A SURVEY OF BLOCKCHAIN APPLICATIONS IN HEALTH INSURANCE

Yisong Chen [1] and Chuqing Zhao [2]

[1] College of Computing, Georgia Institute of Technology, Atlanta, GA. US
[2] School of Engineering and Applied Sciences, Harvard University, Cambridge, MA. US

ABSTRACT

This paper examines blockchain's role in health insurance, particularly in fraud prevention, claims processing, and data security. By integrating blockchain with AI and IoT, we highlight its potential to enhance transparency, automation, and interoperability. Key findings demonstrate improvements in fraud detection, regulatory compliance, and operational efficiency, while challenges such as scalability and regulatory alignment remain. This study 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, Hybrid blockchain, Scalability, Patient-centric systems

1. INTRODUCTION

Effective coordination among patients, providers, and insurers is essential in the health insurance industry to ensure seamless data exchange and timely updates. However, claims submission, adjudication, and payment face persistent challenges, including data silos, fraud, inefficiencies, and compliance with regulations like HIPAA and GDPR, limiting transparency and operational efficiency.

Blockchain technology presents a decentralized, tamper-proof solution to these issues, enhancing trust, transparency, and efficiency in insurance workflows. By eliminating centralized intermediaries, blockchain enables secure, validated data exchanges through consensus mechanisms, making it particularly valuable for fraud prevention, security, and compliance in health insurance.

Key innovations such as smart contracts automate claims adjudication and payments, reducing administrative delays and errors. Additionally, integrating blockchain with AI and IoT enhances fraud detection, real-time monitoring, and data-driven decision-making, driving operational improvements.

Despite its benefits, scalability, energy efficiency, legacy system integration, and regulatory alignment remain barriers to adoption. Addressing these challenges requires technological advancements and stakeholder collaboration.

David C. Wyld et al. (Eds): ADCO, CMCA, NeCoM, NLPI, CSITEC, BDBS, DMML, SP – 2025
pp. 217-231, 2025. CS & IT - CSCP 2025 DOI: 10.5121/csit.2025.150517

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.

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. 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 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

This study employed a systematic review approach to analyze the application of blockchain technology in health insurance. Searches were conducted across PubMed, Scopus, ACM Digital Library, and ScienceDirect using the keywords: healthcare + insurance + blockchain. From the initial 307 articles retrieved, duplicates were removed, and a rigorous screening process was applied. A final set of 26 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.
- 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.

The initial search across all databases retrieved 304 papers. After removing duplicates and rigorously applying the inclusion and exclusion criteria, 39 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 26 high-quality papers that aligned with the review's objectives and standards. The selection process is illustrated in Figure 1 below.

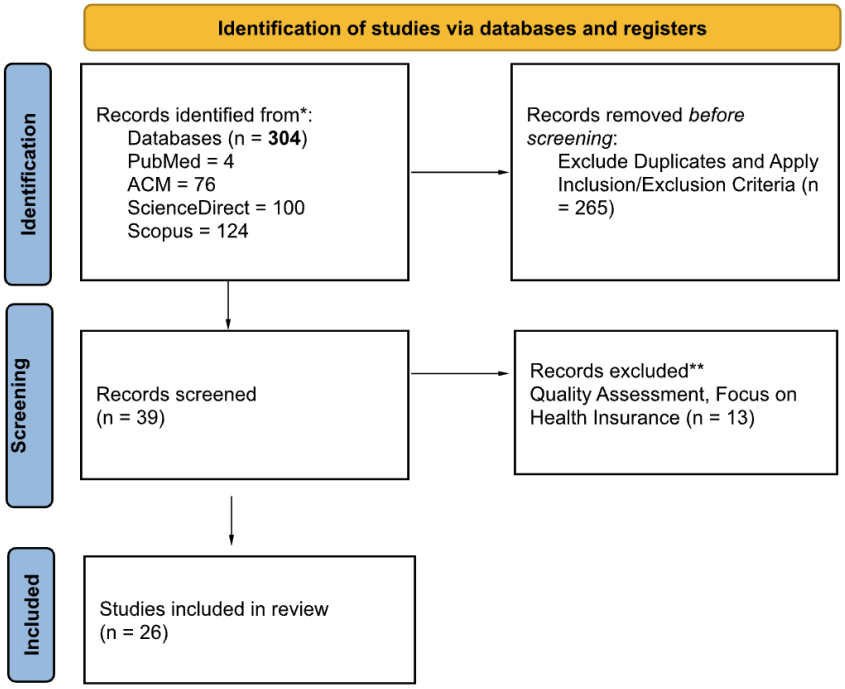

Figure 1. Systematic Literature Selection Process for Blockchain in Health Insurance

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.

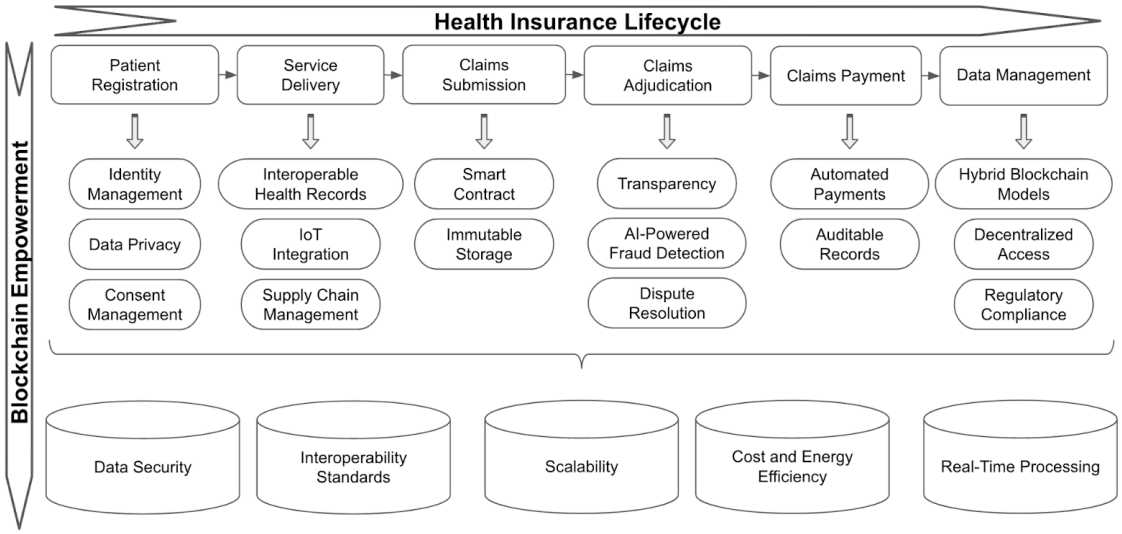

Figure 2. Health Insurance Lifecycle with Blockchain Applications

We also quantitatively explored the keywords co-occurrence in blockchain papers using VOSviewer, a bibliometric analysis software in Figure 3.

4.1. Patient Registration

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[1].

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[2]. In blockchain-based EHR systems, each account address ID is unique and can function as the primary key, streamlining record management and access control[6].

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[3].

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[16]. Once consent is granted, other operators on the blockchain may create tailored financial or medical services based on the approved data[4]. 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[14]. 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)[9].

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[29]. Similarly, MedRec system was proposed by MIT researchers and provides a secure way of patient registration [30].

4.2. Service Delivery

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[19]. A real-world example is Robomed, which captures patient data via blockchain and securely distributes it to the healthcare professionals[18]. 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) devices further revolutionizes service delivery by enabling real-time health monitoring and secure data collection[2] and enhances data reliability[17]. Smart contracts enhance IoT integration by facilitating real-time patient monitoring and automated notifications for hospitals and patients via a secure, blockchain-backed platform[21]. 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) 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[11]. Furthermore, DLT's decentralized framework enables real-time tracking and verification of medical products, mitigating counterfeiting risks, supply chain fraud, and unauthorized diversions[8]. 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 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.

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. 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[5]. 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 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.

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[27]. 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[28].

4.4. Claims Adjudication

Blockchain revolutionizes claims adjudication by enhancing transparency, enabling AIpowered fraud detection, and streamlining dispute resolution[5]. 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[13].

AI-powered fraud detection further strengthens the process by leveraging blockchain's immutable records to analyze patterns, detect anomalies, and flag potential fraud[5]. 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[10]. Additionally, smart contracts automatically enforce policy terms, reducing processing delays and ensuring fair and consistent outcomes for all stakeholders.

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[13].

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[10]. This accelerates claim settlement, 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[10].

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[26]. 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[1].

Regulatory compliance is seamlessly integrated into blockchain's architecture. HIPAA regulations define standards for secure data exchange, covering healthcare plans, providers, clearinghouses, and business associates[8]. Additionally, GDPR mandates that users must be informed about collected data, even when sourced indirectly[9]. 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[22]. By leveraging blockchain's immutable records, machine learning models can identify fraudulent patterns, optimize risk assessment, and enhance decision-making in health insurance operations[20]. 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[12].

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[18]. By enabling real-time, permissioned data sharing, Avaneer Health seeks to reduce administrative inefficiencies, lower costs, and improve overall healthcare interoperability.

Table 1 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.

Table 1. Comparison of Traditional vs. Blockchain-Based Health Insurance Processes

Processes	Traditional Approach	Blockchain-Based Approach
Patient Registration	**- Identity issues:** Data duplication & 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 & hard to retrieve. **- Manual verification:** Slow processes. **- Security risks:** Prone to tampering & unauthorized access.	**- Tamper-proof records:** Immutable blockchain data. **- Real-time access:** Faster, efficient care. **- Smart contracts:** Automate verification.
Claims Submission	**- Slow processing:** Manual & 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.

Processes	Traditional Approach	Blockchain-Based Approach
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 & decentralized. **- Patient ownership:** Users control access. **- Automated compliance:** Smart contracts enforce rules.

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 3 also shows that AI and data related nodes (i.e. ”AI drive application”, ”data security”, ”data authenticity”) are widely connected to other health care and insurance domains.

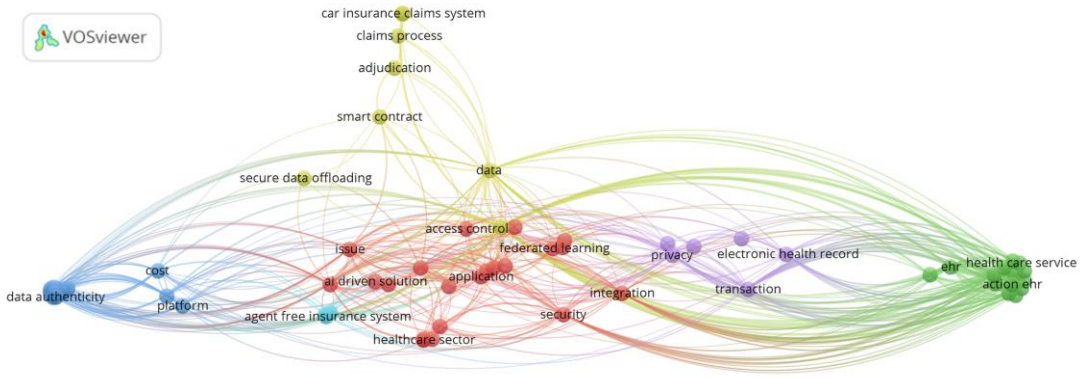

Figure 3. Network Analysis for Keyword Co-occurrence in Blockchain Papers

5. 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.

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 [7], 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 [23]. 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, 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[18]. To enhance data security and provenance, the MeDShare system employs four-layer system architecture—comprising the User Layer, Data Query Layer, Data Structuring & Provenance Layer, and Existing Database Infrastructure Layer— to ensure secure access, structured processing, authenticated transactions, and immutable record-keeping[25]. 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[24]. 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[15] 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.

6. 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.

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.

7. CONCLUSIONS

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.

ACKNOWLEDGEMENTS

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.

REFERENCES

[1] A. Dubovitskaya, F. Baig, Z. Xu, R. Shukla, P. S. Zambani, A. Swaminathan, M. M. Jahangir, K. Chowdhry, R. Lachhani, N. Idnani, M. Schumacher, K. Aberer, S. D. Stoller, S. Ryu, and F. Wang, "ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care," Journal of Medical Internet Research, vol. 22, no. 8, p. e13598, 2020.

[2] Q. He, Z. Feng, H. Fang, X. Wang, L. Zhao, Y. Yao, and K. Yu, "A blockchain-based scheme for secure data offloading in healthcare with deep reinforcement learning," IEEE/ACM Transactions on Networking, vol. 31, no. 6, pp. 2345–2358, Dec. 2023. [Online]. Available: https://dl.acm.org/doi/10.1109/TNET.2023.3274631

[3] C. L. Chen, Y. M. Zheng, D. C. Huang, L. C. Liu, and H. C. Chen, "A blockchain and IPFS-based anticounterfeit traceable functionality of car insurance claims system," Journal of Information Security and Applications, vol. 66, p. 103110, 2023.

[4] W.-Y. Lin, K.-Y. Tai, and F. Y.-S. Lin, "A trustable and secure usage-based insurance policy auction mechanism and platform using blockchain and smart contract technologies," Sensors, vol. 23, no. 14, p. 6482, 2023. [Online]. Available: https://doi.org/10.3390/s23146482

[5] W. El-Samad, M. Adda, and M. Atieh, "AI-driven data aggregation level smart contracts for blockchain healthcare insurance claims adjudication," Journal of Medical Systems, vol. 48, no. 1, p. 5, 2024. [Online]. Available: https://doi.org/10.1007/s10916-023-01860-7

[6] A. Karmakar, P. Ghosh, P. S. Banerjee, and D. De, "ChainSure: Agent-free insurance system using blockchain for healthcare 4.0," Intelligent Systems with Applications, vol. 17, p. 200177, 2023. [Online]. Available: https://doi.org/10.1016/j.iswa.2023.200177

[7] M. Abdelhamid, L. Sliman, R. Ben Djemaa, and G. Perboli, "A review on blockchain technology, current challenges, and AI-driven solutions," ACM Computing Surveys, vol. 57, no. 3, Article 73, pp. 1–39, 2024. [Online]. Available: https://doi.org/10.1145/3700641

[8] E. J. de Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," ACM Computing Surveys, vol. 53, no. 2, Article 27, pp. 1–27, 2020. [Online]. Available: https://doi.org/10.1145/3376915

[9] M. S. Arbabi, C. Lal, N. R. Veeraragavan, D. Marijan, J. F. Nygård, and R. Vitenberg, "A survey on blockchain for healthcare: Challenges, benefits, and future directions," IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 386–414, 2023. [Online]. Available: https://doi.org/10.1109/COMST.2022.3224644

[10] C.-L. Chen, Y.-Y. Deng, W.-J. Tsaur, C.-T. Li, C.-C. Lee, and C.-M. Wu, "A traceable online insurance claims system based on blockchain and smart contract technology," Sustainability, vol. 13, no. 16, p. 9386, 2021. [Online]. Available: https://doi.org/10.3390/su13169386

[11] S. Hu, M. Schmidt-Kraepein, S. Thiebes, and A. Sunyaev, "Mapping distributed ledger technology characteristics to use cases in healthcare: A structured literature review," ACM Transactions on Computing for Healthcare, vol. 5, no. 3, Article 15, pp. 1–33, 2024. [Online]. Available: https://doi.org/10.1145/3653076

[12] M. Joshi, A. Pal, and M. Sankarasubbu, "Federated learning for healthcare domain pipeline, applications and challenges," ACM Transactions on Computing for Healthcare, vol. 3, no. 4, Article 40, pp. 1–36, 2022. [Online]. Available: https://doi.org/10.1145/3533708

[13] M. S. B. Kasyapa and C. Vanmathi, "Blockchain integration in healthcare: A comprehensive investigation of use cases, performance issues, and mitigation strategies," Frontiers in Digital Health, vol. 6, p. 1359858, 2024. [Online]. Available: https://doi.org/10.3389/fdgth.2024.1359858

[14] V. Merlo, G. Pio, F. Giusto, and M. Bilancia, "On the exploitation of the blockchain technology in the healthcare sector: A systematic review," Expert Systems with Applications, vol. 213, p. 118897, 2023. [Online]. Available: https://doi.org/10.1016/j.eswa.2022.118897

[15] D. C. Nguyen, Q.-V. Pham, P. N. Pathirana, M. Ding, A. Seneviratne, Z. Lin, O. Dobre, and W.-J. Hwang, "Federated learning for smart healthcare: A survey," ACM Computing Surveys, vol. 1, no. 1, Article 1, pp. 1–35, 2021. [Online]. Available: https://doi.org/10.1145/nnnnnnn.nnnnnnn

[16] R. Nowrozy, K. Ahmed, A. S. M. Kayes, H. Wang, and T. R. McIntosh, "Privacy preservation of electronic health records in the modern era: A systematic survey," ACM Computing Surveys, vol. 56, no. 8, Article 204, pp. 1–37, 2024. [Online]. Available: https://doi.org/10.1145/3653297

[17] L. Shen, Z. Zhang, Y. Zhou, and Y. Xu, "Applying blockchain technology and the internet of things to improve the data reliability for livestock insurance," Sensors, vol. 23, no. 14, p. 6290, 2023. [Online]. Available: https://doi.org/10.3390/s23146290

[18] Y. Singh, M. A. Jabbar, S. K. Shandilya, O. Vovk, and Y. Hnatiuk, "Exploring applications of blockchain in healthcare: Road map and future directions," Frontiers in Public Health, vol. 11, p. 1229386, 2023. [Online]. Available: https://doi.org/10.3389/fpubh.2023.1229386

[19] M. Sookhak, M. R. Jabbarpour, N. S. Safa, and F. R. Yu, "Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues," Journal of Network and Computer Applications, vol. 178, p. 102950, 2021. [Online]. Available: https://doi.org/10.1016/j.jnca.2020.102950

[20] Y. Chen, C. Zhao, Y. Xu, and C. Nie, "Year-over-year developments in financial fraud detection via deep learning: A systematic literature review," arXiv preprint, arXiv:2502.00201, 2025. [Online]. Available: https://arxiv.org/abs/2502.00201

[21] A. I. Taloba, A. Rayan, A. Elhadad, A. Abozeid, O. R. Shahin, and R. M. Abd El-Aziz, "A framework for secure healthcare data management using blockchain technology," International Journal of Advanced Computer Science and Applications, vol. 12, no. 12, 2021. [Online]. Available: https://doi.org/10.14569/IJACSA.2021.0121280

[22] M. E. Haque and M. E. Tozal, "Negative insurance claim generation using distance pooling on positive diagnosis-procedure bipartite graphs," ACM Journal of Data and Information Quality, vol. 14, no. 3, Article 17, pp. 1–26, 2022. [Online]. Available: https://doi.org/10.1145/3531347

[23] V. Sharma, A. Gupta, N. U. Hasan, M. Shabaz, and I. Ofori, "Blockchain in secure healthcare systems: State of the art, limitations, and future directions," Security and Communication Networks, vol. 2022, Article ID 9697545, 15 pages, 2022. [Online]. Available: https://doi.org/10.1155/2022/9697545

[24] E. Chondrogiannis, V. Andronikou, E. Karanastasis, A. Litke, and T. Varvarigou, "Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations," Blockchain: Research and Applications, vol. 3, p. 100049, 2022. [Online]. Available: https://doi.org/10.1016/j.bcra.2021.100049

[25] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14757–14767, 2017. [Online]. Available: https://doi.org/10.1109/ACCESS.2017.2730843

[26] A. Gropper, "Powering the physician-patient relationship with HIE of One blockchain health IT," U.S. Department of Health and Human Services, 2016. [Online]. Available: https://www.healthit.gov/sites/default/files/7-29-poweringthephysician-patientrelationshipwithblockchainhealthit.pdf

[27] G. Shaw and J. Eckenrode, "Blockchain in health and life insurance: Turning a buzzword into a breakthrough," Deloitte Insights, 2016. [Online]. Available: https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/blockchain-in-insurance.html

[28] G. Alsdorf and J. Berkun, "Is blockchain the next big thing for insurance companies?" Reuters, Oct. 9, 2024. [Online]. Available: https://www.reuters.com/legal/legalindustry/is-blockchain-next-big-thing-insurance-companies-2024-10-09/

[29] H. Andre, A. K. Dewi, F. Pangemanan, and G. Wang, "Designing blockchain to minimize fraud in state-owned national insurance company (BPJS Kesehatan)," International Journal of Emerging Trends in Engineering Research, vol. 7, no. 12, pp. 794–797, 2019. [Online]. Available: https://doi.org/10.30534/ijeter/2019/117122019

[30] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in Proceedings of the 2nd International Conference on Open and Big Data (OBD), IEEE, 2016, pp. 25–30.

AUTHORS

Yisong Chen, Senior Decision Scientist at CVS Health, specializes in healthcare cost management using AI. He holds an MA in Econometrics from New York University and is pursuing an MS in Computer Science at Georgia Institute of Technology.

Chuqing Zhao, Data Scientist at Walmart Inc, specializes in customer behavior analysis using AI techniques. She holds an MS in Data Science from Harvard University.