ISSN : 2347 - 2243

Indo - American Journal of Life Sciences and Biotechnology

www.iajlb.com
Email : editor@iajlb.com or iajlb.editor@gamil.com

Indo-Am. J. of Life Sc& Bt.,2016- *ISSN:2347-2243www.iajlb.com*
Vol.13, Issue.2, June 2016

Indo-American Journal of Life Sciences and Biotechnology

The Study of Population Genetics Structure of Holothuria parva in the Persian Gulf Using mt DNA Sequences

Mohammad Ali Salari Ali-Abadi

ABSTRACT

The healthcare industry has historically faced challenges in the transmission of medical records from one facility to another due to privacy concerns and the apprehension that others may exploit the exchange of information. Nevertheless, this is evolving.

Health care organizations are unable to obtain long-term patient information as a result of inconsistent policies and permissions that have been granted. The ability to exchange electronic health records will enhance the accuracy of diagnostics when it comes to identifying medical conditions. In order to enhance patient data security and prevent the loss or manipulation of medical records, this system is advised to implement blockchain technology. This survey aims to gain a deeper understanding of the technology's functionality and potential applications in the healthcare sector, specifically the concept of mining and smart contracts. Block chain technology is a secure method of sharing and preserving medical records with other organizations, ensuring that they are not tampered with.

Keywords:- "Miners" are also considered members of the mining community in this context.

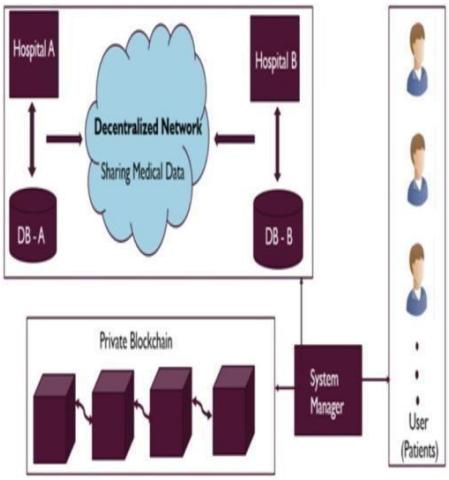
INTRODUCTION

Electronic health data exchange will enhance the precision of categorization in systems that prioritize security and privacy. The immutability characteristics of blockchain have recently been recognized as a viable solution for the exchange of personal health information (PHI) while maintaining security and privacy. This paper suggests data exchange schemes for e-Health systems that are based on block chains. The block chain will encompass all of the patient's medical information. history, which encompasses the patient's familial history of medical issues, as well as their current and previous therapies. This will guarantee that medical records are never lost or altered, as they will be permanently stored, transferable, and readily accessible.

[1]M.tech Student,Department of ECE,Siddharth Institute Of Engineering And Technology,Puttur
[2]Assistant Professor,Departmento f ECE,Siddharth in statute of engineering and technology,puttur

Block chains will assume control over a diverse array of stakeholders and purposes. The utilization of blockchain technology may facilitate the accessibility of electronic health records by establishing a frictionless connection that is supported by reliable permission and solid contracts. In order to verify that the original signed note has not been altered, it may be compared to a tamperproof ledger of hashes.

1. That degree of security cannot be provided by standard information technology. It



is a blockchain-based application. By exchanging information with one another, hospital systems from across the nation have collaborated to enhance interoperability. Nevertheless, the patient-centered capability is accompanied by new and critical demands and issues related to technology, incentives, governance, and security and privacy that must be resolved in order for this form of data sharing to operate on a large scale. This transformation may be facilitated by blockchain technology, which offers mechanisms such as (1) digital access rules, (2) digital data aggregation, (3) data liquidity, (4) patient identification, and (5) data immutability. Subsequently, we will examine roadblocks to patient care.

The number of clinical data transactions, privacy and security, and appointment scheduling for patients are all examples of the driven interoperability that block chains provide. Although the patient-driven ability is a thrilling trend in care, it remains to be seen whether block chain technology can facilitate the transition from institution-centric to patient-focused data exchange, given these constraints. The health care block chain technology will have three distinct effects. Patient data is ultimately dispersed across multiple locations as a result of the interaction between these centralised systems. A dearth of trustworthy information and sluggish user interfaces could have catastrophic consequences. Consequently, it is imperative to establish a blockchain-based system that can store clinically pertinent patient data and facilitate immediate access from any location.

3. Patient information is exclusively accessible to individuals who have been medically approved to use a secure local network, guaranteeing that patients' privacy is guaranteed at all times. Medical centers are unable to dispense medication due to digital patient data.

4. Rather than relying on centralized servers to store data from multiple locations, we can store it locally on the devices of each facility. As evidenced by the recent ransomware attacks on NHS hospitals in the United Kingdom, they are a primary target for hackers. The issue of fragmentation persists, even in the absence of any proven security concerns. As a consequence, there has been a recent emphasis on patient-driven capabilities, which is characterized by the increasing prevalence of patient-mediated and patient-driven health data exchange. The following are definitions for terms that are frequently encountered in academic writing: 5. Block chain: A block chain is a collection of linked blocks, each of which contains valuable data.

not under the supervision of a central authority. Using cryptography, it is both secure and unalterable.

6. Blockchain is characterized as decentralised due to the absence of a central authority that supervises all aspects.

7. Consensus mechanisms may facilitate the resolution of certain matters in decentralized networks.

8. Miners: Individuals who utilize the computing capacity of their devices to mine for data.

9. The creation and maintenance of a public block chain are challenging for a variety of reasons [4].

EXISTINGSYSTEM

As a result of the widely diverse and inconsistent data processing techniques used by hospitals and clinics, patient records are often incomplete or inconsistent. Authentication and secrecy are important considerations for health care programmes like MedRec, which make use of the blockchain to make data exchange easier.Due to privacy issues, the transfer of health care data from one institution to another has been a difficult undertaking.

Fear of allowing others to get an unfair advantage by providing information Health careinstitutions cannot get real-time access to patient data because of inconsistency in policies and agreements. The accuracy of diagnosis may be improved via electronic health record exchange, where security and privacy protection are essential considerations. Healthcare firms must be prepared to build the necessary technological infrastructure before blockchain can have a positive impact on the sector's operations. Block chain is expensive, there are questions about its integration with current technology, and there is a lot of conjecture about how it will be adopted culturally. It's clear that block chain has taken the healthcare industry by storm in the last year, with huge investments in the technology. With so many possibilities, it's no wonder that block chain is quickly becoming one of the most important cornerstones of the digital world's infrastructure. And maybe one day, the big datalandscape will be transformed by it. New cost- effective analyses are now available to the public thanks to the release of accountable treatment data and insurance billing information. Auditable e-Health records are provided by our system, while patient privacy and security are also protected. The huge e-Health blocks are available to medical researchers, while government and regulatory organisations are granted extra identities for audit and conformity reasons, as well. Block chain technology will ultimately become widely adopted in e-Health due to a huge number of developers and significant levels of interest in the field. Our method is a decent effort to further enhance the efficiency and dependability inherent in the block chain's design. Additional tailored treatment is made possible by the comprehensive and consistent data blocks accessible to all service providers engaged when computational logics are implemented in e-Health block chains. The e-We're equipped to handle anything from security audits to regulatory compliance reporting to billing updates to notifications from test findings and drug occurrences.

Private block chain view

LITERATURESURVEY–

Research on healthcare blockchain began with the following articles.

Open Big Data, IEEE 2nd Int. Conf., p. 6, 2016, MedRec: Using Blockchain for Medical Data Access and Permission Management, Azaria, Ekblaw, Vieira, and Lippman. [1], four primary challenges are addressed by the MedRecblockchain implementation: Patients' agency; better data quality and quantity for medical research; sluggish and fragmented access to medical information. We create a blockchain ledger from a collection of references to various pieces of medical data. The breadcrumb trail of medical history may be traced back to these sources. Our Individuals are given the opportunity to authenticate, audit, and share their own data

thanks to the system's on-chain permissioning and data integrity logic. For interoperability, we provide strong, modular APIs that may be integrated with the databases of current serviceproviders. This paper has a lot going for it. Key encryption is accomplished via the usage of Public-Key Cryptography. Transactions may be monitored using Smart Contracts. There will be no disclosure of the

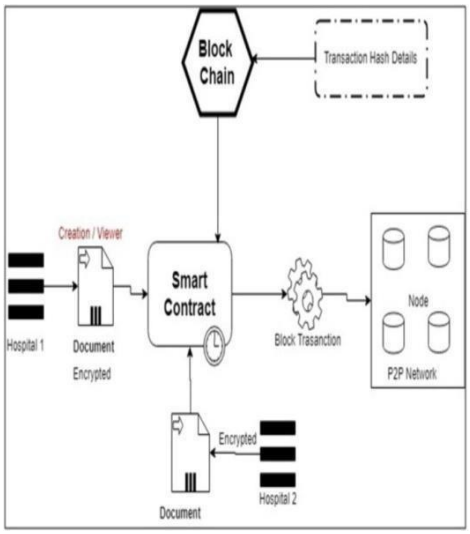
patient's identity or private health information (PHI). There is no time limit for key access to viewing rights for third parties in this publication, which is a drawback.

TowardsSecure&Privac

y-

PreservingDataSharingin

E-



healthSystemsviaConsortiumBlockchain,It's been published by Springer in June 2018 [2]: Aiqing Zhang XiaodongLin, published in June 2018 by Springer in 2018. Blockchains may be divided into two types, based on their data architecture and consensus mechanisms: private blockchain and consortium blockchain.The PHI is stored on the private blockchain, and the secure indexes of the PHI are recorded on the consortium blockchain. The PHI, keywords, and patient identities are all public key encrypted with keyword search to ensure data security, access control, and privacy preservation. To ensure system availability, block producers are needed to show evidence of conformity before adding new blocks to the blockchains. positive aspects of this work Metadata concerning record ownership and permissions is included in Smart Contracts.

Private blockchains for individual hospitals and consortium blockchains for hospitals are both based on the token trapdoor concept. This document has a flaw. Due to the use of several blockchains, there is an increase in storage requirements.

There is also an increase in transaction publication time costs.

Towards Blockchain for Health-CareSystems-Public key cryptography and bilinear pairing technology are used in the work of Hsin-Te Wu and Chun-Wei Tsai, published in IEEE in June 2018 [3]. In order to avoid the identification of a specific patient, a set of anonymous IDs is produced together with a shared secret key. Wearable gadgets and an Android app are used to capture real-time data. This paper's main flaw is the lack of a system manager to track all of the keys. Centralized database administration is employed in private hospitals. A whole healthcare blockchain system has been developed. The database where the organization's medical records are housed contains all of such information.

SecureAttribute-BasedSignatureSchemewith Multiple Authorities for Blockchainin Electronic Health Records Systems R.GUO,H.SHI,Q.ZHAO,andD.ZHENG,

Vol. 12, 2018 [4] of IEEE These EHRs have been encased in blockchain, and to ensure their authenticity, we provide an attribute-based signature system with additional proof other than his attestation. As a result, the escrow issue is avoided and the blockchain's distributeddata storage method is adhered to by numerous authorities that produce and disseminate the patient's public/private keys. Corruption attacks from corrupted authorities can only be prevented by sharing the secret pseudorandom function seed with other authorities. This paper has a lot going for it.Multi-authority safeguards the confidentiality ofdata and the identification of patients. The problem with this study is that as the number ofauthorities and the attributes of the patient rise, so does the expense of the procedure..

AdvancedBlock-ChainArchitecturefore-HealthSystemsT.Mundie,w.liu,szhu,T.

In June 2017, Mundie was published in IEEE. Itis described in [5] as a novel system solution for safe and efficient medical record exchanges on our blockchain architecture.

Advancement in healthcare and changing social standards necessitated the development of AdvancedBlock-Chain (ABC). while yet protecting the privacy and security of patients, providing auditable e-health records Researchers in the medical field may access the enormous e- Health blocks, while government and regulatoryorganisations are granted extra IDs for audit and compliance reasons. If you need it, the e- Health Advanced Block Chain engine is ready to handle embedded security audits as well as reporting on regulatory compliance as well as billing changes and notifications from test findings and medication occurrences.

PROPOSEDSYSTEM

Smart contract-based blockchain-based P2P medical records sharing system diagram

When a customer seeks access to patient records, the system will begin mining the dataOnce they've been processed, the private data records may be exchanged directly between service providers and customers across a block chain. In order to protect the privacy of the patient, it is essential that the patient's identity be kept secret and that access to the patient's data is only permitted after the patient has given their consent. [3] [5]

There are three ways in which the health care block chain will be utilised:

The location of a patient's medical records in a Ledger.

2. Smart Contracts to identify who has access tothe data in question.

To guarantee that only authorised parties have access to the data, key pairs are used.

The purpose of this research is to identify and analyse the pain spots in the healthcare industry, and then utilise the principles of blockchain to implement a solution. In addition

to providing patients with a full, unalterable record of their medical history, it also makes it simple for them to access that data from many healthcare providers and treatment facilities. By using unique blockchain features, MedRec ensures that sensitive information is protected from tampering and unauthorised disclosure. Tokens may be

created on blockchains, particularly Smart Contract-enabled blockchains like Ethereum ", it's a. For the sake of this discussion, we'll refer to tokens as "new digital currencies" whose laws are quite flexible. Thereis a token economy since those tokens may be traded for other tokens on the blockchain. It is possible to generate millions of dollars in only a few minutes via Initial Coin Offerings (ICOs), which allow anybody to launch an auction fortokens (or coins) they have developed. It's possible to specify restrictions for how the money may be used, and the smart contractitself enforces those rules. Because everyone is aware of how the contract will operate, there ismore room for trust. Using'reputation systems' is another important feature of decentralisation"which may be implemented on a computer Transparent use of blockchains.

Medicalresearchers might be rewarded with tokens of reputation, based on the quality of their work, in a marketplace

for medical research. Reputation-based diagnostics are a natural extension of this; a patient answers targeted questions and supplies his medical data, and a pool of

trustworthy physicians delivers independent diagnoses and

collaborativelyagree on a diagnosis. Machine learning methods like DeepMind Health may be used to further improve this. Additionally, a healthcare prediction market might be developed where players who are more often than not accurate in their predictions are compensated openly for their work in the field.

CONCLUSION

Asymmetric key cryptography, public key cryptography, SHA 256, attribute-based encryption, and other approaches were studied in conjunction with blockchain principles and techniques. Medical records

were typically housed in the cloud or in an individual database, and exchanging them was time- consuming and vulnerable to assault. The system will be more secure than the currentmethod since it uses blockchain technology to facilitate the transfer of medical data across companies. In order to further enhance the security of the system, other security approaches, such as encryption and cryptographic ones, will be investigated.

REFERENCES

The IEEE 2nd International Conference on Open Big Data in 2016 featured the presentation "MedRec: Using Blockchain for Medical Data Access and Permission Management" by Azaria, A. Ekblaw, T. Vieira, and A. Lippman.

1. "Secure Attribute-Based Signature Scheme with Multiple Authority for Blockchain in Electronic Health Records Systems" conducted by R. GUO,

The IEEE, volume 12, 2018, contains an article by H. SHI, Q. ZHAO, and D. ZHENG.

"Online Medical Pre-Diagnosis Framework Using Nonlinear SVM for Efficient and Privacy-Preserving Online Medical Pre-Diagnosis," IEEE Journal of Biomedical and Health Information, vol. 12, H. Zhu et al 2.Supriya Thakur Aras and Vrushali Kulkarni

\Blockchain and Its Applications- A Detailed Survey", International Journal of Computer Applications (0975-8887), Volume 180, No. 3,

December 2017

Springer Journal of Medical Systems: "MedBlock: Secure and Efficient Medical Data Sharing through Blockchain," by Kai Fan, Shangyang Wang, Yanhui Ren, Hui Li, and Yintang Yang, published on June 12, 2018.

3. AntonisMichelalas and Noam Weingarten's "HealthShare: Using Attribute-Based Encryption for Secure Data Sharing Between Multiple Clouds"

4. IEEE 1063-7125/17, International Symposium on Computer-Based Medical Systems

5. The following paper is titled "BMPLS: Blockchain-Based Multi-Level Privacy-Preserving Location Scheme for Telecare Medical Information Systems" and was authored by Junwei Zhang and Jianfeng Ma.

A Springer Nature company, Chao Yang, Xin Yao, and Yaxian Ji June 18, 2018

Ms. HarleenKaur, M. AfsharAlam, RoshanJameel, Ashish Kumar Mourya, and Victor Chang, "A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment," published in the Springer Nature series on June 26, 2018,

6. The paper "Blockchain-Based Data Preservation System for Medical Data" was published in the Journal of the American Medical Informatics Association, a Springer Nature 2018 publication, and lists ten authors.

7. Jiaping Lin, Jianwei Niu, and Hui Li, "PCD: A Privacy-preserving Predictive Clinical Decision Scheme with E-Health Big Data Based on RNNs," Computer Communications, IEEE, 2017, 978-1-5386-2784-6.