

A REPORT
ON
BLOCKCHAIN TECHNOLOGY IN HEALTHCARE
In partial fulfilment for the award of the degree of
BACHELOR OF TECHNOLOGY
In
INFORMATION TECHNOLOGY
Submitted by
POLI VARDHINI REDDY (21BIT0382)
R VINAY KUMAR (21BIT0484)
P LOKESH (21BIT0405)
Submitted to
Prof. Priya V
Slot : TAA1



**SCHOOL OF COMPUTER SCIENCE ENGINEERING AND INFORMATION
SYSTEMS**

VIT UNIVERSITY, VELLORE, 632014

March 2023

S NO.	TITLE AND SUBTITLES	PAGE NO.
1.	ABSTRACT	3
2.	INTRODUCTION	3-4
3.	OVERVIEW OF BLOCKCHAIN	5-7
4.	OPERATIONS OF BLOCKCHAIN	7-8
5.	USE CASES OF HEALTHCARE BLOCKCHAIN	9-11
6.	SECURITY AND PRIVACY CHALLENGES	11-12
7.	PERFORMANCE EVALUATION METRICS OF HEALTHCARE BLOCKCHAIN	13
8.	DISCUSSIONS, CHALLENGES AND RESEARCH OPPORTUNITIES	14
9.	CONCLUSION	15
10.	REFERENCES	16

Abstract

Blockchain technology has surged in popularity, underpinning cryptocurrencies like Bitcoin, Ethereum, and Ripple, while offering a robust platform for decentralization and trust across various domains including finance, commerce, IoT, reputation systems, and healthcare. This surge is primarily due to blockchain's ability to maintain data integrity across a decentralized network, making transactions transparent and tamper-proof. The decentralized nature of blockchain not only fosters trust but also enables varied applications, each benefiting from the technology's inherent security and transparency features.

Implementing blockchain in healthcare poses challenges due to strict regulations like HIPAA, which require rigorous authentication and record-sharing standards. This article explores blockchain's application in healthcare, focusing on how it can improve interoperability. It details blockchain's operation in healthcare, including the use of consensus algorithms vital for data integrity and confidentiality. The discussion also covers different blockchain architectures and platforms, helping to identify the best fit for healthcare needs.

The article reviews current blockchain research and applications in healthcare, addressing the technology's scalability, resilience, security, and privacy challenges. It outlines future research areas and performance metrics needed for blockchain's growth in healthcare. Additionally, it examines blockchain-specific security threats, analyzing threat models and protection strategies. Recommendations for improving blockchain network security and privacy are given, offering a detailed guide for those implementing this technology in healthcare settings.

1. Introduction

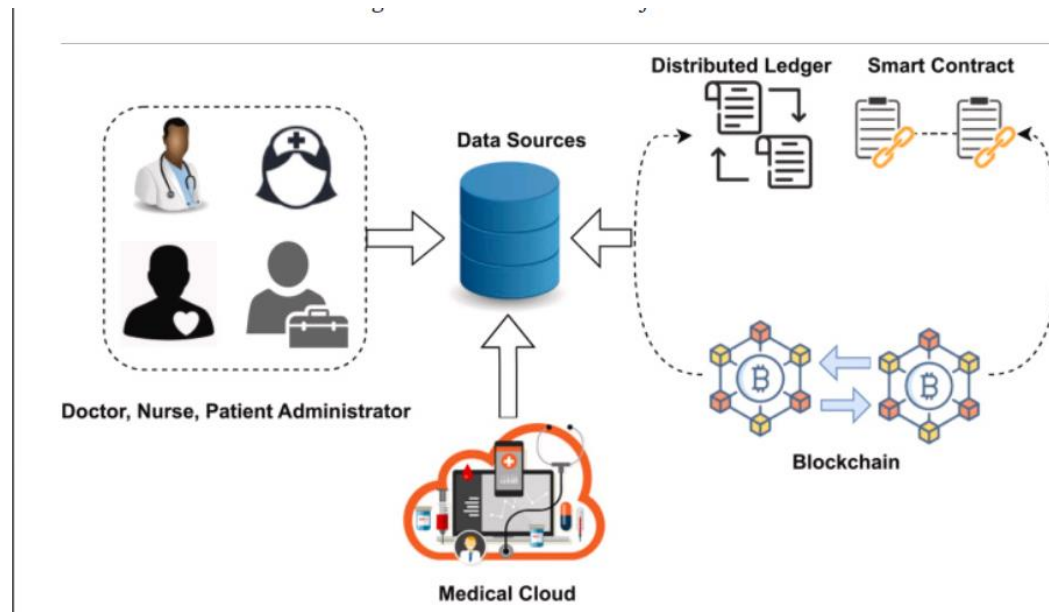
Blockchain technology holds significant promise for transforming the healthcare industry by addressing critical issues such as data security, interoperability, and patient privacy.

1. **Data Security and Integrity:** Healthcare data is highly sensitive and valuable, containing personal information, medical records, and billing details. Traditional centralized databases are vulnerable to breaches and cyberattacks. Blockchain offers a decentralized and tamper-resistant solution by storing data across a network of nodes. Each transaction is cryptographically linked to the previous one, ensuring the integrity of the data. This heightened security reduces the risk of unauthorized access and data manipulation.
2. **Interoperability:** Healthcare systems often struggle with interoperability, hindering the seamless exchange of patient information between different providers and systems. Blockchain facilitates interoperability by creating a unified and standardized platform for data sharing. With blockchain-based health records, patients can securely share their medical history with healthcare providers, regardless of the underlying electronic health record (EHR) system. This interoperability streamlines care coordination and improves patient outcomes.

3. **Patient-Centric Data Management:** Blockchain empowers patients to have greater control over their health data. Through encrypted keys and permissioned access, patients can grant or revoke access to their health records as needed. This ensures privacy and data sovereignty while enabling patients to actively participate in their healthcare decisions. Additionally, blockchain-based identity management solutions enhance patient authentication and prevent identity theft.
4. **Clinical Trials and Research:** Blockchain technology enhances transparency and traceability in clinical trials and research studies. Smart contracts automate the execution of agreements between researchers, patients, and sponsors, ensuring compliance with study protocols and data sharing agreements. By securely recording trial data on the blockchain, researchers can verify the authenticity and integrity of results, accelerating the drug development process and promoting scientific collaboration.
5. **Supply Chain Management:** The pharmaceutical supply chain is complex, involving multiple stakeholders and regulatory requirements. Blockchain enables end-to-end visibility and traceability of pharmaceutical products, from manufacturing to distribution and delivery. By recording each transaction on the blockchain, stakeholders can track the movement of drugs, verify their authenticity, and detect counterfeit products. This transparency enhances patient safety and regulatory compliance.
6. **Healthcare Payments and Billing:** Blockchain technology simplifies healthcare payments and billing processes by automating claim adjudication, reducing administrative overhead, and minimizing fraud. Smart contracts facilitate transparent and verifiable payment agreements between payers, providers, and patients, ensuring timely and accurate reimbursement. Additionally, blockchain-based tokenization enables new models of value-based care and incentivizes positive health outcomes.

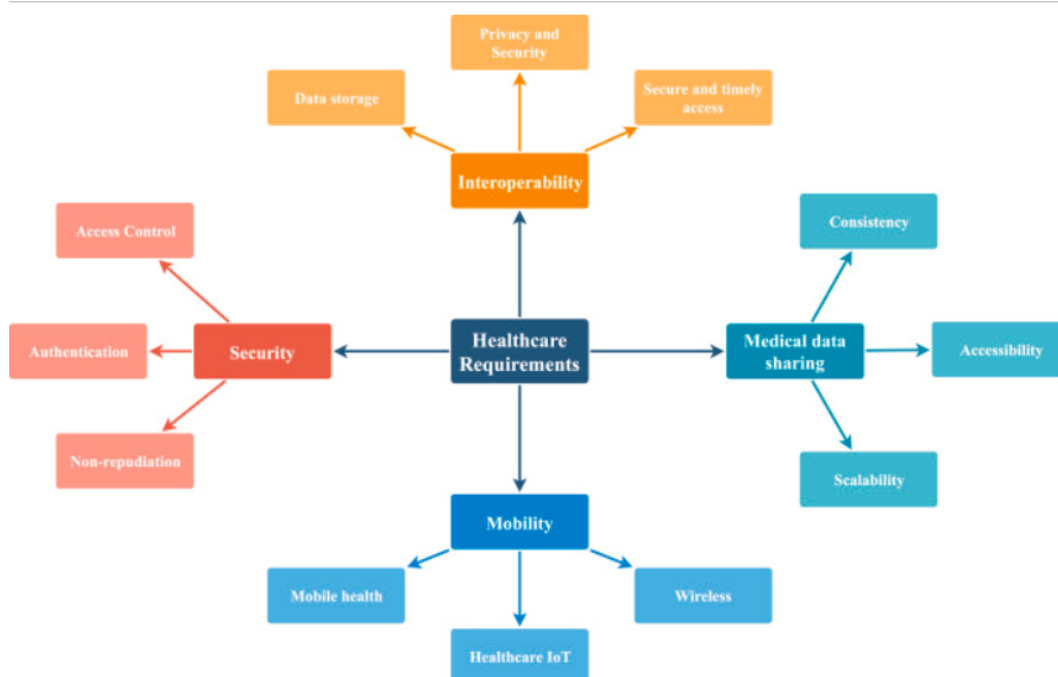
In summary, blockchain technology has the potential to revolutionize healthcare by improving data security, interoperability, patient-centricity, and efficiency across the industry. While still in its early stages of adoption, ongoing research and pilot projects demonstrate the transformative impact of blockchain on healthcare delivery, research, and management.

2. Overview of blockchain



2.1 Blockchain in Healthcare

Blockchain technology in healthcare offers a secure and efficient way to manage and share medical records. By creating an immutable, decentralized ledger of patient data, it ensures that information is accessible only to authorized individuals, enhancing both privacy and data security. This system also facilitates seamless communication between different healthcare providers, allowing for more accurate diagnoses and timely treatments. Furthermore, blockchain can streamline administrative processes, reducing costs and increasing the overall efficiency of healthcare services.



2.2 Blockchain user requirements

In healthcare, blockchain technology is tailored to meet several crucial user requirements. First, it ensures the security and privacy of sensitive patient data by enabling secure, tamper-proof storage and sharing. This helps in complying with strict regulations like HIPAA. Second, blockchain enhances interoperability among various healthcare systems, allowing seamless access and exchange of patient records across different providers and facilities. This is crucial for improving treatment continuity and accuracy. Additionally, blockchain can facilitate the verification of medical credentials, streamline billing processes, and support health data analytics by providing a reliable and immutable data source. Overall, these capabilities aim to increase trust and efficiency in healthcare services, benefiting both providers and patients.



2.2.2 Security

At every stage of hospital operation, the Healthcare system is in charge of managing enormous amounts of data generation, information sharing, storage, and analysis. It delivers strong, multi-layered security to all data transfers to the cloud and adopts other cutting-edge digital technologies for safeguarding the system against information loss or misuse. The platform often adheres to the strictest data security and privacy regulations imposed by a nation. The hospital system is shielded against hacks because it is hosted on cloud-based servers that are situated outside of the facilities. Overall, blockchain-based healthcare system encourages openness, safeguards privacy, guard against data theft and provide a safe and secure environment for hospitals to continue operating. Creating a blockchain network between two healthcare organizations allows organizations to communicate data over a distributed database with Hyperledger without requiring each user to have trust in every other user. Additionally, it enables the quick, secure, and transparent interchange of medical transactions.

2.2.3 Performance

Many processes are streamlined and integrated by blockchain-based healthcare systems greatly boosts the system's speed, agility, and efficiency. It improves a healthcare facility's performance and patient-treatment capacities because of its intra-operability and flexibility. The platform features are specifically created for a variety of tasks, including management of OPDs, IPDs and diagnostics, emergency care response, invoicing and payments, and operations. The system can grant role-based control to users, enabling them to access a single function or a number of them, and assisting in the monitoring and tracking of all activities required for the provision of healthcare.

2.2.4 Reliability

The blockchain-based healthcare system is extremely resilient to any technological disruptions, downtime, or breakdowns experienced by other technological systems. From the perspective of data security, it is quite secure and has an intuitive and sophisticated user interface that makes them simple to use. Its upkeep tasks can be divided into pre-scheduled intervals based on when they are least demanding, and upgrading doesn't require much time. The medical records are remotely updated and enhanced without impairing the daily routine activities. The availability of the system and resources at all times is crucial for the success of the system.

2.2.5 Interoperability

Patient consent, governance, security, privacy, and patient participation are just a few of the issues that the move towards patient-centered interoperability raises. By providing a framework for the safe exchange of data, blockchain technology provides an alluring approach to overcoming these difficulties. In summary, blockchain offers a high-level framework for how a patient may communicate securely with several stakeholders, identify themselves across each institution, and aggregate their health data in a durable manner.

2.2.6 Access Control

A doctor should request consent from the patient before accessing the patient's medical records. The system will deny access if the doctor's actions are not taken otherwise. Similar to this, a doctor should personally inquire with a patient about granting a regular access privilege if they wish to obtain one. For the patient, this means that he must first provide permission for any access to his medical records. The patient can also independently grant temporary access and grant or remove any access privileges for or from other users of the system.

3. Operations of blockchain

Blockchain operations primarily involve securely storing and sharing patient data across a network of authorized participants. Each block in the blockchain contains a record of transactions, which could include anything from patient health updates to treatment records. Once a transaction is entered, it is encrypted and linked to the previous block, forming a chain. This linkage ensures that each entry is tamper-proof and permanent. For data to be added to the blockchain, consensus must be reached

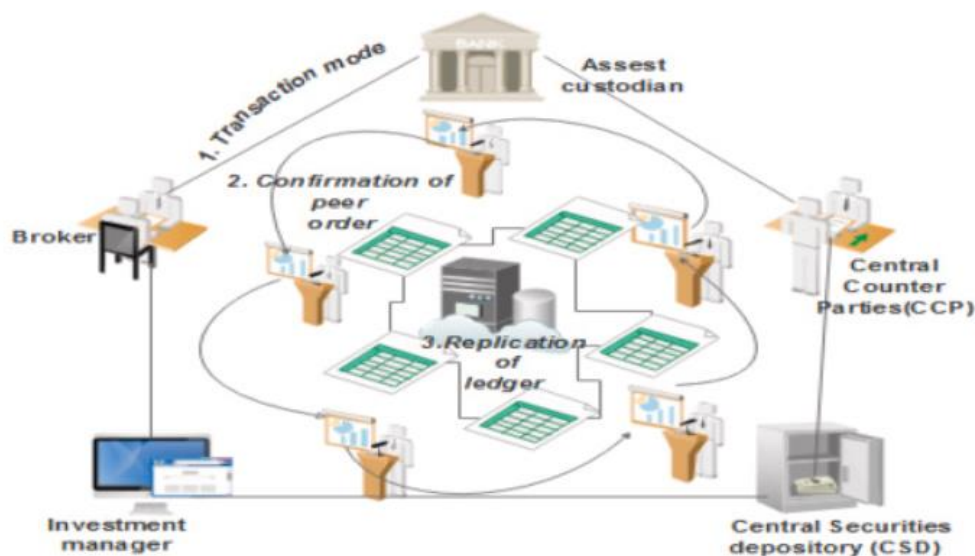
among all participating nodes (computers) in the network, which verifies the authenticity of the data. This decentralized verification mechanism enhances security and prevents unauthorized access, making patient data safer and more reliable. Moreover, blockchain enables real-time, transparent, and immutable data access, which is crucial for accurate diagnosis, treatment, and billing in healthcare.

3.1 Working model of Blockchain

Blockchain technology offers significant enhancements to trade finance services by utilizing a decentralized, cryptographic peer-to-peer network. It provides a secure platform for digital transactions, eliminating the need for intermediaries and enabling direct exchanges of goods and services. This technology ensures traceability and security for user transactions and cryptocurrencies. Moreover, blockchain faces challenges like ensuring security, scalability, and performance in real-time applications. However, its ability to facilitate transparent transactions has the potential to transform the trade industry by reducing vulnerabilities traditionally associated with central authorities.

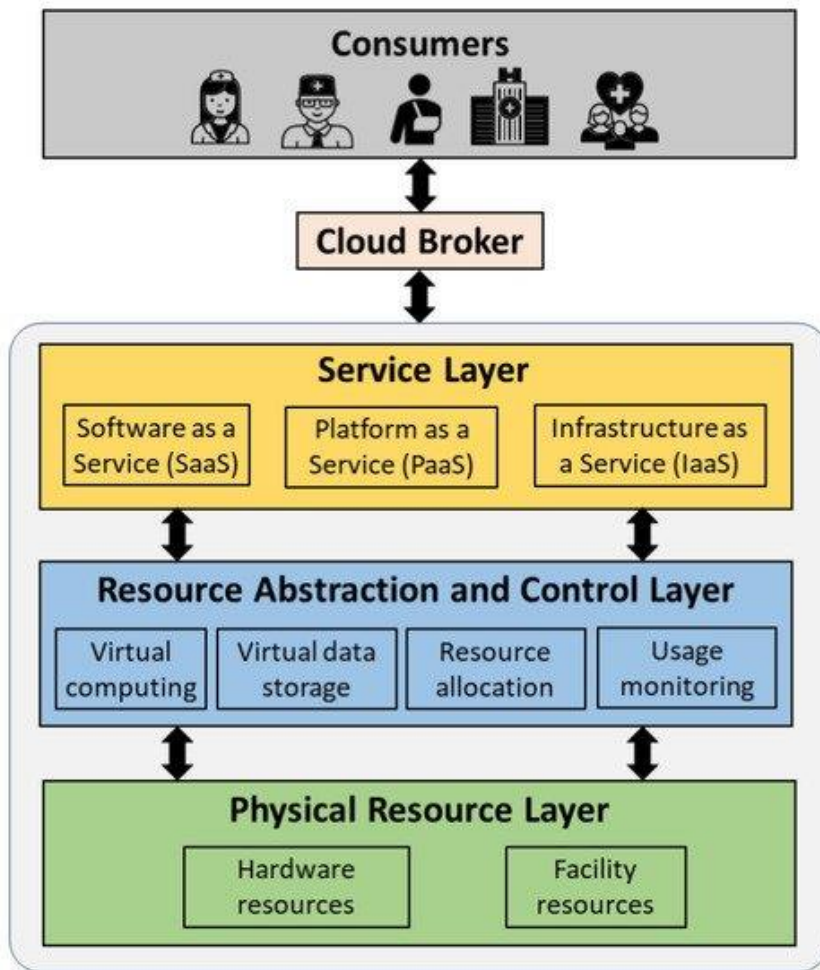
The working of blockchain can be summarized in four steps. They are.

- 1. The transaction is executed
- 2. The transaction is verified and then validated
- 3. The transaction is stored in the block
- 4. The block is hashed and added to the blockchain



3.2. Architecture of blockchain

To understand the working of blockchain technology, a layered approach is followed. The architectural layers are more generalized to suit the diversity of any application. To attract more customers, the business that requires high scalability and reliability can utilize the blockchain to improve its services.



4. Use cases of healthcare blockchain

4.1 Patient data management

Blockchain technology is increasingly utilized in healthcare for managing patient data, aiming to enhance security and reduce costs. It securely stores medical records electronically, manages patient appointments, handles billing, and records lab tests within electronic health record (EHR) systems. Blockchain ensures that these medical records are safe, cannot be tampered with, and can be shared across different healthcare platforms. It maintains a complete and secure history of a patient's medical records, accessible by patients, doctors, hospitals, insurance companies, and regulatory bodies. This decentralized record-keeping method provides a comprehensive, secure, and easily shareable way to manage health information.

4.2 Drug Traceability

Blockchain technology is being used to tackle the issue of counterfeit medications, which harm public health and pharmaceutical industries. Researchers like Musamih et al. (2021a) have developed a blockchain-based drug traceability system that uses smart contracts to securely and transparently track medications. This system allows stakeholders to interact through decentralized apps (dApps) and ensures safer drug transactions. Similarly, Tseng et al. (2018) created the G-coin blockchain to protect public health data and enhance transparency in drug transactions.

4.3 Cryptocurrency Payments

Cryptocurrency payments in healthcare offer several benefits due to the use of blockchain technology. This technology acts as a ledger that records all transactions, ensuring their authenticity. As a decentralized form of currency not controlled by banks or governments, cryptocurrency allows patients to make direct transactions without intermediaries like merchants or banks. This simplifies the billing process and reduces the need for approval from central authorities. Additionally, blockchain can verify the identities of patients participating in clinical activities, ensuring the validity of their details and the eligibility of transactions (Kombe et al., 2018).

4.4 Clinical Trials and data security

In clinical studies, it is critical to collect authentic and correct data. This is important to correlate, measure, and make analyses. Also, from the standpoint of a patient, it adds a layer of safety and security to the personally identifiable and sensitive information that a patient would be concerned about if it were breached into locations where identity theft may occur. Several studies have explored the importance of blockchain for clinical trials ([Jahankhani et al., 2019](#))– ([Omar et al., 2020](#)). From the beginning of the procedure, with registration and informed permission, to the release of results and drug administration, clinical trials are being made more transparently available with blockchain technology.

4.5 Device Tracking

Blockchain technology can significantly improve the tracking and management of medical devices in healthcare. Traditional methods struggle with locating equipment efficiently, especially in emergencies, leading to unnecessary repurchases and potential fraud. A blockchain-based system ensures that the location and history of medical devices are recorded immutably and securely, making them tamper-proof. This allows hospitals to easily locate equipment when needed, automate inventory processes, and ensure devices are used and stored properly, enhancing regulatory compliance and operational efficiency (Jafri and Singh, 2022).

4.6 Secure Healthcare Setups

Smart Healthcare has advanced to a high level of sophistication in terms of efficiently supplying and dictating medical health care to patients while maintaining the privacy of their data, as well as the process of presenting real-time accurate and trusted data to medical practitioners ([Chakraborty et al., 2019](#)). IoT has also performed admirably in the healthcare sector, facilitating simpler diagnosis and monitoring of patients.

4.7 Health Insurance: claims Processing

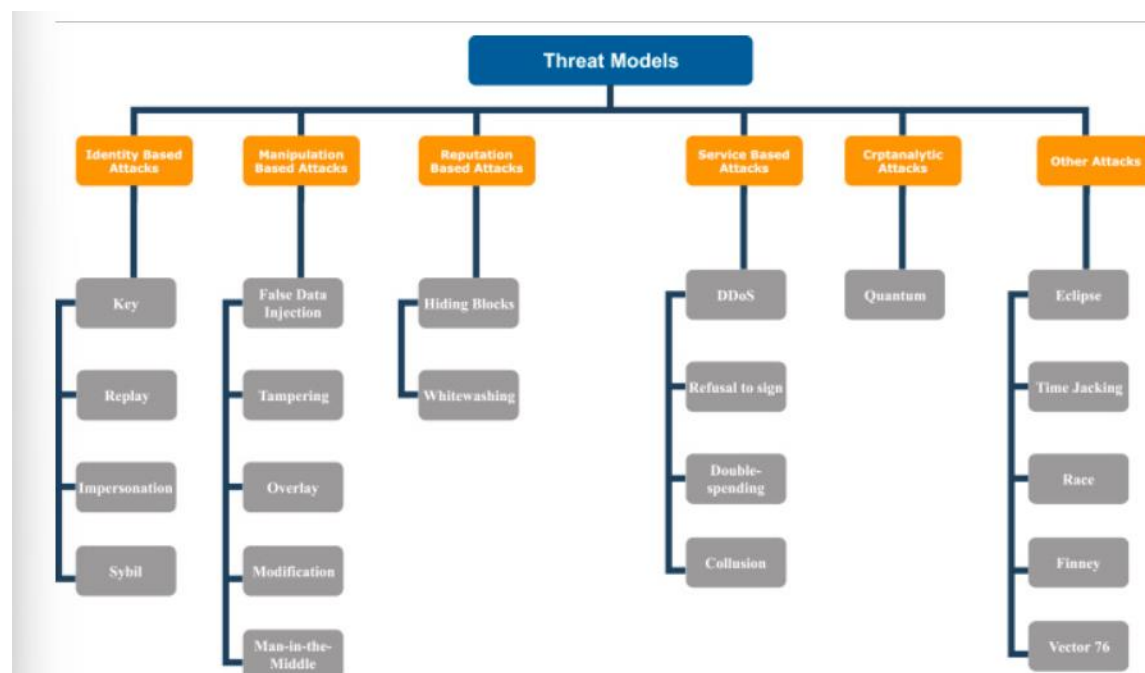
Health insurance is essential for managing the high costs associated with medical emergencies, providing financial security and peace of mind. However, the industry faces significant challenges with security, privacy, and fraud. These issues result in substantial losses, making the detection and prevention of fraudulent activities critical. Modern fintech systems, including those leveraging blockchain technology, offer solutions by using an immutable ledger to enhance transparency and reduce fraud risks. Blockchain enables more efficient claim processing by automatically verifying claims and applying contracts, thereby streamlining operations and bolstering trust between insurers and policyholders (Raikwar et al., 2018; Guo et al., 2018). This technology not only helps in managing assets and preventing fraud but also ensures the security of personal and commercial data.

4.8 Blockchain technology for Covid-19

The COVID-19 pandemic accelerated the integration of digital health technologies to manage its widespread impact, driving the medical community to develop innovative solutions. Key advancements included the deployment of reliable surveillance systems, the expansion of telehealth services, the enhancement of diagnostic and clinical tools, the use of wearables for monitoring health, and the launch of interactive services for public education on COVID-19 (Kapoor et al., 2020). Additionally, blockchain technology played a crucial role in addressing various challenges, such as improving the Healthcare Waste Management (HCWM) system to reduce environmental and public health impacts (Shah et al., 2021). These technologies collectively helped mitigate the pandemic's effects and improved overall healthcare response.

6. Security & privacy challenges

Blockchain technology is essentially secure. The data entered in blockchain cannot be changed or modified hence it is said to be more secure. Additionally, it has a very good consensus mechanism that is used to make a decision and cryptographic proofs that make the blockchain impossible to hack. Even though blockchain is very secure and impossible to hack it has some security issues. Some of the security attacks their effect, detection method, and how to protect them are presented and their explanation is listed below. Figure shows the taxonomy of the threat model for blockchain.



Security and privacy challenges are significant considerations in implementing blockchain technology in healthcare systems. Here are some of the key challenges:

1. Data Privacy: Protecting the privacy of sensitive healthcare data is paramount. Blockchain systems must ensure that patient information is securely stored and accessed only by authorized parties. However, achieving privacy while maintaining the transparency and immutability of the blockchain poses a challenge. Techniques such as data encryption, zero-knowledge proofs, and differential privacy can help address this challenge by allowing selective disclosure of information.

2. Identity Management: Establishing and managing identities on the blockchain securely is crucial for maintaining data integrity and preventing unauthorized access. Identity management solutions must address issues such as identity theft, impersonation, and ensuring the authenticity of participants in the network. Public-key cryptography and digital signatures are commonly used to manage identities in blockchain systems.

3. Data Confidentiality: In addition to protecting data privacy, ensuring data confidentiality is essential, especially in healthcare where sensitive patient information is involved. Blockchain systems need to employ robust encryption techniques to safeguard data against unauthorized access or disclosure, both on the blockchain itself and during data transmission.

4. Regulatory Compliance: Healthcare regulations, such as HIPAA in the United States and GDPR in the European Union, impose strict requirements on the handling and protection of patient data. Blockchain implementations in healthcare must comply with these regulations, which often include provisions related to data privacy, security, consent management, and data breach reporting. Achieving regulatory compliance while leveraging the benefits of blockchain technology requires careful design and implementation.

5. Network Security: Blockchain networks are susceptible to various security threats, including 51% attacks, Sybil attacks, and distributed denial-of-service (DDoS) attacks. Securing the network infrastructure, consensus mechanisms, and communication protocols is essential to prevent malicious actors from compromising the integrity and availability of the blockchain system.

6. Smart Contract Vulnerabilities: Smart contracts, which automate the execution of predefined agreements on the blockchain, are prone to vulnerabilities that can be exploited by attackers. Common smart contract vulnerabilities include reentrancy attacks, integer overflow/underflow, and logic errors. Thorough code review, testing, and the use of formal verification techniques can help mitigate these vulnerabilities.

7. Interoperability Challenges: Integrating blockchain-based healthcare systems with existing IT infrastructure and ensuring interoperability with external systems pose challenges. Data exchange standards, such as FHIR and HL7, help facilitate interoperability, but technical and semantic interoperability issues may still arise, particularly when dealing with disparate systems and data formats.

Addressing these security and privacy challenges requires a multi-faceted approach, involving a combination of cryptographic techniques, secure software development practices, regulatory compliance measures, and ongoing monitoring and auditing of blockchain systems. Collaboration among stakeholders, including healthcare providers, technology vendors, regulators, and cybersecurity experts, is essential to develop and deploy blockchain solutions that effectively address the security and privacy needs of the healthcare industry.

7. Performance evaluation metrics of healthcare blockchain

1. **Transaction Throughput:** Transaction throughput refers to the number of transactions processed by the blockchain network per unit of time (e.g., transactions per second or TPS). Higher transaction throughput indicates better scalability and the ability to handle increased workload, which is crucial for healthcare systems processing a large volume of transactions, such as electronic health record (EHR) systems or claims processing platforms.
2. **Latency:** Latency measures the time it takes for a transaction to be confirmed and added to the blockchain. Low latency is desirable in healthcare applications where real-time access to data and timely execution of transactions are critical, such as in emergency medical situations or medication administration. Minimizing latency enhances the responsiveness of the blockchain system and improves user experience.
3. **Consensus Overhead:** Consensus overhead refers to the computational resources required to achieve consensus among network participants. This includes the time and energy expended by nodes in validating transactions, reaching agreement on the next block, and maintaining the integrity of the blockchain. Minimizing consensus overhead helps improve the overall efficiency and sustainability of the blockchain network, particularly in permissionless (public) blockchain systems.
4. **Resource Consumption:** Resource consumption metrics include factors such as CPU usage, memory utilization, disk space, and network bandwidth required to operate the blockchain network. Optimizing resource consumption is essential for minimizing operational costs, maximizing system efficiency, and ensuring the sustainability of healthcare blockchain implementations, particularly in resource-constrained environments such as edge computing devices or mobile platforms.
5. **Data Storage Efficiency:** Data storage efficiency measures the space required to store data on the blockchain, including transaction records, smart contracts, and other metadata. Efficient data storage mechanisms help reduce storage costs, improve system performance, and mitigate scalability challenges associated with storing large volumes of healthcare data on the blockchain. Techniques such as data compression, pruning, and off-chain storage can enhance data storage efficiency while maintaining data integrity and accessibility.
6. **Security and Privacy Metrics:** Security and privacy metrics assess the robustness of the blockchain system against various threats, including unauthorized access, data tampering, and privacy breaches. Key security and privacy metrics include cryptographic strength, resistance to attacks, compliance with regulatory requirements (e.g., HIPAA, GDPR), and adherence to best practices for secure software development and deployment.

8. Discussions, challenges & research opportunities

Discussions, challenges, and research opportunities in healthcare blockchain are diverse and continually evolving. Here are some key areas for consideration:

1. **Interoperability:** Achieving interoperability between different blockchain platforms and legacy healthcare systems remains a significant challenge. Research is needed to develop standardized protocols, data formats, and interoperability frameworks that facilitate seamless data exchange and integration across heterogeneous healthcare IT environments.
2. **Privacy-Preserving Techniques:** Enhancing privacy protections while maintaining the transparency and auditability of blockchain-based healthcare systems is a critical area of research. Techniques such as zero-knowledge proofs, homomorphic encryption, and differential privacy offer promising avenues for preserving patient confidentiality and data privacy in healthcare blockchain applications.
3. **Scalability and Performance Optimization:** Improving the scalability and performance of blockchain networks to accommodate the growing volume of healthcare data and transactions is essential. Research efforts focus on developing scalable consensus mechanisms, off-chain scaling solutions, and optimization techniques to enhance transaction throughput, reduce latency, and minimize resource consumption in healthcare blockchain systems.
4. **Regulatory Compliance and Governance:** Research is needed to navigate the complex regulatory landscape governing healthcare data privacy, security, and interoperability. Developing governance frameworks, compliance mechanisms, and regulatory guidance tailored to blockchain-based healthcare systems can help foster trust, ensure accountability, and facilitate regulatory compliance across different jurisdictions.
5. **User Experience and Adoption:** Improving the user experience and fostering user adoption of blockchain-based healthcare solutions are critical challenges. Research efforts focus on user-centric design principles, intuitive interfaces, and educational initiatives to increase awareness, acceptance, and engagement among healthcare professionals, patients, and other stakeholders.
6. **Real-World Use Cases and Validation:** Conducting empirical studies and real-world implementations of blockchain technology in healthcare settings are essential for validating its efficacy, identifying best practices, and assessing its impact on clinical outcomes, patient care, and healthcare delivery. Research collaborations between academia, industry, and healthcare providers can facilitate the design, deployment, and evaluation of blockchain-based healthcare applications in diverse healthcare domains.

Overall, addressing these discussions, challenges, and research opportunities requires interdisciplinary collaboration, leveraging expertise from fields such as computer science, healthcare informatics, cryptography, regulatory compliance, and human-computer interaction. By advancing the state-of-the-art in healthcare blockchain research, we can unlock the full potential of blockchain technology to revolutionize healthcare delivery, improve patient outcomes, and transform the healthcare ecosystem.

9. Conclusion

Blockchain technology holds significant promise for enhancing data security, integrity, and sharing in the healthcare industry. It creates a decentralized and tamper-proof ledger system that ensures the safety and authenticity of medical records. However, the integration of emerging technologies like IoT and smart devices in healthcare raises concerns about vulnerabilities that could be exploited by malicious actors, leading to issues such as data breaches and misdiagnosis. Despite these challenges, blockchain offers potential solutions by providing patients with greater control over their medical data, allowing them to share it securely with healthcare providers.

Nonetheless, blockchain is not a one-size-fits-all solution and requires careful consideration of its application within the healthcare sector. Issues such as mining incentives, the risk of specific blockchain attacks, and overestimation of its capabilities need thorough exploration. Furthermore, while blockchain ensures the security of the data stored on it, it does not guarantee the accuracy of the data entered, which can still be influenced by human error or malicious intent. This is particularly concerning in cases involving vulnerable populations, where consent and data access could be manipulated.

The adoption of blockchain in healthcare also faces practical hurdles, including a shortage of skilled professionals and the high cost of hiring blockchain experts. Combining blockchain with AI could potentially elevate healthcare standards by making services more efficient and reducing costs. As blockchain continues to evolve, increasing awareness and training in blockchain technology will be crucial for maximizing its benefits in healthcare.

10. References

1. [Abdellatif et al., 2021](#)

A.A. Abdellatif, *et al.*

MEdge-chain: leveraging edge computing and blockchain for efficient medical data exchange

IEEE Internet Things J., 8 (21) (2021), pp. 15762-15775, [10.1109/JIOT.2021.3052910](#)

[View at publisher_](#)

[View in Scopus](#)[Google Scholar](#)

2. [Abou El Houda et al., 2022](#)

Z. Abou El Houda, A.S. Hafid, L. Khoukhi, B. Brik

When collaborative federated learning meets blockchain to preserve privacy in healthcare

IEEE Trans. Netw. Sci. Eng. (2022), pp. 1-11, [10.1109/TNSE.2022.3211192](#)

[View at publisher_](#)

[Google Scholar](#)

3. [Agbo et al., 2019](#)

C. Agbo, Q. Mahmoud, J. Eklund

Blockchain technology in healthcare: a systematic review

Healthcare, 7 (2) (2019), p. 56, [10.3390/healthcare7020056](#)

Apr