

Blockchain and its Applications in Healthcare Data: A Survey

Shruthi K¹ and Dr.A.S.Poornima²

¹⁻²Siddaganga Institute of Technology /C.S.E, Tumkur, India
Email: shruthik@sit.ac.in, aspoornima@sit.ac.in

Abstract—Blockchain is one of the wonderful technologies which is used in the next decade and taken a huge variety of uses with it. Most of the researches are carried out to identify the advantages of Blockchain. Blockchain is decentralized in nature. Blockchain is considered has the security mechanism to shield the privacies of the objects to access through mobile devices. Blockchain is used in many applications, they are banking applications, e-voting applications and digital forensic programs and healthcare data sharing. This paper gives a comparative look of blockchain and additionally explains the taxonomy and architecture of blockchain, explains an evaluation among different consensus mechanisms. It is guaranteed that safe sharing of healthcare data is achieved by utilising the programs of blockchain for the shipping of secure healthcare data. Blockchain is the conforming healthcare practices to a greater dependable means, and remedy through safe and comfortable healthcare data sharing. In future, blockchain can help in bespoke, proper, and comfort healthcare by way of merging the complete actual-time clinical statistics of a patient's health and presenting it in an up-to-date healthcare setup. This article gives an updated survey on different situations, open troubles encountered in healthcare due to the legacy security features along with the security necessities of such situation. It also merges the strengths of blockchain as a trusted security degree, highlights capability challenges inside the healthcare field, and presents an investigation of various blockchain-based safety algorithms.

Index Terms— Blockchain, HealthCare, Consensus procedures, Distributed Ledger Technology, Health Information Exchange, Security, Electronic Health Record.

I. INTRODUCTION

Blockchain is a special type of database. It is different from a legacy database in the way it stores data blockchain stores data in blocks that are chained together. As new data comes it is entered into a new block. Once the block is loaded with data it is linked onto the previous block, which makes the data chained together in sequential order. Blockchain is used in a disseminate fashion so that no single person or group has control instead, all users are provided with control. Each block contains a cryptographic hash of the predecessor block, a timestamp, and transaction data (usually represented as a Merkle tree). Once the data is recorded, the data in any given block cannot be modified without modification of all successor blocks. The blockchain is an open, distributed ledger that will document the transactions between two parties successfully. The blockchain is a form of payment chain. Blockchain is used for financial, buying and selling transactions.

A. Definition

Blockchain is defined as a cryptocurrencies like bitcoin, ripple etc. but actually, application of blockchain is not only confined to finance. Blockchain ledger cannot be stolen, corrupted or modified by anyone, it can change the financial system and business structure [1].

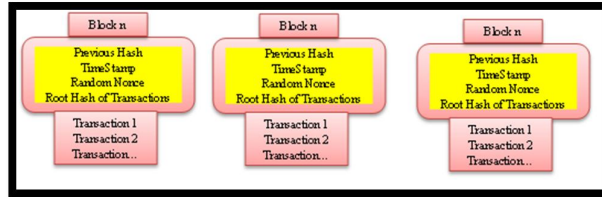


Figure 1. Blockchain scheme

A blockchain is a progression of squares associated with one another, where the last square interfaces with the past one, etc. The dispersed record assembled utilizing cryptographic mechanism it contains time-stamp data in a framework that is invulnerable to misrepresentation or focal control if the preparing force of the blockchain is disseminated by various hubs. Each square contains data, when a hub makes a square it will add that square to the chain. The excess hubs need to confirm each square. When testing of the square is fruitful, the hubs will acknowledge the new square, outstretch the blockchain. The calculations, used to paw the check and agreement between numerous substances, can be distinctive for each blockchain effort. Figure. 1 addresses how the squares are associated with one another in a blockchain [2]. The top piece of the square is the header and the lower part is the body of the square. The body contains the transaction details of that block. The square header contains the past hash the past hash is a hash of the header of the past block. Adding the hash of the past square to another square makes a chain. The header likewise contains the timestamp, an arbitrary nonce, and the root hash of the exchanges in the body. The irregular nonce is a self-assertive number utilized once. The root hash of exchanges is the top hash of a Merkle tree exhibited in Figure. 2 [3].

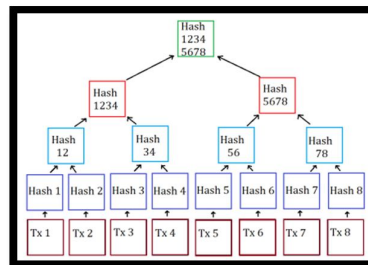


Figure. 2 Merkle tree for root hash of transactions

B. Blockchain Structure

Blockchain is a chain of squares (Nodes) that are associated with each other Fig 3. The transactions are stored in the form of network. When a new transaction is initiated, it needs to be tested first after successful validation it will be added to the previous node in order to form a chain called Blockchain. The verification is done using the consensus algorithm between the nodes, consensus algorithms like [proof of work \(POW\)](#) [proof of stake \(POS\)](#) Proof of Capacity (POC) can be used. Blockchain statistics cannot be altered until the consensus is authenticated which results in malicious free node.

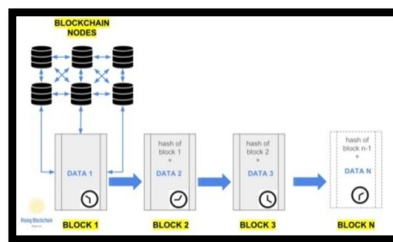


Figure.3 Blockchain Structure

C. Blockchain Capabilities

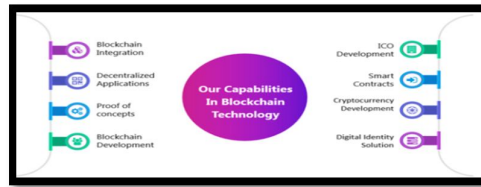


Figure. 4 Blockchain capabilities

During the blockchain generation, the technology offers the ability to mitigate the need for a trusted third party. Blockchain is shared record that gives an agreement component a specific recognition of secrecy and privateness in an untrusted network. Blockchain period be the ground for brilliant agreements that grant exchanges with various styles of approvals in which the check happens in a straightforward way. The transactions are unchangeable and it is not viable to tamper the file [4]. The Blockchain technology offers multiple advantages [5] as shown in Figure.4.

- **Skeptical:** The substances are in charge of the insights and two elements could make a trade without the need of a confided in outsider.
- **Indignity:** The execution of exchanges is by and large as the convention orders.
- **Translucency:** Adjustments to public blockchains are public and can be examined and available to all elements making straightforwardness.
- **Loftiness data:** The information in the blockchain is finished, steady and permanent.
- **Liability:** Blockchain utilizes a distributed organization, this kills the main issue of disappointment issue and improves endurance from assaults.

D. Blockchain Applications

Blockchain can be used in various applications. Bitcoin is a digital currency designed in 2008. This technology can be used for finding solutions in different domains like healthcare, balloting, identity management, governance, deliver chain, energy resources and so on. Fig. 5 represents a number of the application domains of the blockchain.



Figure. 5 Application domains of Blockchain technology

E. Healthcare

Blockchain is presently being utilized for record the board in applications, for example, general wellbeing and clinical exploration dependent on close to home patient information. Assessment measurements dependent on plausibility, planned ability, and consistence can be utilized to evaluate blockchain based decentralized applications in the space of medical care [2].

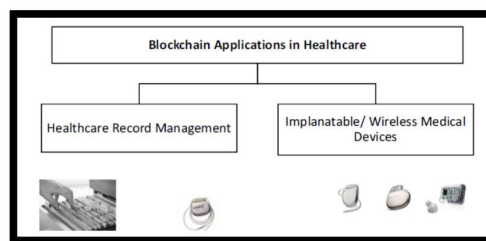


Figure.6 Blockchain applications in healthcare systems

Numerous nations, like Estonia, are utilizing blockchain to get wellbeing and clinical preliminary records by connecting admittance to information with authorization settings. Blockchain additionally offers security through straightforwardness, which empowers the examining of standardized identification labeled medications and following them through secure computerized blocks at whatever point they change hands, subsequently diminishing the odds of forging. This can be additionally gotten by permitting just approved gatherings at the most distant finish of the store network to get to the records continuously. There are assorted arrangement of uses where blockchain can be used, specifically information sharing, access control, wellbeing records, dealing with a review trail, store network [3]. Dynamic logical work being done in a portion of these spaces is overviewed next. At last, in the space of medical care investigation, a blockchain-based application for putting away and dealing with the information base of patients and specialists during medical procedure is expressed in Ref. [14]. A structure, in light of counterfeit frameworks, computational trials, and equal execution utilizing blockchain innovation, which acquires the advantages of an equal medical care framework has been proposed in Ref. [15]. A proposition to oversee wellbeing information at individual and foundation level utilizing private blockchain arrangement has been made in Ref. [16].

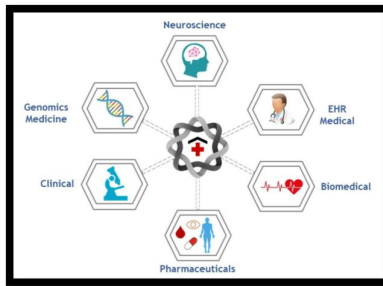


Figure.7 Applications of blockchains in healthcare

II. RESEARCH METHODOLOGY OF DIFFERENT PAPERS

A. Blockchain and Machine Learning in Health Care and Management

In the above mentioned paper they proposed solutions to the problems associated with healthcare statistics control using machine learning and Blockchain. Extracting relevant statistics from the facts is possible using machine learning. This is completed using trained algorithms. As soon as this statistics is stored, the subsequent problem is statistics sharing and its reliability. Blockchain plays a major role in data sharing in secured way. The agreement in Blockchain verifies that records are genuine and exchanges are secure. Blockchain period can most likely substitute wellness care control for the better with the guide of putting patient at the focal point of the medical services and developing the security and interoperability of wellness records. In this article it focuses typically on fixing healthcare data management issues by the use of Blockchain consensus mechanism and together with a few critical features of machine learning to give improved solution in terms of security.

In this model, double Blockchain structure is used, the underlying portion grants induction to prosperity data and is amassed using the Hyperledger Fabric. The second piece of the plan works on Ethereum and plays out all application and organizations. Clinical information is uncommonly delicate and individual so a shut Blockchain, for instance, Hyperledger Fabric helps in holding central insurance required. Additionally, the patient's data is made far off and unalterable. The Blockchain goes probably as a pointer, and gives the bearing to the space of the set aside data, inferring that anyone endeavoring to get the patient data will be denied. The prosperity data is gotten between the patient and the affirmed trained professional(Doctor). Right when the endorsed expert adds additional information to the patients record history, the system will thus revive it. Simply those clinicians who have affirmed permission can see the updates. None of the experts are given never-ending endorsement, the passage for the expert closes when the patient necessities with the objective that the expert can as of now don't invigorate the record or access it.

In certain circumstances where there is a need to change the expert in charge, thus, with the help of Blockchain the information move will be basic and secure. Issues related with the trading of information by clinical association labourers are completely cleared out and there will be no more data discharges conceivable in this exchange. In specific conditions like, when the patient is absent and unable to give such a commitment on his wellbeing, it is vital for approach the patient's wellbeing records. This information helps in performing lifesaving, operations as history of past prescriptions and disorders are urgent before performing a particularly

huge operation. In this article, they utilized Supervised learning, how to set up the Machine learning estimation on the datasets gained through various sources like Medline, and to decrease the dimensionality of the data they used the "sack of words" computation which will take simply the important bits of the dataset to set up the Machine learning model. The Patient clinical consideration data is gotten using Blockchain network through which trades among patient and the affirmed expert is made.

B. Blockchain and Smart Healthcare Security: A survey

Certifiable computerized assault concerns have emerged in clinical consideration organizations during the past couple of years. A record number of cases have been represented in the year 2019, where Health Insurance Portability and Accountability Act (HIPAA) breaks came to 418, and an amount of 34.9 million US inhabitants had their secured Health information (PHI) compromised in that year [9].

The current structure is not good for giving assurance against such information penetrates, which can be long run examine the insurance and security of patients' wellbeing information. The executed models of clinical consideration records open another window towards a risky circumstance, i.e., the patient's data being taken care of by wellbeing association, leaving patients' information in question, and causing wasteful information conveyance towards patients' clinical consideration. For instance, considering the way that the information about a patient's wellbeing is not sent from one specialist organization to the next on schedule, the patient's therapy may get conceded.

EHR has such limits nearly, which can be overwhelmed by utilizing blockchain. As of late, blockchain has been trailed through a few specialists, non-public, and public-private banded together tasks [10]. Blockchain's ability benefits in the field of medical services had been seen while the USA food and Drug the board (FDA) and IBM Watson wellbeing zeroed in on a blockchain system to protect realities related with oncology [11]. It is accepted by utilizing FDA and IBM that blockchain has the usefulness to help data trade gathered from different sources with the agreement of victims and the terms commonly conceded to [12].

Carried out models have the colony on passwords, which may contain privileged information that should be traded and for the most part saved money on temperamental and significantly less secure cloud[13]. This provoked a few notable digital mishaps, the greatest notable of which changed into the solitary that occurred in 2014, when programmers encroached into US wellness back up plan Anthem's workers and the delicate realities of around eighty million individuals (patients and representatives) got taken [13].

It is likewise vital that the medical services records access must be treated with safety measures. Moreover, normalized reviewing is unavoidable for ensuring data honesty. Blockchain decreases the potential outcomes of such sad penetrates and ensures data trustworthiness, secrecy, and strong stockpiling. Also, single-factor-of-disappointment is similarly relieved as this adaptation stores information in a distributive manner. We examined how blockchain-based answers can defeat over various assurance inconveniences in an effective, distributive, and adaptable way.

C. A Survey Paper On Consensus Algorithm Of Mobile-Healthcare In Blockchain Network

Versatile wellbeing has been presented with secure trade of information between the patients and specialists from different emergency clinics through different contraptions and applications through the web to give straight imposition, security, moreover, on-going organization and to get people and their properties. The current system plan of blockchain while every center point is related on the organization has comparable data due to the dispersed record. In addition, it uses the understanding procedure where by every center agrees to the route toward sharing the square ensuing to being perceived by one digger and invigorated on own chain.

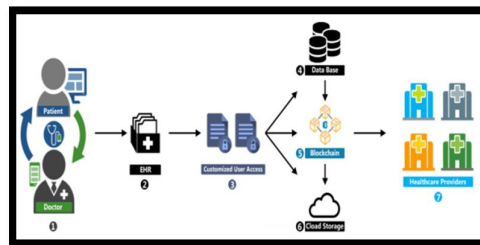


Figure. 8 Mobile-healthcare blockchain Architecture

The proposed Mobile-medical care blockchain structure has two segments, one of them is sensors identified with the patient's casing gathers ongoing measurements and ship off the instrument which can be wireless or pc to

TABLE I. BLOCKCHAIN-BASED SECURITY SOLUTIONS IN SMART HEALTHCARE SYSTEMS

RF	Issues Addressed	Blockchain Solution	Advantage
15	Entry control, data perplexity	Ethereum-based brilliant agreements and cryptography with no money related based mining motivations	Data tenancy, rectitude, and gullibility
16	Privacy Detriment, Single-point-of-downfall, and Subtle Attack	Privacy Perpetuate, Data Encryption, Access Regulate, and key Administration	Seclusion, Liability, and on-Demand Retraction
17	Seclusion, Eavesdrop, and trespass attacks	Dispensed web platform, Access Regulate	Pseudonyms, Isolation, Sincerity, Liability.
18	Confidentiality issues	Infantry blockchain and confederacy blockchain	Access Regulate, Investigate, Infantry safeguarding, protected search, and time-protected retraction
19	Real-time patient supervise security.	Petitioned and organization managed blockchain.	Confidentiality, Possibility, perpetuation, irascibility, Infantry and clarity.
20	Data exposure, malignant operation, and deceptive user.	Custommade pursuit indicant-based blockchain.	pageant analysis, dependable search results, covertness, rectitude, anti-tinkering, and irascibility.
21	Data purity and abrogation issues	Blockchain-based stamp	Data purity, non-abrogation, data missioning.
22	Data distribution, gullibility, and Quality of Service (QoS) issues	Blockchain-based brainy and protected Healthcare system	Gullibility, data distribution, QoS, efficient, distant monitoring.
23	Penetralia and unsigned information distribution issues	Two-layer consortium blockchain alongside another agreement calculation (MBFT)	penetralia protection, meddle - resistance, high blunder tolerance and energetic transaction handling
24	Single-point-of-failure, man-in-the-middle attack, denial of service, and data sniffing attacks	RHM solution using blockchain	penetralia preserving, identity administration, preservation.

house the product and send them to hubs, the gadget sends data and gets the outcomes from the specialist as clarified in figure 6. Besides, in the second piece of this design, the insights should notice the idea of the blockchain of dispersed record. In various words, the insights is decentralized all through medical clinics (recollect that each medical clinic has own information base, specialists, labs and the board) at the blockchain network. This proposed format of neighbor checking and refreshing model may likewise assist with staying away from that one hub or clinical foundation will have long blockchain on network simultaneously as others having short chains.

To stress, this plan keeps the arrangement of decides that every hub at the organization should show the neighbors and ensures that each hub is state-of-the-art in each square before some other evidence of work is started on the local area. This can resolve the issues of fragmented information or lacking realities in a solitary hub (possessed by an emergency clinic). For example, when the hub which holds the long-chain comes up short and transforms into a shortcoming model, and the equivalent records is accessible into unique information bases of all hubs in blockchain network each time a patient interfaces for conclusion. In addition, this thought configuration may not permit the hub to make more than varieties of the chains in a similar hub. Further, this design may likewise abstain from twofold spending, decrease the limit of a hub to dam sure IP locations and exchanges between unprecedented clinics on the blockchain network with a circulated record instrument.

D. Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research

This proposition incorporates the use of a public blockchain as an entrance control chairman to wellbeing records that are taken care of off blockchain. There are correct now no open standards or executions of blockchain that utilization this strategy yet research reinforces the chance of the proposed game plan. Bitcoin has viably shown that accepted, auditable enlisting is possible using an appropriated network joined by a typical record. Additionally, the advances for data amassing, security and encryption exist and are being utilized today. Any Blockchains for clinical consideration ought to be public and would similarly need to fuse imaginative responses for three key parts: adaptability, access security and information protection.

- *Scalability*

Exchanges in the squares would contain a client's remarkable identifier, an encoded connected to the wellbeing record and a timestamp for when the exchange was made. To improve information access productivity, the

exchange would contain the sort of information contained in the wellbeing record and whatever other metadata that would work with habitually utilized questions (the metadata could be added as labels). The wellbeing blockchain would contain a total filed history of all clinical information, including formal clinical records just as wellbeing information from versatile applications and wearable sensors, and would follow an individual client for the duration of his life.

All clinical information would be put away off blockchain in an information storehouse called an information lake. Information lakes are profoundly adaptable and can store a wide assortment of information, from pictures to records to key worth stores. Information lakes would be significant devices for wellbeing research and would be utilized for an assortment of investigation including digging for factors that sway results, deciding ideal treatment alternatives dependent on hereditary markers and recognizing components that impact precaution medication. Information lakes support intuitive questions, text mining, text investigation and AI. All data put away in the information lake would be scrambled and carefully endorsed to guarantee security and genuineness of the data.

At the point when a medical services supplier makes a clinical record (solution, lab test, pathology result, MRI) a computerized mark would be made to check realness of the archive or picture. The wellbeing information would be encoded and shipped off the information lake for capacity. Each time data is saved to the information lake a pointer to the wellbeing record is enrolled in the blockchain alongside the client's remarkable identifier. The patient is told that wellbeing information was added to his blockchain. In a similar style a patient would have the option to add wellbeing information with advanced marks and encryption from versatile applications and wearable sensors.

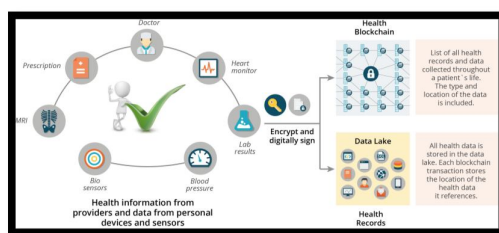


Figure.9 Mobile Healthcare Blockchain Architecture

- *Access Security and Data Privacy*

The client would have full admittance to his information and command over how his information would be shared. The client would appoint a bunch of access authorizations and assign who can question and compose information to his blockchain. A portable dashboard application would permit the client to see who has consent to get to his blockchain. The client would likewise have the option to see a review log of who gotten to his blockchain, including when and what information was gotten to. A similar dashboard would permit the client to give and repudiate access authorizations to any person who has an interesting identifier. After a medical services supplier is allowed admittance to a client's wellbeing data, he questions the blockchain for the client's information and uses the advanced mark to verify the information. The medical care supplier could use a modified best-of-breed application to examine the wellbeing information.

Character validation would follow the accepted procedures set up by monetary establishments and controllers. In a perfect world, biometric character frameworks would be used as they offer improved security over secret key and token (smartcard) based techniques for personality verification.

Given this model, the client has particular command over his information and the ability to allow admittance to explicit medical care suppliers as well as medical care substances for correspondence and joint effort in illness therapy and avoidance. The decentralized idea of the blockchain joined with carefully marked exchanges guarantee that an enemy can't act like the client or degenerate the organization as that would suggest the foe produced a computerized signature or oversaw most of the organization's assets. Essentially, an enemy would not have the option to take in anything from the common public record as just hashed pointers and encoded data would be contained inside the exchanges.

III. CONCLUSIONS

An overview of the examination papers done in this paper shows blockchain and their inalienable blend of agreement calculations, appropriated information stockpiling, and secure conventions can be used to construct vigor and unwavering quality in medical services frameworks. Blockchain gives a conveyed record framework

that approves exchanges and guarantees that nobody can alter them, whenever they are added to the chain. On the off chance that somebody attempts to alter the records, it is not difficult to recognize the adjustment of example and take safeguarding strategies.

Blockchain additionally kills the dangers related with an incorporated engineering as the part of approving exchanges is disseminated with entertainers who have critical interest in the organization, either estimated as confirmation of stake or verification of speculation. This arising innovation gives web clients the capacity to make esteem and verify the computerized data. The overview results introduced in this paper exhibit that Blockchain enjoys unmistakable benefits for medical services applications when contrasted with different applications.

REFERENCES

- [1] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, I. Ghafir, The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey, *Sensors* 19 (8) (2019) 1788.
- [2] N. Kshetri, Blockchain and electronic healthcare records [cybertrust], *Computer* 51 (12) (2018) 59–63.
- [3] G. G. Dagher, J. Mohler, M. Milojkovic, P. B. Marella, Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, *Sustainable cities and society* 39 (2018) 283–297.
- [4] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, N. Yu, Healthchain: A blockchain-based privacy preserving scheme for large-scale health data, *IEEE Internet of Things Journal* 6 (5) (2019) 8770–8781.
- [5] A. Al Omar, M. S. Rahman, A. Basu, S. Kiyomoto, Medibchain: A blockchain based privacy preserving platform for healthcare data, in: *International conference on security, privacy and anonymity in computation, communication and storage*, Springer, 2017, pp. 534–543.
- [6] A. Zhang, X. Lin, Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain, *Journal of medical systems* 42 (8) (2018) 140.
- [7] K. N. Griggs, O. Ossipova, C. P. Kohlhos, A. N. Baccarini, E. A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, *Journal of medical systems* 42 (7) (2018) 130.
- [8] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, N. Zhang, Blockchain based searchable encryption for electronic health record sharing, *Future Generation Computer Systems* 95 (2019) 420–429.
- [9] A.-S. Kleinaki, P. Mytis-Gkometh, G. Drosatos, P. S. Efraimidis, E. Kaldoudi, A blockchain-based notarization service for biomedical knowledge retrieval, *Computational and structural biotechnology journal* 16 (2018) 288–297.
- [10] A. A. Abdellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini, A. Refaey, sshealth: Toward secure, blockchain-enabled health-care systems, *IEEE Network* (2020).