The Impact of Blockchain Technology in Healthcare

Naman, Kamal Nain Sharma

LKCTC, Jalandhar

Corresponding author: Kamal Nain Sharma, Email: kamalnain3@gmail.com

Nowadays, healthcare systems are facing various problems in the fields of information security, data immutability, data sharing and management, trust, the privacy of the patients and transparency. The management of data by the patients and healthcare professionals is complicated as the existing healthcare systems are centralized. Blockchain technology can digitalize and change the way data is managed with its decentralized and peer-to-peer network approach. In this way, healthcare systems can benefit a lot from Blockchain technology. This paper helps to get an improved review of the recent works done on Healthcare applications based on Blockchain.

Keywords: Healthcare, Blockchain technology, data management, healthcare data, data sharing, privacy, security and transparency.

2023. In Vikram Dhiman & Pooja Dhand (eds.), *Emerging Trends in Engineering and Management*, 65–74. Computing & Intelligent Systems, SCRS, India.
https://doi.org/10.56155/978-81-955020-3-5-08

1. Introduction

The Healthcare industry has become a vital division of Information Technology (IT) because of the change in Electronic Health Records (EHR). This development is considered as an issue tackled by remote Healthcare professionals. The complex and enormous healthcare data gathered through a lot of sources lead to problems with medical data quality, including diagnosis, prediction and complicated analysis. It also leads to the threat of data confidentiality, which in turn leads to the rise in cybercrimes. Security of data is considered as a very important division of healthcare which also has a major part in sensitive data protection. The healthcare data get information of patients which must not be given to untrustworthy other people because of data abuses and security. The data consists of medical records containing personal patient information gathered from a patient's illness to recovery. Blockchain technology ensures reliability, trust and transparency. It permits various people to interact without the need of a central authority. It provides lots of benefits and helps in dealing with the healthcare challenges. The aim of this paper is to approve the potential roles of Blockchain technology in healthcare applications. This paper contains the recent research and related works of Blockchain technology in healthcare applications. In this paper, we present Blockchain overview, Blockchain for healthcare applications and some related works.

2. Blockchain Overview

In 2008, Blockchain technology was presented by Satoshi Nakamoto with the concept of Bitcoin cryptocurrency. Blockchain is a technology that combines incentive systems, data management, encryption and networking to allow participants to execute, record and check the transactions. Blockchain eliminates the requirement of a centralized and single authority still allowing for "trustless" and secure transactions among parties [1]. Blockchain is de-centralised as it is not owned by any one entity. The data inside the Blockchain cannot be tampered by anyone as the Blockchain is immutable. The transparency property allows a person to track the data easily.

2.1.1 Data structure

Blockchain consists of blocks of data joined cryptographically. Deploying the cryptographic hash, these blocks are chained in a series. A hash is created from a message or document. A hash is a specific length number. In a Blockchain network, a block consists of 4 parts: the previous block's hash, the current block's hash (an identifying number), information and the time stamp. The Blockchain consists of a chain of blocks which consists of the complete information of transaction records, eg : a classic public register. The header of block contains the version of block that specifies which rules of block validation should be used. The Merkle tree root hash states the hash values for every transaction in a block. The current time in seconds is determined by time stamp using universal time. The block-hash depicts the observed block data hash value [2].

The figure defines the structure of Blockchain:

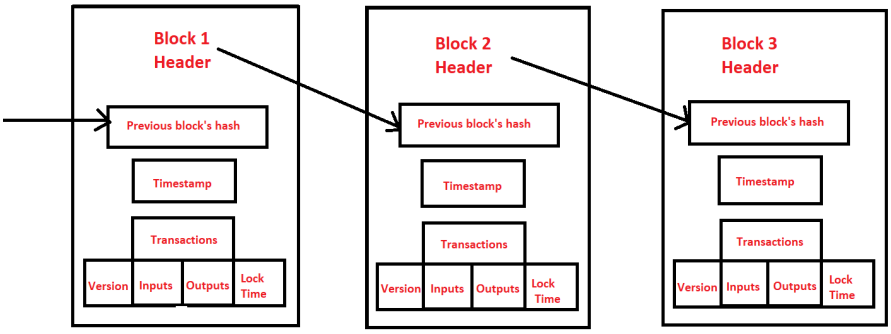

Fig. 1 : The structure of Blockchain.

A Blockchain is a DLT (distributed ledger technology). A massive computer database is used in the Blockchain to store and persist a continuous set of tries. The database consists of geographically unconstrained, various interconnected devices (computers, phones, embedded systems, etc).

Cryptography is an important technique that assures Blockchain's availability as well as security. Cryptography uses secure hash functions. Hashing is used to calculate a particularly unique output (digest or message digest) when provided by the input by using some cryptographic hash function. One may have some input, then hash it and get the identical/same output. This ensures that data is not changed. The output digest is entirely different even with a small change in its input. The key element of Blockchain security is hash. Anyone can verify if there is an inconsistency or an adversary trying to change the block's content by calculating a hash and then, matching it with the hash which is stored at the place of the previous hash of the following block.

The transfer of data/information among two or more different parties is known as a transaction. The transfer of crypto-currency between the participants of a Blockchain network is known as a transaction in the crypto-currency world. In a business to business context, the transaction is a way of maintaining an activity on physical or digital asset.

2.1.2 Distributed Network

The nodes are the participants of Blockchain which have a peer to peer network. The transactions of these participants are distributed and verified among a network of nodes. Each node stores its own local copy of Blockchain. Whenever a node retrieves the Blockchain, it checks and ensures the blocks' integrity by calculating all the hash values. Each node can easily send the transactions to the network and ask for these transactions to be put into the Blockchain; miners then validate the pending transactions. These miners are the peers who use their computational powers to mine a block. For generating a block, the miner nodes must solve a computational problem and utilize a particular amount of computer resources. The winner is the one who resolves the problem at first. This winner gets the right to create a new block [3].

2.1.3 Asymmetric Key Cryptography

The famous asymmetric public/private key and a hash cryptographic method is employed by the

Blockchain for validating the transaction authentication. The transactions of each node are signed using their private keys. All these transactions are broadcast across the whole network after being signed with a private key. Asymmetric algorithms are applied to encrypt data on Blockchain. For the encryption of plain text and decryption of cipher text in the asymmetric algorithms, we use distinct keys, commonly known as public key encryption. In this form of encryption, the receiver and the transmitter, both have a private and public key pairs. The key which is public, is distributed among the network, but the generating nodes only, are having the private key [4].

2.1.4 Digital signature

To verify the validity of digital messages or documents, we use a mathematical technique called a digital signature. Each user has a private as well as a public key pair. For signing the transactions, the private key is used , this key should be kept secretly. These transactions that are signed digitally, are then distributed among the entire network. There are two phases in a digital signature: the signing phase and the verification phase. These digital signatures are used to confirm the integrity of a file or message.

Overview regarding how Blockchain networks use the asymmetric-key cryptography:

- The transactions are signed digitally with the private keys.
- Addresses are formed using public keys.
- The signatures which are generated through the private keys are checked using the public keys.
- The asymmetric-key cryptography allows users to check if the person which is sending a value to another person have the private key required for signing the transaction or not.

2.2 Blockchain Deployment Models

There are 3 types of Blockchain deployment platforms : private, consortium and public.

2.2.1 Public Blockchain

The public blockchain is a decentralized and permission less Blockchain in which all the nodes of the network can access the information and can take part in its acceptance. It is also an open Blockchain which permits anyone to connect as a node and perform transactions. It ensures integrity and reliability by checking the work of the participants. The public Blockchain examples are Ethereum and Bitcoin. This Blockchain model ensures security with the help of its proof-of-work or proof-of-stake consensus process which creates an agreement between all the peers [5].

2.2.2 Private Blockchain

This type of Blockchain uses the Blockchain technology in the centralized way for increasing transaction speed and security. Unlike the public ones, private Blockchains cannot be accessed by the public and are controlled by only one entity. These Blockchains are not open and have access restrictions. This type of Blockchain is a permission network which controls that which of the nodes are allowed for processing transactions, executing smart contracts, and operating as the miners. A single trusted entity, or a third party oversees them [6]. Example: Hyperledger which is both a private and a permission Blockchain.

2.2.3 Consortium Blockchain

The Consortium Blockchain, are also known as the federated Blockchains are those where the data is easily accessible to every user, but only some groups can approve or modify it. It is a mixture of both private and

public Blockchains and contains both decentralized features and centralized features. Like private Blockchains, the Consortium Blockchains allow authorized persons only to write data as well as take part in the consensus processes. The Blockchain guarantees the public Blockchain's security while maintaining the decentralization and it also provides the entities with much security of sensitive data. Consortium Blockchains are mainly used in the financial sector.

2.3 Consensus Models

The Blockchain technology is an electronic ledger, which is distributed, and consists of digital data, transactions and events which are cryptographically secured, very hard to fake, and are not mutable by all the nodes which are connected with the help of a consensus mechanism. The nodes agree about how to accept or reject the transactions and blocks for avoiding any future disagreements, in the absence of a trusted party.

2.3.1 Proof-of-work

Satoshi Nakamoto proposed Proof-of-work (PoW). To record transactions in a decentralized network, someone must be chosen. The Proof-of-Work works on cryptography, that utilizes mathematical equations which only the computers are able to solve. After solving a computationally difficult problem first, a user can publish the new block in this PoW paradigm. It is highly complex structured which makes it very difficult to compute, but, checking the answer is very easy. It permits every complete node to easily check any of the recommended future blocks. Any of the suggested block which do not fulfill the solution's requirements will get rejected. It is also vulnerable to attacks. Hence, when a node wants to publish any block of transactions, it should first prove that these are not going to harm their network.

2.3.2 Proof-of-stake

Cryptographic algorithms are used for validation in proof-of-stake. The main idea of this type of consensus method is to use the stake (how many coins they hold) for choosing that who will get to mine for the next block of chain. The more stake a person has, the greater will be his mining power, and the more are the instances that he will be selected to check the new block. By utilizing the stake as a proof for gaining a profit, the person who has a larger stake may feel much at ease. This person may be easily forced to take part in a fraudulent thing for getting access to the various benefits of the chain.

2.3.3 Delegated Proof-of-stake

In the DPoS system, participants may vote for the nodes which use their resources in this Blockchain system. The strength of the vote of an individual is measured by the total number of tokens he has. Thus, a small collection of strong nodes can choose the witness and control the network. The nodes responsible for creating blocks are the nodes having a large number of votes or witnesses, whose efforts are compensated. For keeping the job, the witness should compete, as the network grows. This protocol consists of a continuous voting process.

2.3.4 Practical Byzantine Fault Tolerance (pBFT)

Derived from Byzantine general issues, BFT (Byzantine Fault Tolerance) tries to get a consensus between entities of a distributed network even when some of the nodes respond along with misleading information or fail in replying. The BFT mechanism makes collective decisions to reduce the effect of some faulty nodes

to protect networks from failures. Practical BFT works good with a small number of nodes, in dispersed networks, although, with every new node added in the network, the communication cost grows exponentially [7].

2.4 Smart Contract

In 1994, Nick proposed the term smart contract, as a computerized transaction protocol which uses the conditions of a contract. For meeting the common contractual criteria (for example : secrecy, enforcement, payment periods, and even liens), reduce unintentional and malicious exceptions, and to eradicate the requirement of trusted intermediaries are the main goals of smart contract design. The smart contract is a group of algorithms which are self-executing, tamper-resistant and self-verifying. The smart contracts are the contracts which execute automatically without the need of an intermediary, once all the conditions which are written in the computer code are satisfied. The Smart contracts which consists of Blockchain technology can do various tasks in real time with greater levels of security and low cost. The Smart contracts also does the part of trusted third parties, and intermediaries among contract participants. The Blockchain is a distributed network and is validated by the nodes of the network. They make use of automated code execution.

3 Blockchain in Healthcare Applications

3.1 Benefits of Blockchain

3.1.1 Decentralised storage

Decentralization states that there is not any central point of control. In reality, the decisions are taken through a consensus in a distributed computer network. Blockchain helps to store data transparently and with the originator's permission, provides it to the third parties. The best characteristic of a decentralized storage of data is that numerous copies of such information are kept at various locations.

3.1.2 Transparency

The entities should have a trust worthy connection for achieving information transparency in any technology. The Blockchains are called open-source as one can easily use these to view the transactions or their source codes. The healthcare record or medical data must be secure and safe. The data is spread between the network and saved in the Blockchain. This makes it much safer and transparent against the interference of third-parties [8].

3.1.3 Anonymity

Data movement and even transactions are anonymous as the Blockchain addresses the issue of entity-to-entity trust. Here, all what is needed is the Blockchain's address of a person.

3.1.4 Immutability

In most of the cases, a transaction which is added into the Blockchain ledger could not be reversed. This immutability is a very important characteristic which adds to the Blockchain transactions' integrity. Encryption is used to ensure the immutability of the Blockchain [9]. The new block is added only when a hard mathematical problem was solved and checked through a consensus mechanism. Every new block has a unique cryptographic key made from the previous block’s data and the key is added in a formula.

3.1.5 Security and Privacy

Security of a Blockchain ensures that it is protected from attacks. When the content of a block gets changed, then, that block's hash will also change. So, it will break the chain because each block has the hash of its preceding block. Therefore, for a chain to be intact, while modifying the data, its next blocks should also be changed.

3.2 Blockchain Disadvantages

3.2.1 Environmental Impact

The Blockchain networks, for example, Bitcoin, consumes loads of electricity to check the transactions, this leads to environmental issues.

3.2.2 Personal Responsibility

When investing in open source public Blockchains, you should be very careful because once you lose your seed phrases, then you cannot recover your wallets. There is no way going back and your money is lost forever.

3.2.3 Growing Pains

Very slow speed of transactions.

3.2.4 False Narratives

Many crypto-currencies are being used in illegal activities.

3.3 Blockchain in the Healthcare Application

The information transformations must be done in a secure environment. To automate a variety of methodological activities, data transformation technologies must be used, permitting entities to complete the transactions much faster. The previous healthcare application systems were used for building a trust worthy network, but they have 2 disadvantages. Greater transaction costs are required frequently by these circumstances than the public Blockchains, these should also be trusted much blindly, with very less consent for internal policies, ethics, or security. Secondly, using modern encryption, the information contained in the distributed public ledger is encrypted with much security, therefore, it is also resistant to any manipulations. It removes the requirement of centralized devices in linked objects and various other types of networking, allowing connected devices to handle problems, communicate directly, and update software.

4. Related Works

This part represents the related works of Blockchain in healthcare applications. This study assumes that the responsibility of management of consent is dispersed and assured among multiple entities, where each of them have different interests. Such technique increases confidence a lot. Since the third-party auditability of consent is available, the transparency is also offered. Here, we describe a healthcare data management system which is a patient-centric approach, that employs storage medium in the form of

Blockchain for ensuring anonymity. The utilization of various cryptographic methods for securing a patient's data ensures pseudonymity. Thus, the systems called MediBchain guarantees integrity, accountability, privacy, pseudonymity, and security of the healthcare data.M. A. Alam and H. Kaur developed the term Block Cloud. It defines the mixture of cloud computing and Blockchain. The main goal of the use of cloud is to have the data secure and dispersed under a single roof without any requirement of third parties. When we talk about enforcing and collaborating policies, research looks at the issues that public health agencies, medical organizations and practitioners, healthcare service providers, and governments have. The ProvChain is a provenance architecture based on cloud which aims at improving data privacy and availability. It is a completely decentralized system that works on cloud computing for providing tamper-proof access with the usage of Blockchain technology.

H Wang and X Yue gave the HGD (Healthcare Data Gateway) application's architecture. Such Blockchain-based application permits patients to share, own and control their information in a safer way without affecting their privacy. They also describe it as a new way of increasing intelligence of healthcare systems still protecting the privacy of the patient's data. The patients manage and own their health information by the access paradigm which is purpose centric. It offers a simple, unified Indicator Centric Schema (ICS) which gives an opportunity for managing every kind of personal health information simply and easily. The aim of J Ren and W. Tang is to increase the trust among caregivers and patients. They also suggested the healthcare system that preserves privacy in a trusted network. For locating and removing the phony patient from the network, it uses the Sybil attack. To grant entry of the authenticated individual to the healthcare centre, the recommended approach is used. The authors present the Healthchain as a privacy-preserving system for a lot of health data, which is works on Blockchain technology. We encrypt this healthcare data for performing fine-grained access control. Individuals can effectively add or remove the authorized doctors, by applying the user transactions for key management. Additionally, it helps to avoid medical conflicts because through the use of Healthchain, the doctor diagnoses and the IoT data, both would be nearly impossible to tamper with or remove. The table below, lists the examples of the applications, projects and platforms which work on Blockchain technology and used in the healthcare sector:

Table 1. Blockchain in healthcare applications

Application	Platform	Description	Scenario
BloCHIE	BloCHIE Platform	This platform analyses the requirements of healthcare data sharing, mainly for electronic medical records and personal healthcare data. It interacts with a number of other data types by integrating the Blockchains in multiple sources [11].	Healthcare information interoperability Data storage Privacy and authenticability Data sharing
MedBlock	MedBlock Platform	This is a secure method based on Blockchain, used for sharing the electronic medical details between individuals who are authorized.	Data security Data management Data sharing and privacy
OmniPHR	OmniPHR Platform	Through a public health record (PHR), the patients can access their information. For keeping updated information and for distinguishing between personal and electronic health records, this approach was created.	Security and privacy Data sharing Interoperability

MedRec	Ethereum	This record management system is decentralized. This is based on Blockchain model for confidentiality, authentication, data sharing and data management. It also employs every characteristic of the Blockchain, for eg, decentralized data and smart contracts.	Permission management Data management Data sharing Digital Rights Management Data integrity
MedChain	Ethereum	This is used to improve the current systems by permitting health care givers, patients and various other parties to use the medical records in a secure, effective and interoperable manner, along with maintaining the privacy of a patient. MedChain use the time based smart contracts for managing the transactions and limiting accessibility to the electronic medical information [10].	Security and privacy Data sharing Data management
MedShare	MedShare Platform	The data auditing, control, and provenance of medical data, which is exchanged in the cloud repositories by healthcare practitioners, medical researchers, and healthcare organizations, is enabled by a blockchain-based system. Furthermore, an access control mechanism and the smart contracts are also used in this architecture for tracking the activities of data efficiently.	Data security Data sharing Access control

5. Conclusion

Blockchain applications are used very widely. There are various challenges that must be addressed. Thus, the Blockchain will be much scalable, sustainable, and efficient. Regarding differently, the characteristics which they give are not novel, much of the systems they rely on are known from years. The collection of these various characteristics considers them best for a huge variety of applications. This depicts the huge rates of interest from a large number of sections. This article discusses some important application areas of healthcare in which the Blockchain technology can create a worthy impact. We also provide information about the various healthcare requirements and their solutions based on Blockchain.

References

[1] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. Available: https://bitcoin.org/bitcoin.pdf.
[2] M. Gupta, Blockchain for Dummies, IBM Limited Edition, 2017.
[3] J. A. Kroll, I. C. Davey, and E. W. Felten, The economics of bitcoin mining, or bitcoin in the presence of adversaries, Proc. WEIS, 2013.
[4] Gautam Srivastava, Shalini Dhar, Ashutosh Dhar Dwivedi, Jorge Crichigno, Blockchain Education, 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), 2019.
[5] Kim, Jin-whan, «Blockchain Technology and Its Applications: Case Studies, Journal of System and Management Sciences, 2020.
[6] Marko Hölbl, Marko Kompara, Aida Kamišali´c, Lili Nemec Zlatolas, A Systematic Review of the Use of Blockchain n Healthcare, Symmetry, 2018.
[7] V. Gramoli, From blockchain consensus back to byzantine consensus, Future Generation Computer Systems, 2017.
[8] Ayesha Shahnaz, Usman Qamar, And Ayesha Khalid, Using Blockchain for Electronic Health Records, IEEE Access, 2019.
[9] OECD Blockchain Primer, https://www.oecd.org/finance/OECD_Blockchain-Primer.pdf, 2018.
[10] Bingqing Shen, Jingzhi Guo, and Yilong Yang, MedChain: Efficient Healthcare Data Sharing via Blockchain, Applied sciences, 2019.
[11] Jiang, Shan, et al., «BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange, IEEE International Conference on Smart Computing, 2018.
[12] Impact of Blockchain technology in Healthcare