FMDB *Transactions on Sustainable Technoprise Letters*

Implementation of Blockchain Technology Across International Healthcare Markets

Ela Vashishtha[1,*], Himanshu Kapoor[2]

[1]Master of Health Administration, Texas Health Resources, Texas, USA.
[2]Master of Science in Engineering, Product Management and Strategy Leader, University of Washington, Seattle, USA.
elavashishtha@texashealth.org[1], kapoor91@uw.edu[2],

Abstract: Blockchain in healthcare is expected to reach USD 14.25 billion by 2032, growing 34.02 percent from 2023 to 2032. Data breaches and the need for effective solutions fuel this growth. Health data management, pharmaceutical counterfeiting, and strategic measures drive healthcare blockchain usage. IBM, Athenahealth, and Allscripts see Blockchain's potential, while the Synaptic Health Alliance facilitates data interchange. Medical system and blockchain technology investments should boost market growth. Public healthcare data management networks provide most blockchain market revenue. Privacy, rapid transactions, and increased security will fuel private network growth. Pharma supply chain management ensures data integrity, interoperability, and regulatory compliance. Data management and security are expected to improve with clinical trials and eConsent. The biopharmaceutical and medical device sector lead end-users, followed by hospitals. Europe dominates the market, while North America is demanding secure medical record management. Blockchain technology may improve healthcare record security and efficiency. Its combination with AI and IoT has transformed healthcare, improving EHR management, remote patient monitoring, and precision medicine. Telemedicine and fog monitoring systems use blockchain for remote patient monitoring and big data analytics. Blockchain, federated learning, explainable AI, and 5G/6G networks have improved drug development and Intelligent Telesurgery technologies. Deep learning is used for secure image transfer and healthcare cyberattack defence.

Keywords: Blockchain; Internet of Things (IoT); Healthcare Technology; Artificial Intelligence (AI); Data Management; Global Healthcare; Health Records; Cyber Security; Healthcare Security; Interoperability; Medical Supply Chain.

Received on: 27/10/2022, **Revised on:** 16/12/2022, **Accepted on:** 03/02/2023, **Published on:** 07/03/2023

Cited by: E. Vashishtha and H. Kapoor, "Implementation of Blockchain Technology Across International Healthcare Markets," *FMDB Transactions on Sustainable Technoprise Letters*., vol. 1, no. 1, pp. 1–12, 2023.

1. Introduction

In 2021, the United States national health expenditure accounted for 18.3% of its Gross Domestic Product (GDP). With the continuously rising healthcare costs, there is a pressing need for disruptive solutions to limit these expenses. One potential technology with disruptive potential is Blockchain. Originally developed for the cryptocurrency Bitcoin, Blockchain is a decentralized transaction and data management technology [1]. What sets Blockchain apart is its capacity to integrate, secure, and validate data without the involvement of third parties in transactions. This results in efficient data transfer at minimal costs. So, how does it work? Let's delve into an example to better understand this technology.

[*]Corresponding author.

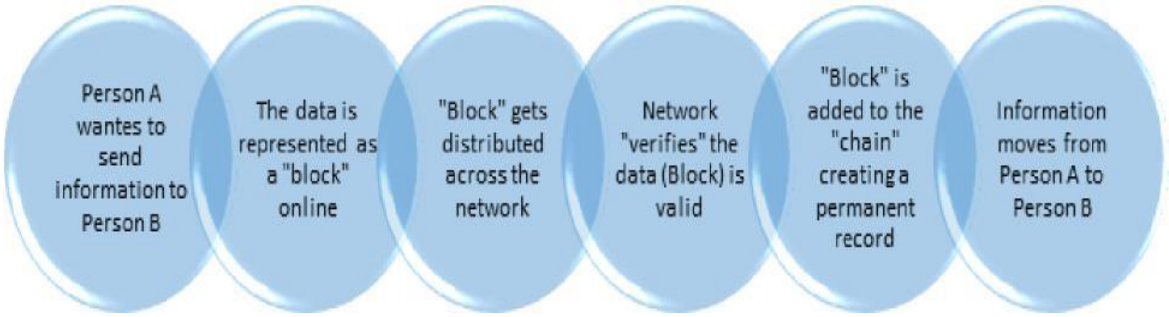

Figure 1: Process how information flows from Person A to Person B in blockchains

In the given time frame (fig.1), data is sent safely from person A to person B within a verified and coordinated setting. As a technical matter, Blockchain can be thought of as a distributed database system that keeps a growing list of data records confirmed by participating nodes. This means businesses can validate their data internally rather than relying on third-party vendors. Blockchain also assures that all transactions are public and easy to access, which greatly increases the trustworthiness of the system.

1.1. Types of Blockchains

There are three main classifications of Blockchains that may be made based on the data type and the intended use by the participating organisation [2].

- In a permissionless public blockchain, anyone can use the technology.
- Consortium (public authorization) - restricts network participation in the distributed consensus process to an authorised group of nodes.
- Only selected nodes are allowed to join the network in a private mode.

1.2. Market Overview of Blockchain in Healthcare

In 2022, the global Blockchain in healthcare market was valued at $0.76 billion, but by 2032, that number is projected to rise to $14.25 billion, representing a compound annual growth rate (CAGR) of 34.02 percent (table 1).

Table 1: Forecasted blockchain healthcare market [3]

No.	Forecast Year	USD in Billion
1.	2022	$0.76 billion
2.	2023	$1.02 billion
3.	2024	$1.30 billion
4.	2025	$1.83 billion
5.	2026	$2.46 billion
6.	2027	$3.29 billion
7.	2028	$4.41 billion
8.	2029	$5.92 billion
9.	2030	$7.93 billion
10.	2031	$10.63 billion
11.	2032	$14.25 billion

The proliferation of data leaks and breaches (fig.2), as well as the rising importance of addressing them, have helped propel the sector forward. Strategic steps taken by key stakeholders, the requirement for effective health data management systems, and the fight against drug counterfeiting are all driving forces behind the widespread deployment of blockchain technology in healthcare.

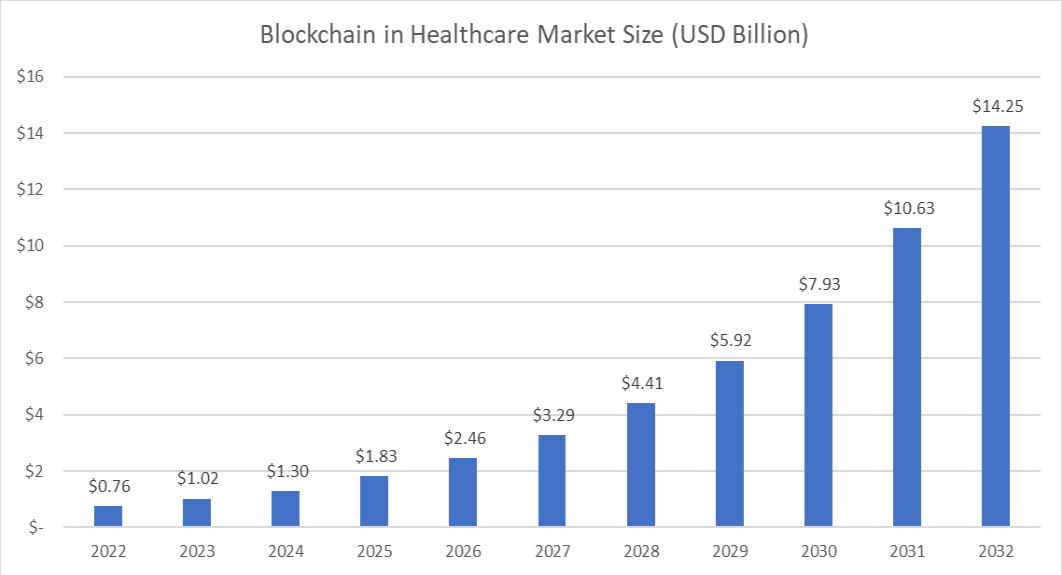

Figure 2: Graph showing a 10-year forecasted trend for global blockchain market in healthcare [3]

In order to verify the legitimacy of immunisation records, MDS Mexico (A Medical Services company), for instance, implemented a COVID-19 testing service in October 2021 using blockchain technology. The COVID-19 epidemic has increased the need for and interest in blockchain-based healthcare solutions. Although Blockchain is still in its infancy as a technology, many industry players have presented use cases and proposals to promote its adoption and enhance health results. IBM's Rapid Supplier Connect was introduced in April of 2020. This blockchain-based network will bring together hospitals, governments, and alternative equipment and supply companies to combat the effects of the COVID-19 pandemic. Blockchain was used by Chinese hospitals to track drugs and ensure prompt delivery to COVID-19 patients' homes.

Research Foundry is a revolutionary blockchain application created by the OECD (Organization for Economic Cooperation and Development) that streamlines rights and consent management for the exchange and accessibility of health data, metadata, software code, and other parts of healthcare R&D (Research and Development). Moreover, the healthcare business is poised to reap the benefits of increased expenditures in building efficient medical examination systems, wearable device cryptography, and healthcare record systems.

Blockchain technology is important to the corporate world, according to HMS (Health Management Systems) Holdings. Prominent IT companies' ancillary technology suppliers have been involved in industry talks. Companies like Athenahealth, Allscripts, and Cerner are showing interest in the healthcare industry. Market growth is anticipated to be spurred by the widespread adoption of blockchain technology in the healthcare industry.

To improve communication amongst healthcare providers, leading institutions have formed the Synaptic Health Alliance. The alliance's founding members include three well-established healthcare providers: Quest Diagnostics, Humana, and Optum. Synaptic claims that blockchain technology can improve healthcare efficiency and lower costs in a number of different ways. Diseases are becoming more common, which means more data is being generated, which in turn increases the need for efficient data management. Blockchain technology can be used to create immutable and trustworthy medical records. The market has been given a boost by the increased investments of major players in the industry. In March 2018, for example, IBM released a cheap platform for companies to use in developing blockchain applications. Efforts like these are likely to increase the number of healthcare businesses using Blockchain and accelerate technological progress in the industry.

2. Global Market Insights on Blockchain Utilization in Healthcare

2.1. Insights on Network Types

In terms of income, government agencies generated 57% of the total worldwide blockchain market in 2022. Private, governmental, and other forms of networks are all used in the healthcare sector. The growing use of public networks for data management is a major factor in the public sector's commanding market share. Ethereum is a public network, or "permission-less" blockchain system, that is frequently used in the healthcare industry. The growth of these public networks is primarily motivated by the low cost and ready availability of massive databases [3].

There will likely be a lot of expansion in the private sector in the future years. One such implementation of a private network is the Linux Foundation's Hyperledger Fabric. Private networks are well-suited to the unique requirements of businesses because of the increased privacy, the speed of transactions, and the heightened security they provide. Recording capabilities, effective data management, and rising demand for highly secure supply chain networks are all factors in the expansion of the private sector. It is projected that the usage of Blockchain in healthcare would be further fueled by future technological breakthroughs.

2.2. Insights on Applications

In 2022, supply chain management will account for more than 26 percent of the healthcare industry's blockchain technology market share. Pharmaceutical firms can improve interoperability with IoT devices and maintain the integrity of their data with the help of blockchain technologies. They help with clinical trial recruitment and drug supply chain regulation as well. Blockchain has the potential to change the healthcare business by lowering operational costs, eliminating data corruption, and expediting processes.

It is anticipated that the clinical trials and eConsent areas would expand rapidly in the next years. When applied to clinical studies, blockchain technology enhances both data management and security. In addition, it allows doctors to communicate with one another in a safe, private environment. Blockchain's inability to be altered protects the accuracy of any recorded data. The same ideas are applicable to clinical trials, where record-keeping must adhere to strict guidelines to avoid breaking the law.

2.3. Insights on End-Users

In 2022, the biopharmaceutical and medical device industry accounted for about 41 percent of the market share among end-users. These sectors devote significant resources to R&D and have a need for the interoperability, security, and effective management of massive data sets related to drug discovery and development. Their large share of the market is attributable, in large part, to the widespread adoption of blockchain technology for use in authenticating drug authenticity, safeguarding pharmaceutical supply chain integrity, combating counterfeiting, guaranteeing transparency and traceability in clinical trials, and improving the accuracy and reliability of clinical trial data.

As hospitals like the Massachusetts General Hospital (MGH) implement blockchain technology, this market is projected to expand rapidly. Effective patient data storage, streamlined patient classification, and leveraging of historical records to back up doctor's appointments are all priorities for hospitals and healthcare facilities. Information such as credit card numbers, addresses, and phone numbers are safe within the system since it is encrypted and protected from data breaches and hackers.

2.4. Regional Insights

In 2022, Europe's 36 percent market share was the highest, thanks in large part to the region's governments' efforts to proactively prevent data breaches. Along with the meteoric rise of blockchain technology, the European Union's (EU) implementation of the General Data Protection Regulation (GDPR) in 2018 has opened up numerous doors for regional firms. The demand for safe medical record keeping in North America is predicted to make the region the second largest market.

Although there are still problems with EMRs, the U.S. healthcare sector is investing more in cutting-edge technologies. In response to the increased demand for secure and managed data sharing between enterprises, major players and healthcare organisations are entering the blockchain sector. The April 2018 cooperation between UnitedHealth Group, Quest Diagnostics, MultiPlan, and Humana to use Blockchain's safe information sharing capabilities is one example that will contribute to the expansion of the business.

2.5. Key Players on Global Scale

The global market is fiercely competitive, with various factors driving its growth, including government initiatives, emerging startups, significant company activities, and collaborations between technology and healthcare organizations. As the industry is still in its early stages, extensive research is being conducted to explore the potential applications of Blockchain across different levels. Several key players have formed partnerships and engaged in strategic acquisitions to enhance their platforms and portfolios.

An example of such collaboration is Change Healthcare's acquisition of PokitDok in December 2018. This move aimed to leverage PokitDok's blockchain technology and use cases to expand the capabilities of Change Healthcare's Intelligent Healthcare Network. In another instance, Optum, a division of UnitedHealth Group, announced its intention to acquire Change Healthcare in January 2021, to streamline crucial administrative, clinical, and financial processes.

The Blockchain in the healthcare market includes various notable participants, including [3]:

- PATIENTORY INC.
- IBM
- iSolve, LLC
- Guardtime
- Oracle
- Solve. Care
- BurstIQ
- Change Healthcare
- Blockpharma
- Medicalchain SA

These players contribute to the healthcare industry's dynamic and evolving landscape of blockchain technology.

3. Evolution of the Current Healthcare Ecosystem

The global healthcare landscape has revolutionized the current healthcare systems through real-time monitoring, leveraging AI, and harnessing data analytics. In 2016, Blockchain emerged as a potential solution to address inefficiencies and organizational challenges and secure electronic transfers and exchange of healthcare records. It also showed promise in monitoring drug manufacturing systems. The MedRec framework, based on blockchain technology, was proposed to effectively manage Electronic Medical Records (EMRs). Furthermore, Blockchain facilitated the development of trusted data marketplaces. Recognizing privacy concerns in public networks, the privacy-focused healthcare data management system, MediBchain, was introduced [5].

A revolutionary new method has arisen in 2018 that drastically alters the healthcare system by combining Blockchain, artificial intelligence, and the IoT. This collaboration improved EHR administration, opened the door to telemedicine, autonomous diagnosis, and parallel distributed computing for precision medicine [4]. In 2019, a prototype blockchain-based telemedicine framework was developed to protect sensitive patient health data during remote healthcare delivery to rural and distant places in Bangladesh. In 2019, we introduced a breakthrough fog monitoring platform that uses Blockchain to extend e-Healthcare by detecting human activity through clustered feature vectors. A remote patient monitoring system powered by big data analytics was a crucial component of this architecture.

By 2020, federated learning, explainable AI, and the combination of 5G and 6G networks had all converged with Blockchain. Given the importance of privacy in the collection, management, and distribution of EHR data, the combination of AI and Blockchain has paved the way for a blockchain-assisted open bio-network of private healthcare records, which has the potential to hasten breakthroughs in drug development and preventive medicine. Intelligent telesurgery technology enabled by 6G-enabled Tactile Internet (TI) built on the Blockchain was launched, ushering in a new age in medical treatment. High efficiency and efficacy in virtual healthcare delivery were made possible by this ground-breaking development.

By early 2021, studies aimed at improving the safety of image processing and sharing have incorporated Blockchain. A new method was created for the IoMT setting that uses deep learning (DL) in conjunction with blockchain technology to ensure the secure transfer of images and the accuracy of diagnoses. The healthcare sector has found Hyperledger Fabric technology to be useful in offering robust protection against cyberattacks [5].

4. Summary of Opportunities for Blockchain in Healthcare

Blockchain technology holds immense potential to enhance patient care quality while maintaining cost-effectiveness. It offers solutions to challenges related to multi-level authentication [6]. Several areas within healthcare can benefit from blockchain technology, including:

4.1. Pharmaceutical Industry

The pharmaceutical business is a prospective area for blockchain deployment due to the industry's high demand for data security and compliance with standards like HIPAA. The discovery of new drugs can be sped up by the secure exchange of data, patient pools, and test results between different initiatives [7].

4.2. Personal Health Information, Privacy, and Authenticity

The permissioned consortium administration and anonymized accounts made possible by blockchain's distributed ledger features guarantee authenticity and verifiability [8].

4.3. Interoperability

Smart contracts and permissioned blockchains, in addition to blockchain's emphasis on sharing, distributing, and encrypting healthcare data, can improve the interoperability of healthcare systems with a focus on the patient [9].

There is hope that this technology will help move interoperability forward by leaps and bounds. As a distributed ledger, it allows businesses to see all of their digital assets and transactions in one place. Although it cannot ensure interoperability on its own, it does present a chance and serves as an impetus toward that end.

For Blockchain to be truly useful in the healthcare industry, it must fully leverage existing interoperability standards such as IHE (Integrating the Health Experience) and HL7 FHIR (Health Level 7 Fast Healthcare Interoperability Resources). In order to standardise the transfer of Protected Health Information (PHI), pilots and initiatives are already making use of frameworks like IHE within the blockchain's underlying architecture. Semantic interoperability between systems and organisations within a given network is made possible by implementing standards like FHIR into the Blockchain.

Interoperability standards are chosen for a healthcare network based on the entities involved, the scenarios being addressed, and the information being exchanged. New transactions and blocks must be added to ensure compatibility, and this may be done with the help of application programming interfaces (APIs) and smart contracts. Blockchain paves the way for the transparent and immutable sharing of medical records across a network of peers.

Taking care of network interoperability is just as crucial as making sure healthcare data is compatible within a blockchain. As more and more healthcare solutions appear on public and private platforms, businesses may join several networks. Even if two blockchains are interoperable within the same network, that doesn't mean they will be across networks. Payers, for instance, may achieve interoperability within each chain but not between the clinical and claims domains if they participate in blockchain networks for clinical and claims metadata. As more and more businesses work to combine medical and administrative records, this issue has greater importance.

There are now ongoing efforts to construct inter-platform bridges that will facilitate the unhindered transfer of assets between various blockchain networks.

4.4. Micropayments

Blockchain technology has many applications in healthcare, and it also provides incentives for patients. Blockchain systems can be used to incentivize patients to participate in clinical trials and research, adhere to treatment programmes, keep appointments, and otherwise take good care of their health.

4.5. Healthcare Improvement

The use of blockchain technology in healthcare improves efficiency and rewards patients for their participation. Patients who agree to participate in clinical trials or research and who adhere to treatment programmes, keep scheduled visits, and otherwise take care of their health can earn incentives in the form of tokens stored in a blockchain.

4.6. Medical Supply Chain Management

Decentralizing supply chain management in the pharmacy sector ensures transparency throughout the shipping process. Blockchain records each step of a drug's journey, including origin, handling, and delivery, promoting accountability and even helping monitor waste emissions.

4.7. Genomics Breakthroughs

Blockchain can securely store billions of genetic data points. People can sell their encrypted genetic information, contributing to a vast genetic database that scientists can access for research and development purposes.

4.8. Credentialing Verification

Blockchain technology can streamline the verification and tracking of medical professionals' credentials, simplifying the hiring process. For example, ProCredEx, a US-based company, has developed a medical credentialing verification system using the R3 Corda blockchain protocol.

These are just a few examples of how blockchain technology can revolutionize various aspects of the healthcare industry, improving efficiency, security, and patient outcomes.

5. Challenges and Other Considerations

5.1. Real-Time Data and Verification

Acquiring and acting on data in real time is crucial in the healthcare industry. It is possible to delay the time it takes for a block to be verified; however, this will still cause some wait time.

5.2. Maintaining security over a large distribution system

When dealing with patients' medical records, it's crucial to protect their privacy and avoid unauthorised disclosures. Between July 2021 and June 2022, roughly 692 healthcare data breaches were recorded. Blockchain's need for widespread verification and authentication raises concerns about the potential for future breaches of patient privacy and compliance with HIPAA (Health Insurance Portability and Accountability Act) regulations for the handling of sensitive health data.

5.3. Data Sharing Agreements

When working with patients' medical records, privacy and confidentiality become paramount concerns. From July 2021 to June 2022, there were around 692 healthcare data breaches recorded. Blockchain's need for widespread verification and authentication raises concerns about potential HIPAA violations associated with the administration of patient data and the protection of their privacy.

5.4. Privacy Considerations

Patient health information poses unique challenges for data security and exchange. From July 2021 to June 2022, around 692 healthcare data breaches were recorded. Blockchain's need for third-party validation and authentication raises concerns about the privacy of patients' personal information and the potential for future breaches to occur, which might be in violation of HIPAA.

6. Permitting Individual Access to Records

How to incorporate people as final users of the blockchain system or application is a crucial factor to think about. The privacy of individuals must be protected at all costs. The HIPAA law mandates specific procedures to be followed when a patient requests access to their medical records. Government regulations advocate patient ownership of health data to encourage active engagement in controlling one's health and care, although no particular dataset is mandated for access. Data can be shared for treatment, payment, and operations under HIPAA without the patient's express permission. However, it does not deal with rules for using external healthcare apps (apps). HIPAA's disclosure audit log criteria can be met with the help of distributed ledger technology (DLT). The right of access is also highlighted in the GDPR. Article 15 stipulates that people have the right to have their data moved freely from one data storage provider to another. This furthers the argument that the person should have control over their own data. Given the immutable nature of Blockchain, it is of paramount importance to ensure that personal information cannot be traced back to a specific person. Article 17 of the GDPR, titled "right to erasure" or "right to be forgotten," deals with this issue. Data storage considerations must be given great attention throughout development. When dealing with parties that are not subject to HIPAA, implementers should additionally take into account any other federal or state rules or regulations that may have an effect on privacy.

6.1. Security Considerations

The confidentiality, integrity, and availability of critical information and infrastructure must be ensured at all costs. Securing the Blockchain, each node, and the healthcare organisations and corporate systems that are part of the network is essential for any healthcare blockchain implementation.

6.2. Confidentiality

To protect the privacy of business records, only authorised personnel should have access to the books. The ledger's validity and consistency are maintained via several techniques, one of which is consensus. Healthcare blockchain implementations often use private blockchains where all participating organisations are recognised and trusted. Organizations can be given only the permissions they need on the network through the use of permissioning. Data encryption provides an additional layer of protection against unauthorised access. Additional methods of protecting privacy are used by several Distributed Ledger Technology (DLT) platforms. Channel architecture is used by Hyperledger Fabric, constellation networks are utilised by Quorum, and notary services are implemented in Corda. The implementation process is heavily influenced by the organization's selected method for maintaining secrecy.

6.3. Integrity

With enough decentralisation, in which nodes are deployed and controlled by diverse organisations, the possibility of collusion can be reduced while still preserving the immutability of the shared ledger. Users can have faith that the information stored on the Blockchain has not been tampered with because of the technology's immutable nature. New information can be added to the chain, but no changes can be made to the existing information. Predetermined trust between nodes in private or consortium networks is an additional safeguard for sensitive information.

6.4. Availability

The decentralised nature of the blockchain network improves its overall availability. The network continues to operate even if some nodes go down, and when they come back up, they synchronise to guarantee the integrity of the data in the distributed ledgers. However, it should be noted that the technology does not guarantee the availability of individual nodes. Protecting healthcare organisations' network access is crucial as they increasingly rely on Blockchain for mission-critical services. The entity whose node is being deployed is responsible for this (s). Redundancy across availability zones, load balancing, automated failover, backup and restore procedures, business continuity and disaster recovery plans, and other techniques can all be used to protect nodes in a blockchain network, just as they can in traditional IT infrastructures.

7. Technical Advancements in Blockchain

7.1. Advancements in Blockchain

7.1.1. Quantum Blockchain

A "quantum blockchain" is a blockchain that uses quantum computing and quantum information theory to create a distributed, encrypted, and decentralised database. Its primary benefits are its safety and effectiveness. In order to keep communications between nodes safe, quantum techniques like quantum secure direct communication (QSDC) and quantum key distribution (QKD) can be used. Quantum physics' peculiarities serve as a means of secure network authentication. While quantum computers may be able to break traditional encryption methods like RSA (Rivest-Shamir-Adleman), the quantum Blockchain is able to achieve quantum security by employing quantum digital signature mechanisms. The usage of quantum technology also facilitates rapid transaction processing.

7.1.2. Hyperledger

Hyperledger is an open source blockchain technology with a focus on improving healthcare data management. In recent months, Hyperledger Fabric has emerged as a frontrunner among blockchain deployment solutions in the healthcare industry. Hyperledger is a Linux Foundation-hosted open-source community with the stated goal of providing a solid basis, rules, libraries, and tools for developing enterprise-level blockchain applications on a global scale. It's great for use in the healthcare industry, and it gives you complete command over smart contracts written in languages like Node.js and JavaScript. Hyperledger's capacity to process up to 3000 transactions per second puts it ahead of both Ethereum and Bitcoin. Hyperledger Fabric is the most advanced blockchain architecture because of its high transaction throughput and low transaction costs.

7.1.3. Zero-Knowledge Proof (ZKP)

One of the most reliable approaches to protecting the privacy of financial transactions is zero-knowledge proof (ZKP). A prover can use this to successfully persuade a verifier of a truth without disclosing any of the supporting evidence. There are two main varieties of zero-knowledge proof: interactive and non-interactive. In order to win over the verifier in an interactive ZKP, the prover must carry out actions in accordance with mathematical probability rules. Conversely, non-interactive ZKPs obviate the

requirement for user participation. The prover in a non-interactive ZKP produces all challenges at once, and the verifier provides a response thereafter. Among the alternatives to ZKPs, Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs) has emerged as a major player. Using a quadratic equation that takes into account both public and private information as well as input data, zkSNARK can help with evidence generation.

7.1.4. Homomorphic Encryption

When it comes to protecting the privacy of your financial transactions, Zero-Knowledge Proof (ZKP) is one of the most reliable approaches. Its features allow a prover to persuade a verifier of a truth without disclosing that truth. Zero-knowledge proofs (ZKPs) come in two main varieties: interactive and non-interactive. The prover in an interactive ZKP must carry out actions based on mathematical probability concepts in order to win over the verifier. Conversely, non-interactive ZKPs do away with the necessity of human participation altogether. The prover in a non-interactive ZKP produces all challenges at once, and the verifier gives a response thereafter. Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs) is another significant ZKP that has emerged as a viable alternative. Evidence can be generated with the use of zkSNARK's quadratic equation that includes input data, public data, and private data.

Because of inherent flaws and scalability concerns, researchers have looked into other distributed ledger technologies outside blockchain. As a result, new technologies like the Hashgraph, DAG (Directed Acyclic Graph), and Holochain have emerged. These innovations build upon Blockchain's initial functionality to solve additional problems. Hashgraph is a consensus-based distributed ledger technology (DLT) that ensures transaction agreement among network nodes through consensus timestamping. Unlike traditional DLT networks, transaction success in Hashgraph relies solely on consensus, providing network stability and excellence. Virtual voting and gossip methods enable fairness and prevent blockchain issues like transaction cancellation or future block inclusion. Without proof of work, Hashgraph can achieve thousands of transactions per second (TPS).

DAG, another DLT, utilizes consensus methods where transactions only require majority network support. This collaborative network promotes equal opportunities and democratizes the Internet economy. Unlike private blockchain networks led by centralized authorities, DAG assigns equal weight to every node, eliminating the need for node referencing. IOTA's Tangle, a well-known DAG network, allows miners/nodes to perform dual functions simultaneously, originating and approving transactions. Holochain aims to establish a distributed network for the "next-generation internet," combining Blockchain, BitTorrent, and GitHub elements. This DLT distributes data across nodes to limit centralized control, with each node running on its chain. Users can store data in a distributed hash table (DHT) using specific keys while physically distributed worldwide.

8. Deployment Considerations for Blockchain in Healthcare

8.1. Performance

Performance in software is typically assessed based on the amount of data transferred between endpoints. In Blockchain, performance is influenced by network latency, bandwidth, and the number of consensus nodes involved. For private consortium platforms, typical performance ranges from hundreds to thousands of blocks per second. However, real-world healthcare applications of Blockchain are limited, and performance metrics may vary depending on the specific data involved.

Best practices suggest that smaller data sets are preferable for optimal performance. However, most electronic health records (EHR) and clinical data sets contain large amounts of data, including historical information from multiple institutions. As the ledger grows with each new transaction, performance may be affected due to the need to present a full copy of the ledger. To maintain stable performance, it may be beneficial to include only essential data sets such as demographics, encounters, diagnoses, and medications while excluding larger data like images or notes.

Network bandwidth also plays a role, and other factors beyond the Blockchain's architectural design may impact node performance. Patient ownership of data and the ability to control access are potential use cases for Blockchain in healthcare that are less affected by performance constraints. On the other hand, scenarios requiring fast access to critical patient information, such as sharing medication allergies during an emergency encounter, would rely on high-performance solutions.

8.2. Throughput

Blocks added to the chain per second are a common metric for measuring throughput in blockchain technologies. How the nodes coordinate to verify transactions and ensure that all copies of the shared ledger are always in sync with one another is what the consensus algorithm is measuring. Design decisions, data size, and scope are all elements that might affect throughput. Limiting factors include designing for a reduced data footprint by prioritising vital data over secondary data. Blockchain

technology necessitates a mentality that prioritises moving a limited data set for best throughput, in contrast to existing data trends that emphasis sharing everything and utilising what is needed. Demographic information, medical diagnoses, and service dates are all examples of discrete pieces of data that can be stored in a single data point [10].

8.3. Scalability

Metadata, transactions, provenance, and audit data that are relatively small in size scale well on blockchains. On the other hand, they could struggle to handle larger data volumes, such as photos or full genomic databases. Each node in the network is responsible for keeping a copy of the whole shared ledger, from the beginning of the chain to the most recent transaction [10]. Software implementations must be scalable in order to meet the needs of growing businesses, which is especially true for startups with a modest initial customer base.

The same holds true for blockchains that store healthcare data, which are currently in an expansionary phase. Since demographics tend to change seldom and interactions tend to change frequently, one scalability option could be to use numerous blockchains with separate data sets. Scalability considerations should be baked into the early design.

As the Blockchain expands, refactoring the data it has amassed presents new issues. Scalability can be improved by beginning with the appropriate data set from the outset; nevertheless, this is not a simple process. The efficiency, throughput, and scalability of a technology are all affected by how it was originally conceived. These aspects are shaped by a thorough comprehension of the issue at hand, the relevant parties and data, and the desired outcome.

As the Blockchain expands, it becomes more difficult to refactor existing data. Scalability can be improved by beginning with the correct data set from the get-go. The technology's performance, throughput, and scalability are profoundly affected by its initial design. These components are shaped by the problem at hand, the stakeholders and information required to solve it, and the desired conclusion.

8.4. Deployment Architecture

As the Blockchain expands, there will be a need to refactor the data it has amassed. Improving the possibility of scaling up requires beginning with the correct data set from the start. Performance, throughput, and scalability are all heavily influenced by how the technology is initially conceived. The problem at hand, the people and data that need to be involved, and the desired solution all play a role in shaping these factors.

8.5. On-Promise Deployments

On-premises installations place the onus for hardware acquisition, software installation and configuration, patch management, and network configuration that allows nodes to communicate with one another over the internet on the healthcare organisation.

8.6. PaaS Model

PaaS implementations in the cloud have benefits in terms of price, flexibility, and scalability. The blockchain network does not need to be supported within healthcare organisations' data centres; however, organisations are still responsible for managing acquisition, configuration, and maintenance. Availability can be maintained by the use of load balancing, automatic failover, and redundant nodes spread over many availability zones.

8.7. IaaS Model

With cloud-based IaaS installations, enterprises can create and host nodes on demand, without incurring any upfront expenditures or ongoing maintenance responsibilities. The security precautions, availability zones, and load balancers provided by cloud service providers make it easy and quick for healthcare firms to implement Blockchain. Blockchain technology is not a silver bullet; rather, it is an integral part of a larger system.

Integration with corporate infrastructure is essential. These systems can be deployed in a variety of ways, such as locally or in the cloud. It is crucial to provide a public interface for retrieving data from enterprise systems that store records referred to by the Blockchain. Integration with external interfaces in the cloud or a demilitarised zone (DMZ) within the intranet of a healthcare company might accomplish this (fig.3). The following flowchart helps summarize the ideal architectural framework for healthcare blockchain in the cloud [11].

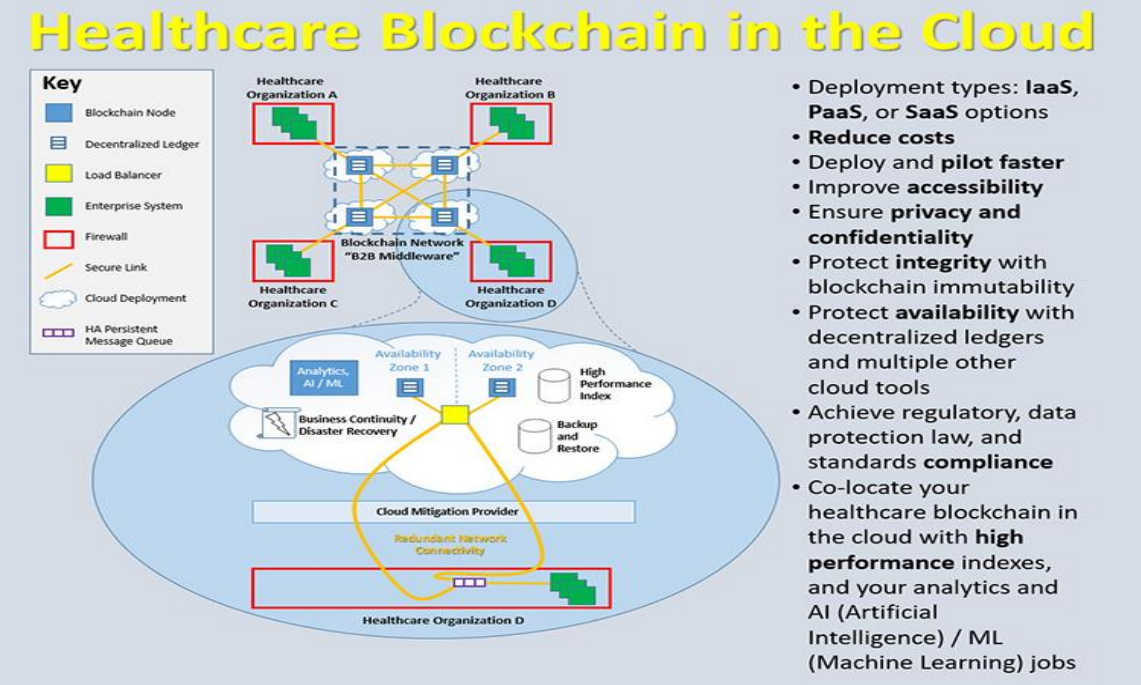

Figure 3: Healthcare blockchain in the cloud [11]

Overall, the choice of deployment model depends on factors such as cost, maintenance, availability requirements, and the specific needs of the healthcare organization integrating blockchain technology.

9. Conclusion

Blockchain has the potential to revolutionize several areas of the healthcare industry. In the pharmaceutical sector, it can enhance data security, accelerate drug development, and ensure the authenticity and privacy of personal health information. Blockchain's focus on sharing and encrypting healthcare data improves interoperability, providing a unified view of digital assets and transactions. It enables micropayments, incentivizing patient participation in research or care plans. Integrating AI and machine learning improves healthcare outcomes through personalized medicine and data linkage. Supply chain management benefits from Blockchain's transparency and accountability, while securely storing genetic data contributes to genomics research breakthroughs. Moreover, Blockchain streamlines credentialing verification for medical professionals, simplifying the hiring process. Implementing blockchain technology in healthcare requires careful consideration and addressing various challenges. Real-time data accumulation and verification may introduce minor delays. Ensuring security over a large distribution system is crucial to avoid breaches and violations of privacy regulations. Patient matching algorithms and governance rules need to be considered for data-sharing agreements. Patient privacy concerns require well-defined strategies for collecting, using, accessing, disclosing, storing, and disposing of Protected Health Information (PHI). Comprehensive security measures, including consensus, permissions, and encryption, are necessary to protect sensitive data and systems. Deployment considerations for Blockchain in healthcare involve performance, throughput, scalability, and deployment architecture. Performance is influenced by network latency, bandwidth, and the number of consensus nodes involved. Throughput depends on the consensus algorithm used and design choices made. Scalability is important when dealing with different data types, and planning for scalability from the beginning is crucial. Deployment architecture options include on-premises setups, cloud-based PaaS and IaaS models. Integration with enterprise systems and external interfaces is essential for seamless data retrieval. In conclusion, the global Blockchain in the healthcare market is poised for significant growth driven by the need for secure data management.

Acknowledgement: We thank our family and friends for supporting our endeavors. Their constant motivation has helped us achieve our goals.

Data Availability Statement: The study is based on the Baldrige Excellence Framework publicly available at the National Institute of Standards and Technology (USA Department of Commerce).

Funding Statement: No funding was received to help prepare this manuscript and research work.

Conflicts of Interest Statement: No conflicts of interest are declared by the author(s). This is the author's fresh work. Citations and references are mentioned as per the used information.

Ethics and Consent Statement: Authors of the work unanimously consent to make this publication available to all interested people for reading, teaching, and learning.

References

1. J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? A systematic review," PloS one, vol. 11, no. 10, pp. e0163477, 2016.
2. M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A Systematic Review of the Use of Blockchain in Healthcare," Symmetry, vol. 10, no. 10, pp. 470, 2018.
3. "Precedence research - market research reports & consulting firm," Precedenceresearch.com. [Online]. Available: https://www.precedenceresearch.com/blockchain-in-healthcare-market. [Accessed: 25-Oct.-2022].
4. V. Veeraiah, A. Pankajam, E. Vashishtha, D. Dhabliya, P. Karthikeyan and R. R. Chandan, "Efficient COVID-19 Identification Using Deep Learning for IoT," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 128-133, doi: 10.1109/IC3I56241.2022.10073443.
5. R. Shinde, S. Patil, K. Kotecha, V. Potdar, G. Selvachandran, and A. Abraham, "Securing AI-based healthcare systems using Blockchain Technology: A state-of-the-art Systematic Literature Review and future research directions," arXiv [cs.CR], 2022.
6. M. Pratap, "Blockchain in healthcare: Opportunities, challenges, and applications," Hackernoon.com, 06-Aug-2018. [Online]. Available: https://hackernoon.com/blockchain-in-healthcare-opportunities-challenges-and-applications-d6b286da6e1f. [Accessed: 25-Oct.-2022].
7. T. R. Weiss, "How blockchain could improve healthcare security," SQL Server Pro, Nov. 16, 2017. [Online]. Available: http://ezp.twu.edu/docview/1964473642?accountid=7102. [Accessed: 25-Oct.-2022]
8. K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring," Journal of medical systems, vol. 42, no. 7, pp. 130, 2018.
9. W. J. Gordon and C. Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability," Computational and structural biotechnology journal, vol. 16, pp. 224-230, 2018.
10. "Blockchain in healthcare," HIMSS, 01-May-2020. [Online]. Available: https://www.himss.org/resources/blockchain-healthcare. [Accessed: 25-Oct.-2022].
11. D. Houlding, "Healthcare Blockchain in the Cloud," LinkedIn, [Online]. Available: https://www.linkedin.com/pulse/healthcare-blockchain-cloud-david-houlding-cissp-cipp/. [Accessed: 25-Oct.-2022]