International Organization of Research & Development (IORD)
ISSN: 2348-0831
Vol 10 Issue 01 | 2022

A Secure Transaction of Electronic Health Record in Healthcare System Using Block-Chain Technology

Kiran Sanjay Khanderao[1], Ashok Purushottam Kankale[2]
[1,2] Department of Computer Science and Engineering, RSCE Buldhana

DOI: 10.5281/zenodo.7447672

ABSTRACT

This paper deals with the secure transaction of electronic health record, for storing information of the patient which consist of the medical reports. Electronic Health Records (EHRs) are entirely controlled by Hospitals instead of patients, which complicates seeking medical advices from different hospitals. In the existing system of storing details of the patients are very dependent on the servers of the organization. In the proposed all the information of the patient are stored in the blockchain by using the Meta mask and these details are stored in the block chain as a block of data. Each block consists of the data which is encrypted data. Electronic Health Record (EHR) systems record health-related information on an individual so that it can be consulted by clinicians or staff for patient care. The data is encrypted by the algorithm known as SHA-256 which is used to encrypt all the data of the patients into a single line 256-bit encrypted text which will be stored in the block at ethers can. These records for not only useful for the consultation but also for creation of historic family health information tree that keeps track of genetic health issues and diseases it can also be used for any health service with the authorization from both the patient and medical organization.

Index Terms- Blockchain, SHA 256 algorithm, Encryption of data, Meta mask.

1. INTRODUCTION

The objective of this paper is to provide the application which is user friendly and cost effective. The major advantage of this paper is security. A securable system is more important to be reliable. Electronic Health Records (EHRs) provide a convenient health record storage service, which promotes traditional patient medical records on paper to be electronically accessible on the web. This system was designed to allow patients to possess the control of generating, managing and sharing EHRs with family, friends, healthcare providers and other authorized data consumers. Moreover, provided that the healthcare researcher and providers of such service access theseEHRs across-the aboard, the transition program of healthcare solution is expected to be achieved. However, in the current situation, patients scatter their EHRs across the different areas. Duringlife events, causing the EHRs to move from one service provider database to another. Therefore, the patient may lose control of the existing healthcare data, while the service provider usually maintains the primary stewardship. Patient access permissions to EHRs are very limited, and patients are typically unable to easily share these data with researchers or providers.

A blockchain ledger has the traits of being un-tamper able and publicly verifiable, and the data contained inside it has the attributes of being non-tamper able and publicly verifiable. There are three sorts of blockchains in the realm of blockchain technology: public blockchains, consortium blockchains, and privately controlled blockchains. In accordance with its name, the public blockchain is available to any and all people participating in the system. Nodes have access to the information stored in the ledger since it is distributed. The private blockchain is only used by private organizations and is not accessible to the general public. It is a distributed ledger technology. A similarity exists between consortium blockchains and this in that they are established by organizational norms that describe the accounting, reading, and writing rights of the blockchain. Figure 1 depicts a conceptual representation of blockchain technology in its most basic form.

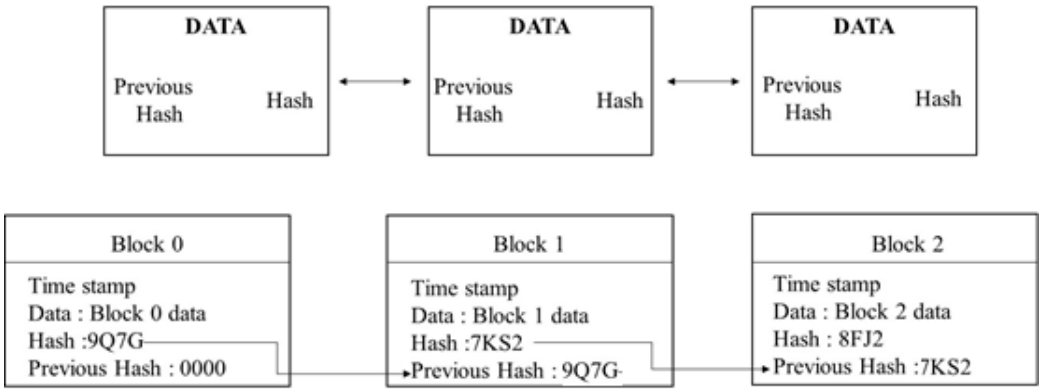

Figure 1: The Blockchain's Organizational Structure

It is possible to create a public record that includes decentralized digital information that can be viewed by anybody from any computer system that is connected to the internet using blockchain technology, which is becoming more popular. In the database, the block is referred to as the data, and it is held in a chain that is made up of numerous bits of data and is referred to as the database chain. As the first digital system to offer a shared digital record for unprotected parties, the block chain is considered to be a pioneer in the field of information technology.

Figure 2 displays a business network that makes use of blockchain technology, as seen on the right in the illustration. Users may collaborate on a shared ledger that is updated on a peer-to-peer basis whenever a transaction is successfully completed, which is a crucial aspect of the blockchain architecture. A peer-to-peer replication network is characterized by the fact that each participant (node) acts as both the publisher and subscriber at the same time, a process known as "dual-role replication." During the course of a transaction, data may be received or delivered between nodes, and as data travels from one node to another, it is synchronized across the network.

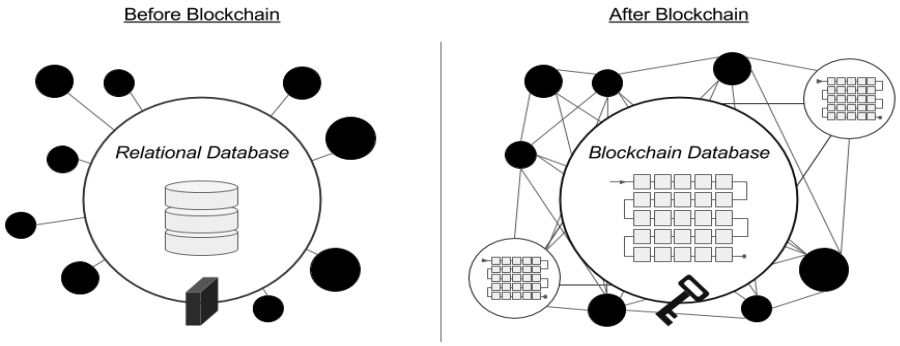

Figure 2: Business networks before and after blockchain.

The blockchain network is both economical due to the fact that it decreases the need for middlemen by eliminating the necessity for duplication of effort. It is also less sensitive to infection. since it validates information via the use of consensus models. Security, authentication, and verifiability are all features of the platform's transactions.

Automobile leasing firms make it seem simple, but in truth, it may be a difficult process to navigate. Because, despite the fact that the Today's automobile leasing networks have a substantial efficiency problem due to the fact that the physical supply chain is often linked, but the supporting systems are sometimes scattered. Each member in the network maintains a separate ledger, which may take many days or weeks to sync with the ledgers of the other participants.

Every member, regardless of where the vehicle is in its life cycle at any one moment, may access, and analyse the physical condition of the vehicle via a shared ledger on a blockchain network. The use of blockchain technology helps to build trust among members of a business network. When you operate on a blockchain network, it is not that you cannot trust the folks with whom you do business; rather, it is that you do not have to do so in order to conduct business. In order to increase the degree of trust among network members, blockchain technology is quite effective. This is crucial. Given that each transaction is built on top of the transaction that came before it, any corruption is immediately apparent, and everyone is made aware of the situation. Because of this, the need to rely on existing legal

or regulatory safeguards and penalties to monitor and manage the flow of commercial transactions may be reduced to a lesser extent. This is accomplished by the community of participants. As a result of the use of blockchain technology, the regulatory system is less stressed since it is simpler for auditors and regulators to analyze relevant transaction information and verify compliance when third-party monitoring is necessary.

This technology is referred to as blockchain because it saves transaction data in blocks that are connected together to create a chain, hence earning the term blockchain. The blockchain's size increases in lockstep with the number of transactions that occur on it. Block transactions are recorded and confirmed in blocks, which are subsequently added to the blockchain to complete the transaction chain. This is accomplished via the use of a separate network that is regulated by rules that have been agreed upon by the network's members.

In addition to the preceding block's hash, each block includes timestamped batches of recent valid transactions as well as the hash of the prior block. The hash from the preceding block is also included. The previous block hash connects the blocks together and prohibits any block from being updated or placed between two existing blocks in the order in which they appeared in the chain of events. Therefore, each new block contributes to the strengthening of previous blocks' verification and, ultimately, to the strengthening of the blockchain as a whole. When the approach is used, the blockchain becomes tamper-evident, which contributes to the blockchain's immutability, which is a critical characteristic.

This technology is referred to as blockchain because it saves transaction data in blocks that are connected together to create a chain, hence earning the term blockchain (see Figure 3). The blockchain's size increases in lockstep with the number of transactions that occur on it. Block transactions are recorded and confirmed in blocks, which are subsequently added to the blockchain to complete the transaction chain. This is accomplished via the use of a separate network that is regulated by rules that have been agreed upon by the network's members.

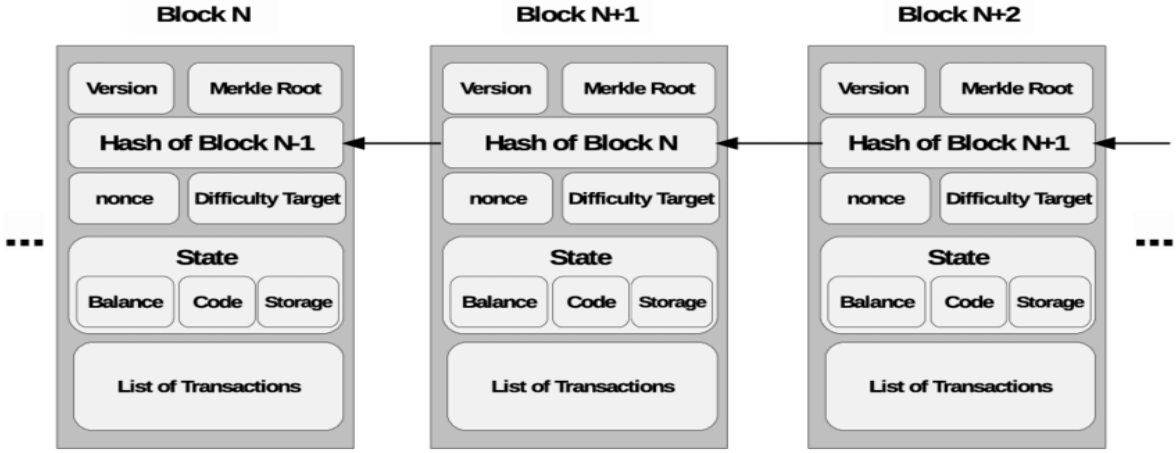

Figure 3: Blockchain tracks transactions in a network of linked blocks.

In addition to the hash (also called as a digital fingerprint or a unique identity), each block includes timestamped batches of recent valid transactions, as well as the hash of the preceding block, which makes up the whole blockchain. The previous block hash connects the blocks together and prohibits any block from being updated or placed between two existing blocks in the order in which they appeared in the chain of events. As a result, each succeeding block contributes to the strengthening of the verification of the prior block and, ultimately, the whole blockchain. When the approach is used, the blockchain becomes tamper-evident, which contributes to the blockchain's immutability, which is a critical characteristic. The fact that a blockchain for business is a private, mission-specific network with known identities and no need for cryptocurrencies distinguishes it from a blockchain for financial transactions, which relies on the exchange of cryptocurrency with anonymous users on a public network (as in the case of bitcoin).

Blockchain is a decentralized database whose data block is connected chronologically. In the healthcare industry, there are many different parties who need to collaboratively manage personal EHRs blockchain (in a model of consortium blockchain), such as medical specialists, hospitals, insurance departments, etc. Electronic Record Systems are proprietary that is centralized bydesign. This means that, there's a single supplier that controls the code base, database and the system outputs and supplies the monitoring tools at the same time. It is difficult for centralized systems to gain trust from patients, doctors and hospital management. Open source, independently verifiable systems solve this issue. This paper deals with the Electronic Records for storing information of the patient which consist of the medical reports. Electronic Records (EHRs) are entirely controlled by Hospitals instead of

patients, which complicates seeking medical advices from different hospitals. These details are stored using the blockchain technology. In the existing system of storing details of the patients are very dependent on the servers of the organization. In the proposed all the information of the patient are stored in the blockchain by using the Meta mask and these details are stored in the block chain as a block of data. Each block consists of the data which is encrypted data. Electronic Record (EHR) systems record health-related information on anindividual so that it can be consulted by clinicians or staff for patient care. The data is encrypted by the algorithm known as SHA-256 which is used to encrypt all the data of the patients into a single line 256-bit encrypted text which will be stored in the block at Ether scan.

2. LITERATURE REVIEW

Electronic health data sharing and storage may be revolutionized by using blockchain technology. With its decentralized peer-to-peer network, blockchain technology has the potential to revolutionize the way electronic health records are exchanged and kept in the healthcare business. A Systematic Literature Review was selected to help and simplify this distributed ledger technology's knowledge. Research issues about EHR in a Blockchain context prompted a review of current literature on Blockchain in healthcare and the identification of any existing obstacles or open questions. Patients with chronic diseases, such as cancer, are more likely to seek out several hospitals or clinics for diagnosis and treatment because of the increased specialization of health care services and high levels of patient movement. A deeper understanding of a patient's medical history allows doctors to make faster clinical decisions, resulting in better, safer, and more efficient treatment for the patient. The majority of EHR data is still shared via fax or mail, despite the fact that electronic health records (EHR) offer greater privacy and sensitivity. This is due to a lack of systemic infrastructure support for secure, trustworthy health data sharing, which can cause significant delays in patient care. The current status of health care records is disconnected due to a lack of common designs and standards that would allow the safe transfer of sensitive information between stakeholders. Patients have limited access to their medical records in the current EHR context, and they are frequently unable to freely share their information with researchers or healthcare providers. Despite all of the advancements in medicine, various electronic health record systems do not interact efficiently with one another. Even today, fax machines and snail mail remain the major ways of sending healthcare information from one health facility to another. Each time a medical service is delivered, a health care institution records the service, monitors the patient's clinical information set, and updates the clinical information set. There is information about the patient's personal data, such as his or her gender and date of birth, and information about the particular service offered, such as the procedure done and the treatment plan, in this information. Those records are often kept in a database inside the company or among a predetermined network of health-care stakeholders, depending on the situation. This flow of information, which originates with the patient and continues through the health care organization each time a service is given, should not be limited to the level of the particular organization or to the level of the health care network alone, but should be expanded. Instead, the information pertaining to each patient encounter should be sent to a countrywide blockchain transaction layer, which would be secure and anonymous. Information saved on the blockchain, as a result, might be made generally accessible to a single person by virtue of his or her own private key on the blockchain. Patients may more easily communicate their information with multiple health-care institutions when they use a private key, which is more secure. Healthcare information is sensitive information that must be kept confidential at all costs. Consequently, each health organization's EHR system must create privacy measures to guarantee that only the patient and healthcare professionals have access to patient information.

Blockchain is considered as a new technological revolution that was introduced as the backbone of the Bitcoin cryptocurrency. It is a peer-to-peer distributed ledger technology to record transactions, agreements, and sales. The benefits of the blockchain technology are decentralized maintenance, data saving in the block-then-chain structure, secure transporting and accessing of data as well as anti-tamper and undeniable data security. Taking advantage ofthese distinguishing features above in an EHRs system, blockchain enables the management of authentication, confidentiality, accountability and data sharing while handing information related to privacy, medical resource saving and facilitating for the patient, and making population healthcare smarter. Assuming that there is an EHRs system in a cloud storage platform, which consists of some departments, such as hos- petals, pharmaceutical departments, insurance departments, disease research departments and so on, EHRs systems can be jointly managed. All departments can offer services for patients together and restrict the rights of each department to prevent EHRs abuse. Thus, an EHRs system with a blockchain structure is designed. Suppose that every patient owns one blockchain of healthcare alone. After being treated in a hospital, all the information including EHRs, consumption records, insurance records, etc. is encapsulated in one block. Patient treatments at different times will be generated in different bloc

3. SYSTEM HIERARCHY

3.1 Existing System

A single electronic health record was never intended to be managed by a single provider, but rather was scrambled among many institutions. Each hospital patient's data is kept by a single physician, and it's hard to look at the other doctors' earlier health records. (Greene, 2012). Each organization has its own access control system, which chooses whether to grant or prohibit access to certain individuals. Administration and management of the access control list are handled by a single organization. The centralized solution has two major drawbacks: it has a weak link and it has a unified power. A weak link happens when the unified admittance control framework fizzles; around then, nobody can get to the entire organization.

In the existing system the records are stored and maintained under the organization. So that,the patient can't able to access these records for further references. When the particular server(database) gets crashed then all the records will be spoiled. To overcome these drawbacks the proposed system is developed. Electronic Records (EHRs) provide a convenient record storage service, which promotes traditional patient medical records on paper to be electronically accessible on the web. In the current situation, patients scatter their EHRs across the different areas during life events, causing the EHRs to move from one service provider database to another.Therefore, the patient may lose control of the existing healthcare data, while the service provider usually maintains the primary stewardship. Patient access permissions to EHRs are very limited, and patients are typically unable to easily share these data with researchers or providers. Interoperability challenges between different providers, hospitals. The patient should have right toaccess his EHRs for managing and sharing them independently Institutions, etc.

This system was designed to allow patients to possess the control of generating, managing andsharing EHRs with family, friends, healthcare providers and other authorized data consumers. Moreover, provided that the healthcare researcher and providers of such service access theseEHRs across-the aboard, the transition program of healthcare solution is expected to be achieved. Without coordinated data management and exchange, the records are fragmented instead ofcohesive. If the patient has the capability of managing and sharing his EHRs securely and completely.

3.2 Proposed System

In the proposed future system, the patient should have right to access his EHRs for managing and sharing them independently. The patient can be accessing his medical report directly and can use the digitalized report with anyone. By storing the data in the blockchain the user's data isencrypted and stored as blocks in the ethers can. The user stores data by two-way authentication process such as getting secret key generated by the Meta mask. Electronic Health Record Systems are proprietary that is centralized by design. This means that, there's a single supplier that controlsthe code base, database and the system outputs and supplies the monitoring tools at the same time.It is difficult for centralized systems to gain trust from patients and doctors and hospital management. Open source, independently verifiable systems solve this issue. This system was designed to allow patients to possess the control of generating, managing and sharing EHRs with family, friends, healthcare providers and other authorized data consumers. Moreover, provided that the healthcare researcher and providers of such service access these EHRs across-the aboard, the transition program of healthcare solution is expected to be achieved.

Blockchain was at first gotten from the terms square and chain, with the term block alluding to a rundown of transactions that was related with the cryptographic Tech. Each square is connected to the square header that preceded it. Fundamentally, a blockchain is an organization of shared PCs controlling a circulated information base. Use it to monitor information and access it later. Each square contains the square header and every one of the transactions in it. The hash of the past block header, the timestamp, the nonce, and the Merkle root esteem are totally kept in the square header. The wellbeing information entered in the square can't be changed. Blockchain Tech's. essential objective is to eliminate information inconsistencies.

Utilizing the blockchain, monetary transactions might be recorded in a disseminated record. Bunch individuals might impart information to other specialist co-ops without the inclusion of an outsider and keep up with track of the transaction utilizing this assistance. Rather of putting away the information on a solitary server, it is repeated among a few PCs, making it undeniably challenging to control or wipe. Those sealed properties are reserved, and they are utilized in conjunction with a framework that guarantees any information went into the blockchain is authentic and encourages confidence among the gathering's members

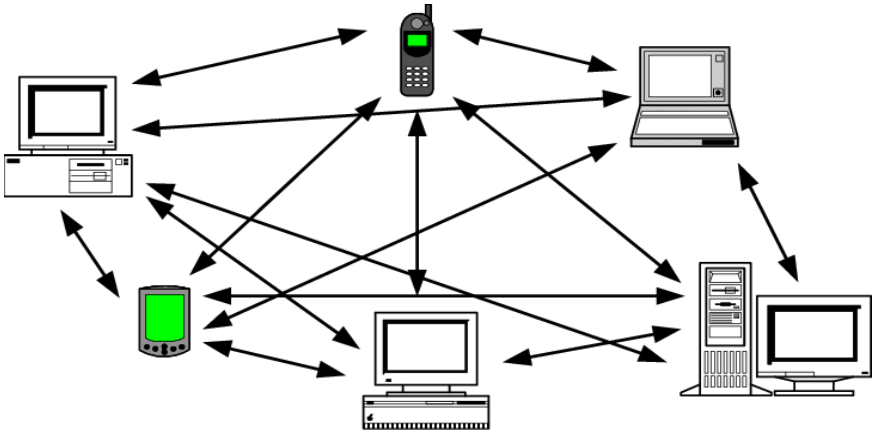

Figure 4: Peer-to-Peer Network

A blockchain is managed by a network of computers where there is no single computer is responsible for maintaining or storing the data, and any computers can enter or leave this network at any time Using Blockchain for records can make the whole process End to End verifiable and transparent. The stored data will be transactions, from which we can create a blockchain that will keep track of the database of the patient records. Using this approach, all the patients can make use of the records by themselves, and because of the blockchain they can use these records without any permission request from the organization directly by using the secret key given to them.

3.3 Module Description

Modules present in the proposed system are

- Ethereum
- Smart Contract
- Frontend Contract
- Truffle Framework
- Mist Browser

The combination of blockchain Tech. what's more, IPFS is great. A colossal amount of information has been put away in IPFS, and the content location of the information is changeless and structures a long-lasting connection, with the content location being given as contribution to the blockchain framework. The timestamp that is appended to the furthest limit of the information on a blockchain. The information is saved in the IPFS, and a connection is set up in the blockchain. Information ought to be saved in the IPFS organization and the hash worth ought to be recorded in the blockchain so the respectability of the information might be protected in the blockchain.

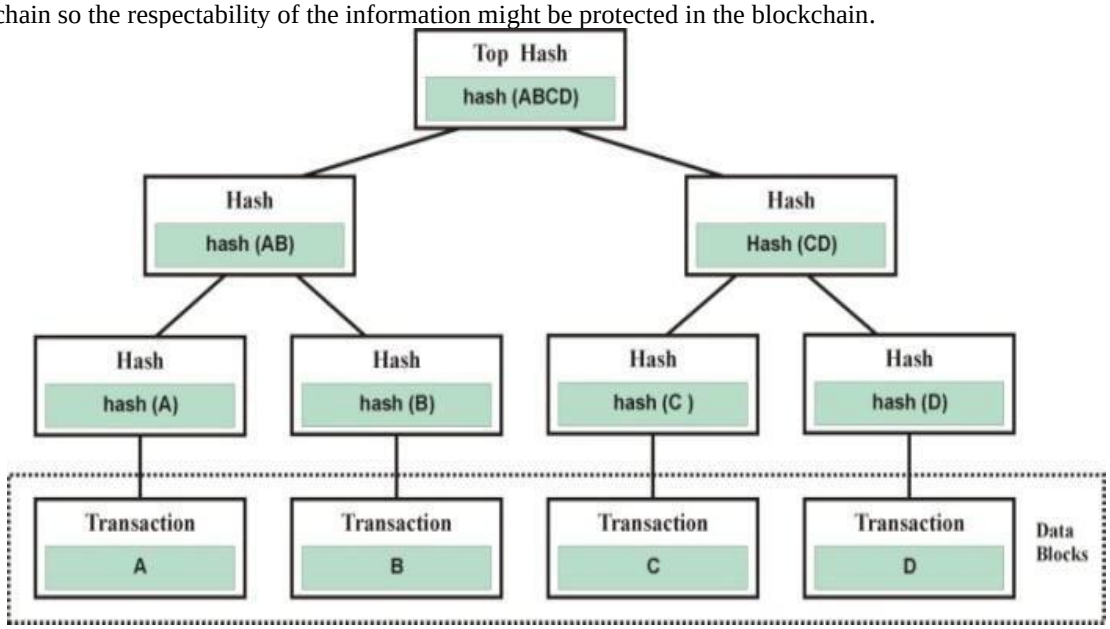

Figure 5: Process of Merkle Tree

4. RESULTS AND DISCUSSION

More practically and specifically for users, interoperability also refers to the objective of allowing users (for example, application developers) to operate with any blockchain without being limited by its implementation. Currently, one big limitation is that users must have thorough understanding of the technical aspects in order to connect with multiple blockchains, which is a significant barrier for many. Blockchains and cryptocurrency, on the other hand, if they become extensively utilized and present in everyday life, it is necessary to hide this complexity from the user and replace it with simple and clear interfaces. As a result, this thesis presents a method for delivering an easy-to-use interface for the interaction with numerous blockchains while maintaining security.

Models are Litecoin, which uses the Script hash function rather than the SHA256 hash function for evidence of work, and Touch coin, which records transactions on the blockchain multiple times speedier than both. Litecoin is a digital currency that was framed as a hard fork of the Bitcoin blockchain and has its own blockchain. Run is a digital currency that is to some degree like Bitcoin in that it utilizes the X11 hashing strategy to demonstrate that it has been dealt with (Duffield and Diaz 2014). Run, as Litecoin, works on a different blockchain, with transaction speeds that are multiple times faster than those of Bitcoin. Z-Money is an exceptionally safe digital currency that depends on zero-information evidences to secure its clients' protection and anonymity. As a consequence, clients' security and anonymity are considerably reinforced. The recommended SHA 256 with checked mystery key calculation's exhibition as far as square chain size, block generation, and absolute execution is displayed in Table 4. With various squares going from 50 to 500, as the quantity of squares changes, the square chain memory will grow attributable to the implanting of additional information into the square chain memory. The time it takes to produce a square is shown graphically as a straight function of the quantity of squares created. Block creation time ascends to 9.9747s when the blockchain memory is reached out to 0.2850Mb, demonstrating that the square generation time will develop assuming the quantity of squares is expanded also. The proposed SHA256-VK concerning blockchain memory is displayed in Fig. 6, and the proposed SHA256-VK with respect to obstruct creation is portrayed. The proposed SHA256-VK with respect to obstruct generation is portrayed in Fig.7.

Table 4. Quantitative analysis for the proposed SHA 256 with verifiable secret key Algorithm in terms of block generation time with respect to the memory acquire

Number of Blocks	Block Chain Memory Size (Mb)	Block Generation Time (secs)
50	0.28331	0.9973
100	0.28353	1.9946
150	0.28365	2.9919
200	0.28386	3.9913
250	0.28393	4.9867
300	0.28423	5.9852
350	0.28426	6.9825
400	0.28442	7.9796
450	0.28481	8.9774
500	0.2850	9.9747

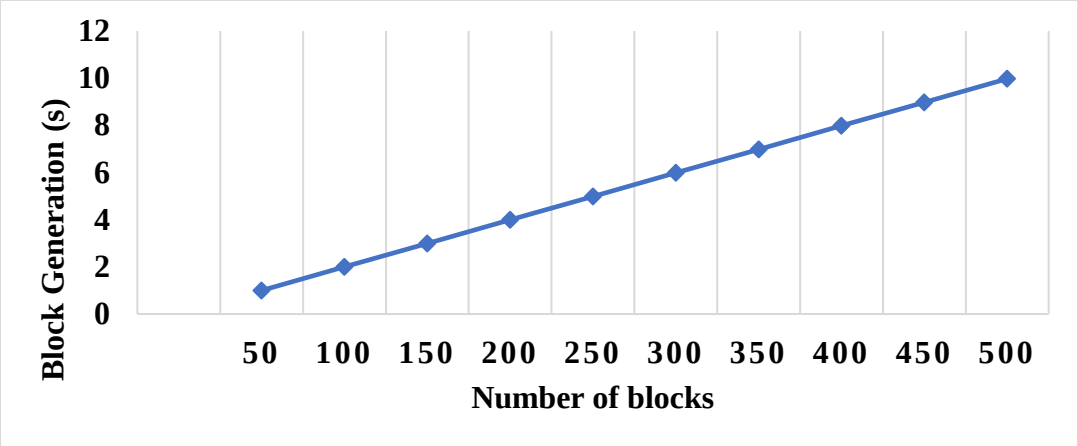

Figure 6: The graphical representation for the proposed SHA256-VK with respect to blockchain memory

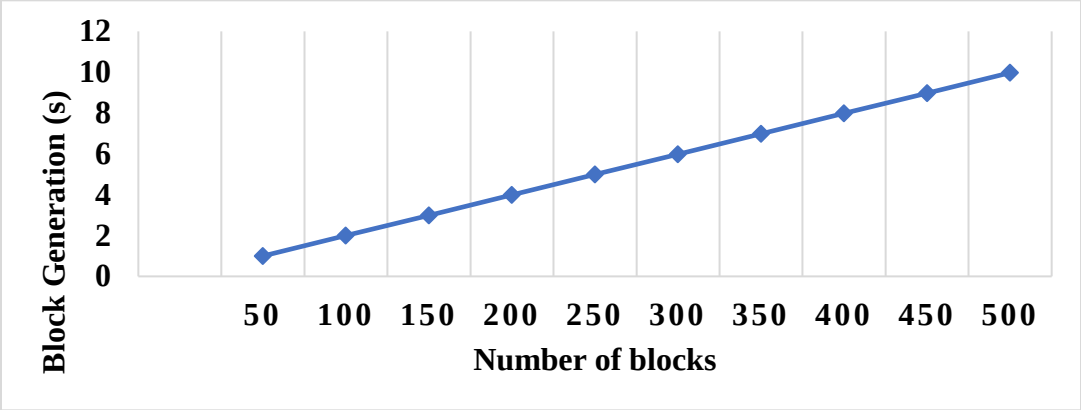

Figure 7: The graphical representation for the proposed SHA256-VK with respect to block generation

Table 5: Quantitative analysis for the proposed SHA 256-VK cryptographic scheme in terms of number of blocks with respect to the time execution (secs)

Number Of Blocks	Total Execution Time(secs)
50	58.897
100	60.835
150	61.835
200	61.888
250	63.829
300	63.839
350	64.839
400	69.844
450	70.867
500	78.791

As the number of block chains in the system grows, the overall time required for execution by the system grows as well. As the number of blocks rose from 50 to 500, the overall execution time in seconds climbed from 58.897 s to 78.71 s, indicating a decrease in efficiency. The quantitative analysis of the proposed SHA 256-VK cryptographic strategy in terms of the number of blocks with regard to the time required for its execution is shown in Table 5. (secs). Figure 8 depicts a graphical depiction of the entire time required for the execution of the programme.

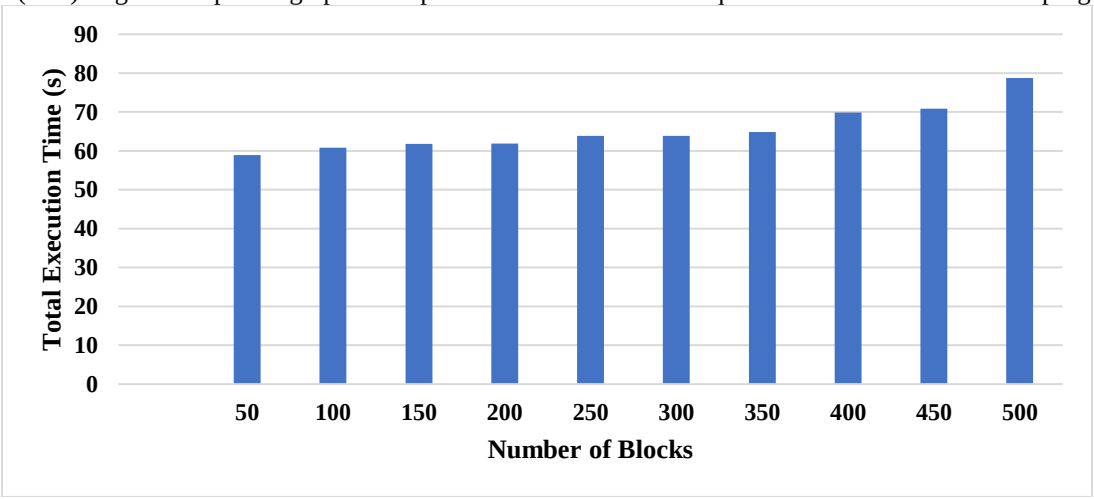

Figure 8 : The graphical representation for the proposed SHA256-VK with respect to total execution time (s)

A critical component of the recently recommended SHA256-VK cryptographic hashing approach is that it expands the security of the patient's information in such a way that an aggressor will not be able to switch the hashing system. This is because of the way that the SHA256 calculation utilizes a checked key, which has the ability of confirming or matching the new secret key by contrasting it with the authentication got, so working on both the

security and the handling speed. The relative examination for the current exploration work and the proposed research work is introduced in the table 4, and the graphical representation for the current examination work and the recommended procedure is shown in the figure 9.

Table 6: Comparative Analysis for the existing and the proposed research work

Authors	Methodology	Avg block time (s)
Lanxiang Chen et al [14]	Searchable Encryption	48.125
S. K. Tanzir Mehedi et al [12]	Smart-Contract Ethereum Distributed Ledger	14
Shailendra Rathore et al [13]	Decentralized Security -Software Defined Networking (SDN)	10
MyeongHyun Kim et al [15]	Elliptic Curve Cryptosystems (ECC)	5.88
Proposed method	**SHA256 with verification secret key**	5.48612

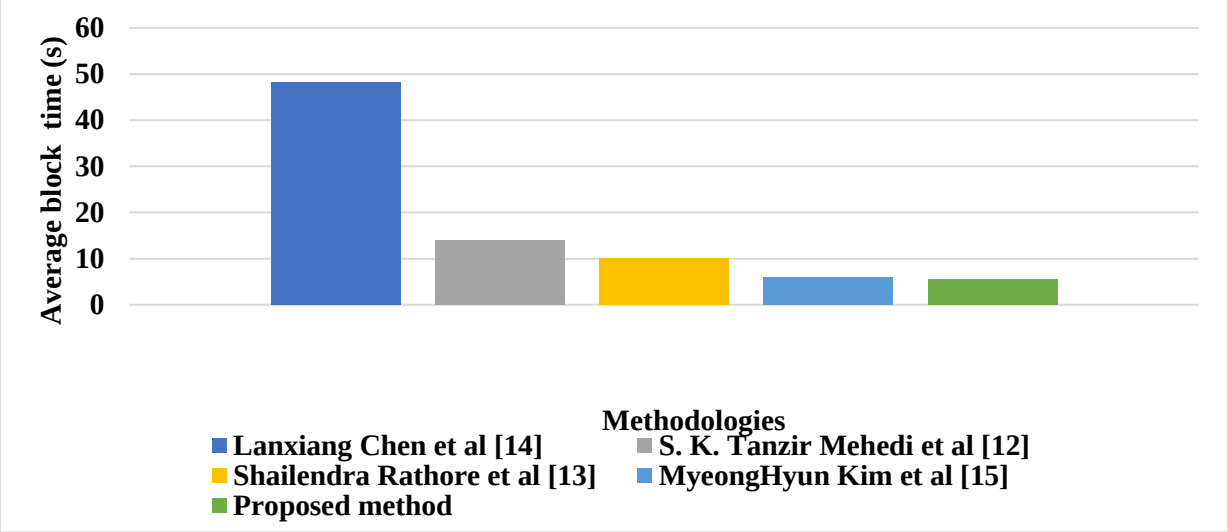

Figure 9: Graphical representation for the existing and the proposed SHA-256 VK scheme

5. CONCLUSION

The blockchain is considered as a capacity production network in which each operation can be approved, is responsible, and is permanent, and in which each transaction is recorded. Blockchain is a circulated, unchangeable record that makes the most common way of recording transactions and overseeing resources in a corporate organization more straightforward to oversee and follow. A resource might be either physical (like a home, vehicle, money, or land) or immaterial (like a business) (licensed innovation, licenses, copyrights, marking). For all intents and purposes everything of worth might be recorded and traded on a blockchain network, bringing down the danger and bringing down the expenses for everyone who is locked in. Information is the backbone of business. The more rapidly it is gotten and the more precisely it is determined, the better. Blockchain Tech. is fantastic for giving such information since it conveys constant, shareable, and totally straightforward information that is kept on a changeless record that must be gotten to by network clients who have been allowed permission to do as such. A blockchain organization might be utilized to monitor orders, instalments, records, production, and an assortment of different things. In addition, since individuals have a brought together point of view of reality, you can see each viewpoint beginning to end, giving you more confidence while additionally empowering you to exploit new efficiencies and potential outcomes. Operations frequently invest energy and assets on repetitive record keeping and outsider validations. It is workable for record-keeping frameworks to be exposed to extortion and cyberattacks. Information verification may be eased back by an absence of transparency. Moreover, with the introduction of the Internet of Things, transaction volumes have soar. All of this adversely affects organization and the reality, demonstrating that we want a more viable solution. This is the place where blockchain comes in.

6. FUTURE SCOPE

Medicine has become an indispensable aspect of our lives, and medical data such as prescriptions and past medical records has grown more important in the diagnosis of patients and the subsequent course of action. The traditional method of storing medical data was on paper, which was prone to being destroyed and altered over time.
Accordingly, it was needed to save the information in electronic structure. The clinical data set, on the other hand, might be modified with or totally cleaned. Then, at that point, there was the issue of information blockage, which caused some tension. Information obstructing happens when an element, for instance, a person, with or without his motivation, approaches information that ought not have been seen without the information on patients or clinics. In any event, with regards to working on the nature of treatment or tending to challenges like asset allocation and information blockage, Tech. has consistently assumed a significant part. On account of clinical consideration information trade, Tech. has needed to create through time.
The proposed Blockchain-based solution is a reasonable methodology that permits one to expand on SHA256 cryptographic calculations to guarantee information uprightness, normalized examining, and some formalized contracts for information access. It depends on SHA256 cryptographic calculations, which guarantees information uprightness, normalized reviewing, and some formalized contracts for information access. Since it is safer and proficient than other practically equivalent to techniques, the proposed SHA 256-VK calculation was viewed as proper for implementation in a genuine medical services framework for EHRs. Due to the utilization of a checked key in the current review, one advantage of using the proposed SHA 256 is that it is hard for programmers to reassemble the information from the hash esteem. Endeavors to reproduce the information by an interloper will bring about the confirmed key checking for the unique new secret word by contrasting it with the verified secret key being utilized.

7. REFERENCES

[1] R.Sangeetha, B.Harshini, A.Shanmugapriya, T.K.P. Rajagopal, "Electronic Health Record System using Blockchain", Rajagopal T K P et al. / International Research Journal of Multidisciplinary Technovation /2019, 1(2), 57-61

[2] .K. D. Mandl, P. Szolovits, and I. S.Kohane, Public standards and patients' control: How to keep electronic medical records accessible but private, *BMJ*, 2001, vol. 322, no. 7281, pp. 283_287.

[3] G. Irving and J. Holden, How blockchain-timestamped protocols could improve the trustworthiness of medical science ,F1000Research, 2016, vol. 5, p. 222.

[4] M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media,2015, pp. 53_68.

[5] M. Weinger, Dangers of postoperative opioids, APSF Newslett., 2007, vol. 21,no. 4, pp. 61– 68.

[6] Sung-Huai Hsieh, Sheau-Ling Hsieh, Po-Hsun Cheng, and Feipei Lai E-Health and Healthcare Enterprise Information System Leveraging Service-Oriented Architectur, Telemedicine and e-Health, 2012, Volume 18, No. 3.

[7] S.D. Cannoy and A.F. Salam, A Framework for Health Care Information Assurance Policy and Compliance, communications of the ACM, 2010 ,vol. 53, no. 3.

[8] Y.S.Rao and R. Dutta, Efficient attribute-based signature and signcryption realizing expressive access structures" IntJ. Seu, 2016 , vol. 15. no. 1, pp. 81-109.

[9] K. Gu, W. Jia, G. Wang, and S. Wen, Efficient and secure attribute-based signature for monotone predicates, Acta Inf., 2017, vol. 54. no. 5, pp, 521-541,.

[10] J Liu la Protecting mobile health records in cloud computing secure, efficient, and anonymous design | ACM Trans. Embed. Comput Syst., Apr. 2017, vol. 16. 10. 2.