International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Implementing Blockchains For Efficient Health Care

MRS. Sonawane Minakshi J. and Prof. Kumbharde M.V.

Department of Computer Engineering SND College of Engg. Yeola

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

Blockchains are used as a technology emerged to facilitate money replace transactions and reduce the need for a trusted intermediary to notarize and verify such transactions for shield data its security and privacy. New structures of Blockchains have been designed to put up the need for this technology in other fields such as e-health, tourism and energy. This paper is apprehensive with the use of Blockchains in managing and using electronic health and medical report to allow patients, hospitals, clinics, and other medical stakeholder to share data amongst them, and improves interoperability. The Process of the Block chains , in which architecture of blockchain depends on the entities participating in the constructed chain network. Although the use of Blockchains may reduce idleness and provide caregivers with regular records about their patients facing with few challenges of the whole network of stakeholders. In this paper, we investigate different Blockchains structures to check out existing challenges and supply the possible solutions. We see also various problem that may rendering attacks.

Keywords*: Smart Contracts, Healthcare including Block Chains, Interoperability of Healthcare,*

Introduction

Blockchain is nothing but a normally platform that alleviates the reliance based on a single, centralized authority, yet still transactions directly at the end interacting entities [1].It offers transference, immutability, and compromise via cryptography and game theory. This technology provides the foundations for a number of application domains, including crypto currency and Decentralized Apps (DApps) [2]. elegant contracts are enhancements to Blockchain technologies, as implemented in the Ethereum Blockchain [3], that helps code to directly control the interactions or redeployments of digital assets (such as crypto-tokens or some pieces of data) between two or more parties according to certain rules or agreements previously established between involved participants. Smart contracts can accumulate data objects and define operations on the data, permitting development of DApps to interact with Blockchains and provide continuous services to the end users..

In the study of healthcare, smart agreements can be useful to create protected and effective technical infrastructures to increase care dexterity and quality and thus increase the security of individuals and groups [4]. Ideally, software apps as well as technology stages in an interoperable healthcare atmosphere should be able to lead into securely, interchanging data, and use the switched data across health establishments and app purveyors [5]. These health systems should also assures guarantee for effective care. while, providers feel unwilling to exchange data due to sensitivities. The patients health and identification information protection regulations prevent such distribution and (2) potential responsibility, financial magnitudes associated with data sharing [6, 7]. Besides, vendor-specific and ill-assorted health systems that generates gaps inside healthcare communications, making it tough to coordinate and provide patient centric care.

Literature Review

While protecting healthcare professionals with some level of anonymity (privacy) of data standards like HL7 [10] and today indicating production healthcare systems deficiency of secure links that can connect all liberated health systems together. To begin an endwise reachable net- work [9] while shielding healthcare professionals with some level of secrecy.

Even though data standards such as HL7 [10] and FHIR [11] gives fundamental interoperability for data exchange between reliable systems, In most all cases level of interoperability is up to some degree to the implemented standards and needs data mapping between systems.

Maintainability of these systems is also stiff to achieve since an interface change on one system needs other parties in the reliable network to get used to the change also. This paper is emphasizing issues in healthcare, focusing on interoperability and patient oriented care, also explores issues in healthcare today

which focusing on interoperability challenges that has boundary of data sharing and block patient-centered care nurtured by healthcare interoperability that allows patients to access and control their own health information.

The Electronic Health Record (EHR) system is used to communicate, exchange data, and use the swapped data. Allowing information systems to work together within and across organizational limitations is supreme to increase real care delivery for beings and communities such as interoperability allows providers to securely and accessible share patient medical reports with one another with patients consents to do so irrespective of provider location and trust affairs between them. Protected and accessible data sharing is vital to provide effective collaborative treatment and care decisions for patients.

Data distribution helps improve diagnostic accuracy by collecting approvals or recommendations from a group of medical experts, as well as preventing insufficiencies and mistakes in treatment strategy and prescription.

Similarly, gathered intelligence and insights helps clinicians to know patient needs and in fit apply more effective treatments. Like groups of physicians with different specialties in cancer care from tumor boards that come across regularly to discuss cancer cases, share knowledge, and decide effective cancer treatment and care strategies for patients. As another example, if a cancer patient under treatment is admitted to the emergency in a different hospital, then it would be critical for the ER provider to access patients. Cancer care provider should be reported that the patient is being treated in the ER..

Regardless of the importance of medical data sharing, today's healthcare systems regularly require patients to get and share their individual medical records with other providers whichever physical paper copies or electronic hard disk copies. This procedure of obtaining and sharing medical records is useless for the following reasons: as it is slow since copies of medical records must be prepared, delivered, and picked up by patients. The law permits providers up to 30 days to supply medical data to patients, while some providers may only take 5-10 working days to prepare non-critical health records .It is not protected as data copies may be lost orpinched during their physical transmission by patients from one location to another.
It is incomplete since as patients health history may be patchy because their data is stored in unequal and soloed systems. There is various sources that stores all the medical records of an individual, so patients must be accountable for keeping track of when and where they will get health services. In order to demand copies of their medical history.

Proposed System

It is not assuring that a system is 100% safe; however, constructing a robust system that helps reducing exposure to probable security risks that is the main intention. Therefore, we propose to alleviate the risks of the above-mentioned challenges that may point towards a blockchain operation in a healthcare. Context for the illegal access challenge, we suggest, as a part of any suggested solution is the implementation of a blockchain. By using this system will also eliminate the Sybil attack which cannot be banned but can be mitigated by forcing each miner node which may compete to solve a difficult mathematical problem. This Mathematical solution is referred as the proof of work before they can add as a new block to the blockchain.

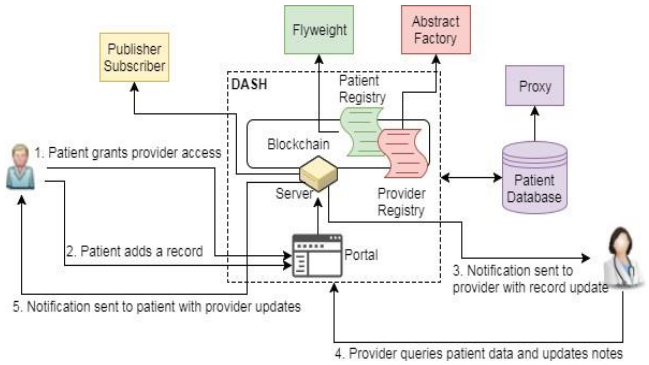
Now a days, the average time to resolve such a problem takes approximately 10 minutes and since the opponent has to regulate more than 50% of the network to conquest this, recognition of such an attack can always be possible. So that by using Blockchains as a technology has the potential of ending this attack. Therefore, it is essential to work on new architecture designs for Blockchains that do not depend on current cryptographic algorithms. We begin with an overview of our system. As illustrated in Figure 1, our system is mobile comprising of the three entities. Guaranteeing that a system is 100% secure. however, building a robust system that help decrease exposure to possible security risks is what can one aim for.

Applying this solution will also Referring to [25], a Sybil attack that cannot be banned but can be mitigated by forcing each miner node to contest in solving a difficult mathematical problem which is referred to as the proof of work before they can add a new block to the blockchain. Currently, the average time to solve such a problem takes around 10 minutes and since the adversary has to control more than 50% of the network to defeat this, detection of such an attack can always be possible. Finally, quantum computing when used has the potential of ending the utilization of Blockchains as a technology. Therefore, scientists should come up with new architecture designs for Blockchains that do not rely on current cryptographic algorithms (e.g. using post- quantum cryptographic algorithms instead).We begin with an overview of our system.

System Architecture

This section presents the structure and functionality of a case study DApp for Smart Health; we developed to explore the effectiveness of applying Blockchain technology to the healthcare area. This prototype was implemented on an Ethereum test Blockchain to emulate a minimal version of a personal EHR system. It provides a web-based portal for patients to self-report and getting their medical records, as well as submits treatment requests. DASH also contain a staff portal for providers to assessment of patient data and fulfill treatment requests based on consents given by patients. Figure shows the structure and workflow of DASH.

The fundamental user features supported in DASH can be summarized as the follows:



Patients can grant provider authorizations to access their health records or treatment requests via the DASH Portal.

Patients can add a health record through a uniform, preformatted form through the DASH Portal.

Health related activities (i.e., prescription requests and health record additions) related to a patient are sent to provider with authorized access to the patient's data with secure notification messages.

Provider with authorized access to a patient's records can query, make changes, and upload physician notes to the data, as well as fulfill the patient's prescription requests.

Patients will be notified of any update to their health record performed by the provider.

DASH uses a Patient Registry agreement to store a planning, or relationship that links unique patient identifiers to their associated Patient Account contract addresses. Each Patient Account contract keeps a list of healthcare providers (using unique provider identifiers) who are granted read/write access to the patient's medical records.

qPresently, DASH is restricted to only offer data access services to two types of users: patients and providers. Patient health records are stored off-chain in a protected database, applying the FHIR data standards. The motive of storing patient data in a unified database is to simulate a data silo, as it is in.

Today's health systems, to later on exercise data incorporation with other siloes databases. Our database server generates a secure socket to exchange consent based tokenized access to patient data using standard public key cryptography. Provider and patient users who are members of DASH are each furnished with two protected cryptographic key couples for (1) encrypting and decrypting data orientations for permitting access to a patient dataset and (2) signing new health records and confirming signatures to prevent altering to the data.

Design with software pattern applications to address the following design challenges:

- ABSTRACT FACTORY assists with organization/individual account creation and manage- ment based on user types, especially in a structured or evolving organization
- FLYWEIGHT ensures unique account creation on the Blockchain and maximizes sharing of common, intrinsic data
- PROXY protects health information privacy while facilitating seamless interactions be- tween separate components in the system to ensure appropriate levels of data accessibility.

Publisher-Subscriber aids in scalably managing health change events and actively no- tifying healthcare participants when and only when relevant changes occur.

System Analysis

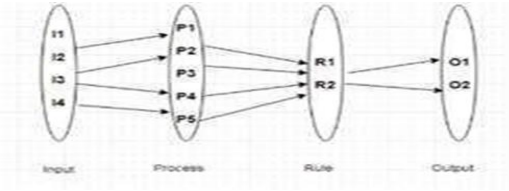
Mathematical Model

A mathematical model is a description of a system using mathematical concepts and language. The process of developing a mathematical model is termed as mathematical modeling. As the project is having finite input and finite output, it comes under P-Problem.

Set theory

Let the system be described by S, S={ I, P, R, O}
Where,
S : is a System. I: is Input
R: is set of Rules O: Final Output. I= { I1; I2; I3; I4}
Where,
I1 = Enter Patient I2 = Enter Doctor Information I3= Enter Disease Symptoms.
I4= Feedback by Patient.
P is set of procedure or function or processes or methods. P =
{ P1, P2, P3};
Where,
P1 = Check login for patient. P2 = Searching for Doctor. P3 = Read Disease Symptom. P4 = Predicting Medication. P5 = View Patient List.
R is set of Rules R =R1, R2; R1 = Enter Valid Information.
R2 = Match the Disease with Symptoms. O={O1,O2,O3}
Where,
O1 = Predict Medication.
O2 = Download Prescription Paper.

Venn Diagram



- Where
- I1, I2 , I3. I4 are inputs,
- P1, P2, P3, P4, P5 are process R1. R2 is rules

And O1, O2, O3 are output .

Conclusion and Future Work

In this section of paper, we discussed about authorized and unauthorized Blockchains with their architecture, and also how they could be executed in healthcare. In addition, we also try to discuss related safety and secrecy challenges, involving the Sybil attack, and how the use of Blockchains could come to an end due to quantum computers. Moreover, the paper recommended possible solutions for the above-mentioned problems.

If the challenges of interoperability stay to be overcome, dependable privacy established, good anonymization protocols developed, and agreement achieved around the types of contracts needed to regulate information, then a new future of healthcare may be found. These are noteworthy challenges, but as described above, companies have previously prepared significant inroads into presenting them even at this early stage. This century's technology monsters have already shown us that they are good at using artificial intelligence to learn from data; the same form of technology is composed to produce troublesome new visions with the kind of data now being produced around health, with confidentiality and patient control as an important central belief.

While other pointed important step towards the "health singularity": a transformative event where individualized healthcare is brought based on a deep indulgent of the personal biology of each individual.

Acknowledgment

I would like to take this opportunity to express my deep gratitude and deep honor to my Project Guide Prof. M. V.Kumbharde for his exemplary guidance, valued feedback and constant encouragement throughout the duration of the project. Also Prof. V.N. Dhakane (PG coordinator) who provided facilities to explore the subject with more interest. I express my immense pleasure and thankfulness to all the teachers and staff of the Department of Computer Engineering, S.N.D. College of Engineering and Research Center, Yeola, Nasik for their co-operation and support.

References

[1]. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aladhari andM. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols,and Applications," IEEE Communication Surveys & Tutorials, vol. 17, no. 4, pp. 2347- 2376, 2015.

[2]. Department of Health, "Whole System Demonstrator Programme Headline Findings – December 2011," United Kingdom Department of Health, 2011.

[3]. Zyskind, Guy, and Oz Nathan. "Decenterilized privacy: Using blockchain to protect personal data." Proceedings of the 2015 IEEE Security and Privacy Workshop (SPW), May 21-21, 2015, San Jose, California, USA. pp 180-184

[4]. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system,", White paper, Oct. 2008, available at https://bitcoin.org/bitcoin.pdf.

[5]. N. Zhumabekuly Aitzhan; D. Svetinovic, "Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams," in IEEE Transactions on Dependable and Secure Computing , vol.PP, no.99, pp.1-1 doi: 10.1109/TDSC.2016.2616861.

[6]. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, no., pp. 2292-2303.

[7]. A. Yasin and L. Liu, "An Online Identity and Smart Contract Management System," 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC),

[8]. Atlanta,GA, 2016, pp. 192- 198. doi: 10.1109/COMPSAC.

[9]. A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy- Preserving Smart Contracts," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2016, pp. 839-858.

[10]. A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2016 2nd International Conference on Open and Big Data (OBD), Vienna, 2016, pp. 25-30.

[11]. Adopting Blockchain Technology for Electronic Health Record Interoperability, available at https://oncprojectracking.healthit.gov/wiki/download/ att achment

[12]. Kadena: Confidentiality in Private Blockchain, available at http://kadena.io/docs/Kadena-

[13]. Y. Yuan and F. Y. Wang, "Towards blockchain-based intelligent transportation systems," 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, 2016, pp. 2663-2668.

[14]. On Public and Private Blockchains, available at https://blog.ethereum.org/2015/08/07/on-public-and-private- blockchains.