

**ADDRESSING TRANSPARENCY VIS-A-VIS PRIVACY IN PORTABILITY OF HEALTH INSURANCE THROUGH BLOCKCHAIN****Govind Murari Upadhyay\*<sup>1</sup>, Monica Sharma<sup>2</sup> & Pankaj Kumar Varshney<sup>3</sup>**<sup>1</sup>Department of Computer Science, Institute of Innovation in Technology and Management

Janakpuri, New Delhi (India)

<sup>2</sup>Department of Management, Institute of Innovation in Technology and Management Janakpuri, New Delhi (India)<sup>3</sup>Department of Computer Science, Institute of Information Technology and Management Janakpuri, New Delhi (India)**DOI: 10.5281/zenodo.4660047****KEYWORDS:** Blockchain, Insurance, Network nodes, Healthcare, Ledger.**ABSTRACT**

A blockchain is a community ledger deal out in excess of a set-up that testimony operations (memorandums send commencing individual system knot to a further) carry out in the middle of network contributors. Every operation is confirmed by network nodes according to a mainstream agreement method prior to being added to the block chain. Recorded information is able to not be revolutionized or wipe away and the past of each operation can exist re-formed by the side of in the least time. Authors have been proposed a system using block chain mechanism for health insurance entails institution of burly procedures for health data collection and compilation right from grass root level. Recommended technique bestows the precise to the policyholder of health insurance to relocate the credit gained him for pre-existing conditions and time vault keeping outs in case he chooses to switch the insurance provider.

**INTRODUCTION**

Product development has adorned each and every aspect of business and insurance is no exception. While more than 55% of customers are ready to explore new insurance models, only 26% of insurers are exploring such models [19]. Insurance products traded decades ago have lost their sheen and shine, and newer improved products have substituted them which have made portability a wide prevalent choice with the policyholders. Portability gives the right to the policyholder of health insurance to transfer the credit gained him for pre-existing conditions and time bound exclusions in case he chooses to switch the insurance provider.

Portability of health insurance requires establishment of strong procedures for health data collection and compilation right from grass root level. Traditional paper based health records have no practical value in today's regime of electronic information exchange, therefore maintenance Electronic Health Records (EHRs) has been considered to be a feasible option[1]. It has been observed that the e-health data aggregated may contain sensitive information on each individual such as the name, age, and HIV status, may damage the person's reputation and trust of the company and hence robust privacy protection mechanisms are also required. Some studies have proposed an efficient and secure e-health data release scheme with differential privacy to provide the necessary privacy guarantee.[2][4]. With the introduction of the US law Health Insurance Portability and Accountability Act (HIPAA) in 1996, policies, technology, and record-keeping at medical facilities, health insurance companies, HMOs, and healthcare billing services are all impacted. According to HIPAA (Health Insurance Portability and Accountability Act), the medical insurance claim process is carried out by healthcare providers, insurance companies, and clearinghouses. [18] Further in 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH) widened privacy and security protections imposed by HIPAA.

More recently the European Union's General Data Protection Regulation (GDPR), which was made operational on 25th May 2018, envisaged a new set of rules governing the privacy and security of personal data replacing all of Europe's earlier privacy laws and thus having a far reaching impact on the data driven insurance industry.

Currently web-based facilities do exist regarding procurement and maintenance data for all types of health insurance policies issued by various insurance of providers which can be accessed by the new company to which



## Global Journal of Engineering Science and Research Management

a policyholder wishes to port his policy. But the existing algorithms are neither fair nor transparent. Further, many of them are not available online and not adaptive [3] To worsen the situation, insurance frauds have not only tormented the lives of innocent people but also the insurance industry. Insurance frauds may be committed at any point ranging from application stage to portability to settlement of final claims. [3] According to the McKinsey & Company report of 2017, nearly 5 to 10 percent of insurance claims are fraudulent.

The insurance industry is working together with the health providers on things like fraud detection and prevention on one hand and improving the client experience by adhering to sound data management principles like data privacy and effective data usage. A thorough review of the related work throws light on the possibility of weaving a blockchain based network between insurance and health providers so that twin goals of transparency and privacy are met in one go. Thus, our model is novel as it not only imparts transparency to the system but also checks fraudulent opportunities arising out of insurance portability option.

Motivation for writing this paper came out of observation of breeding possibilities of fraud in the Indian Insurance sector which may be committed by any policyholder while porting the health insurance policy from one insurance company to the other. Say a health insurance policy is lapsing on 1<sup>st</sup> January and the policyholder ports it to another company on 30<sup>th</sup> November against no claim bonus prior to the date of lapse. Now during this one month the policyholder meets a health hazard which he had insured and takes the claim from his previous insurance company. As the portability request has already been processed, by any chance the second insurance company is not able to take cognizance of this incident unless the policyholder himself notifies it to the new insurance company. So there is a need to devise a system so as to adjust the benefit given to the policyholder at the time of portability. We propose to deploy blockchain-enabled technology where all insurance-providers collaborate with healthcare providers (ie hospitals or private clinics) without undergoing any additional process of negotiating with insured seeking portability.

Blockchain is a public distributed database which holds the encrypted ledger. It is encrypted to keep the details of the people involved in it completely anonymous. A block is a collection of all the recent transactions that have happened and is verified. We group those transaction details using the hash code and then store in a block chain. Once a transaction is verified by the miner, that block becomes a permanent part of the blockchain, and the chain keeps growing. It is the belief that in every ten minutes the block is created and the blockchain grows accordingly. The number of transactions performed in a time frame that are grouped in a block and then stored in a blockchain. A ledger is maintained to hold the record of all the transactions. If we want to change any specific transaction the change or modification in block is not possible because all the participants in the distributed environment have the copy of all the records. In this if anybody wants to modify the record that record must be verified by the specified miner. Once the miner verifies the transaction then only the record can be uploaded in the system and the copy of that updated ledger will be available to all in the distributed environment. Every block uses the previous hash code. Every block has specific hash code associated with it, used in identifying factors for that block. This hash is oriented with a very complex hashing algorithm. If we make a minute change in hash input it makes a highly different output as whole. We cannot reverse engineer this hash code as well. The algorithm is designed in such a way that no one can get the complete data by reverse engineering the hash code. We have the complete hash details of every transaction that has happened as part of that block. There could be multiple transactions in a ledger so every verified and validated transaction gets added to block thereby ensuring that transactions cannot be manipulated. The ledger is generated by the people using software that solves the mathematical problems.

The use of the blockchain enabled technology in applications for healthcare and health insurance has been investigated by several researchers. More than 55% of insurance firms have implemented innovative technologies like machine learning, artificial intelligent and advanced analytics to quantify risks[19].

It has been observed that if the insurers are able to record transactions on the Blockchain at each point in the transactional lifecycle from seeking a quotation to binding a policy contract, the immutable life record of that policy or the policy holder can be traced [7]. Blockchain technology offers many advantages and disadvantages in the insurance sector ( e.g. Car insurance, farming insurance, delay insurance and home insurance) which can



## Global Journal of Engineering Science and Research Management

be generalized and applied to other sectors. The advantages include: Using smart contracts to improve customer experience and lower operating costs in case, Fraud prevention, Data entry/identity verification, Pay-per-use insurance and Peer-to-peer insurance. However some of these may be case sensitive. [17]

Another study was conducted to address the performance and security concerns of insurance processes by designing a blockchain enabled solution for the insurance industry. The objective was to (a) to automate and speed up business processes in the insurance industry, from client registration and policy issuance to claims handling, (b) to make fraud-detection easier using decentralized digital repository, (c) to make client data confidential and accessible only to the authorized parties, (d) to reduce administrative and operational costs, and (e) to enable regulators and auditors to detect suspicious transaction patterns and market behaviors. The authors not only discussed the main design requirements, corresponding design propositions, and encode various insurance processes as smart contracts but also conducted extensive experiments in order to figure out performance of the suggested framework and security of the proposed design. [8]

By taking the example of parametric insurance a study has shown that in the insurance industry, blockchain-based smart contracts can enable the automation of simple life insurance policies, thus reducing costs of administration, and provide a platform for new insurance products where transparency, trust, and simplicity offer value[10].

Another research proposed blockchain-based medical insurance storage system which is expected to help an insurance company in obtaining patient's medical expenditure records. By taking four parties viz. patients, hospitals, servers and insurance companies in the model along with Ethereum blockchain and small memory and CPU, the proposed system enjoys special advantages, e.g., decentralization, tamper-resistance etc.[11]. In another study, a self-organizing framework for insurance based on IoT and blockchain has been proposed which recognizes even the use of cryptocurrencies for making payments using of peer to peer communication protocols. [3]

A related work cited that the breeding inefficiencies of the current model of electronic data handling of the patients cause wastage of time, money and also delays patient care. Cloud-based EHRs also suffer centralized problem, i.e., cloud service center and key-generation center therefore blockchain-based EHRs and an authentication scheme for blockchain-based EHRs has been proposed.[1] In the same vein another study focussed on developing an efficient, interoperable and highly secure blockchain network to store and manage Electronic Health Records (EHR) of all patients would enable seamless access to historic and real-time patient data while eliminating the burden and cost of data reconciliation.[5] Blockchain may provide a solution to both secure patient health data from unauthorized breaches and at the same time make access to such data easier for patients[6]

One study highlighted the potential use of blockchain technology in association with mobile-based healthcare applications thus imparting patient centric care as well as offering patients' complete authority over the sharing and privacy of their data [12]. In a related work, a privacy-preserving DML model has been proposed for a permissioned blockchain network to resolve such important issues for tackling the issues of privacy, security and efficiency. It has been shown that machine learning fits better in a permissioned blockchain with differential privacy than restrictive applications in a permission-less blockchain (e.g., cryptocurrencies)[9].

Safe and convenient data sharing of personal health records is vital to improving the interactions and collaborations between insurance and healthcare industry. Therefore, smart contracts present an opportunity for automating the adjudication process in insurance making claims transparent to the health care provider and insurer, exposing potential errors, and frauds that can be corrected or investigated in a much timelier manner. Another benefit of creating these pre-established agreements via smart contracts is to ensure involved participants are up-to-date and properly notified as policies or rules change [13]. In a study a model incorporating blockchain technology in Smart Contracts has been suggested with the objective of improvising the insurance sector in order to make it more transparent. All important information related to Investments, realized profits, repayments, deadlines, history and future business strategy will be shared with the client through a blockchain network. All the contracts will be modernized and transformed into smart contracts which will be automatically and



# Global Journal of Engineering Science and Research Management

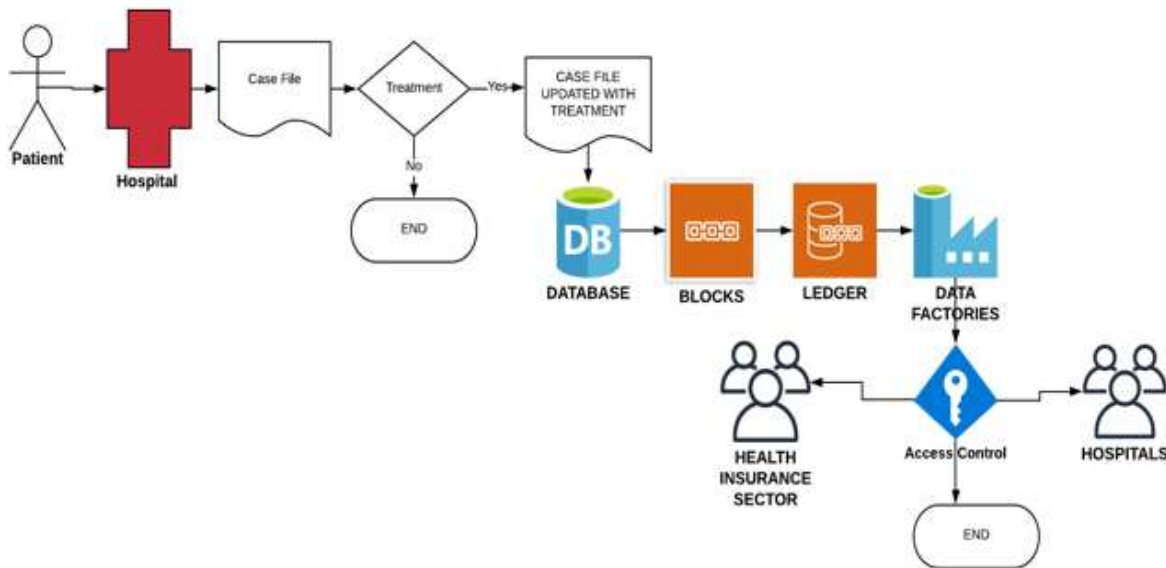
intelligently executed for speedy refunds to the policyholders leaving no room for compensations for fake incidents. [16]

Another research proposed deployment of a blockchain enabled mobile application to collect health data from personal wearable devices, manual input, and medical devices, and synchronizing data to the cloud for data sharing with healthcare providers and health insurance companies. Moreover, for scalable and performance considerations, a tree-based data processing and batching method is adopted to handle large data sets of personal health data collected and uploaded by the mobile platform [15].

Health insurance fraud means deliberately deceiving the health insurance company and as a consequence healthcare benefits are paid illegitimately to an individual or group. The main purpose of fraud is financial benefit. [20] The settlement of health insurance claims is one of the most tedious tasks of the healthcare sector as claims are prone to fraud and can consume the time and energy of the patient and healthcare provider. Thus, data structures must be used to store patient information, medical service record, and insurance payments, as well as provider-insurer agreements in the distributed ledger. The authors used the Hyperledger Fabric blockchain to implement and evaluate the system design and found that their approach is not only feasible but also time-efficient. [18]

## PROPOSED MODEL

As already discussed, in the current scenario if any patient ports a health insurance policy before its due date and registers a claim against the existing policy, the claim details are not transferred to the new insurance policy provider. There is a chance in the existing system that the patients hide their medical history while porting or discontinuing with the old policy provider. This model is proposed to preserve the privacy of the patient and impart transparency in the whole network of patient-healthcare provider-insurance sector.



### Entities of the proposed model

#### *Patient*

The primary entities in our model are – the Patient, who is insured by the insurance company and requests for insurance policies. The patient submits claim requests, and receives refunds, and the Agent, who acts on behalf of the client, and processes the client’s requests to the blockchain network. An agent can have multiple clients.

#### *Healthcare Provider/Hospital*

Once the patient visits the healthcare Provider which may be any of the hospitals (public or private) a casefile for that patient is created and simultaneously uploaded to the blockchain network. Now this network can be used for



## Global Journal of Engineering Science and Research Management

information sharing with other healthcare providers as well as insurance companies where both the later parties will have the right to access data from the patient. Every request for previous health data will be recorded in the blockchain thus imparting transparency among all parties.

### **Database**

Database is software used to store and retrieve information for future prospective. A case file is updated into the hospital database. A block is generated with the details of the patient and the diagnosed disease. A block is a collection of all the recent transactions that have happened and is verified. The details will be verified by the health insurance provider, if correct details the block is created. Once a verified block is created it can't be altered by anyone.

### **Blocks**

Block will hold block header and block body. In the block header there will be information of the previous block hash, time stamp, merkle root, block id and signature. Timestamps show the blocks are connected in chronological order, acquire the details of the block regarding when the block was created and what transaction happened. Merkle root is used to hold the hash code of the blocks. Signature is used for authentication purposes. Block body will hold the details of the different transactions along with the generated hash code.

### **Ledger**

A ledger is a kind of database where confirmed transactions are recorded. Ledger is also called distributed databases. A ledger is maintained to hold the record of all the transactions. If anyone wants to modify the details of any patient it's not possible. Once entry is recorded in a ledger it can't be modified, because it has a certain hash code. In our model when the patient will approach the hospital for diagnosis or hospitalization a digital document regarding his health will be generated, the next level Authority Setup algorithm to generate their master secret keys. Authority Setup algorithm will verify the detail and the details will be updated to the ledger.

### **Data Factories**

These are the kind of repositories used for storing and processing data. It can be a cloud server. The patient history can be mined only by the health insurance providers and hospitals. The patient details will not be available on a public forum.

## **CONCLUSION**

In this paper researchers' has been proposed the solution to addressing transparency & privacy in portability of health insurance all the way through blockchain technique. Suggested method confer the specific to the policyholder of health insurance to move the credit gained him for pre-existing conditions and time jump barring in case he chooses to switch the insurance provider. The aim is also to work in an ecosystem policy by integrating several partners from other fields (travel agencies, telecom, market, etc.) because the final goal is to promote, not only the insurance sector, but the economy as a whole.

## **REFERENCES**

1. Tang, F., Ma, S., Xiang, Y., & Lin, C. (2019). An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records. *IEEE Access*, 1–1. doi:10.1109/access.2019.2904300 (accessed on 3.04.2020)
2. Li, H., Dai, Y., & Xiaodong Lin. (2015). Efficient e-health data release with consistency guarantee under differential privacy. 2015 17th International Conference on E-Health Networking, Application & Services (HealthCom). doi:10.1109/healthcom.2015.7454576
3. Vahdati, M. (2018): A Self-organized Framework for Insurance Based on Internet of Things and Blockchain. *IEEE DOI* 10.1109/FiCloud.2018.00032 (accessed on 1.04.2020)
4. Y. Xiao, L. Xiong, and C. Yuan (2010) "Differentially private data release through multidimensional partitioning," in *Secure Data Management*. Springer, 2010, pp. 150–168.
5. Shah, B., Shah, N., Shakhla, S., & Sawant, V. (2018). Remodeling the Healthcare Industry by employing Blockchain Technology. 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET). doi:10.1109/iccsdet.2018.8821113





## Global Journal of Engineering Science and Research Management

6. Kshetri, N. (2018). Blockchain and Electronic Healthcare Records [Cybertrust]. *Computer*, 51(12), 59–63. doi:10.1109/mc.2018.2880021
7. Nath, I. (2016). Data Exchange Platform to Fight Insurance Fraud on Blockchain. 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW). doi:10.1109/icdmw.2016.0121
8. Raikwar, M., Mazumdar, S., Ruj, S., Sen Gupta, S., Chattopadhyay, A., & Lam, K.-Y. (2018). A Blockchain Framework for Insurance Processes. 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). doi:10.1109/ntms.2018.8328731
9. Kim, H., Kim, S.-H., Hwang, J. Y., & Seo, C. (2019). Efficient Privacy-Preserving Machine Learning for Blockchain Network. *IEEE Access*, 1–1. doi:10.1109/access.2019.2940052
10. Cohn, A. et al (2017) Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids. <https://georgetownlawtechreview.org/wp-content/uploads/2017/04/Cohn-West-Parker-1-GEO.-L.-TECH.-REV.-273.pdf> (accessed on 3.04.2020)
11. Zhou, L., Wang, L. & Sun, Y. MISStore: a Blockchain-Based Medical Insurance Storage System. *J Med Syst* 42, 149 (2018). <https://doi.org/10.1007/s10916-018-0996-4>. (accessed on 3.04.2020)
12. Antonio Clim et al. (2019) Data exchanges based on blockchain in m-Health applications. *Procedia Computer Science* 160 (2019) 281–288.
13. Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain Technology Use Cases in Healthcare. *Advances in Computers*. doi:10.1016/bs.adcom.2018.03.006
14. Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). doi:10.1109/pimrc.2017.8292361
15. Meskini, F. Z. and Aboulaich, R. "Multi-agent based simulation of a smart insurance using Blockchain technology," 2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS), Marrakech, Morocco, 2019, pp. 1-6. DOI: 10.1109/ICDS47004.2019.8942270 (accessed on 3.04.2020)
16. Gatteschi, V. et al. "To Blockchain or Not to Blockchain: That Is the Question," in *IT Professional*, vol. 20, no. 2, pp. 62-74, Mar./Apr. 2018. DOI: 10.1109/MITP.2018.021921652 (accessed on 3.04.2020)
17. Xinchu, He. Et al. "Toward Privacy-Assured Health Insurance Claims," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1634-1641.
18. World Insurance Report 2019. <https://worldinsurancereport.com/> (accessed on 3.04.2020)
19. V. Rawte and G. Anuradha, "Fraud detection in health insurance using data mining techniques," 2015 International Conference on Communication, Information & Computing Technology (ICCICT), Mumbai, 2015, pp. 1-5.