EasyChair Preprint

№ 1626

Blockchain in smart health

Naghza Tul Zahra

October 11, 2019

Blockchain in Smart Health

Naghza Tul Zahra
MSIT-s19-006
Department of CS and IT,
Superior University,
Lahore, Pakistan
naghzatulzahra2016@gmail.com

***Abstract*—Blockchain has been making some vital progress these days because of its secure and amiable structure. The blockchain is emerging in the healthcare sector rapidly. Blockchain is a distributed and decentralized database which deals with transactions. Healthcare has now become a prestigious part of our life as it is making life changing innovations day by day whether it is about artificial intelligence's influence in diagnostic system, expert systems, patient's data storage, retrieval, security and any other healthcare smart services. Smart health is helping us in solving our healthcare needs. When we talk about smart health data is the most important ingredient which makes everything possible. Many researchers are now emerging blockchain in smart health because of its secure, flexible and reliable architecture. So, in this paper we are discussing the major progress made in implementing the blockchain technology in the field of smart health. Our main focus is on the patient's data storage, retrieval, security and interoperability.**

***Keywords*—Smart Health, blockchain, healthcare, date analysis, data retrieval, patient's record.**

1. INTRODUCTION

The blockchain is a circulated record innovation as verified by cryptography, disseminated esteem-based database, and represented by an agreement system. Basically, blockchain is record of automated occasions. Notwithstanding, it isn't "just a record" since it can in like manner contain indicated brilliant contracts, which are programs put away on the blockchain that continue running as executed with no risk of downtime, restriction, or extortion [2].

This is on the grounds that the dispersed trade data and cryptographic justification that deceits at the blockchain's center make it especially alter safe. The impacts of making a solid, reliable disseminated record framework, or record, may be key to how we arrange relational and bury legitimate connections. The overall wellbeing framework relies upon that individuals and affiliations trust different elements to make, store, and disperse basic records. For instance, medicinal facilities create and keep up wellbeing records [1].

Customary healthcare can't oblige everybody's needs because of the huge increment in people. Regardless of having great framework, and cutting-edge innovations, restorative administrations are not receptive or moderate to everybody. One of the goals of smart healthcare is to help clients by teaching them about their therapeutic status and keeping them wellbeing mindful. Smart healthcare enables clients to self-deal with some crisis conditions. It gives an accentuation on improving the quality and experience of the client. Smart healthcare helps in utilizing accessible assets to their most prominent potential. It helps remote checking of patients and aides in decreasing the cost of the treatment for the client. It also encourages therapeutic professionals to broaden their administrations with no land obstructions [2]. With an expanding pattern towards smart urban communities, a powerful smart healthcare framework guarantees a solid living for its residents.

Associated wellbeing when all is said in done alludes to any mechanized healthcare game plan that can work remotely and is an aggregate term for subsets, for instance, telemedicine and portable wellbeing, yet with an additional part of constant checking of wellbeing, crisis recognition and cautioning appropriate individuals normally. Associated wellbeing in a general sense centers around the mission to improve the quality and proficiency of healthcare by empowering self-care and supplementing it with remote-care [1].

It has its motivation in the period of telemedicine, where the clients are instructed about their wellbeing and are given criticism at whatever point required. While smart healthcare alludes to courses of action which can work totally freely, associated healthcare offers answers for the clients to get input from clinicians. The most basic portrayal, which rethinks the economy of the smart healthcare, is the end client showcase. Contingent on whether the healthcare organize is to be actualized for individuals or crisis facilities, the cost, power, and design differs broadly [2].

The following area of this paper will examine about the examinations and work proposed regarding actualizing blockchain into smart healthcare. What's more, after that the end segment finishes up our investigation and toward the end every one of the references are given.

2. LITERATURE REVIEW

Peng Z. et al, [3] proposed a paper that gives assessment measurements to evaluate DApps (Decentralize application) based on blockchain as far as their achievability, expected ability, and consistence in the healthcare area. Evaluation Metric is given in Figure 1.1.

1	Entire workflow is HIPAA compliant
2	Framework employed needs to support Turing-complete operations
3	Support for user identification and authentication
4	Support for structural interoperability at minimum
5	Scalability across large populations of healthcare participants
6	Cost-effectiveness
7	Support of patient-centered care model

Figure 1.1. Assessment Metric

To improve healthcare interoperability this paper depicted a lot of assessment measurements, from both the specialized and zone viewpoints, to evaluate smart health applications by utilizing their innovative model and fill in as a fundamental guide for making future applications around there [3].

Asaph A. at al, [4] proposed a decentralized administration framework to deal with the electronic therapeutic records by utilizing the blockchain innovation called MedRec. MedRec gives usability, access and outright log to patients over all destinations. It suggests the productive blockchain highlights. MedRec deals with the sharing of information, responsibility, secrecy and confirmation. It additionally gives interoperability. The information is verified through verification of work [4].

Their proposed model gives a brief report to the patient about his medical history obtained from all previous medical centers and clinics data repositories. It makes use of blockchain's fruitful properties and it supervises classification, responsibility, verification and information sharing essential examinations when taking care of sensitive data. A particular plan coordinates with current regions supplier's information amassing arrangements. That makes their model more interoperable, diverse and useful. They boost the field's experts to participate in their proposed blockchain based model and to take interest in it. That provides the miners a reward against the verification of records they did which use of the blockchain's proof of work features for validation. Their proposed work in this means enlightens the rise of information economic matters, providing enormous information to enable analysts in process of drawing in diagnosing authorities and the clients in the evaluation of the discharge of data about their logs. The motivation behind their research was to provide a working model ahead of the examinations through which we can examine our methodology.

They dealt with identity confirmation through "open key cryptography" and use an execution like DNS that shows an authoritatively available and for the most part recognized sort of ID to Ethereum address of that person. An altering computation works with the sharing of data "off-chain" in both the databases of the patient and the information providing authority, consequent to refereeing the blockchain for attesting assents by methods for our database confirmation server [5].

Arrangements utilized by their model are following:

1. Summary Contract.
2. Registrar Contract.
3. Patient Provider Relationship Contract.

The complete process of creating a new entry of patient's record is shown in figure 1.2.

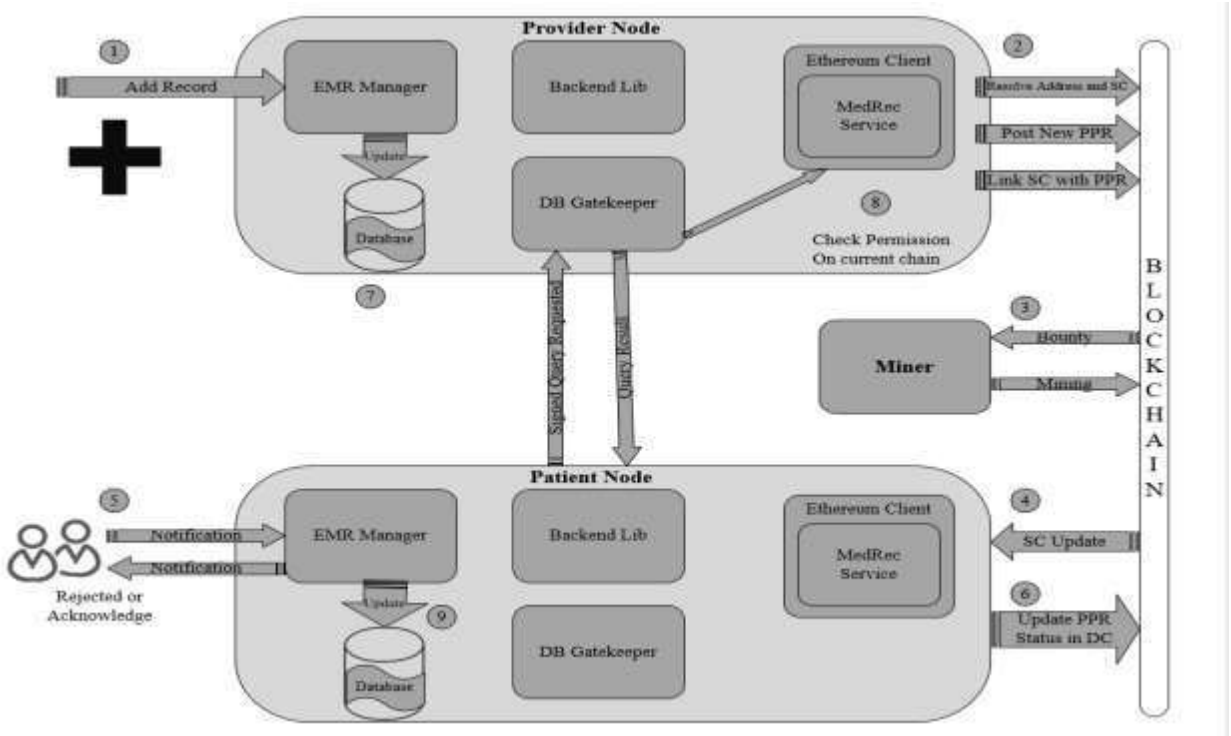

Figure.1.2. Architecture of adding a new patient record.

A specific patient or multiple patients can support sharing of records between suppliers. In the two cases party getting new data gets an electronic advised and can insist the proposed record before suffering or removing the information. This keeps people taught and occupied with the movement of their records [4].

Kevin P. et al, [5] proposed an approach based on blockchain technology to manage patient's data communication. This philosophy crafts a singular fused wellspring of belief for proposed model's accord, and predicates concession to check of helper and semantic interoperability.
The main purpose of this study was to delineate a method to manage to share healthcare information inside a data sharing architecture securely.

The troubles of data sharing inside the healthcare zone are basic. Fundamentally sharing data isn't adequate. They have seemed effective data sharing frameworks require accord on data language structure, which means, and security. They proposed that uses blockchain technology and can expect a key occupation in enabling data sharing inside an architecture, and have described the unusual state structures and traditions imperative to apply their study in real environment in smart health. They exhibited another understanding estimation expected to support data interoperability. Finally, they associated extra extents of security on the blockchain, for instance, sort out wide keys and splendid contracts, keeping security a best need. They believe that a blockchain-based data sharing framework is a suitable response for the confusing issue of sharing healthcare data [5].

Huawei Z. et al, [6] proposed a model to structure a lightweight support and capable recovery plan for keys of wellbeing blockchain using body sensors. The maker's examinations exhibit that the arrangement has high security and execution, and it might be used to guarantee assurance messages on wellbeing blockchain effectively and to propel the utilization of wellbeing blockchain.

In the paper, the creators combined the BSN and the wellbeing blockchain, and used the biosensor center points in the BSN to propose a lightweight fortification and capable recovery plot for keys of wellbeing blockchain. The arrangement has the going with central focuses: (I) biosensor center points in the BSN are in charge of age, fortification, and recovery of the keys of wellbeing blockchain, and it will grow the security of these keys. (ii) In the arrangement, each square on the blockchain can be encoded by a perceived key with lower amassing cost and unrivaled, and it will hugely improve the security of insurance physiological data on the wellbeing blockchain [6].

Figure.1.3. Model Architecture.

Joao. at al, [7] advancing toward this issue with the usage of a passed on record, to be explicit a consortium blockchain, where the errands are secured as trades, we ensure that the different workplaces think about all of the social occasions that can exhibit over the e-Health resources while caring for trustworthiness, auditability, realness, and versatility. We propose a way to manage related issue of information availability in massive scale and coursed systems, as it is found in e-Health circumstances where differing components and customers should likely get to data with different assent levels and granularities. Our technique involves using Blockchain development as a way to deal with accomplish an inexorably strong and customer empowered response for access control the board in an e-Health condition. Such procedure empowers us to portray fine-grained get the opportunity to control while keeping up the understanding in an appropriated system, believability, immutability and auditability. A proof-of-thought of the procedure in this manner depicted and point by point was executed in order to check its reachability.

They used a system like the Access Control Matrix, which allows the establishment of a correspondence between a subject, an article and a great deal of rights [7].

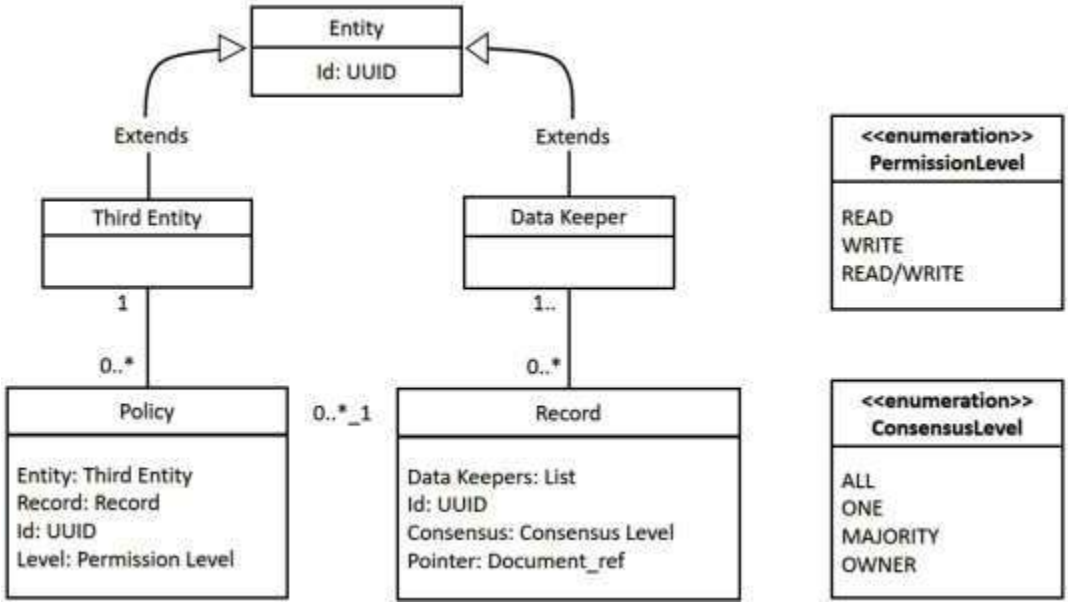

Figure. 1.4. UML Diagram

They did research on a case where they made esteem-based information about electronic health history and access control procedures using the blockchain based technology. The access controls of patients were an influence too behind this study's manifesto's [7].

Koshechkin et al [8] Shut Blockchain development can find the broadest application for refining the idea of open organizations in electronic structure. The depicted instance of the execution of the electronic register of meds reliant on Blockchain development won't require important costs for its improvement and can be realized as fast as time licenses. Each and every imaginative stage and game plans are starting at now made and have gotten sufficient underwriting. It requires to transform simply express application courses of action and to carry them into the creation and regulatory method. We can't resist speculating that the most basic results can be practiced in such domains of data getting ready and upkeep of explicit registers, approving and selection , speaking to remedial thought gave, quality control of treatment, plan of regular portions, support for essential administration, sedate turnover, remote checking of wellbeing status, expel interviews and other [8].

Krawiec et al. [9] presented a couple of existing torment centers in current prosperity information exchange systems and the contrasting openings given by blockchain developments. They furthermore discussed how blockchain can be used in the prosperity IT structures so patients, prosperity providers, or conceivably prosperity affiliations can collaborate.

B. Nichol et al [10] proposed an architectural approach which stores the thoughts advances related to blockchain and guesses on how blockchain can be used to deal with typical interoperability issues going up against social protection.

A gathering at IBM Team [11] received a progressively broad system by stressing on the troubles in social protection business industry and giving strong use cases to include potential employments of advancements made in blockchain technology. Their previous work moreover given programming plan proposals to making general blockchain-based prosperity IT systems Zhang et al. [12] and proposed estimations of imposition for prosperity structures based on blockchain technology.

Zhang et al. [14], which join a subset of the specific essentials described in the ONC direct. This earlier work of our own focused on giving progressively expansive or irregular state recommendations for architects making prosperity IT systems based on blockchain.

Kuo et al. [14] showed a couple blockchain applications in therapeutic administrations, for instance, improved helpful record the administrators and pushed restorative administrations data record, and their defined applications prosperous affection. Then they reviewed the current challenges been intercepted in the blockchain universe for human administrations, including the mystery, flexibility, and delicacy of an ambush on composing blockchain technology advancements. As shown by the authors, some model execution methodology that accoutered encounters are encryption of fragile data or dispersal of just meta data and securing sensitive information off the chain to guarantee order and keeping simply fragmentary, advancing checked trades on the chain instead of the entire trade previous log to manufacture elasticity of the blockchain technology, and the determination of a virtual private framework or HIPAA-predictable parts to keep the 51% ambush.

Ekblaw et al, [15] made a blockchain based technology that board arrange that engages patients to get to their therapeutic history over various providers. This stage used an implied permissioned blockchain to manage verifications and the communication of data and its security through cryptography and proof of work.

They curated an image of useful patient's records using blockchain technology and presented a methodology to increase the interoperability of data. Restorative analysts supported by contributing through mining the blockchain network.

Petarson et al. [16] proposed a research study based on blockchain that used Merkle tree and showed a social protection also considers the blend with the FHIR measures. It presented proof of interoperability as the agreement framework in the midst of fair

mining. Affirmation of interoperability relies upon conformance to the FHIR convention, affirmation that the blockchain transaction operators are able to make use of data and can exchange data with known standards.

Dubovitskya et al, [17] proposed a framework based on the decentralized ledgers technology on supervising and distribution of restorative transactions for threatening development tolerant thought which was permissioned. Their structure used a support organization to affirm selected customers using a username/mystery state plot. Understanding character was made by methods for a mix of before long perceiving information and encoded for additional security purposes. Restorative data records were exchanged to a cloud server which is secured, with their passage supervised by the blockchain method of reasoning.

Gropper [18] focused on the construction and making use of individualities which are based on blockchain for affirmation specialists and directs to the patient organizing test going up against prosperity IT structures. Patients are depended upon to present a propelled wallet all alone devices to make their id's based on blockchain, which would then have the capacity to be used to talk with whatever is left of the framework.

As opposed to securing data, the groper's structure will eat up just the id's based on blockchain and utilizing it to verify the administer access to tolerant information arranged in their proposed architecture.

They proposed a research work model which they specified as an FHIRChain, whose compositional choices were explicitly introduced to insure the key specific essentials portrayed interoperability by the ONC. Their arrangement changes from the work already done on blockchain establishments what's progressively, related understanding instruments since it is decoupled from a particular blockchain structure and rather focuses on plan decisions of splendid contract and other interfacing parts of blockchain. Their proposed model was as such great with any current blockchain at that time, using the pillars of sharp pacts.

P. Zhang et al [9], proposed that their DApp based on FHIRChain displays the usage of modernized prosperity identities that don't explicitly encode private information and would therefore have the capacity to be substituted the omitted identities in the decentralized ledgers also. Their proposed model resembles in utilizing the electronic identities in the Gropper structure, FHIRChain gives a logically streamlined course of action. In extension, we meld an exchange segment of access by tokenizing in their proposed model that alters with their medical patient's information benchmarks. At long last, we impact sweeping key cryptography to streamline safe and secure confirmation what's more, assent endorsements, while at the same time shielding aggressors from getting unapproved data get to.

3. CONCLUSION

In this paper, we discussed the different approaches proposed for emerging blockchain in the smart health sector. Where we discussed the interoperability, security, data sharing, data storing and data retrieval of patients record using blockchain technology. The use of blockchain technology makes data more secure and increases its interoperability. The blockchain makes clinical data globally available while also keeping high security measures. It can further be extended for addressing other interoperability issues in healthcare such as the co-ordination with other companies. The smart contracts offer miscellaneous opportunities to implement in healthcare. In future, the blockchain technology's use expansion in the healthcare sector would be helpful in making the smart cities.

REFERENCES

1. Roman Beck, Michel Avital, Matti Rossi, Jason Bennett Thatcher. "Blockchain Technology in Business and Information Systems Research". Business & Information Systems Engineering. Vol: 59, pp: 381–384: 2017.
2. Prabha S, Elias Kougianos, Saraju P. Mohanty, Madhavi K. "Everything You Wanted to Know about Smart Healthcare ". IEEE Consumer Electronics Magazine. Vol: 7, Issue: 1 , Jan. 2018.
3. Peng Zhang, Michael Walker, Jules White, Douglas C. Schmidt "Metrics For Accessing Block Based Healthcare Decentralized Apps"
4. Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman "MedRec: Using Blockchain for Medical Data Access and Permission Management". 2nd International Conference on Open and Big Data. IEEE 2016
5. Kevin Peterson, Rammohan Deeduvanu, Pradip Kanjamala, and Kelly Boles "A Blockchain-Based Approach to Health Information Exchange Networks"
6. Huawei Zhao, Peidong Bai, Yun Peng, Ruzhi Xu "Efficient Key Management Scheme for Health Blockchain." ISSN 2468-2322. IET.
7. Joao Pedro Dias, Luıs Reis, Hugo Sereno Ferreira, Angelo Martins "Blockchain for Access Control in e-Health Scenarios". 2018.
8. Koshechkin K.A.a, b, Klimenko G.S.a, Ryabkov I.V.a,,Kozhin P.B.a . "Scope for the Application of Blockchain in the Public Healthcare of the Russian Federation". ELSEVIER 2018
9. Peng Zhang a, Jules White a, Douglas C. Schmidt, Gunther Lenz, S. Trent Rosenbloom. "FHIRChain: Applying Blockchain to Securely and Scalable Share Clinical Data"
10. Krawiec R, Housman D, White M, Filipova M, Quarre F, Barr D, et al. Blockchain: Opportunities for health care. Proc. NIST Workshop Blockchain Healthcare. Computational and Structural Biotechnology Journal 16 (2018) 267–278.
11. Peter JB, Nichol B. Co-creation of trust for healthcare: The cryptocitizen. Framework for interoperability with blockchain. 2016.
12. I. G. B. S. P. S. Team. Blockchain: "The chain of trust and its potential to transform healthcare – our point of view" 2016.
13. Zhang P, Walker MA, White J, Schmidt DC, Lenz G. "Metrics for assessing blockchain based healthcare decentralized apps." IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom). 2017.
14. Zhang P, White J, Schmidt DC, Lenz G. "Applying software patterns to address interoperability in blockchain-based healthcare apps" the 24th pattern languages of programming conference. 2017.

15. Kuo T-T, Kim H-E, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc 2017.
16. Ekblaw A, Azaria A, Halamka JD, Lippman A. “A case study for blockchain in healthcare: “medrec” prototype for electronic health records and medical research data.” Proceedings of IEEE Open & Big Data Conference. 2018.
17. Peterson K, Deeduvanu R, Kanjamala P, Boles K. “A blockchain-based approach to health information exchange networks.” 2016.
18. Dubovitskaya A, Xu Z, Ryu S, Schumacher M,Wang F. “Secure and trustable electronic medical records sharing using blockchain” arXiv preprint arXiv:1709.06528. 2017.
19. Gropper A. “Powering the physician-patient relationship with hie of one blockchain health it.” 2016.
20. Al Omar A, Rahman MS, Basu A, Kiyomoto S. Medibchain: “A blockchain based privacy preserving platform for healthcare data.” International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer. 2018. p. 534–43.
21. Yue X, Wang H, Jin D, Li M, Jiang W. “Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control.” J Med Syst. 2016.