SYNOPSIS

Report on

SMART CONTRACT ENABLED PATIENT'S ELECTRONIC HEALTH RECORDS SHARING SYSTEM

by

Kajal Punia (2000290140055)

Niharika Baliyan (2000290140058)

Session:2021-2022 (4th Semester)

Under the supervision of

Prof. (Dr.) Arun Kumar Tripathi

Co-supervisor

Mr. Apoorv Jain (Blockchain developer)

KIET Group of Institutions, Delhi-NCR, Ghaziabad

DEPARTMENT OF COMPUTER APPLICATIONS

KIET GROUP OF INSTITUTIONS, DELHI-NCR, GHAZIABAD-201206

(MARCH- 2022)

ABSTRACT

Due to enhancement of the information technology all over the world, we shifted from an old paper-based medical record system to a digitized one which is a cloud-based system. Although it provided the world with better financial opportunities and increased the control of patients over their records. But it also has numerous downsides like being easily hackable because of a centralized storing system, privacy issues due to third-party involvement, and increased latency issues. We can get a grip on these vulnerabilities with the help of Blockchain. Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets. It is almost impossible to tamper with the data in blockchain due to the use of hashing and different consensus algorithms which ensure data integrity and security. Hashing is a cryptography process for converting any data form into a unique text string. Furthermore, a smart contract that is implemented on the Ethereum blockchain is used to make the system more effective. Smart contracts are computer programs that self-execute when predefined conditions are fulfilled. This paper focuses on a smart contract-enabled health record system. The proposed system completely eliminates the role of third parties which enhances the privacy of a patient and makes the health record system more patient-centric.

KEYWORDS: [Blockchain, Smart Contract, E-health, Ethereum, Electronic Health Records, Healthcare sector Innovation, Proof of stake]

TABLE OF CONTENTS

INTRODUCTION

A blockchain is a distributed decentralized ledger to record transactions between parties [1]. Blockchain has the power to revolutionize the healthcare industry [2]. By providing doctors, patients, clinical trial practitioners, and other healthcare professionals with a mechanism for the controlled exchange of sensitive, permission data, blockchain technology can improve data sharing and interoperability between data systems. Healthcare organization that takes part in a blockchain confederation can share medical information, without worrying about their native electronic health record systems. Blockchain also helps healthcare organizations to deliver more efficacious medications and diagnoses through increased provider data sharing and potentially secure and more powerful clinical trials through research methods. Smart contracts are self-executing contracts with the terms of the agreement between interested parties. They are written in the form of program codes that prevails across a distributed, decentralized blockchain network. Smart contracts allow transactions to be conducted between anonymous or untrusted parties without the need for a central authority [2]. In this paper, we propose a system on how health records could be shared among stakeholders while still taking into consideration of patient privacy and data integrity by using blockchain technology.

LITERATURE REVIEW

In the paper, "A Systematic Mapping Study on Current Research Topics in Smart Contracts" [1], the authors discussed smart contracts in blockchain. A smart contract is an executable code that runs on top of the blockchain to facilitate, execute and enforce an agreement between untrusted parties without the involvement of a trusted third party. The authors conducted a systematic mapping study to collect all research that is relevant to smart contracts from a technical perspective. The aim of doing so is to identify current research topics and open challenges for future studies in smart contract research. They extract 24 papers from different scientific databases. The results show that about two-thirds of the papers focus on identifying and tackling smart contract issues. Four key issues are identified, namely, codifying, security, privacy, and performance issues. The rest of the paper focuses on smart contracts' applications or other smart contract-related topics. Research gaps that need to be addressed in future studies are also provided in the paper.

Zheng and other authors presented an overview of blockchain architecture firstly and compare some typical consensus algorithms used in different blockchains [2]. Blockchain, the foundation of Bitcoin, has received extensive attention recently. The blockchain serves as an immutable ledger that allows transactions to take place in a decentralized manner. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation systems and Internet of Things, and so on. However, there are still many challenges of blockchain technology such as scalability and security problems waiting to be overcome. Furthermore, technical challenges and recent advances are briefly listed. The authors also lay out possible future trends for blockchain.

Simanta Shekhar provided background on Blockchain technology, history, its architecture, how it works, advantages and disadvantages, and its application in different industries [3]. Blockchain is one of the most important technological inventions in recent years. Blockchain is a transparent money exchange system that has transformed the way a business is conducted. Companies and tech giants have started investing significantly in the blockchain market. It has become popular because of its irrefutable security and the ability to provide a complete solution to digital identity issues. It is a digital ledger in a peer-to-peer network.

In this paper, the authors gave the blockchain taxonomy, introduced typical blockchain consensus algorithms, reviewed blockchain applications, and discussed technical challenges as well as recent advances in tackling the challenges [4]. Blockchain has numerous benefits such as decentralization, persistency, anonymity, and audibility. There is a wide spectrum of blockchain applications ranging from cryptocurrency, financial services, risk management, internet of things to public and social services. Although a number of studies focus on using blockchain technology in various application aspects, there is no comprehensive survey on blockchain technology from both technological and application perspectives. To fill this gap, the authors conducted a comprehensive survey on blockchain technology. Moreover, this paper also points out the future directions in blockchain technology.

N. Chaudhry and M. M. Yousaf investigated new ways to design and evaluate different consensus algorithms [5]. Blockchain is a distributed ledger that gained prevalent attention in many areas. Many industries have started to implement blockchain solutions for their application and services. It is important to know the key components, functional characteristics, and architecture of blockchain to understand its impact and applicability to various applications. The most well-known use case of blockchain is bitcoin: a cryptocurrency. Being a distributed ledger,

a consensus mechanism is needed among peer nodes of a blockchain network to ensure its proper working. Many consensus algorithms have been proposed in literature each having its own performance and security characteristics. One consensus algorithm cannot serve the requirements of every application. It is vital to technically compare the available consensus algorithms to highlight their strengths, weaknesses, and use cases. We have identified and discussed parameters related to the performance and security of consensus in the blockchain. The consensus algorithms are analyzed and compared with respect to these parameters. A research gap regarding designing an efficient consensus algorithm and evaluating existing algorithms is presented. This paper will act as a guide for developers and researchers to evaluate and design a consensus algorithm.

In the paper, "Healthcare Data Breaches: Insights and Implications. Healthcare (Basel)" [6], the authors provided detailed information about the digitization of the healthcare industry. The Internet of Medical Things, Smart Devices, Information Systems, and Cloud Services have led to a digital transformation of the healthcare industry. Digital healthcare services have paved the way for easier and more accessible treatment, thus making our lives far more comfortable. However, the present-day healthcare industry has also become the main victim of external as well as internal attacks. Data breaches are not just a concern and complication for security experts; they also affect clients, stakeholders, organizations, and businesses. Though the data breaches are of different types, their impact is almost always the same. This study provides insights into the various categories of data breaches faced by different organizations. The main objective is to do an in-depth analysis of healthcare data breaches and draw inferences from them, thereby using the findings to improve healthcare data confidentiality. The study found that hacking/IT incidents are the most prevalent forms of attack behind healthcare data breaches, followed by unauthorized internal disclosures. The frequency of healthcare data breaches, the magnitude of exposed records,

and financial losses due to breached records are increasing rapidly. Data from the healthcare industry is regarded as being highly valuable. This has become a major lure for the misappropriation and pilferage of healthcare data. Addressing this anomaly, the present study employs the simple moving average method and the simple exponential smoothing method of time series analysis to examine the trend of healthcare data breaches and their cost. Of the two methods, the simple moving average method provided more reliable forecasting results.

The authors of this paper [7] investigated the privacy issues in blockchain-based electronic health systems. Blockchain-based electronic health system growth is hindered by privacy, confidentiality, and security. By protecting against them, this research aims to develop cybersecurity measurement approaches to ensure the security and privacy of patient information using blockchain technology in healthcare. Blockchains need huge resources to store big data. This paper presents an innovative solution, namely patient-centric healthcare data management (PCHDM). It comprises the following: (i) in an on-chain health record database, hashes of health records are stored as health record chains in Hyperledger fabric, and (ii) off-chain solutions that encrypt actual health data and store it securely over the interplanetary file system (IPFS) which is the decentralized cloud storage system that ensures scalability, confidentiality, and resolves the problem of blockchain data storage. A security smart contract hosted through container technology with Byzantine Fault Tolerance consensus ensures patient privacy by verifying patient preferences before sharing health records. The Distributed Ledger technology performance is tested under hyper ledger caliper benchmarks in terms of transaction latency, resource utilization, and transaction per second. The model provides stakeholders with increased confidence in collaborating and sharing their health records.

RESEARCH OBJECTIVE

The main objective of this paper is to set forth the drawbacks of the current cloud-based electronic health record sharing system and propose a new smart contract-based system. The proposed system will enable the patients to share their medical records directly with the doctor without the interference of any third party. The proposed system uses blockchain technology with smart contracts. Thus, making the entire process more secure, reliable, fast, and privacy-oriented.

RESEARCH METHODOLOGY

1. Referencing research papers on Blockchain, smart contracts, and consulting with a blockchain developer.
2. The current cloud-based system has several drawbacks like security breaches, privacy issues, and high controlling costs.
3. The idea is to use multiple smart contracts for the sharing of electronic health records to overcome the above-listed shortcomings.

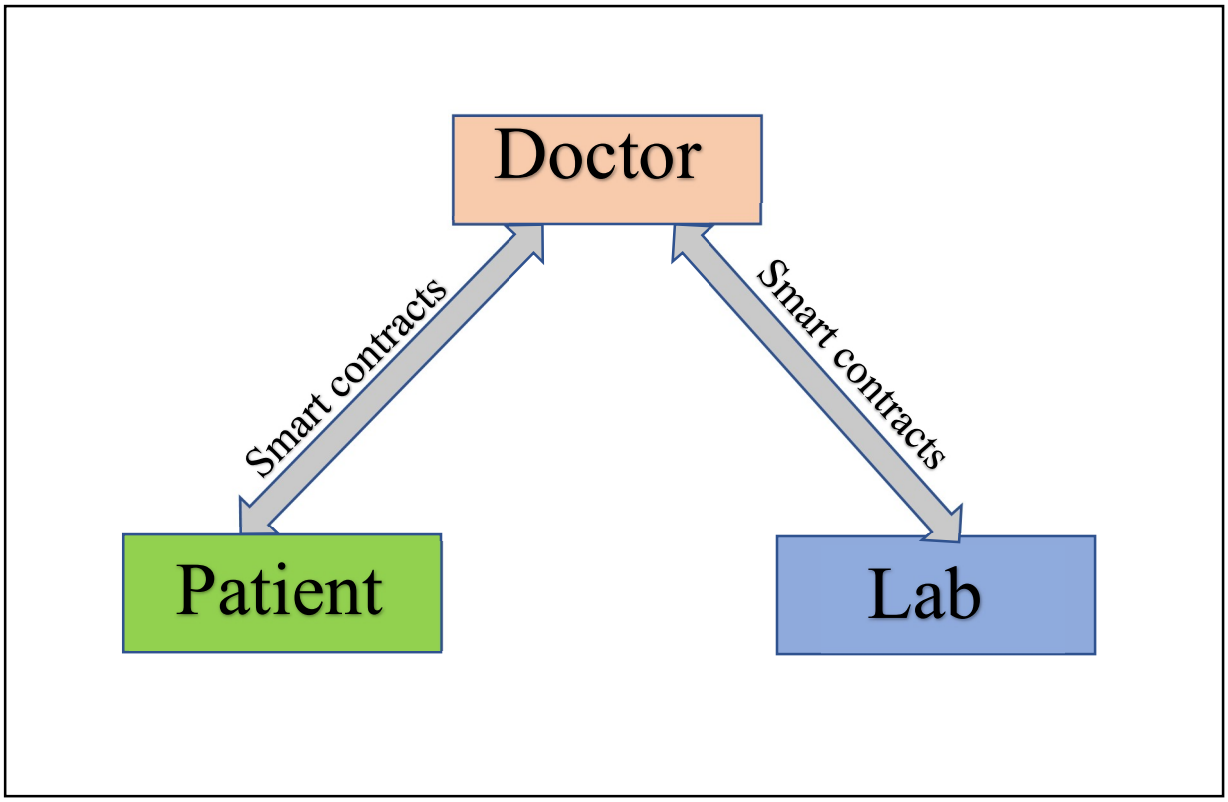

Figure 1: Sharing of data using smart contracts between patient, doctor and lab

RESEARCH OUTCOME

We are focusing on n submitting our paper in Scopus Conference (IEEE/Springer) and then submitting a modified version of this paper in Scopus Journal.

PROPOSED TIME DURATION

The estimated time for the completion of this research paper is of 2 months.

	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8
Feasibility Study								
Research work								
Paper writing								
Implementation								

REFERENCES

[1] Maher Alharby, Amjad Aldweesh, Aad vad Moorsel (2017) "Blockchain-based Smart Contracts: A systematic mapping study of academic research", AIRCC's International Journal of Computer Science and Information Technology, Vol 9, No 5 (2017)
Pages: 151-164

[2] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin, "An Overview of Blockchain Technology: Architecture,
Consensus, and Future Trends", 6th IEEE International Congress on Big Data, June 2017.

[3] Simanta Shekhar Sarmah, Understanding Blockchain Technology, Computer Science and Engineering, Vol. 8 No. 2, 2018, pp. 23-29. doi: 10.5923/j.computer.20180802.02.

[4] Zibin Zheng and Shaoan Xie, Hong-Ning Dai, Xiangping Chen, Huaimin Wang (2018),"Blockchain challenges and opportunities: a survey", Int. J. Web and Grid Services, Vol. 14, No. 4, pp.352–375.

[5] N. Chaudhry and M. M. Yousaf, "Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities," 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), 2018, pp. 54-63, doi: 10.1109/ICOSST.2018.8632190.

[6] Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, Khan RA. "Healthcare Data Breaches: Insights and Implications. Healthcare (Basel)", 2020 May 13;8(2):133. doi: 10.3390/healthcare8020133.

[7] Vinodhini Mani, Prakash Manickam, Youseef Alotaibi, Saleh Alghamdi, Osamah Ibrahim Khalaf (2021) "Hyperledger Healthchain: Patient-Centric IPFS-Based Storage of Health Records", Electronics, Volume 10, Issue 23, page 3003.