International Journal on Applications in Engineering and Technology
Volume 8 : Issue 2 : May 2022, pp 76 – 81 www.aetsjournal.com ISSN (Online) : 2455 - 0523

BLOCK CHAIN ENABLED HEALTHCARE SECURE DATA STORAGE SYSTEM

MOHAMMED ASIF M[1], KRISHNA PRASATH C[2], LOKESH B[3], MURUGESAN R[4]

[1,2,3] Undergraduate student, Department of Computer Science and Engineering
[4] Assistant professor, Department of Computer Science and Engineering

Abstract: *- – This project proposes the establishment of a blockchain-based system for managing medical records called Med Chain. Med Chain is intended to improve current systems by providing patients with interoperable, secure, and effective access to medical information. For managing transactions and limiting access to electronic medical records, Med Chain uses timed-based smart contracts. It uses modern encryption techniques for further protection, as well as an unique incentive scheme that rewards health practitioners for their efforts in keeping medical records up to date and producing new blocks.*

Key words: Med chain, interoperable, secure, electronic medical records.

I. INTRODUCTION

Interoperability in the field of data health is a challenge that has yet to be solved. The fundamental issue is how to enable open access to useful information (health data) Smart contracts and block chain technologies appear to be an intriguing and novel approach to maintain track of electronic health records references (EHRs). The use of block-chain technology in EHR systems has the potential to increase privacy and interoperability. The fast use of digitalization in healthcare has resulted in the creation of huge electronic patient records. As a result of this increase, there are never-before-seen needs for healthcare data security while in use and interchange. The emergence of blockchain technology as a responsible and transparent platform for storing and distributing data is opening the stage for new possibilities in healthcare data privacy, security, and integrity.

The data in each block is then confirmed using a consensus mechanism known as "Proof-of-Work (PoW)." After conducting the consensus method, the block will come into the chain, and every node in the network will admit it, spreading the chain indefinitely. Healthcare is one of the most well-known uses of blockchain technology. Blockchain's promise in healthcare is to solve problems such data security, privacy, sharing, and storage. Interoperability is one of the needs for the healthcare business. It is the capacity of two parties, human or computer, to share data or information in an accurate, efficient, and consistent manner.

1.1 Blockchain-Based Healthcare Applications

In many healthcare applications, blockchain technology is redefining data modelling and governance. This is owing to its versatility and unmatched capacity to segment, safeguard, and exchange medical data and services. Many contemporary advances in the healthcare field are based on blockchain technology.Data sources, blockchain technology, healthcare applications, and stakeholders are the four layers that make up emerging blockchain-based healthcare innovations. A blockchain-based process for healthcare applications is depicted in Figure 1. Initially, data from medical devices, labs, social media, and a variety of other sources is aggregated to generate raw data, which is then scaled up to become big data.

1.2 Blockchain-Based Healthcare Management Applications

New options for health data management, as well as patient ease in accessing and sharing their health data, are opening as electronic health-related data, cloud healthcare data storage, and patient data privacy protection policies advance [64]. Securing data, storage, transactions, and managing their seamless integration are crucial to any data-driven company, particularly in healthcare, where blockchain technology has the ability to address these critical concerns in a robust and effective manner. Figure 3 depicts the seven processes of a blockchain-based healthcare data management workflow, which are explained further below. Data sharing, data management, data storage (e.g., cloud-based apps), and EHR

are examples of blockchain-based applications in this area, which are covered in more detail below.

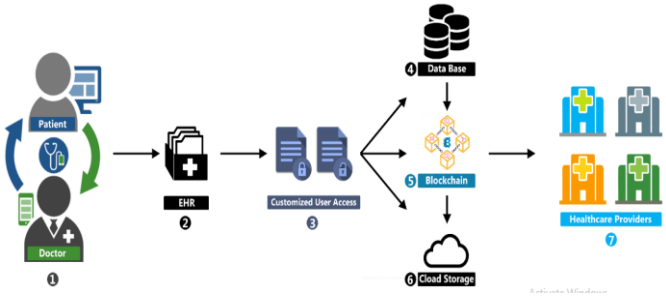


Chart -1: **Healthcare data management in blockchain**

II. Blockchain for Electronic Medical Record (EMR) Data management

The use of blockchain technology in hospitals has begun to be examined in a number of pilot projects throughout the world. Booz Allen Hamilton Consulting created and built a blockchain-based prototype platform in the United States last year to assist the Food and Drug Administration's Office of Translational Sciences in exploring ways to use the technology for healthcare data management (Figure 1). The pilot project, which uses Ethereum to govern data access via virtual private networks, is presently being implemented at four large hospitals. The project is based on IPFS, which allows it to use encryption and prevent data duplication by utilising off-chain cloud components and cryptographic techniques to enable user sharing.

2.1 Blockchain and Healthcare Data Protection

In Europe the relationship between blockchains and the General Data Protection Regulation (GDPR) is somewhat controversial. On one hand, blockchains seem to represent a good alignment with GDPR (when it comes to data portability, as an example, or consent management, data traceability and lawful access auditability). On the other hand, various issues can be identified (when it comes to right to be forgotten, but also when the technical implementation through smart contracts might weaken the actual control over data, through automatic execution). One option to tackle this issue is ‘dynamic consent management’, which is fully in line with the GDPR provision regarding consent. In addition, it is considered that ‘private blockchains’, e.g., Enterprise Blockchain can easily comply with GDPR directives since the transactions of the digital records of the stored information can be modified and erased by private entities or authorities can own and control this platform, using a particular class of consensus algorithm.

2.2 Blockchain for Personal Health Record (PHR) Data Management

Personal life-long data recently has begun to be captured through wearable sensors or medical IoT devices as personal health records (PHR). Real-time artificial intelligence (AI)-powered healthcare analytics will be fed back to the related users, including patients, physicians, pharmaceutical researchers, and payers. This entire PHR service trajectory is becoming a valuable source of data for blockchain service providers. Personal health record data for blockchain service providers or data brokers.Distributed or decentralized applications (Dapps) developed on the blockchain enable physicians and patients to easily participate in telemedicine with no middleman costs aside from the minimal fees of the Ethereum network, thus enhancing patient empowerment.

2.3 PROPOSED SYSTEM

For cancer patient care, a system for administering and EMR sharing information has been developed. A framework is imposed through a paradigm in conjunction with a hospital that assures privacy, security, availability, and fine-grained access management over EMR information. The proposed effort would significantly reduce the time it takes to share EMRs, enhance treatment decision-making, and lower the cost. This presents a unique opportunity to use block chain to create and deploy a secure, trustworthy EMR information management and sharing system.This system is being suggested. ETHEREUM Ethereum is a decentralised blockchain network that is based on the blockchain technology that was first employed in the popular crypto currency Bitcoin.

Ethereum was formally introduced in year 2015 and the idea behind Ethereum was to create a trustless smart contract platform that would be open-source and would also hold the feature of this technology also shares the peer-to-peer networking that makes it distributed.

III. ALGORITHM

Cryptography entails the creation of written code that must be decoded and encrypted by authorised individuals. A network manages the blockchain, which follows standards for nodal communication and verifying new blocks. Transactions are validated by miners before being posted on the blockchain. To validate and extract data, mining necessitates the implementation of an algorithm. Cryptocurrency is a type of digital money in which the regulation and production of currency units are governed via cryptography. Cryptocurrency is secured by encryption, and transactions are recorded via blockchain technology. A blockchain algorithm refers to the complete method, which includes everything from adding to the chain of records to confirming transactions**.** Blockchain technology is a collection of technologies that have been combined in novel ways. It is based on a protocol-based platform, a peer-to-peer network that serves as a system of record, and it employs private key cryptography for identity. A protocol includes an algorithm.As a result, there is no need for a trusted third party in a system of transactional exchanges. The sturdy, simple, yet complex network architecture of blockchain technology itself is implicit in the process of safeguarding digital interactions.

3.1CONSENSUS ALGORITHMS

The chain with the most work defines consensus. You will not have the mining strength to safeguard it if you fork and modify the POW. Accepting transactions, validating transactions, replicating transactions, validating blocks, replicating blocks, serving the blockchain, and storing the blockchain are all tasks that nodes do. Even the Proof-of-Work algorithm that miners must use is defined by nodes.

The Blockchain consensus protocol has several particular goals, including reaching an agreement, cooperation, co-operation, equal rights for all nodes, and each node's required involvement in the consensus process. As a result, a consensus algorithm seeks to identify a common accord that benefits the whole network.

1.Proof of Work (PoW):A miner is chosen for the next block creation using this consensus mechanism. This PoW consensus algorithm is used by Bitcoin. The main goal of this method is to solve a difficult mathematical puzzle and quickly provide a solution. Because this mathematical challenge necessitates a large amount of computer power, the node that solves it first gets to mine the next block. Please see Proof of Work (PoW) Consensus for more information on PoW.

2. Practical Byzantine Fault Tolerance (PBFT): Please see the page on practical Byzantine Fault Tolerance for more information (pBFT).

3. PoS (Proof of Stake):

This is the most popular PoW option. Ethereum's consensus has moved from PoW to PoS. Instead than investing in expensive technology.

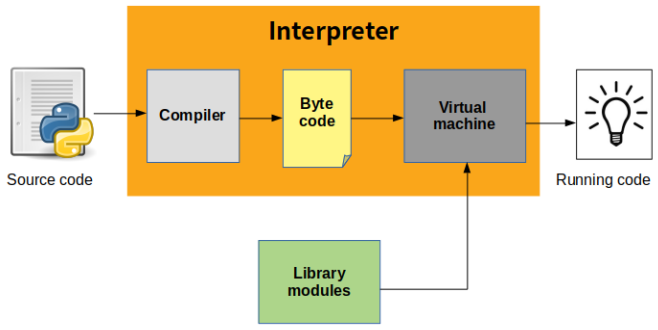
4. Proof of Burn (PoB):

Rather than investing in costly hardware, validators 'burn' coins by transferring them to an address where they are irreversibly lost. Validators gain the right to mine on the system by committing the money to an unreachable address, which is chosen at random. As a result, validators are making a long-term commitment in return for a short-term loss when they burn tokens.o solve a complicated issue, validators invest in the system's currency by locking up part of their coins as stake in this form of consensus process.

The blocks will then be validated by all of the validators. Validators will validate blocks by betting on them if they find one that they believe can be added.

IV.SOFTWARE ENVIRONMENT

Python is a high-level, general-purpose programming language with an interpreter. Procedural, object-oriented, and functional programming are among the programming paradigms supported. Because of its extensive standard library, Python is frequently referred to as a "batteries included" language.



LIMITATIONS

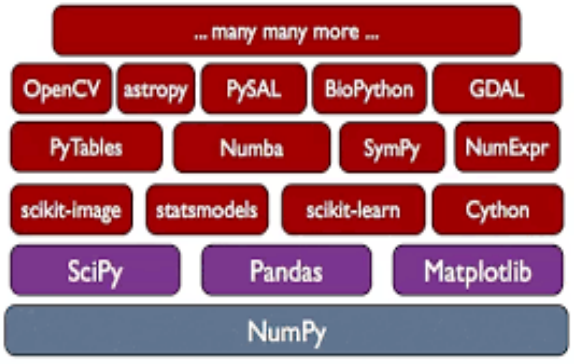
There are several issues with the compiler package's error checking. Syntax problems are detected by the interpreter in two stages. The parser of the interpreter detects one set of problems, while the compiler detects the other. Because the compiler package relies on the interpreter's parser, it receives free error checking in the early stages. It executes the second phase on its own, and it does so in an imperfect manner. When a name appears more than once in an argument list, for example, the compiler package does not produce an error: f(x, x) = f(x, x) = f(x, x) = f ...

IMPLEMENTATIONS

Reference implementation

CPython is the reference implementation of Python. It is written in C, meeting the C89 standard with several select C99 features. It compiles Python programs into an intermediate bytecode which is then executed by its virtual machine. CPython is distributed with a large standard library written PANDAS

In computer programming, pandas is a data manipulation and analysis software package designed for the Python programming language. It includes data structures and methods for manipulating numerical tables and time series, in particular. It's open-source software with a three-clause BSD licence. The word "panel data" is an econometrics term for data sets that comprise ob servations for the same persons over several time periods.



Features of the library

Adding a column to a data structurein a mixture of C and native Python. It is available for many platforms, including Windows and most modern Unix-like systems. Platform portability was one of its earliest priorities.

Other implementations

PyPy is a fast, compliant interpreter of Python 2.7 and 3.5. Its just-in-time compiler brings a significant speed improvement over CPython but several libraries written in C cannot be used with it.

USES

Python has been successfully embedded as a scripting language in many software products, including finite element method software such as Abaqus, 3D parametric modellers such as FreeCAD, 3D animation packages such as 3ds Max, Blender, Cinema 4D, Lightwave, Houdini, Maya, modo, MotionBuilder, Softimage, the visual effects compositor Nuke, 2D imaging programmes such as GIMP, Inkscape, Scribus, and Paint Shop Pro, and musical Python is used by GNU Debugger as a nice printer to display complicated structures such as C++ containers. Python is recommended by Esri as the best language for building scripts.

1) 5.SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

Black Box Testing

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot "see" into it. The test provides inputs and responds to outputs without considering how the software works.

V. CONCLUSION

We offered scenarios of block chain innovation value in a variety of social insurance contexts in this study, including critical attention, restorative data inquiry, and related wellbeing. We discussed how retaining a permanent and simple document, which video displays all of the events that occurred on the device, may help to enhance and encourage the management of therapeutic records. Medical scans give useful data from which value inferences can be drawn, resulting in beneficial outcomes.

In the MedChain, privacy is protected by using timed-based smart contracts to manage transactions and by enforcing appropriate use restrictions to monitor the calculations conducted on EMRs. Data integrity is ensured by the use of hashing algorithms. The department of security and access control is in charge of maintaining security and access control.

We offered scenarios of block chain innovation value in a variety of social insurance contexts in this study, including critical attention, restorative data inquiry, and related wellbeing. We discussed how retaining a permanent and simple document, which video displays all of the events that occurred on the device, may help to enhance and encourage the management of therapeutic records. Medical scans give useful information that may be used with the PoA fo It takes into account the importance of providers' work in keeping medical data and establishing new blocks. Because most existing health providers are welfare-oriented and do not aim to include any monetary value, our approach provides an incentive for the "block's maker" to be integrated to the system. Extensive experiments are conducted to evaluate the MedChain performance on different aspects, including response time, throughput, and communication overhead. Results indicate the efficiency of our proposal in handling a large dataset at low latency.

REFERENCE

[1]. A. R. Rajput, Q. Li, M. T. Ahvanooey, and I. Masood, ``EACMS: Emergency access control management system for personal health record based on blockchain," IEEE Access, vol. 7, pp. 8430484317, 2019.

[2]. R. Guo, H. Shi, Q. Zhao, and D. Zheng, ``Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," IEEE Access, vol. 6, pp. 1167611686, 2018.

[3]. L. X. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang,``Blockchain based searchable encryption for electronic health record sharing," Future Gener. Comput. Syst., vol. 95, pp. 420429, Jun. 2019.

[4]. L. A. Linn and M. B. Koo, ``Blockchain for health data and its potential use in health IT and health care related research," in Proc. ONC/NISTBlockchain Healthcare Res. Workshop., Gaithersburg, MD, USA, 2016,pp. 110.

[5]. D. Ivan, ``Moving toward a blockchain-based method for the secure stor-age of patient records," in Proc. ONC/NIST Blockchain Healthcare Res.Workshop, Gaithersburg, MD, USA, 2016, pp. 111.

[6]. [6] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, ``Integrating blockchainfor data sharing and collaboration in mobile healthcare applications,"in Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC), Montreal, QC, Canada, Oct. 2017, pp. 15.

[7]. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, ``MedRec: Using blockchain for medical data access and permission management," in Proc.2nd Int. Conf. Open Big Data, Aug. 2016, pp. 2530.

[8]. Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani,``MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 1475714767, 2017.

[9]. K. Culver, ``Blockchain technologies: A whitepaper discussing how the claims process can be improved," in Proc. ONC/NIST Use Blockchain Healthcare Res. Workshop, Gaithersburg, MD, USA, 2016. [Online]. Available: https://www.healthit.gov/sites/default/les/3-47-whitepaperblockchainforclaims_v10.pdf

[10]. S. Amofa, E. B. Sifah, K. O.-B. O. Agyekum, S. Abla, Q. Xia, J. C. Gee,and J. Gao, ``Ablockchain-based architecture framework for secure sharingof personal health data," in Proc. IEEE 20th Int. Conf. e-Health Netw.,Appl. Services (Healthcom), Ostrava, Czech Republic, Sep. 2018, pp. 16.

[11]. G.Yang and C. Li, ``Adesign of blockchain-based architecture for the security of electronic health record (EHR) systems," in Proc. IEEE Int. Conf.Cloud Comput. Technol. Sci. (CloudCom), Nicosia, Cyprus, Dec. 2018,pp. 261265.

[12]. G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella,``Ancile:Privacy-preserving framework for access control and interoperability ofelectronic health records using blockchain technology," Sustain. CitiesSoc., vol. 39, pp. 283297, May 2018.

[13]. X. Zhang, S. Poslad, and Z. Ma, ``Block-based access control for blockchain-based electronic medical records (EMRs) query in eHealth,"in Proc. IEEE Global Commun. Conf. (GLOBECOM), Abu Dhabi,United Arab Emirates, Dec. 2018, pp. 17.

[14]. A. A. Alomar, M. Z. A. Bhuiyan, and A. Basu, S. Kiyomoto, and M. S. Rahman, ``Privacy-friendly platform for healthcare data in cloud based on blockchain environment," Future Gener. Comput. Syst., vol. 95, pp. 511521, Jun. 2019.

BIOGRAPHIES

MOHAMMED ASIF M is an Undergraduate student, department of computer science and engineering in paavai college of engineering.

KRISHNA PRASATH C is an Undergraduate student, department of computer science and engineering in paavai college of engineering.

LOKESH B is an Undergraduate student, department of computer science and engineering in paavai college of engineering.

MR. R. MURUGESAN is Associate Professor and Head of Department(HOD),Department Of Computer Science and Engineering in Paavai College Of Engineering.