosystem that requires seamless coordination between patients, healthcare providers, and insurers. The process begins when patients receive medical services, after which providers generate claims containing patient demographics, diagnosis codes, treatment details, and costs. These claims undergo multiple stages—submission, validation, adjudication, and settlement—each ensuring accuracy, compliance, and timely reimbursement.

Validation involves cross-referencing claims with policy terms, verifying medical necessity, and ensuring compliance with coding standards to prevent fraud, overpayments, and duplicate claims. Adjudication determines reimbursement eligibility, while settlement disburses payments to providers or beneficiaries. Transparency, automation, and interoperability are essential for efficiency and fraud prevention.

Regulatory compliance, particularly with HIPAA and GDPR, adds further complexity by mandating secure, privacy-compliant data handling. Fragmented data systems, slow manual processes, and inefficiencies in claims management underscore the need for innovative solutions. Addressing these challenges through advanced technologies like blockchain enhances security, trust, and efficiency, paving the way for a more transparent and patient centric health insurance system.

2.2 Blockchain technology

Blockchain technology offers a decentralized, immutable, and transparent solution to key inefficiencies in health insurance (Wenhua et al., 2023). By maintaining a tamper-proof ledger of

transactions, blockchain eliminates data silos, enhances trust among stakeholders, and reduces administrative burdens in claims processing and fraud prevention.

A key advantage of blockchain is its ability to automate workflows through smart contracts, ensuring real-time claims validation and adjudication while minimizing errors and disputes. Permissioned blockchain networks (Sukhwani et al., 2017; Liu et al., 2019) further enhance security by granting controlled access to authorized participants, ensuring compliance with data protection regulations such as HIPAA and GDPR.

Blockchain also improves interoperability by enabling secure, verifiable data exchange across healthcare providers and insurers. Its integration with IoT and AI strengthens fraud detection by ensuring real-time verification of health data, reducing financial losses, and improving system reliability.

By addressing challenges in data integrity, regulatory compliance, and operational inefficiencies, blockchain establishes a scalable and secure foundation for modernizing health insurance. Beyond claims processing, it supports patient-centric models, public health monitoring, and disaster recovery, reinforcing its transformative potential across the industry.

3 Methodology

In the rapidly advanced domain of Blockchain technology, it has become a basic tool in various applications, especially in health insurance. Nevertheless, although their use is becoming more prevalent, there remains a significant gap in understanding their full potential and limitations within these contexts. This survey employed a systematic review approach to analyze the application of blockchain technology in health insurance. According to the progress in methods, this review aims to amalgamate these existing work.

In our study, we follow the Systematic Literature Review (SLR) methodology as proposed by Barbara Kitchenham (Kitchenham, 2012; Kitchenham et al., 2009), a structured and evidence-based method widely used to systematically gather, assess, and synthesize research in computing and healthcare domains (Aleti et al., 2012; Liu et al., 2023). We organized the research questions (RQs) that guide our SLR process as follows:

RQ1: What blockchain technologies are employed in the Health Insurance Lifecycle? Different domains, such as finance, security, healthcare may require tailed adaptations of blockchain to address domain-specific challenges and heterogeneous data. The question seeks to explore and categorize the different methods and techniques used in various stages of the health insurance lifecycle, which indicates the diversity of blockchain solutions—public, private, and consortium blockchains.

RQ2: What applications using blockchain for Health Insurance? Different segments of the health insurance industry need specialized blockchain solutions to cope with issues such as fragmented data systems, protracted claims processes and vulnerability to fraud or data breaches. This question intends to introduce the representative application scenarios where blockchain has demonstrated notable promise and adoption.

RQ3: What are the limitations and challenges of using blockchain for health insurance? Blockchain presents a transformative potential for health insurance, which has advanced patterns and data requirements. This question enhances the specific limitations, challenges, and future direction in using blockchain for health insurance.

These RQs were derived directly from gaps in the existing literature. Prior surveys of blockchain in healthcare have treated health insurance only peripherally and have not systematically examined insurance-specific technologies, applications, and challenges. To address this gap, RQ1 maps blockchain across the insurance lifecycle, RQ2 evaluates its applications, and RQ3 analyzes challenges and emerging directions. This structured approach differs from earlier reviews by explicitly aligning each RQ with unresolved problems and by ensuring that the results analysis in Sections 4–7 provides evidence-based answers to each question.

RQ1 calls for detailed studies of work used in applying blockchain across various stages in health insurance. RQ2 seeks to evaluate and compare the diverse scenarios of applications. RQ3 necessitates a comprehensive exploration of the obstacles and constraints faced when adopting blockchain technology in health insurance.

After delineating the research questions, we systematically integrate multiple search engines and academic databases, as listed in Table 1, to summarize related works. To ensure coverage of the lasted advancements, we also included OpenReview in our search strategy to capture forthcoming papers that offer significant insights.

Searches were conducted across OpenReview, IEEE, Xplore, Google Scholar, PubMed, Scopus, ACM, Digital Library, and ScienceDirect using the keywords: healthcare + insurance + blockchain. From the initial * articles retrieved, duplicates were removed, and a rigorous screening process was applied. A final set of 74 articles was selected for in-depth analysis based on the following criteria:

3.1 Inclusion criteria

- Studies focusing on blockchain applications in healthcare or health insurance.
- Topics addressing fraud detection, data security, privacy preservation, claims processing, and data management.
- Peer-reviewed publications, conference proceedings, and systematic reviews.
- Articles published in English within the last 10 years.
- Papers presenting practical implementations, frameworks, case studies, or proposals.

3.2 Exclusion criteria

- Studies without blockchain as a primary focus.
- Articles on general healthcare systems without connections to blockchain.
- Non-peer-reviewed publications, editorials, and opinion pieces.

TABLE 1 Search engines and databases for manual search.

Source	Search scheme
IEEE Xplore (https://ieeexplore.ieee.org/)	Title, Topic, Author, Keywords, Abstract
ACM Digital Library (https://dl.acm.org/)	Title, Keywords
PubMed (https://pubmed.ncbi.nlm.nih.gov/)	Keywords, Full Text
ScienceDirect (https://www.sciencedirect.com/)	Title, Keywords
SpringerLink (https://link.springer.com/)	Title, Keywords
Scopus (https://www.scopus.com/)	Title, Keywords, Abstract
Google Scholar (https://scholar.google.com/)	Topic, Author, Full Text

- Duplicate articles and papers unavailable in full text.
- Articles written in languages other than English.

This systematic selection process ensures the findings are based on high-quality, relevant literature, providing a robust foundation for analyzing blockchain's diverse applications in health insurance.

We documented the search, screening, and selection process following the PRISMA 2020 guidelines, which emphasize transparent reporting of systematic reviews. The initial search across all databases retrieved 304 papers. After removing duplicates and rigorously applying the inclusion and exclusion criteria, 105 relevant studies were shortlisted for further evaluation. To ensure the quality and relevance of the final selection, the authors conducted a comprehensive screening process, ultimately refining the set to 74 high-quality papers that aligned with the review's objectives and standards. The selection process is illustrated in Figure 1 below.

4 Result synthesis

This study examines how blockchain enhances efficiency, security, and transparency across the health insurance lifecycle, from patient registration to claims processing and data management. By leveraging decentralization, automation, and cryptographic security, it offers a scalable framework for modernizing healthcare operations. Figure 2, attached below, visually represents blockchain's impact across these stages. We also quantitatively explored the keywords co-occurrence in blockchain papers using VOSviewer, a bibliometric analysis software in Figure 8.

4.1 Patient registration

Patient Registration is a critical step in the healthcare and health insurance system, which Figure 3 summarizes the process. Traditionally, this process relies on centralized databases managed independently by hospitals, clinics, and insurance providers. Registration typically involves manual data entry or scanning physical documents, which are then recorded within siloed electronic systems (Harrell et al., 2022; Barton et al., 2002). Importantly, traditional patient registration now faces several challenges, identity duplication, data fragmentation, privacy and security risks, inefficient consent management (Adeghe et al., 2024; Dib and Rababah, 2020). These limitations will bring unsafe issues and need to control data using high cost.

Blockchain technology fundamentally transforms patient registration by addressing challenges such as identity duplication, fragmented data storage, and privacy concerns. A decentralized framework ensures data integrity and fosters trust among all stakeholders involved. As part of this system, each user is assigned a unique public and private key upon initialization to secure their digital identity (He et al., 2023). In blockchain-based EHR systems (Chouhan et al., 2023; Al Mamun et al., 2022), each account address ID is unique and can function as the primary key, streamlining record management and access control (Karmakar et al., 2023). Electronic Health Records (EHRs) are digital versions of patient medical histories, encompassing diagnoses, treatments, lab results, and other essential health information. They serve as a foundation for informed clinical decision-making and efficient patient care (Dubovitskaya et al., 2020).

One of the most significant advancements introduced by blockchain is identity management. It enables the creation of tamper-proof digital identities, ensuring accurate and seamless verification across healthcare providers, insurers, and other relevant entities. In a consortium blockchain model, this identity system could facilitate secure information exchange between insurance companies, medical institutions, and law enforcement agencies, improving administrative efficiency (Chen et al., 2023).

Consent management is another critical improvement. This process ensures that an individual's identity and personal data are only shared with authorized individuals or departments based on explicit, informed consent (Nowrozy et al., 2024). Once consent is granted, other operators on the blockchain may create tailored financial or medical services based on the approved data (Lin et al., 2023). Blockchain's immutable transparency guarantees that consent records remain verifiable and tamper-proof, empowering patients with full oversight of how their data is accessed. For instance, a doctor may be granted permission to review a patient's historical medical records, but access to future medical data would require re-authorization from the patient (Merlo et al., 2023). Additionally, consent and access preferences must be acquired under specific legal frameworks to comply with data protection regulations such as the General Data Protection Regulation (GDPR) (Arbabi et al., 2023; Protection, 2018).

Furthermore, blockchain enhances data privacy through robust encryption techniques and decentralized storage, significantly reducing the risks associated with centralized databases and single points of failure. By addressing identity verification, consent management, and data privacy, blockchain creates a secure, patient-controlled registration system. This foundation enhances interoperability, reduces administrative burdens, and ensures a seamless healthcare experience.

A research has proposed a real-world blockchain application to BPJS Kesehatan, the national insurance in Indonesia which ensures secure and transparent identity verification during the registration phase (Andre et al., 2019). Similarly, MedRec system was proposed by MIT researchers and provides a secure way of patient registration

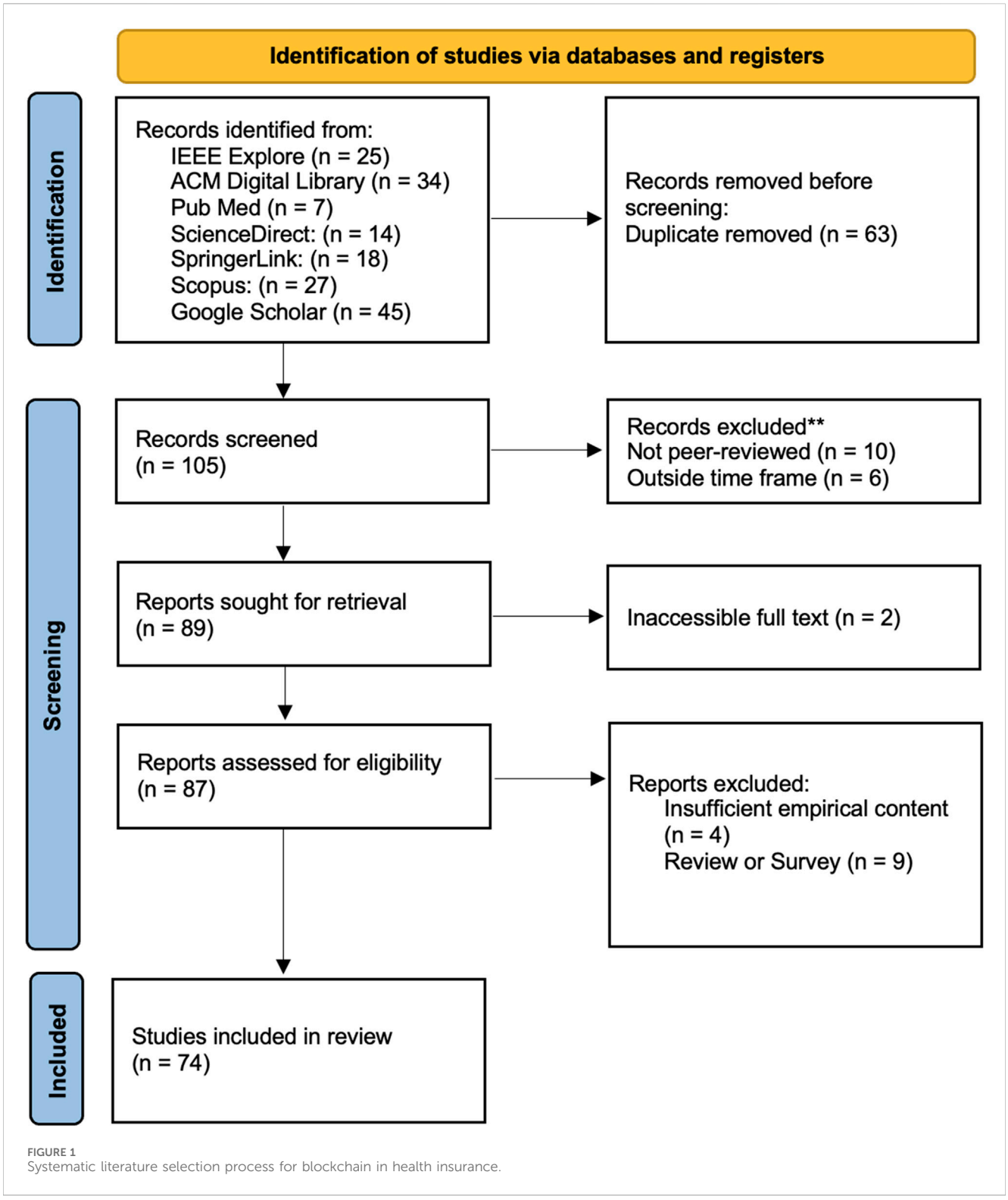

FIGURE 1
Systematic literature selection process for blockchain in health insurance.

(Azaria et al., 2016; Nchinda et al., 2019). In addition, ACTION-EHR (Dubovitskaya et al., 2020), introduced by the team at Stony Brook University, is a patient-centric blockchain-based electronic health record management system designed for oncology care networks. According to Table 2, we can find how these three blockchain applications target patient registration, reflecting their different implementation scopes and technical designs.

4.2 Service delivery

Traditional Service Delivery involves patients visiting healthcare providers where their medical information, diagnoses, and treatments are recorded and processed manually or within siloed electronic systems (Reddick and Turner, 2012). However, the communication and data sharing

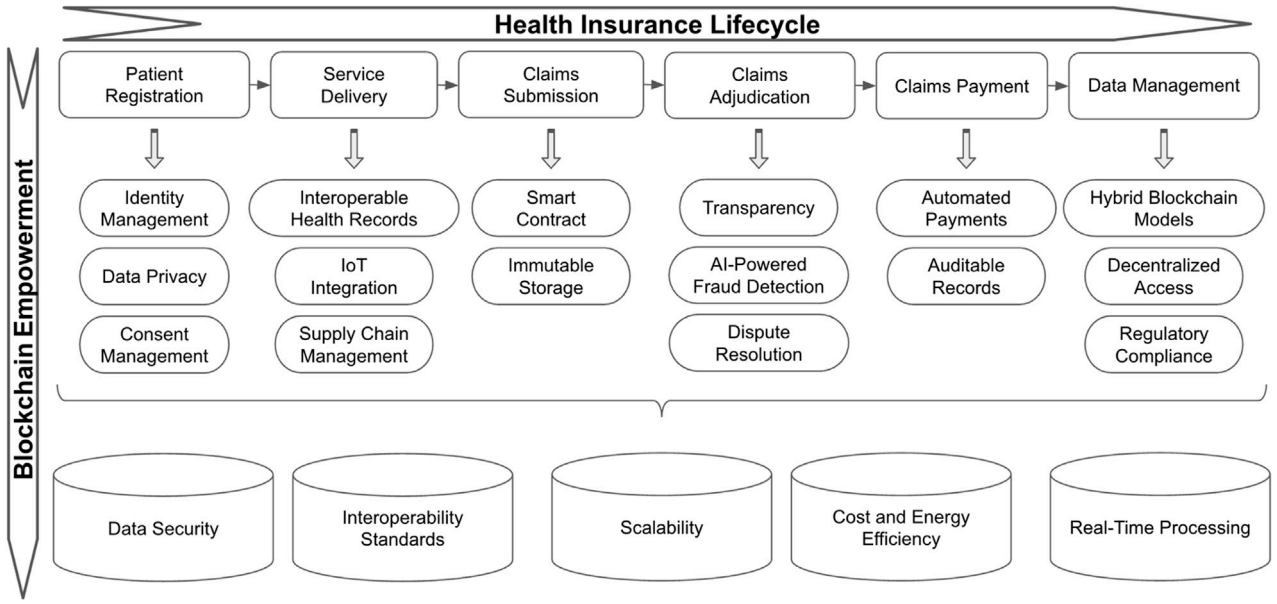

FIGURE 2
Health Insurance Lifecycle with Blockchain Applications.

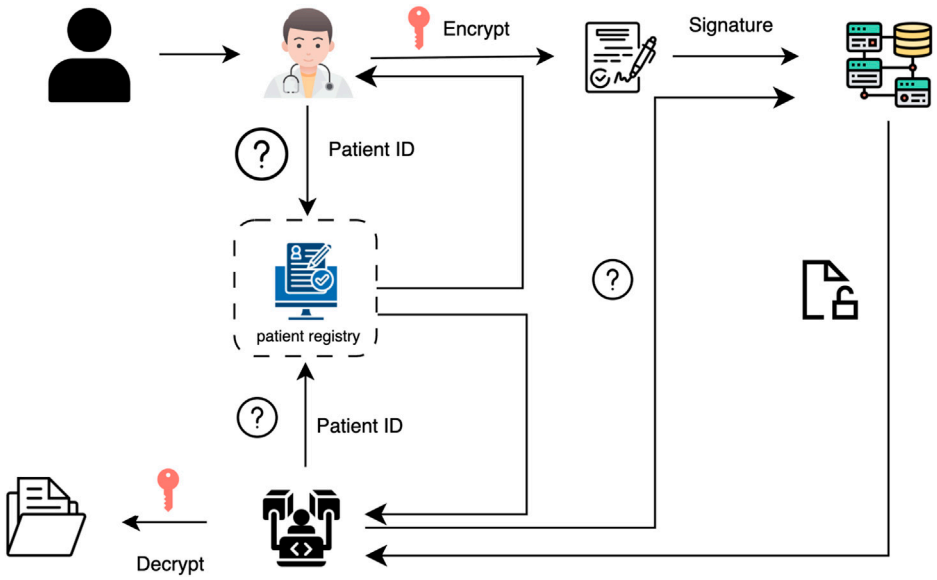

FIGURE 3
Patient registration.

are often slow and rely on centralized databases, which leads to delays, redundant procedures.

As shown in Figure 4, interoperable electronic health records (EHRs) enable the secure and seamless exchange of tamper-proof patient data among healthcare providers, insurers, and other stakeholders. Blockchain technology optimizes service delivery by providing verifiable proof of medical interactions and treatments, thereby ensuring transparency and reducing administrative inefficiencies (Sookhak et al., 2021; Andrew et al., 2023; Khan et al., 2022; Atadoga et al., 2024; Shaikh et al., 2025). A real-world example is Robomed, which captures patient data *via* blockchain and securely distributes it to the healthcare professionals (Singh et al., 2023). This eliminates redundancies, enhances compliance with privacy regulations, and improves care coordination. Additionally, blockchain's immutability guarantees data accuracy, while its permissioned access structure safeguards patient confidentiality.

The integration of Internet of Things (IoT) (Abdul-Qawy et al., 2015) devices further revolutionizes service delivery by enabling

TABLE 2 Patient registration example.

Dimension	BPJS Kesehatan (Indonesia)	MedRec	ACTION-EHR
Identity Management	Unique blockchain identity per member; eliminates duplicate enrollments	Each patient/provider has unique blockchain address	Blockchain account as unified identity; verified mapping
Consent Management	Consent stored immutably for data access across agencies	Smart contracts manage patient permission grants and revocation	Granular patient consent for data requests, tracked and auditable
Data Privacy	Robust encryption, decentralized control, privacy by design	Data encryption, selective sharing; accounts only accessible by authorized parties	Strong access controls, encrypted off-chain storage

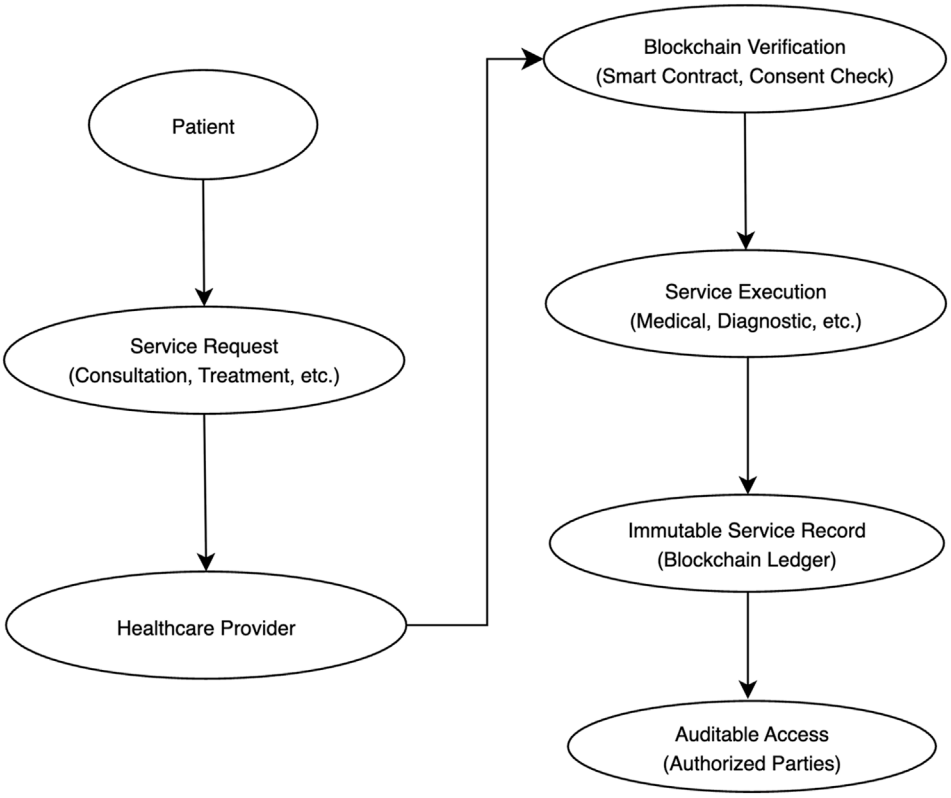

FIGURE 4
Service delivery.

real-time health monitoring and secure data collection (He et al., 2023) and enhances data reliability (Shen et al., 2023). Smart contracts enhance IoT integration by facilitating real-time patient monitoring and automated notifications for hospitals and patients *via* a secure, blockchain-backed platform (Taloba et al., 2021; Mahammad and Kumar, 2023). Wearable devices and medical sensors securely log health data directly onto the blockchain, ensuring tamper-proof records and reducing the risk of data manipulation or fraud. This enhanced data integrity supports patient-centric care models, enabling healthcare providers to make timely, informed decisions based on real-time patient metrics.

Blockchain also enhances supply chain management by ensuring transparency, traceability, and security. Distributed ledger technology (DLT) (Romero Ugarte, 2018; Collomb and Sok, 2016) maintains immutable transaction records, preventing unauthorized alterations and ensuring data consistency across stakeholders. This ensures that every pharmaceutical transaction, from production to distribution, remains verifiable and tamper-proof (Hu et al., 2024). Furthermore, DLT's decentralized framework enables real-time tracking and verification of medical products, mitigating counterfeiting risks, supply chain fraud, and unauthorized diversions (de Aguiar et al., 2020). By maintaining an immutable audit trail, blockchain fosters trust among manufacturers, distributors, and healthcare institutions.

Additionally, real-time monitoring and automated tracking systems improve resource allocation, particularly during health crises such as pandemics. The ability to securely track and authenticate pharmaceuticals, medical supplies, and essential equipment helps streamline logistics, prevent shortages, and reduce misallocation of critical resources.

By securing patient data, improving supply chain transparency, and enabling real-time health monitoring, blockchain modernizes

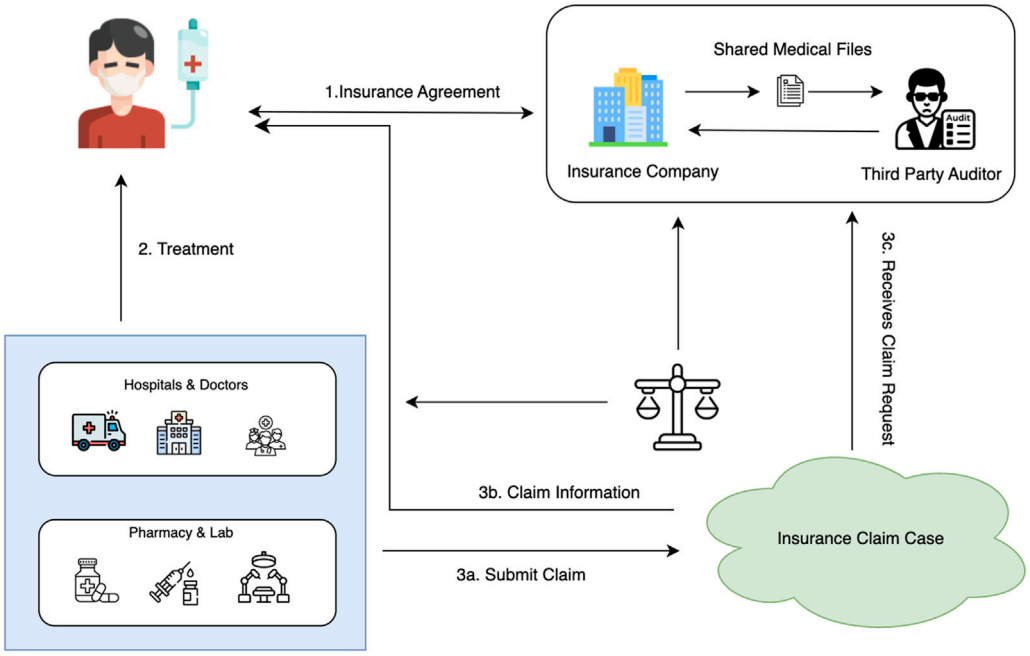

FIGURE 5
Claim submission.

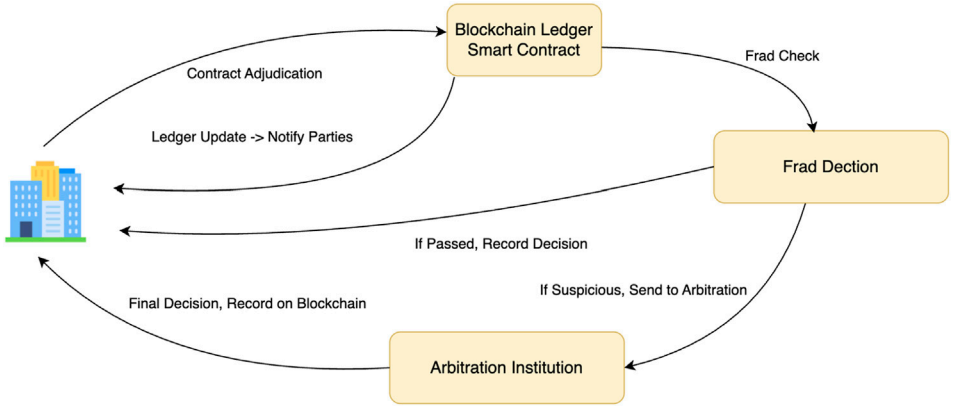

FIGURE 6
Claims adjudication.

healthcare service delivery. These advancements optimize resource allocation, reduce fraud, and improve patient outcomes.

4.3 Claims submission

Traditional claims submission processes are often slow, error-prone, and susceptible to fraud, leading to delays, inefficiencies, and disputes. Blockchain technology introduces a secure and efficient framework that automates workflows, ensures data integrity, and enhances transparency across all stakeholders. Figure 5 describes the main steps in claims submission.

One of the key innovations in blockchain-based claims submission is the use of smart contracts. A smart contract is a self-executing digital script that automatically verifies and processes claims upon submission, eliminating the need for manual intervention (Kolhe, 2019). It validates the patient's identity, checks the claim against the insurance policy, and initiates payments accordingly. Each time a new claim is submitted, the smart contract is re-executed, ensuring continuous validation based on predefined policy terms (El et al., 2024; Narne, 2024). This real-time automation significantly reduces processing times, minimizes errors, and enhances trust between patients, providers, and insurers.

In addition to automation, immutable blockchain storage further strengthens the integrity of claims data. Once a claim is

TABLE 3 Claim submission application.

Feature	Deloitte insurance solution	Lemonade parametric insurance (Kenya)	Forti-Ins (smart City health)
Smart Contract	Automates claim–policy matching and triggers payment	Parametric trigger (e.g., rainfall) for instant payout	End-to-end automation: submission
Immutable Storage	Entire claim process recorded on-chain, auditable	Event and trigger data on-chain, tamper-proof	All claim data on-chain, tamper-proof, auditable

recorded, it cannot be altered or tampered with, creating a transparent, verifiable audit trail that simplifies regulatory compliance, reduces fraud, and expedites dispute resolution.

By eliminating inefficiencies, reducing administrative burdens, and fostering greater collaboration within the health insurance ecosystem, blockchain transforms claims submission into a faster, more reliable, and fraud-resistant process, ultimately enhancing the overall patient and provider experience.

As shown in Table 3, real-world practitioners have explored blockchain-based claims submission. One example is that Deloitte uses smart contracts to reduce the time and cost associated with manual processing. This system enhances transparency and efficiency, benefiting both insurers and policyholders (Shaw and Eckenrode, 2016). Lemonade is one of the first insurance companies to use blockchain-based parametric insurance to support farmers in Kenya. With the application of smart contracts, the system automatically issues claims based on predefined parameters, such as rainfall data. As for 2023, this initiative facilitates prompt payouts to 7,000 farmers affected by drought conditions, eliminating the need for manual claims processing and reducing administrative cost (Alsdorf and Berkun, 2024). Additionally, the Forti-Ins system proposes a blockchain-based framework designed to automate healthcare insurance processing in smart cities, which integrates smart contracts with a distributed file system to enable secure processing (Alruwa et al., 2023).

4.4 Claims adjudication

Blockchain revolutionizes claims adjudication by enhancing transparency, enabling AI-powered fraud detection, and streamlining dispute resolution (El et al., 2024). Traditional adjudication processes often suffer from delays, inefficiencies, and a lack of visibility, requiring extensive manual checks. Blockchain addresses these challenges by providing a secure, automated, and tamper-proof framework that improves accuracy and trust among stakeholders.

Transparency is a major advantage of blockchain in claims adjudication. A decentralized ledger records all claim-related activities, ensuring that authorized stakeholders have real-time access to a single source of truth. This eliminates discrepancies, simplifies audits, and enhances trust in the system. Aetna and IBM are collaborating on a blockchain-based solution aimed at enhancing transparency, reducing administrative inefficiencies, and driving cost savings (Al Amin et al., 2024; Ng et al., 2021; Villarreal et al., 2023; Wang et al., 2023a; Shaikh et al., 2025).

AI-powered fraud detection further strengthens the process by leveraging blockchain's immutable records to analyze patterns, detect anomalies, and flag potential fraud (El et al., 2024). This reduces financial losses, minimizes operational inefficiencies, and enhances overall system reliability by identifying fraudulent claims before they impact insurers and providers.

Dispute resolution is also streamlined through blockchain's immutable records, which serve as verifiable evidence to quickly resolve disagreements. In cases of disputes, arbitration can be conducted efficiently, where the patient appeals to the arbitration institution, which reviews the recorded message content of all parties and makes an informed decision (Chen et al., 2021; Wenhua et al., 2023). Additionally, smart contracts automatically enforce policy terms, reducing processing delays and ensuring fair and consistent outcomes for all stakeholders.

The overall workflow of blockchain-enabled claims adjudication, including fraud detection, arbitration, and final settlement, is illustrated in Figure 6.

By enhancing transparency, leveraging AI for fraud detection, and automating dispute resolution, blockchain transforms claims adjudication into a more efficient, reliable, and equitable process, ultimately fostering trust and operational efficiency in the health insurance ecosystem.

4.5 Claims payment

Blockchain revolutionizes claims payment by automating transactions, ensuring record integrity, and enhancing efficiency through its decentralized and auditable ledger. Traditional payment workflows are slow, error-prone, and reliant on intermediaries, leading to delays and disputes. Blockchain effectively eliminates these inefficiencies by enabling secure, automated, and transparent claim settlements.

One of the earliest blockchain-based solutions for improving scalability and performance is payment channels. These off-chain bidirectional channels allow fast and efficient transactions between multiple participants without recording each transaction on the main blockchain. This method is particularly effective for handling high-frequency, small-value transactions, making it ideal for micropayments, streaming payments, and recurring claims settlements (Kasyapa and Vanmathi, 2024).

Smart contracts further enhance payment automation by executing transactions immediately after claim validation, eliminating manual delays and errors. Once the preset conditions—such as a verified medical diagnosis or insurance incident—are met, the smart contract automatically triggers the claim payment, transferring funds directly to the beneficiary's account (Chen et al., 2021). This accelerates claim settlement,

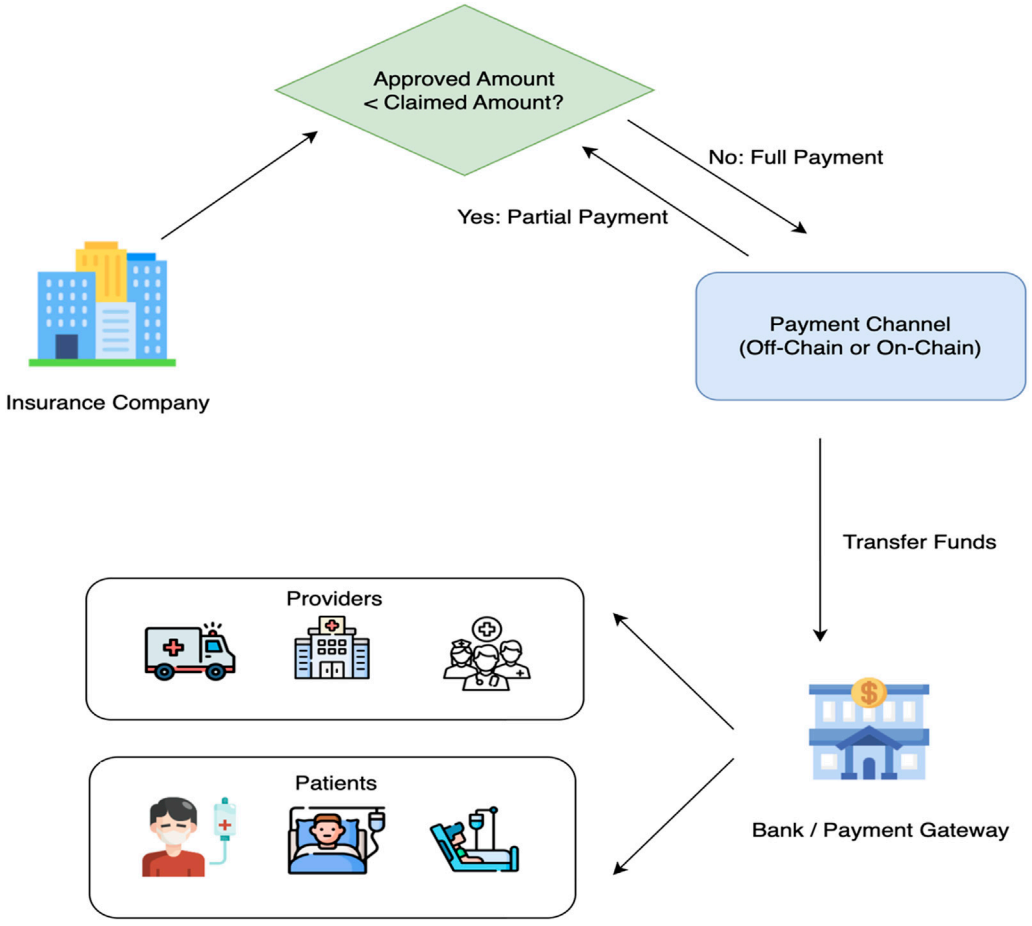

FIGURE 7
Claims payment.

reduces administrative costs, and ensures prompt reimbursements, fostering trust between insurers and policyholders.

Moreover, blockchain's immutable ledger maintains a tamper-proof history of all claim payments, allowing stakeholders to verify transactions transparently and resolve disputes efficiently. From the occurrence of an insurance incident to final payment, all claim-related information is automatically generated and recorded *via* smart contracts, eliminating the need for manual investigation and assessment (Chen et al., 2021).

The overall workflow of blockchain-enabled claims payment from determining approved amounts, selecting payment channels, to final fund transfers to patients or providers is illustrated in Figure 7.

By combining automation with secure, decentralized record-keeping, blockchain streamlines claims payments, ensuring faster processing, reduced errors, and greater accountability within the health insurance ecosystem.

Together, blockchain-driven claims submission, adjudication, and payment create a seamless, fraud-resistant system that accelerates reimbursements, reduces costs, and enhances trust across the insurance ecosystem.

4.6 Data management

Blockchain transforms healthcare data management by enabling hybrid models, decentralized access, and regulatory compliance. Traditional systems struggle with data silos, limited interoperability, and security vulnerabilities, leading to inefficiencies and privacy risks. Blockchain offers a scalable, secure, and patient-centric solution to these challenges. Hybrid blockchain models strike a balance between privacy and transparency by storing sensitive data on private chains while using public chains for validation and audit purposes. This enhances data security and accountability without compromising accessibility. Decentralized access allows authorized stakeholders to securely share data, improving collaboration among healthcare providers while ensuring patients retain control over their health records. The HIE of One model proposes a blockchain-driven authentication framework, where medical credentials are issued by regulatory bodies rather than stored within hospital IT systems, shifting identity control to trusted, decentralized networks (Gropper, 2016). To achieve scalability for EHR data, ACTION-EHR employs a hybrid approach, storing metadata on-chain while encrypting and storing EHR data off-chain in HIPAA-compliant cloud-based storage (Dubovitskaya et al., 2020).

Regulatory compliance is seamlessly integrated into blockchain's architecture. HIPAA regulations define standards for secure data

TABLE 4 Comparison of traditional vs blockchain-based health insurance processes.

Processes	Traditional approach	Blockchain-based approach
Patient Registration	- **Identity issues:** Data duplication and fragmentation. - **Privacy risks:** Centralized storage vulnerable to breaches. - **Limited access:** Hard to share records across providers.	- **Decentralized identity:** Secure, tamper-proof records. - **Seamless sharing:** Interoperability across providers. - **Patient control:** Users manage access permissions.
Service Delivery	- **Siloed data:** Inefficient and hard to retrieve. - **Manual verification:** Slow processes. - **Security risks:** Prone to tampering and unauthorized access.	- **Tamper-proof records:** Immutable blockchain data. - **Real-time access:** Faster, efficient care. - **Smart contracts:** Automate verification.
Claims Submission	- **Slow processing:** Manual and error-prone. - **High fraud risk:** Lack of transparency. - **Disputes:** Frequent errors lead to conflicts.	- **Automated validation:** Smart contracts process claims instantly. - **Fraud prevention:** Immutable records. - **Faster approvals:** Reduces manual work.
Claims Adjudication	- **Time-consuming:** Manual reviews take long. - **Disputes:** Hard to verify claim authenticity. - **Fraud risks:** Lack of real-time detection.	- **Transparent audit trail:** All activities recorded. - **AI fraud detection:** Identifies anomalies. - **Automated resolution:** Smart contracts enforce policies.
Claims Payment	- **Delays:** Manual fund transfers. - **High costs:** Intermediaries add fees. - **Errors:** Tracking issues lead to disputes.	- **Instant settlements:** Smart contracts trigger payments. - **Lower costs:** No intermediaries. - **Real-time tracking:** Reduces disputes.
Data Management	- **Centralized storage:** High breach risks. - **Limited access:** Patients lack control. - **Compliance challenges:** Hard to meet regulations.	- **Hybrid blockchain:** Secure and decentralized. - **Patient ownership:** Users control access. - **Automated compliance:** Smart contracts enforce rules.

exchange, covering healthcare plans, providers, clearinghouses, and business associates (de Aguiar et al., 2020). Additionally, GDPR mandates that users must be informed about collected data, even when sourced indirectly (Arbabi et al., 2023). Blockchain facilitates compliance through immutable records, encryption, pseudonymization, and smart contracts, which automate compliance processes, reduce security risks, and build trust with patients and regulators.

The claim and member data stored in blockchain can be used for machine learning to detect fraud and enhance predictive analytics (Haque and Tozal, 2022). By leveraging blockchain's immutable records, machine learning models can identify fraudulent patterns, optimize risk assessment, and enhance decision-making in health insurance operations (Chen et al., 2025). Federated learning further strengthens privacy-preserving analytics by enabling decentralized AI model training across hospitals, research labs, and mobile devices without exposing sensitive patient data. This approach enhances collaboration while mitigating risks associated with centralized data storage and leakage (Joshi et al., 2022).

Recognizing blockchain's transformative potential, Aetna, Anthem, and Cleveland Clinic are backing the development of Avaneer Health, a blockchain-powered healthcare network aimed at modernizing claims processing, ensuring secure health data exchanges, and enhancing provider directory accuracy (Singh et al., 2023). By enabling real-time, permissioned data sharing, Avaneer Health seeks to reduce administrative inefficiencies, lower costs, and improve overall healthcare interoperability.

Table 4 below compares traditional health insurance processes with blockchain-based solutions, highlighting key differences in efficiency, security, and automation across critical areas such as patient registration, claims processing, and data management.

By integrating hybrid models, decentralized access, and automated compliance, blockchain redefines healthcare data management. This evolution empowers patients, streamlines governance, and fosters a more connected and secure healthcare ecosystem. Figure 8 also shows that AI and data related nodes (i.e., "AI drive application," "data security," "data authenticity") are widely connected to other healthcare and insurance domains.

5 Application

5.1 Secure interoperability and data management

Health insurance systems generate and handle vast volumes of sensitive medical data across various sources, such as hospitals, clinical notes, lab tests, visit records, and wearable devices. For

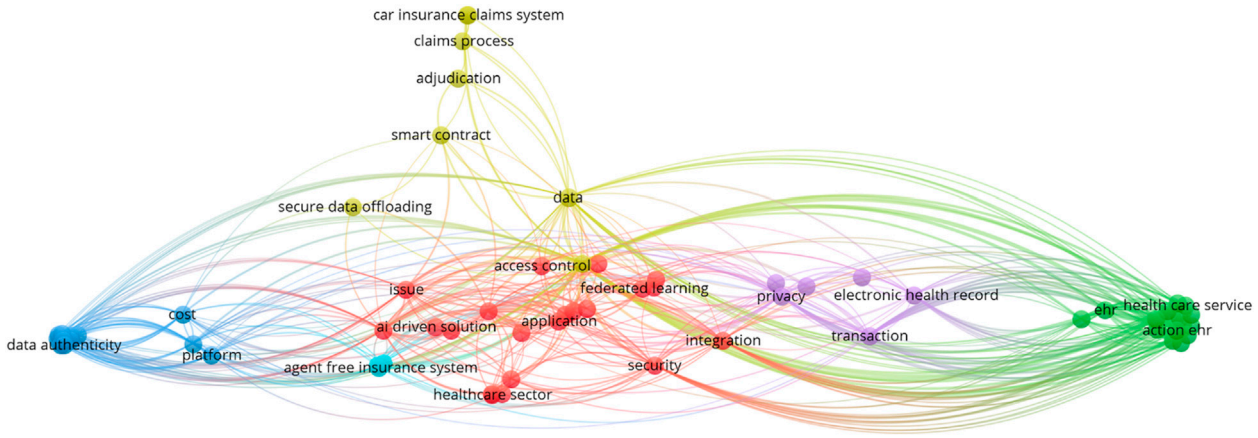

FIGURE 8
Network analysis for keyword Co-occurrence in blockchain papers.

example, in managing prescription drugs (A et al., 2022), blockchain can address longstanding issues of data integrity, fraud, and process inefficiency. Through decentralized ledgers and smart contracts, blockchain ensures the digital prescriptions issued by clinicians are immutable and verifiable. Moreover, Preventing counterfeit (Alhasan et al., 2021) involves tracking and validating the authenticity of medical products or health services data. This blockchain system can prevent counterfeiting in the health insurance sector. Also, BlockMedCare (Azbeg et al., 2022; Karmakar et al., 2024) proposes a novel Digital Twin (DT) driven blockchain framework and models patient data as digital twins. Through combining hybrid on-chain and off-chain storage, this can ensure secure data management. Recent research on Web 3.0 further reinforces this direction, highlighting how blockchain-enabled decentralized applications (dApps) and smart contracts can support transparent and secure health data exchange, extending interoperability beyond insurers and providers to broader ecosystems (Zhang and Lu, 2025).

Blockchain technology offers a solution for secure data sharing and interoperability in this fragmented environment. By using a decentralized ledger, patient records and related health data can be stored and exchanged in an immutable and tamper-evident way, ensuring data integrity across stakeholders (Center for Telehealth and e-Health Law CTeL, 2023). Every update to a patient's record (e.g., a new lab result or treatment note) can be appended as a transaction on the blockchain, visible to authorized parties and impossible to alter retroactively. This transparency and integrity are crucial for insurers who rely on accurate data for claims and underwriting.

One application is in electronic prescriptions and medication data management. For example, when a clinician issues a digital prescription, recording it on a blockchain makes it immutable and verifiable. The insurer and pharmacy can trust that the prescription has not been forged or modified, thereby preventing fraud such as prescription alterations or refills beyond allowed limits. In practice, researchers have designed blockchain-based e-prescription systems where the prescription is encoded in a smart contract—any pharmacy or insurer can cryptographically verify its validity and dispense or reimburse accordingly (ResearchGate, 2022). This ensures that medications billed to insurance are exactly as the doctor ordered, closing a common fraud gap.

Moreover, in the pharmaceutical supply chain, blockchain can record each handoff of a drug (from manufacturer to distributor to pharmacy) to create a traceable history that helps prevent counterfeit or substandard drugs from entering the system (Center for Telehealth and e-Health Law CTeL, 2023). By verifying drug authenticity, insurers can avoid paying claims for fake or unsafe medications, enhancing patient safety and trust.

Another key use is data interoperability between healthcare providers and insurers. Health insurers often need to aggregate medical records from various providers to assess claims or manage care. Traditional data sharing is slow and siloed, but blockchain can enable a unified, permissioned data network. A notable real-world example is a 2019 collaboration between major U.S. insurers (Aetna, Anthem, HCSC) and technology firms to build a blockchain health network. Their goal was to improve transparency and interoperability by allowing insurers, providers, and patients to securely share health information on a common ledger (PR Newswire, 2019b; PR Newswire, 2019c; PR Newswire, 2019d; PR Newswire, 2019e). By reducing administrative errors and friction, such a network could ensure that each party (with proper authorization) can access up-to-date patient data (e.g., eligibility information, prior treatments) almost in real time. This kind of data management not only speeds up processes like pre-authorizations and claims approvals but also enhances security: only authorized nodes (hospitals, insurers, *etc.*) participate in the permissioned blockchain, and patients could even be given keys to control who sees their data (PR Newswire, 2019e).

Beyond conceptual trials, academic frameworks have demonstrated the benefits of blockchain for health data management. BlockMedCare is one such framework that models each patient's data as a digital twin on a hybrid blockchain system (Amofa et al., 2024). In this approach, high-volume or sensitive data (like medical IoT sensor readings or images) are stored off-chain (e.g., in secure databases or IPFS), while the blockchain stores hashes or pointers ensuring integrity and time-stamping of each record. The patient's on-chain "digital twin" is essentially an index of all their health events and data versions.

5.2 Process automation for claims and settlement

For claims and settlement, process automation has been a critical stage that often involves manual verification, prone to errors, delays, and susceptibility to fraud. As depicted in (Khatun et al., 2022; Eletter, 2024), it creates an automated platform built on the Hyperledger Fabric permissioned blockchain, which showcases how insurers and healthcare providers can interact seamlessly in a decentralized manner. Another benefit that process automation can have is from blockchain-enabled parametric insurance models, which claims are triggered automatically based on external data sources. For instance, Lemonade's blockchain-based parametric insurance automates crop insurance claims by using rainfall data as an objective trigger, eliminating paperwork and accelerating relief to farmers (Singhal et al., 2024; Cate, 2025; Okoampah et al., 2023; Bodemer, 2023). IBM-Aetna blockchain initiative aimed at exactly this: promoting efficient claims and payment processing through a shared ledger, thereby cutting down the back-and-forth that occurs today in claims adjudication. Early pilot results in such networks have shown promise in reducing claim processing times from days to minutes, since verification steps that used to be sequential can be executed in parallel by the smart contracts (PR Newswire, 2019a).

This work (Bhamidipati et al., 2021) ClaimChain combines blockchain with IoT to automate the entire claims lifecycle - from initial claim filing to approval and final settlement–using a series of smart contracts. In ClaimChain, when a claim is filed, it is recorded as a unique digital asset on the ledger. Smart contracts then automatically perform tasks like verifying policy validity, checking the claim against known fraud indicators (e.g., whether the same expense has been claimed before), and even routing the claim through an IoT-integrated workflow for supporting data. For instance, if a claim involves a car accident injury (in auto-health combined scenarios), IoT sensors or telematics data about the crash could be attached and verified on-chain. ClaimChain's design includes automation features at multiple levels: (a) running business rules to decide straightforward claims, (b) triggering required approvals (by linking insurers and possibly external investigators on the network), and (c) updating the status in real-time for all stakeholders. By simulating large volumes of transactions, the researchers showed that such a system can scale to handle realistic loads and markedly improve response times for claim handling. In essence, the blockchain acts as a neutral execution engine where insurers and healthcare providers collaborate without a central intermediary, each trustfully following the smart-contract-defined process.

In more conventional health insurance contexts, blockchain is enabling electronic claim management systems that improve on today's processes. South Korea's *eClaim system* is a notable example: it automates claim submission and verification for private health insurance by leveraging standardized electronic medical records and a blockchain backbone. Under eClaim, hospitals submit treatment data in a standard format, which a blockchain-based platform then cross-checks against insurance criteria automatically (PR Newswire, 2019a). Bae and Yi (2022) report that this approach greatly reduced the need for manual document handling and even led to an increase in the number of claims processed (since providers found it easier to file claims electronically). Similar advances in blockchain-driven financial automation have been demonstrated in supply chain finance, where large language models integrated with blockchain platforms enable real-time verification and settlement of financing claims; these parallel innovations underscore the feasibility of applying similar automation to health insurance claims (Yang et al., 2025). This demonstrates that automation can improve efficiency for all parties: providers get paid faster, insurers spend less on processing, and patients benefit from quicker reimbursements.

5.3 Fraud prevention and risk control

Fraud prevention and risk control are critical challenges in the health insurance blockchain ecosystem. This study presents an approach that integrates AI-Driven machine learning models (Amponsah et al., 2022; Pingili, 2025) to analyze the records stored in blockchain and identify anomalies indicative of fraud. IPFS-Blockchain (Mali et al., 2024) introduces the permissioned blockchain network where only authorized parties can participate and provides feature engineering to record each decision data frame (Ismail and Zeadally, 2021). uses multi-signature claim processing to reduce fraudulent activities, which ensure enhanced fraud prevention.

Beyond passive transparency, blockchain-based solutions actively integrate fraud detection algorithms and multi-party validation to catch anomalies. One approach is to harness Artificial Intelligence on the trustworthy data that blockchain provides. Because blockchain ensures data quality (no tampering, consistent format), AI models can reliably analyze claim records for patterns of fraud. For example, a recent framework combined blockchain with Large Language Models (LLMs) to scan through both structured claim data and unstructured medical notes stored on the ledger. In this system, the blockchain recorded all claim-related events and also stored references to detailed medical records in a decentralized storage (IPFS), ensuring the AI had a single source of truth. The LLM could then dynamically retrieve those records and evaluate if the clinical notes support the billed services, flagging discrepancies in real time. This context-aware analysis means even sophisticated frauds (like notes manipulation or unnecessary services) can be detected by cross-verifying narrative medical data with billing codes–a task very hard to do in legacy systems.

Another powerful mechanism is enforcing collaborative verification and access control to prevent fraud. Blockchain consortia in insurance allow multiple stakeholders (insurers, providers, regulators) to jointly verify claims. For example, the Block-HI framework (Islayem et al., 2025) proposes a consortium blockchain where insurers share data about claims and use smart contracts to detect fraud across the network. In such a setup, if a fraudster tried to scam multiple insurers with the same claim (a common trick when insurers' databases are siloed), the shared ledger would immediately reveal the duplicate submissions. Block-HI goes further by defining a taxonomy of healthcare fraud patterns and encoding detection rules on-chain, so that claims are checked against multiple fraud scenarios automatically.

6 Discussion

Blockchain technology presents a transformative opportunity for healthcare, addressing persistent challenges and establishing a

more secure, efficient, and transparent system. Five key enablers—data security, interoperability, scalability, cost and energy efficiency, and real-time processing—define blockchain's impact on the healthcare ecosystem and its potential for large-scale adoption. Emerging fields such as quantum science and quantum machine learning further broaden the horizon for blockchain in health insurance, as quantum-based methods could enhance computational efficiency, secure data exchange, and enable more advanced fraud detection and predictive modeling (Ye and Lu, 2022).

Data security is one of the most critical benefits of blockchain in healthcare. By leveraging encryption, pseudonymization, and decentralized storage, blockchain ensures that patient information remains protected from unauthorized access and tampering. The immutability of blockchain records enhances trust by creating a tamper-proof history (Abdelhamid et al., 2024; Wang X. et al., 2023), mitigating the risks of data breaches while ensuring compliance with privacy regulations such as HIPAA and GDPR. Compared to traditional centralized systems, blockchain-based identity management has been shown to significantly reduce the likelihood of medical identity theft, a growing concern in healthcare cybersecurity. Additional studies exploring real-world implementations of blockchain-driven privacy enhancements would further support these claims.

Interoperability remains a major challenge in healthcare due to fragmented data silos that limit seamless data exchange among stakeholders (Sharma et al., 2022). Blockchain eliminates these barriers by providing a decentralized framework that facilitates secure, real-time collaboration between healthcare providers, insurers, and researchers. The adoption of interoperability standards, such as Fast Healthcare Interoperability Resources (FHIR) in blockchain based systems (Vorisek et al., 2022; Reegu et al., 2023), has demonstrated potential in streamlining medical record-sharing and reducing administrative inefficiencies. Smart contracts play a crucial role in automating data access permissions, ensuring that only authorized parties can retrieve sensitive patient information. Further research into blockchain interoperability frameworks and real-world applications would strengthen the case for its broader implementation.

Scalability is a critical concern as healthcare systems generate vast amounts of data, requiring blockchain networks to process high transaction volumes efficiently. Traditional blockchains face processing speed and storage limitations, but hybrid blockchain models, Layer-2 scaling solutions (e.g., rollups), and alternative consensus mechanisms like Proof of Stake (PoS) and sharding offer promising solutions (Singh et al., 2023; Atadoga et al., 2024). To enhance data security and provenance, the MeDShare system employs four-layer system architecture—comprising the User Layer, Data Query Layer, Data Structuring and Provenance Layer, and Existing Database Infrastructure Layer—to ensure secure access, structured processing, authenticated transactions, and immutable record-keeping (Xia et al., 2017). These advancements optimize privacy, efficiency, and computational performance, making blockchain more viable for real-time healthcare applications. Further empirical studies evaluating blockchain scalability in large-scale healthcare deployments would provide valuable insights into its long-term feasibility and adoption.

Cost and energy efficiency are important considerations in determining blockchain's sustainability in healthcare. The transition from energy-intensive consensus mechanisms such as Proof of Work (PoW) to more sustainable models like PoS and Byzantine Fault Tolerance (BFT) reduces environmental impact while maintaining security and decentralization (Chondrogiannis et al., 2022; Nelaturu et al., 2022). Blockchain also drives cost reductions by automating processes such as claims adjudication, fraud detection, and provider reimbursements through smart contracts, which minimize administrative overhead and accelerate payment cycles. Comparative analyses between blockchain-enabled and traditional healthcare IT systems in terms of cost efficiency and operational impact would provide further validation.

Real-time processing capabilities offered by blockchain redefine decision-making and responsiveness in healthcare. By integrating blockchain with IoT and AI-powered analytics, continuous patient monitoring and real-time fraud detection become feasible. Wearable health devices and sensor-based systems can be assisted by artificial intelligence (Nguyen et al., 2021) and securely transmit data to blockchain networks, supporting automated claim verification, remote diagnostics, and personalized treatment plans. Additionally, decentralized data storage ensures critical patient records remain accessible even during system failures or natural disasters, reinforcing healthcare resilience. Research focusing on blockchain-IoT integrations in real-world healthcare settings would further solidify its role in advancing medical technology.

By focusing on these five key enablers, blockchain lays the foundation for a secure, scalable, and patient-centric healthcare system. However, challenges such as regulatory uncertainty, integration complexities with legacy systems, and ensuring global interoperability remain significant barriers to widespread adoption. Continued collaboration among policymakers, industry leaders, and technology experts will be essential in bridging these gaps and accelerating blockchain's adoption in healthcare.

7 Trends and open challenges

The integration of blockchain into healthcare continues to evolve, introducing innovations while presenting challenges that must be addressed for widespread adoption. Key emerging trends include clinical trial management, patient-centric models, disaster recovery, public health monitoring, and fraud analytics, all of which leverage blockchain's transparency, security, and automation.

Blockchain enhances clinical trial management by ensuring data authenticity and preventing manipulation. Decentralized ledgers provide a single source of truth for researchers, regulators, and sponsors, streamlining approvals and improving trial credibility. Patient-centric models further empower individuals by granting them control over their health records, promoting secure data-sharing and consent management while complying with evolving privacy laws.

The resilience of blockchain infrastructure makes it an effective tool for disaster recovery by preserving medical records even during cyberattacks or system failures. Similarly, public health monitoring benefits from blockchain's ability to aggregate real-time epidemiological data, aiding in disease tracking, vaccination

management, and crisis response coordination among healthcare institutions and government agencies.

Fraud prevention and analytics are significantly improved through blockchain's immutable records, AI-driven fraud detection, and IoT integration. These tools enable real-time verification of insurance claims and reduce financial losses by detecting fraudulent patterns.

Despite these advancements, regulatory hurdles, interoperability challenges, and scalability limitations continue to impede adoption. Many healthcare systems still rely on legacy infrastructures that require seamless blockchain integration, and standardized frameworks are needed to ensure compliance with privacy and security laws. Additionally, concerns regarding energy consumption and computational efficiency necessitate further research into sustainable blockchain solutions.

Beyond these broad concerns, blockchain in health insurance faces multi-layered obstacles that require careful navigation. On the technical side, scalability, latency, and data storage remain unresolved issues, while interoperability with legacy health IT continues to limit real-world integration. Regulatory uncertainty further complicates adoption, particularly where immutability conflicts with requirements such as GDPR's "right to be forgotten." Organizationally, high implementation costs, limited technical literacy among insurers, and resistance from entrenched stakeholders pose barriers to deployment. Nevertheless, emerging solutions—including Layer-2 scaling, hybrid blockchain models, federated learning for privacy-preserving analytics, and collaborative consortia like Avaneer Health—offer realistic pathways forward. Beyond these developments, recent surveys of quantum science and quantum machine learning suggest that the convergence of blockchain with quantum technologies may unlock unprecedented security and scalability, offering a pathway for long-term resilience in health insurance ecosystems (Lu et al., 2024). These developments suggest that while blockchain adoption will be gradual, its long-term prospects in improving efficiency, security, and patient-centric care remain strong.

Looking ahead, reconciling decentralized data systems with global privacy regimes will be essential. Cross-border insurance networks must navigate heterogeneous laws, from HIPAA in the United States to GDPR in Europe and evolving digital health regulations in Asia and Africa. Ethical reconciliation will likely require hybrid governance models, where blockchain ensures technical trust but oversight mechanisms—such as privacy-preserving computation, selective disclosure protocols, and ethics boards—guarantee alignment with patient rights and social values. Addressing these ethical dimensions is critical for building not just legally compliant but socially trustworthy blockchain health insurance systems.

Beyond regulatory compliance, blockchain in health insurance raises important ethical questions. Decentralized identity management, while empowering patients with control over their data, also shifts responsibility and potential liability onto individuals who may lack the expertise to manage cryptographic keys. Ethical concerns arise if patients lose access to their health data or if identity credentials are compromised. Furthermore, while blockchain's immutability ensures data integrity, it also creates tension with ethical obligations to allow data correction or erasure, especially under laws like the GDPR's "right to be forgotten." These issues underscore the need for governance frameworks that align technological capabilities with ethical standards of patient autonomy, beneficence, and justice.

To fully realize blockchain's potential in healthcare, collaborative efforts among policymakers, technology developers, and healthcare institutions are essential. By addressing these open challenges, blockchain can drive a more transparent, resilient, and efficient healthcare ecosystem that benefits patients, providers, and insurers alike.

8 Conclusion

Blockchain technology presents a transformative opportunity to enhance security, efficiency, and transparency in health insurance. By enabling immutable records, smart contracts, and decentralized data management, blockchain addresses key challenges in claims processing, fraud prevention, and interoperability. Its integration with AI and IoT strengthens fraud detection, streamlines workflows, and improves real-time decision-making.

Despite its potential, scalability, regulatory alignment, and integration with legacy systems remain critical challenges. Overcoming these barriers will require collaborative efforts among policymakers, industry leaders, and technology developers to establish standardized frameworks and scalable blockchain solutions.

As blockchain adoption continues to evolve, its role in patient-centric healthcare, public health monitoring, and automated insurance processes will expand. Future research should focus on real-world implementations, regulatory adaptation, and optimizing blockchain's energy efficiency. By addressing these challenges, blockchain can drive a more transparent, resilient, and patient-focused health insurance ecosystem.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

YC: Investigation, Conceptualization, Writing – review and editing, Writing – original draft. CZ: Writing – review and editing, Writing – original draft. YG: Writing – review and editing, Writing – original draft.

Funding

The author(s) declare that no financial support was received for the research and/or publication of this article.

Acknowledgments

We sincerely thank the researchers and institutions whose work has contributed to this study. Their valuable insights into blockchain applications in health insurance, fraud detection, claims processing, and data security have provided a strong foundation for this

research. Their dedication to innovation continues to drive progress in this field.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Alnuaimi, A., Alshehhi, A., Salah, K., Jayaraman, R., Omar, I. A., and Battah, A. (2022). Blockchain-based processing of health insurance claims for prescription drugs. *Ieee Access* 10, 118093–118107. doi:10.1109/access.2022.3219837

Abdelhamid, M., Sliman, L., Ben Djemaa, R., and Perboli, G. (2024). A review on blockchain technology, current challenges, and AI-driven solutions. *ACM Comput. Surv.* 57 (3), 1–39. doi:10.1145/3700641

Abdul-Qawy, A. S., Pramod, P. J., Magesh, E., and Srinivasulu, T. (2015). The internet of things (iot): an overview. *Int. J. Eng. Res. Appl.* 5 (12), 71–82.

Adeghe, E. P., Okolo, C. A., and Ojeyinka, O. T. (2024). Evaluating the impact of blockchain technology in healthcare data management: a review of security, privacy, and patient outcomes. *Open Access Res. J. Sci. Technol.* 10 (2), 013–020. doi:10.53022/oarjst.2024.10.2.0044

Al Amin, M., Shah, R., Tummala, H., and Ray, I. (2024). "Utilizing blockchain and smart contracts for enhanced fraud prevention and minimization in health insurance through multi-signature claim processing," in *2024 international conference on emerging trends in networks and computer communications (ETNCC)*, Windhoek, Namibia, 1–9. doi:10.1109/ETNCC63262.2024.10767491

Al Mamun, A., Azam, S., and Gritti, C. (2022). Blockchain-based electronic health records management: a comprehensive review and future research direction. *IEEE Access* 10, 5768–5789. doi:10.1109/access.2022.3141079

Aleti, A., Buhnova, B., Grunske, L., Koziolek, A., and Meedeniya, I. (2012). Software architecture optimization methods: a systematic literature review. *IEEE Trans. Softw. Eng.* 39 (5), 658–683. doi:10.1109/tse.2012.64

Alhasan, B., Qatawneh, M., and Almobaideen, W. (2021). "Blockchain technology for preventing counterfeit in health insurance," in *2021 international conference on information technology (ICIT)* (IEEE), 935–941.

Alruwaill, M. N., Mohanty, S. P., and Kougianos, E. (2023). "Forti-Ins: a blockchain based framework to automate healthcare insurance processing in smart cities," in *2023 IEEE international symposium on smart electronic systems (iSES)*. Ahmedabad, India, 353–358. doi:10.1109/iSES58672.2023.00078

Alsdorf, G., and Berkun, J. (2024). Is blockchain the next big thing for insurance companies? *Reuters*. Accessed October 9, 2024. Available online at: https://www.reuters.com/legal/legalindustry/is-blockchain-next-big-thing-insurance-companies-2024-10-09/.

Amofa, S., Xia, Q., Xia, H., Obiri, I. A., Adjei-Arthur, B., Yang, J., et al. (2024). Blockchain-secure patient digital Twin in healthcare using smart contracts. *PLoS One* 19 (2), e0286120. doi:10.1371/journal.pone.0286120

Amponsah, A. A., Adekoya, A. F., and Weyori, B. A. (2022). A novel fraud detection and prevention method for healthcare claim processing using machine learning and blockchain technology. *Decis. Anal. J.* 4, 100122. doi:10.1016/j.dajour.2022.100122

Andre, H., Dewi, A. K., Pangemanan, F., and Wang, G. (2019). Designing blockchain to minimize fraud in state-owned national insurance company (BPJS Kesehatan). *Int. J. Emerg. Trends Eng. Res.* 7 (12), 794–797. doi:10.30534/ijeter/2019/117122019

Andrew, J., Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y., and Eunice, J. (2023). Blockchain for healthcare systems: architecture, security challenges, trends and future directions. *J. Netw. Comput. Appl.* 215, 103633. doi:10.1016/j.jnca.2023.103633

Arbabi, M. S., Lal, C., Veeraragavan, N. R., Marijan, D., Nygård, J. F., and Vitenberg, R. (2023). A survey on blockchain for healthcare: challenges, benefits, and future directions. *IEEE Commun. Surv. Tutorials* 25 (1), 386–424. doi:10.1109/COMST.2022.3224644

Atadoga, A., Elufioye, O. A., Omaghomi, T. T., Akomolafe, O., Odilibe, I. P., and Owolabi, O. R. (2024). Blockchain in healthcare: a comprehensive review of applications and security concerns. *Int. J. Sci. Res. Archive* 11 (1), 1605–1613. doi:10.30574/ijsra.2024.11.1.0244

Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). "MedRec: using blockchain for medical data access and permission management," in *Proceedings of the 2nd international conference on open and big data (OBD)* (IEEE), 25–30.

Azbeg, K., Ouchetto, O., and Andaloussi, S. J. (2022). Egyptian informatics journal.

Bae, S., and Yi, B.-K. (2022). Development of eClaim system for private indemnity health insurance in South Korea: compatibility and interoperability. *Health Inf. J.* 28 (1), 14604582211071019. doi:10.1177/14604582211071019

Barton, J., Kindberg, T., and Sadalgi, S. (2002). Physical registration: configuring electronic directories using handheld devices. *IEEE Wirel. Commun.* 9 (1), 30–38. doi:10.1109/mwc.2002.986456

Bhamidipati, N. R., Vakkavanthula, V., Stafford, G., Dahir, M., Neupane, R., Bonnah, E., et al. (2021). "Claimchain: secure blockchain platform for handling insurance claims processing," in *2021 IEEE international conference on blockchain (Blockchain)* (IEEE), 55–64.

Bodemer, O. (2023). Transforming the insurance industry with blockchain and smart contracts: enhancing efficiency, transparency, and trust. *Authorea Prepr.*

Cate, M. (2025). *Leveraging blockchain for smart contract automation in insurance.*

Center for Telehealth and e-Health Law (CTeL) (2023). Blockchain in health insurance and data management. Available online at: https://www.ctel.org (Accessed August 30, 2025).

Chen, C.-L., Deng, Y.-Y., Tsaur, W.-J., Li, C.-T., Lee, C.-C., and Wu, C.-M. (2021). A traceable online insurance claims system based on blockchain and smart contract technology. *Sustainability* 13 (16), 9386. doi:10.3390/su13169386

Chen, C. L., Zheng, Y. M., Huang, D. C., Liu, L. C., and Chen, H. C. (2023). A blockchain and IPFS-based anticounterfeit traceable functionality of car insurance claims system. *J. Inf. Secur. Appl.* 66, 103110.

Chen, Y., Zhao, C., Xu, Y., and Nie, C. (2025). Year-over-year developments in financial fraud detection *via* deep learning: a systematic literature review. *arXiv Prepr. arXiv:2502.00201*. Available online at: https://arxiv.org/abs/2502.00201.

Chondrogiannis, E., Andronikou, V., Karanastasis, E., Litke, A., and Varvarigou, T. (2022). Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations. *Blockchain Res. Appl.* 3, 100049. doi:10.1016/j.bcra.2021.100049

Chouhan, A. S., Qaseem, M. S., Basheer, Q. M. A., and Mehdia, M. A. (2023). Blockchain based EHR system architecture and the need of blockchain inhealthcare. *Mater. Today Proc.* 80, 2064–2070. doi:10.1016/j.matpr.2021.06.114

Collomb, A., and Sok, K. (2016). Blockchain/distributed ledger technology (DLT): what impact on the financial sector? *Digiworld Econ. J.* (103).

de Aguiar, E. J., Faiçal, B. S., Krishnamachari, B., and Ueyama, J. (2020). A survey of blockchain-based strategies for healthcare. *ACM Comput. Surv.* 53 (2), 1–27. doi:10.1145/3376915

Dib, O., and Rababah, B. (2020). Decentralized identity systems: architecture, challenges, solutions and future directions. *Ann. Emerg. Technol. Comput. (AETiC)* 4 (5), 19–40. doi:10.33166/aetic.2020.05.002

Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P. S., Swaminathan, A., et al. (2020). ACTION-EHR: patient-centric blockchain-based electronic health record data management for cancer care. *J. Med. Internet Res.* 22 (8), e13598. doi:10.2196/13598

El-Samad, W., Adda, M., and Atieh, M. (2024). AI-driven data aggregation level smart contracts for blockchain healthcare insurance claims adjudication. *J. Med. Syst.* 48 (1), 5. doi:10.1007/s10916-023-01860-7

Eletter, S. F. (2024). The use of blockchain in the insurance industry: a bibliometric analysis. *Insur. Mark. Co.* 15 (1), 12–29. doi:10.21511/ins.15(1).2024.02

Gropper, A. (2016). *Powering the physician-patient relationship with HIE of one blockchain health IT*. U.S. Department of Health and Human Services. Available online at: https://www.healthit.gov/sites/default/files/7-29-poweringthephysician-patientrelationshipwithblockchainhealthit.pdf.

Haque, M. E., and Tozal, M. E. (2022). Negative insurance claim generation using distance pooling on positive diagnosis-procedure bipartite graphs. *ACM J. Data Inf. Qual.* 14, 1–26. doi:10.1145/3531347

Harrell, D. T., Usman, M., Hanson, L., Abdul-Moheeth, M., Desai, I., Shriram, J., et al. (2022). Technical design and development of a self-sovereign identity management platform for patient-centric health care using blockchain technology. *Blockchain Healthc. Today* 5, 10–30953. doi:10.30953/bhty.v5.196

He, Q., Feng, Z., Fang, H., Wang, X., Zhao, L., Yao, Y., et al. (2023). A blockchain-based scheme for secure data offloading in healthcare with deep reinforcement learning. *IEEE/ACM Trans. Netw.* 31 (6), 2345–2358. Available online at: https://dl.acm.org/doi/10.1109/TNET.2023.3274631.

Hu, S., Schmidt-Kraepein, M., Thiebes, S., and Sunyaev, A. (2024). Mapping distributed ledger technology characteristics to use cases in healthcare: a structured literature review. *ACM Trans. Comput. Healthc.* 5 (3), 1–33. doi:10.1145/3653076

Islayem, R., Gebreab, S., AlKhader, W., Musamih, A., Salah, K., Jayaraman, R., et al. (2025). Using large language models for enhanced fraud analysis and detection in blockchain based health insurance claims. *Sci. Rep.* 15, 29763. doi:10.1038/s41598-025-15676-4

Ismail, L., and Zeadally, S. (2021). Healthcare insurance frauds: taxonomy and blockchain-based detection framework (Block-HI). *IT Prof.* 23 (4), 36–43. doi:10.1109/mitp.2021.3071534

Joshi, M., Pal, A., and Sankarasubbu, M. (2022). Federated learning for healthcare domain pipeline, applications and challenges. *ACM Trans. Comput. Healthc.* 3 (4), 1–36. doi:10.1145/3533708

Karmakar, A., Ghosh, P., Banerjee, P. S., and De, D. (2023). ChainSure: agent-free insurance system using blockchain for healthcare 4.0. *Intelligent Syst. Appl.* 17, 200177. doi:10.1016/j.iswa.2023.200177

Karmakar, A., Ghosh, P., Banerjee, P. S., and De, D. (2024). Intelligent systems with applications.

Kasyapa, M. S. B., and Vanmathi, C. (2024). Blockchain integration in healthcare: a comprehensive investigation of use cases, performance issues, and mitigation strategies. *Front. Digital Health* 6, 1359858. doi:10.3389/fdgth.2024.1359858

Khan, A. A., Wagan, A. A., Laghari, A. A., Gilal, A. R., Aziz, I. A., and Talpur, B. A. (2022). BIoMT: a state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts. *IEEE Access* 10, 78887–78898. doi:10.1109/access.2022.3194195

Khatun, M., Islam, R. A., and Islam, S. (2022). B-SAHIC: a blockchain based secured and automated health insurance claim processing system. *J. Intelligent Fuzzy Syst.* 44 (3), 4869–4890. doi:10.3233/JIFS-220690

Kitchenham, B. A. (2012). "Systematic review in software engineering: where we are and where we should be going," in *Proceedings of the 2nd international workshop on evidential assessment of software technologies* (ACM), 1–2.

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., and Linkman, S. (2009). Systematic literature reviews in software engineering–a systematic literature review. *Inf. Softw. Technol.* 51 (1), 7–15. doi:10.1016/j.infsof.2008.09.009

Kolhe, S. (2019). *Blockchain-based smart contracts for business process automation*.

Lin, W.-Y., Tai, K.-Y., and Lin, F. Y.-S. (2023). A trustable and secure usage-based insurance policy auction mechanism and platform using blockchain and smart contract technologies. *Sensors* 23 (14), 6482. doi:10.3390/s23146482

Liu, M., Wu, K., and Xu, J. J. (2019). How will blockchain technology impact auditing and accounting: permissionless *versus* permissioned blockchain. *Curr. Issues Auditing 1* 13 (2), A19–A29. doi:10.2308/ciia-52540

Liu, P., Yuan, W., Fu, J., Jiang, Z., Hayashi, H., and Neubig, G. (2023). Pre-train, prompt, and predict: a systematic survey of prompting methods in natural language processing. *ACM Comput. Surv.* 55 (9), 1–35. doi:10.1145/3560815

Lu, W., Lu, Y., Li, J., Sigov, A., Ratkin, L., and Ivanov, L. A. (2024). Quantum machine learning: classifications, challenges, and solutions. *J. Industrial Inf. Integration* 42, 100736. doi:10.1016/j.jii.2024.100736

Mahammad, A. B., and Kumar, R. (2023). "Scalable and security framework to secure and maintain healthcare data using blockchain technology," in *2023 international conference on computational intelligence and sustainable engineering solutions (CISES)* (IEEE), 417–423.

Mali, M., Pophale, V., Gulalkari, S., Deshpande, T., and Chougale, P. (2024). "IPFS-blockchain technology for health insurance Fraud Prevention and wellness incentives," in *2024 IEEE international conference on blockchain and distributed systems security (ICBDS)* (IEEE), 1–7.

Merlo, V., Pio, G., Giusto, F., and Bilancia, M. (2023). On the exploitation of the blockchain technology in the healthcare sector: a systematic review. *Expert Syst. Appl.* 213, 118897. doi:10.1016/j.eswa.2022.118897

Narne, H. (2024). Machine learning for health Insurance Fraud detection: techniques, insights, and implementation strategies. *Int. J. Res. Anal. Rev.*

Nchinda, N., Cameron, A., Retzepi, K., and Lippman, A. (2019). "MedRec: a network for personal information distribution," in *2019 international conference on computing, networking and communications (ICNC)* (IEEE), 637–641.

Nelaturu, K., Du, H., and Le, D.-P. (2022). A review of blockchain in fintech: taxonomy, challenges, and future directions. *Cryptography* 6 (2), 18. doi:10.3390/cryptography6020018

Ng, W. Y., Tan, T. E., Movva, P. V., Fang, A. H. S., Yeo, K. K., Ho, D., et al. (2021). Blockchain applications in health care for COVID-19 and beyond: a systematic review. *Lancet Digital Health* 3 (12), e819–e829. doi:10.1016/s2589-7500(21)00210-7

Nguyen, D. C., Pham, Q.-V., Pathirana, P. N., Ding, M., Seneviratne, A., Lin, Z., et al. (2021). Federated learning for smart healthcare: a survey. *ACM Comput. Surv.* 1 (1), 1–37. doi:10.1145/3501296

Nowrozy, R., Ahmed, K., Kayes, A. S. M., Wang, H., and McIntosh, T. R. (2024). Privacy preservation of electronic health records in the modern era: a systematic survey. *ACM Comput. Surv.* 56 (8), 1–37. doi:10.1145/3653297

Okoampah, E., Takyi, K., Gyening, R. M. O. M., Owusu-Agyemang, K., and Drah, K. (2023). *Adoption of blockchain technology to streamline the claims settlement in the health insurance industry in Ghana*.

Omoseebi, A., Bennett, L., and Hughes, A. (2023). *A comprehensive framework for ensuring HIPAA compliance in health insurance claims using blockchain technology*

Pingili, R. (2025). AI-driven intelligent document processing for healthcare and insurance. *Int. J. Sci. Res. Archive*.

PR Newswire (2019a). *Aetna, Anthem, Health Care Service Corporation, PNC Bank, and IBM announce collaboration to establish blockchain-based ecosystem for the healthcare industry*.

PR Newswire (2019b). Aetna, Anthem, and HCSC collaborate on blockchain health network. Available online at: https://www.prnewswire.com.

PR Newswire (2019c). Blockchain consortium aims to improve healthcare transparency. Available online at: https://www.prnewswire.com.

PR Newswire (2019d). Insurers launch blockchain initiative to share health data securely. Available online at: https://www.prnewswire.com.

PR Newswire (2019e). Blockchain network to enhance patient data security and accuracy. Available online at: https://www.prnewswire.com.

Protection, F. D. (2018). *General data protection regulation (GDPR)*. Intersoft Consulting.

Reddick, C. G., and Turner, M. (2012). Channel choice and public service delivery in Canada: comparing e-government to traditional service delivery. *Gov. Inf. Q.* 29 (1), 1–11. doi:10.1016/j.giq.2011.03.005

Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., et al. (2023). Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability* 15 (8), 6337. doi:10.3390/su15086337

ResearchGate (2022). Blockchain-based electronic prescription systems. Available online at: https://www.researchgate.net.

Romero Ugarte, J. L. (2018). *Distributed ledger technology (DLT): introduction. Banco de Espana Article, 19, 18*.

Shaikh, M., Memon, S. A., Ebrahimi, A., and Wiil, U. K. (2025). A systematic literature review for blockchain-based healthcare implementations. *Healthcare* 13 (9), 1087. doi:10.3390/healthcare13091087

Sharma, V., Gupta, A., Hasan, N. U., Shabaz, M., and Ofori, I. (2022). Blockchain in secure healthcare systems: state of the art, limitations, and future directions. *Secur. Commun. Netw.* 2022, 1–15. doi:10.1155/2022/9697545

Shaw, G., and Eckenrode, J. (2016). *Blockchain in health and life insurance: turning a buzzword into a breakthrough*. Deloitte Insights. Available online at: https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/blockchain-in-insurance.html.

Shen, L., Zhang, Z., Zhou, Y., and Xu, Y. (2023). Applying blockchain technology and the internet of things to improve the data reliability for livestock insurance. *Sensors* 23 (14), 6290. doi:10.3390/s23146290

Singh, Y., Jabbar, M. A., Shandilya, S. K., Vovk, O., and Hnatiuk, Y. (2023). Exploring applications of blockchain in healthcare: road map and future directions. *Front. Public Health* 11, 1229386. doi:10.3389/fpubh.2023.1229386

Singhal, N., Goyal, S., and Singhal, T. (2024). *Potential, risks, and ethical implications of decentralized insurance*. Palgrave Macmillan.

Sookhak, M., Jabbarpour, M. R., Safa, N. S., and Yu, F. R. (2021). Blockchain and smart contract for access control in healthcare: a survey, issues and challenges, and open issues. *J. Netw. Comput. Appl.* 178, 102950. doi:10.1016/j.jnca.2020.102950

Sukhwani, H., Martínez, J. M., Chang, X., Trivedi, K. S., and Rindos, A. (2017). "Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)," in *2017 IEEE 36th symposium on reliable distributed systems (SRDS)* (IEEE), 253–255.

Taloba, A. I., Rayan, A., Elhadad, A., Abozeid, A., Shahin, O. R., and Abd El-Aziz, R. M. (2021). A framework for secure healthcare data management using blockchain technology. *Int. J. Adv. Comput. Sci. Appl.* 12 (12) 951–961. doi:10.14569/IJACSA.2021.0121280

Villarreal, E. R. D., García-Alonso, J., Moguel, E., and Alegría, J. A. H. (2023). Blockchain for healthcare management systems: a survey on interoperability and security. *IEEE Access* 11, 5629–5652. doi:10.1109/access.2023.3236505

Vorisek, C. N., Lehne, M., Klopfenstein, S. A. I., Mayer, P. J., Bartschke, A., Haese, T., et al. (2022). Fast healthcare interoperability resources (FHIR) for interoperability in health research: systematic review. *JMIR Med. Inf.* 10 (7), e35724. doi:10.2196/35724

Wang, L., Jiang, S., Shi, Y., Du, X., Xiao, Y., Ma, Y., et al. (2023a). Blockchain-based dynamic energy management mode for distributed energy system with high penetration of renewable energy. *Int. J. Electr. Power Energy Syst.* 148, 108933. doi:10.1016/j.ijepes.2022.108933

Wang, X., Li, H., Yi, L., Ning, Z., Tao, X., Guo, S., et al. (2023b). A survey on off-chain networks: frameworks, technologies, solutions and challenges. *ACM Comput. Surv.* 57, 1–35. doi:10.1145/3735124

Wenhua, Z., Qamar, F., Abdali, T.-A. N., Hassan, R., Jafri, S. T. A., and Nguyen, Q. N. (2023). Blockchain technology: security issues, healthcare applications, challenges and future trends. *Electronics* 12 (3), 546. doi:10.3390/electronics12030546

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., and Guizani, M. (2017). MeDShare: trust-less medical data sharing among cloud service providers *via* blockchain. *IEEE Access* 5, 14757–14767. doi:10.1109/ACCESS.2017.2730843

Yang, L., Hou, Q., Zhu, X., Lu, Y., and Xu, L. D. (2025). Potential of large language models in blockchain-based supply chain finance. *Enterp. Inf. Syst.* 2541199. doi:10.1080/17517575.2025.2541199

Ye, Z., and Lu, Y. (2022). Quantum science: a review and current research trends. *J. Manag. Anal.* 9 (3), 383–402. doi:10.1080/23270012.2022.2089064

Zhang, H., and Lu, Y. (2025). Web 3.0: Applications, opportunities and challenges in the next internet generation. *Syst. Res. Behav. Sci.* doi:10.1002/sres.3273