



AN ENHANCED AND RELIABLE BLOCK CHAIN FOR HEALTHCARE AND INSURANCE POLICY

K.Bindu Priya¹, S.V.C Gupta², Dr B.Raja Srinivasa Reddy³

¹ M. Tech., Dept of CSE, Sri vasavi institute of Engineering & technology JNTUK University. AP, India, bindupriyakammili000@gmail.com

² M. Tech., Dept of CSE, Sri vasavi institute of Engineering & technology JNTUK University. AP, India, svcgupta@sviet.edu.in

³ M. Tech., Dept of CSE, Sri vasavi institute of Engineering & technology JNTUK University. AP, India, brsreddy208@@gmail.com

Abstract:- Block chain is so far well-known for its potential applications in financial and banking sectors. However, block chain as a decentralized and distributed technology can be utilized as a powerful tool for immense daily life applications. Healthcare is one of the prominent applications area among others where block chain is supposed to make a strong impact. It is generating wide range of opportunities and possibilities in current healthcare systems. Therefore, this paper is all about exploring the potential applications of block chain technology in current healthcare systems along with insurance policy covered in real time scenario and highlights the most important requirements to fulfil the need of such systems such as trust less and transparent healthcare systems. In addition, this work also presents the challenges and obstacles needed to resolve before the successful adoption of block chain technology in healthcare systems. Furthermore, we introduce the smart contract for block chain based healthcare systems which are key for defining the pre-defined agreements among various involved stake holders.

Keywords-Block chain, decision-trees, machine learning

I. INTRODUCTION:-

The research community has started to realize the potential of block chain beyond the financial applications. Block chain as a decentralized technology can be utilized in immense useful applications such as healthcare, logistics, supply chain management and Internet of Things (IoTs) among others [1], [2], [3]. Block chain provides secure distributed database that can perform their tasks without any intervention of third-party or central administration. It is highly useful in the case when various relevant parties want to access same kind of the information. Thus, block chain based systems have huge potential to minimize the cost and resources of current intermediates. Block chain, generally uses cryptographic (such as hash functions, asymmetric encryption and digital signatures) based approaches among various stakeholders in a given system that helps in preserving trust among them while interaction. Internet of things (IoTs) [4] and other communication related technologies (such as 5G) [5], [6] are putting a huge impact on the healthcare services and providing consumer better and improved medical services but provides an opportunity to the involved stakeholders to generate the revenue. Medical data storing and sharing is an integral part in healthcare systems in order to enhance the quality and services of overall healthcare systems. However, sharing data records among various entities through unsecure means can lead to leakage of the patient's personal and critical information. Also, the lack of the user control over their

personal information can cause harmful consequences such as unauthorized entities can access the personal medical information. While sharing the patients information might be fragmented in various healthcare systems and that can lead to various risks [3]. One of the core issues in current electronic health/medical records (EHR/EMR) is maintaining the interoperability among various involved stakeholders [7]. This issue may cause obstacles in the data transaction among each other. The lack of coordinated data management and sharing mechanism among various entities may cause in fragmentation of the healthcare information. Apart from interoperability, data security and privacy are another key challenges in the current ways of data storing and sharing data through EHR/EMR systems [7], [9]. Most of the patients are hesitant about sharing and storing their personal medical information due to the data leakage and potential shortcoming in security mechanism [10], [11]. Therefore, there is a clear need of distributed way of data sharing and storing where patients are surer about their data security and privacy and in addition all the involved stakeholders can see the holistic view of overall transaction and interactions [7]. Therefore, considering these challenges in the current healthcare systems, it is vital to utilized the potential block chain technology in the healthcare sector [3]. Block chain technology can play a key role in number of healthcare applications, for example, using block chain for electronic healthcare records (EHR/EMR) can ensure the security of the critical information of the patients and can

make sure that only valid and authorized entities should access the data [8], [12], [13], [14]. Block chain for healthcare also uses the concept of smart contracts which enables trustless features among various entities in the system. Smart contracts consist of computer program that presents the agreements and principles on which all the involved parties in the network agrees upon and therefore no trusted third party is required [15], [16]. Block chain based healthcare system are also proposed in a way that they support the interoperability feature in the system. Hence, the main aim of this work is to overview and explores the block chain technology for the purpose of healthcare based applications. In addition to that, this paper discusses the potential requirement and challenges for building block chain based healthcare systems. Furthermore, we will also discuss the the need of the smart contracts for the block chain based healthcare systems.

II. Related Work:-

Block chain technologies A block is a part of the block chain in which it records all the transactions and once it is completed enters into a permanent database in the block chain. In Block chain, the blocks are linked one after other like a linked list. Every block consists the hash of the previous block as shown in Figure 2. [2]

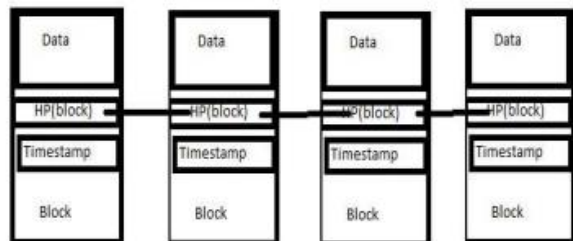


Fig. 2: Blockchain as A Linked List of Blocks Connected by Hash Pointers.

Block chain consists of a set of nodes formed like a peer to peer network. With the help of public/private keys, users can interact in the block chain. The private key is used to sign their own transaction and is addressed in the network with the public key. It provides authentication, integrity, and non-repudiation in the network. Each node in the block chain makes sure that incoming transaction is valid before transmitting further. Invalid transactions are discarded. [3] Each Block chain network should provide certain rules for each database transaction. These rules are programmed to each block chain client, then verifying that incoming transaction is valid or not. [7]

3.1. Types of block chain Block chains are classified into three types. 1) Public Block chain, 2) Private Block chain 3) Permission Block chain. [11] In Public Block chain,

everyone can contribute and no trust relationships among the nodes. The transactions on the public block chain can never be changed and cancelled. The Consensus algorithms used in this Block chain are PoW, PoS and DPoS. In Private Block chain, only the owner of the Block chain has the authority to modify the information and rest of nodes has limited access. PBFT consensus algorithm is used in the Private Block chain. In Permission Block chain, Each participant selects its own consensus node based on specified rules. This one is suitable for the semi-closed network which is made by different enterprises.

3.2. Technologies involved in block chain Public Key Cryptography is one of the technologies used in Blockchain technology and it is used for encryption and decryption of sensitive data and message authenticity.

3.2.1 Encryption and Decryption: In asymmetric encryption, public and private key pairs will be used. The public key is used for encryption and the private key is used for decryption. Suppose there is a communication between Alice and Bob, Alice sends a message that is encrypted with Bob public key and then sends to bob. Bob decrypted the message with its own private key. To know the communication between Alice and Bob, the attacker must get both the private keys.

3.2.2. Digital signatures PKC can be used for authentication also. The digital signature can be done by sender's private key and later it verified by the receiver using sender's public key.

3.2.3. Hash functions It is nothing but a mathematical function that maps data of any arbitrary size to specific fixed length, called the hash. Hash functions are one-way functions that are of the hash value never get an original data. it is also deterministic; the same data always produce the same hash value.

3.2.4. Homomorphic encryption Arithmetic operations can be carried on encrypted values

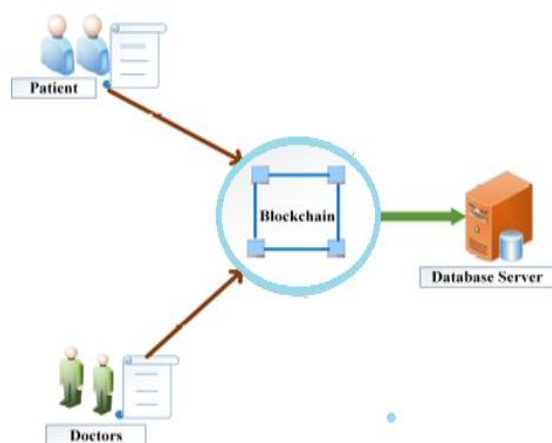
. Plaintext1 with Encryption changed to Ciphertext1
Plaintext2 with Encryption changed to Ciphertext2
 $\text{Ciphertext1} * \text{Ciphertext2} = \text{Ciphertext3}$

Cipher text3 with decryption converted to Plaintext3
 $\text{Plaintext1} * \text{Plaintext2} = \text{Plaintext3}$

4. Security issues involved in block chain systems Block chains mainly concentrating on three security concepts that are confidentiality, integrity, and availability. Basically, Block chain is a distributed system, so it provides availability and all the nodes in the block chain agreed based on a chain of transactions then the integrity of data is maintained. With the help of appropriate cryptographic keys confidentiality of transactions can be addressed. Holistic approach in Block chain systems includes authentication and authorization of entities using the block chain, transaction transparency, verification and communication infrastructure security, security from unauthorized insiders, compromised nodes or server failure. Block chain systems mainly to look at security in the following aspects. [1]

- 1) Ledger level security.
- 2) Network level security.
- 3) Transaction-level security.
- 4) Associated surround system security.
- 5) Smart contract security

SYSTEM ARCHITECTURE



- We created chain linking process between patient and doctor.
- We used Database server to provide data for patient and doctor.
- We applied selected algorithm to generate Rating and Ranking.
- We Generated results in the form of Graphs those will help us to Display on web page for analysis purpose.

III. Literature Survey:-

Title:-Block chain technology in healthcare: The revolution starts here

Authors:- M. Mettler

Description:-Block chain technology has shown its considerable adaptability in recent years as a variety of market sectors sought ways of incorporating its abilities into their operations. While so far most of the focus has been on the financial services industry, several projects in other service related areas such as healthcare show this is beginning to change. Numerous starting points for Block chain technology in the healthcare industry are the focus of this report. With examples for public healthcare management, user-oriented medical research and drug counterfeiting in the pharmaceutical sector, this report aims to illustrate possible influences, goals and potentials connected to this disruptive technology.

Title:- A block chain-based approach to health information exchange networks.

Authors:- K.Peterson, Kevin

Description:-

Timely clinical data exchange has been the primary function of Health Information Exchanges (HIEs). However, there have been growing needs for sharing public health related

data among government entities. Because the primary stakeholders for public health data are different from clinical data, data are stored over multiple systems, making the retrieval of related public health data items a hard process. In such situations, block chain technology may be used to connect and securely exchange those scattered data items. In this paper, we proposed an enterprise architecture (EA) for HIEs to adopt block chain technology so they could store and exchange both clinical and other health related data for efficient general public healthcare management. With the proposed solution, HIEs can not only exchange relevant data items, but also securely manage, record, and transfer complete health records. In our approach, we have incorporated a Hyper ledger Fabric (HLF) Network block chain technology that utilizes Block chain as a Service (BaaS) to enterprise architecture so that HIEs can manage comprehensive health data.

Title:- Identity privacy preserving biometric based authentication scheme for Naked healthcare environment

Authors:- T. Kumar, A. Braeken, M. Liyanage and M. Ylianttila

Description:- Recent developments in Internet of Things (IoT) technologies have already put a huge impact on the medical and health sector. Thus, the patient treatment can be performed in more efficient ways compared with traditional methods. Secure identification is a key system requirement for patients to acquire these health related services. Fast and convenient identification is important in the case of critical and elderly or disabled patients who required frequent health services. In this paper, we are presenting concept of the Naked environment where patients can get health services from smart and intelligent surroundings of hospital without using explicit gadgets. Patients would have direct interaction with the environment and get identified through it. We propose a biometric based authentication scheme for the Naked hospital environment that also protects the patients identity privacy. In addition, we show that this authentication scheme can resist various well known attacks such as insider attacks, replay attacks and identity privacy among others.

Title:- Sustainable block chain-enabled services: Smart contracts

Authors:- C. Wright and A. Serguieva,

Description:- This paper introduces some of the interdependent components within the multifaceted solution our team is developing towards accelerating the functionality, complexity and versatility of block chain-enabled services. The focus here is particularly on introducing and bringing together selected individual components of the solution to achieve a synergistic effect in expanding the functionality of blockchain-enforced smart contracts. The contributions of this paper include: (i) proposing a method for automated management of contracts with hierarchical conditionality structures through an hierarchy of intelligent agents and the use of hierarchical cryptographic key-pairs; (ii) proposing a method for efficient and secure matching and transfer of smart-contract underlyings (entities) among disparate smart

contracts/subcontracts; (iii) proposing a method for producing an hierarchy of common secrets to facilitate hierarchical communication channels of increased security, and applying this method both in the context of method (i) and method (ii); and (iv) proposing the use of distributed hash tables DHT in building secure and optimized repositories in the context of method (i) and in the context method (ii), where the former involves a DHT repository of smart contracts and the latter involves a DHT repository of entities underlying smart contracts that are being exchanged among different smart contracts and subcontracts. The smart-contract focused methods introduced in this paper contribute to the overall goal towards a sustainable adaptive mechanism for processing evolving volumes, versatility, and complexity of blockchain transactions, traffic, and services. Blockchain-enabled services are efficient, secure, automated, and allowing worldwide distribution of resources. They present a more efficient and sustainable alternative to current service infrastructures within a range of domains, particularly the legal and financial domains. They also set a sustainable infrastructure for emerging Internet-of-things services.

V. REFERENCES

- [1] T. Aste, P. Tasca, and T. D. Matteo, Blockchain technologies: The foreseeable impact on society and industry, Computer, vol. 50, no. 9, pp. 1828, 2017.
- [2] R. Beck, Beyond bitcoin: The rise of blockchain world, Computer, vol. 51, no. 2, pp. 5458, February 2018.
- [3] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, 2016, pp. 1-3.
- [4] S. B. Baker, W. Xiang, and I. Atkinson, Internet of things for smart healthcare: Technologies, challenges, and opportunities, IEEE Access, vol. 5, pp. 26 52126 544, 2017.
- [5] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "Overview of 5G Security Challenges and Solutions," in IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36-43, MARCH 2018.
- [6] T. Kumar, M. Liyanage, I. Ahmad, et al. User privacy, identity and trust in 5G. In: A Comprehensive Guide to 5G Security. Hoboken: Wiley, 2018.
- [7] K. Peterson, Kevin, et al. "A blockchain-based approach to health information exchange networks." In Proc. NIST Workshop Blockchain Healthcare, vol. 1, pp. 1-10. 2016.
- [8] C. Esposito, A. De Santis, G. Tortora, H. Chang and K. K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," in IEEE Cloud Computing, vol. 5, no. 1, pp. 31-37, Jan./Feb. 2018.
- [9] Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. International Conference on Open and Big Data (OBD). Vienna, Austria: IEEE; 2016:2530.
- [10] T. Kumar, A. Braeken, M. Liyanage and M. Ylianttila, "Identity privacy preserving biometric based authentication scheme for Naked healthcare environment," 2017 IEEE International Conference on Communications (ICC), Paris, 2017, pp. 1-7.
- [11] T. Kumar, M. Liyanage, A. Braeken, I. Ahmad and M. Ylianttila, "From gadget to gadget-free hyperconnected world: Conceptual analysis of user privacy challenges," 2017 European Conference on Networks and Communications (EuCNC), Oulu, 2017, pp. 1-6.
- [12] Peng Zhang, Michael A. Walker, Jules White, Douglas C. Schmidt, Metrics for Assessing Blockchain-based Healthcare Decentralized Apps, 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), 2017.
- [13] Yue, X., Wang, H., Jin, D., Li, M., Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on Blockchain with novel privacy risk control. Journal of Medical Systems, 40(218).
- [14] Yli-Huoma, J., Ko, D., Choi, S., Park, S., Smolander, K. (2016). Where is current research on blockchain technology? a systematic review. PloS one, 11(10).
- [15] Massimo Bartoletti and Livio Pompianu, "An empirical analysis of smart contracts: platforms, applications, and design patterns", Università degli studi di Cagliari, 2017.
- [16] C. Wright and A. Sergueeva, "Sustainable blockchain-enabled services: Smart contracts," 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, 2017, pp. 4255-4264.
- [17] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating block chain for data sharing and collaboration in mobile healthcare applications," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile

IV. Conclusion:- With the recent advancements in internet and network technologies, there is a clear need of the enhancement in the quality of medical and healthcare services. There are numerous shortcomings in the current healthcare systems that seek solutions based on distributed and decentralized approaches. In this context, block chain technology can play a leading role in providing the solutions that are decentralized and can ensure the security and integrity of the medical information. Therefore, the main focus of this work is to provide an overview of block chain technology in the healthcare sector. This article identifies key application areas in the healthcare domain where block chain technology can be a useful addition. Moreover, various requirements and challenges for block chain based healthcare systems are presented in this work. Finally the concept of smart contracts for block chain based healthcare systems is highlighted. This paper proposes a block chain-based framework for implementing insurance transaction processes as smart contracts. Experiments conducted to study the scalability clearly showed the parameters used during block chain creation should be chosen carefully, as they have a direct effect on the network latency. Though the database is currently not encrypted, it can be encrypted with fine-grained access control. In our model, each smart contract has its own set of endorsing peers, and this can be extended even to the transaction level, to enable separate set of endorsing peers for each transaction.

Radio Communications (PIMRC), Montreal, QC, 2017, pp. 1-5.

[18] Kuo, Tsung-Ting, Hyeon-Eui Kim, and Lucila Ohno-Machado. "Blockchain distributed ledger technologies for biomedical and health care applications." *Journal of the American Medical Informatics Association* 24.6 (2017): 1211-1220.

[19] Huihui Yang, Bian yang, "A Blockchain-based Approach to the Secure Sharing of Healthcare Data." *Journal of Norwegian University of science and technology*, 2018.

[20] RJ Krawiec, Dan Housman, Mark White, Mariya Filipova, Florian Quarre, Dan Barr, Allen Nesbitt, Kate Fedosova, Jason Killmeyer, Adam Israel, Lindsay Tsai, Blockchain : Opportunities for health care Deloitte, 2016.

[21] Nugent, Timothy and Upton, David and Cimpoesu, Mihai "Improving data transparency in clinical trials using blockchain smart contracts", *F1000Research*, vol.5, 2016.

[22] Benchoufi, Mehdi, Raphael Porcher, and Philippe Ravaud. Block chain Protocols in Clinical Trials: Transparency and Traceability of Consent. *F1000Research* 6 (2017): 66. PMC. Web. 2 May 2018.

[23] enchoufi, Mehdi, and Philippe Ravaud. Blockchain Technology for Improving Clinical Research Quality. *Trials* 18 (2017): 335. PMC. Web. 2 May 2018.

[24] Chet Stgnaro, "White Paper: Innovative Blockchain Uses in Healthcare", Freed Associates, 2017.

[25] Clauson, Kevin A., et al. "Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare." *Blockchain in Healthcare Today* (2018).

[26] Clauson, Engelhardt, Mark A. "Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector." *Technology Innovation Management Review* 7, no. 10 (2017).

[27] Boulos, M. N. K., Wilson, J. T., Clauson, K. A. (2018). Geospatial blockchain: promises, challenges, and scenarios in health and healthcare, *International Journal of Health Geographics*, 17:25, 2018.

[28] M. Puppala, T. He, X. Yu, S. Chen, R. Ogunti, and S. T. C. Wong, Data security and privacy management in healthcare applications and clinical data warehouse environment, in 2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI), Feb 2016, pp.58

[29] Al Omar, A., Rahman, M. S., Basu, A., Kiyomoto, S. (2017). Medibchain: A blockchain based privacy preserving platform for healthcare data. In International conference on security, privacy and anonymity in computation, communication and storage (pp. 534543).

[30] G. Zyskind, O. Nathan and A. ' . Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," 2015 IEEE Security and Privacy Workshops, San Jose, CA, 2015, pp. 180-184.

[31] Q. 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," in *IEEE Access*, vol. 5, pp. 14757-14767, 2017.

[32] Laure A.Linn, Martha B.Koo, Blockchain for health data and its potential use in health IT and health care related research, 2016.

[33] Begley, Robert. "Information Records Management and Block chain Technology: Understanding its Potential." PhD diss., Northumbria University, 2017.

[34] P. F. Edemekong, M. J. Haydel, (2018). Health Insurance Portability and Accountability Act (HIPAA). In *StatPearls* [Internet]. StatPearls Publishing.

[35] Simon Janin, Smart contract in healthcare *Health Management.org* (Vol. 18, issue 1), 2018.

[36] Dr. Maciej Hulicki, The legal framework and challenges of smart contracts applications, Cardinal Wyszynski University of Warsaw, 2017.



K. Bindu Priya is a student of Sri Vasavi Institute of Engineering & Technology, Nandamuru. Present she is pursuing M.Tech(CSE) from this college and she received B.Tech from JNTUK



S.V.C Gupta is Head of the Department in Sri Vasavi Institute of Engineering & Technology, Nandamuru. He is completed Master Degree and also Having 22 years of Experience in Teaching.



Dr B Raja Srinivasa Reddy is Professor in Sri Vasavi Institute of Engineering & Technology, Nandamuru. He completed PhD and Master Degree also Having 24 years of Experience in Teaching

