

Use of Blockchain Technology in integrating Health Insurance Company and Hospital

Nukala Poorna Viswanadha Sravan, Pallav Kumar Baruah, Sathya Sai Mudigonda, and Phani Krihsna K

Abstract— Function of Health Insurance Industry is multi-faceted. The service provider needs to manage the claims of policy holders. This task involves authentication of data from multiple sources. While servicing the claims it also needs to take care of the interests of multiple agencies like health care service providers. There is possibility of error and fraud happening at each and every stage of the process of validating a claim. This is due to the involvement of multiple data handlers like agents, and different service providers to authenticate the data. It is a fact that insurance companies are incurring huge losses due to such frauds or errors. It is found that the degree of Transparency, Trust while processing a transaction, claim settlement time, security of data, etc. are important for validating a claim efficiently.

We propose a framework based on Blockchain Technology to provide an efficient and fraud free solution to the above problem of validating insurance claims. Through smart contracts our platform supports for the interaction between current transaction system and Blockchain.

This paper focuses on the design of processing Health Insurance related transactions using the Blockchain. The framework has been developed on Ethereum, an open source permissionless blockchain framework. The process of authentication is role based for various parties involved in the network

Index Terms— Blockchain, Bitcoin, Cryptography, Decentralisation, Distributed Ledger, Smart Contract, Health Insurance.

1 INTRODUCTION

Currently data is an invaluable resource, which guides the business decisions. There is possibility of tampering the data, which leads to serious problems in decision taking in Health Insurance Industry. This is true in the centralized databases. Data owners have no control on their data like the storage and access. Blockchain promises the data integrity as well as the distributed control of the data.

Nukala Poorna Viswanadha Sravan is currently pursuing masters degree in Computer Science in Department of Mathematics and Computer Science in Sri Sathya Sai Institute of Higher Learning, Puttaparthi, India. PH: +91 8125558414, Email: poorna.sravan@gmail.com.

Pallav Kumar Baruah, Head of Department, Department of Mathematics and Computer Science in Sri Sathya Sai Institute of Higher Learning, Puttaparthi, India. PH: +91 9440699887, Email: pkbaruah@sssihl.edu.in.

Satya Sai Mudigonda is a professionally qualified associate actuary and management consultant. He is currently teaching the postgraduate students in Department of Mathematics and Computer Science in Sri Sathya Sai Institute of Higher Learning, Puttaparthi, India. PH: +91 9603573032, Email: satyaibabamudigonda@sssihl.edu.in

Phani Krishna Kandala, is currently Assistant Vice President in Swiss Re. He has done in Master's from Sri Sathya Sai Institute of Higher Learning, Puttaparthi, India. PH: +91 91 82 472136, Email: kandala.phanikrishna@gmail.com.

Blockchain is an underlying technology of Bitcoin which emerged as the discovery of Satoshi Nakamoto [1], thus making Bitcoin as the first cryptocurrency which leads to many future Blockchain implementations. This technology offers a novel way of building distributed systems. Blockchain is a distributed ledger that has all transactions that has not yet executed in the system. The Blockchain is widely applicable to many industrial areas (industrial domains) where there is a need for transparency and trust among distributed different parties in the network. It is a Peer2Peer network where every full node stores a copy of the Blockchain ledger. There is no central authority that manages the Blockchain database. The Consistency of the ledger is achieved by using various consistency protocols involving all parties in the network. Selection of consensus protocol depends on the trust model and the business environment. Immutability of the ledger is achieved by using the cryptographic techniques [2]. For validation and authorization of transactions, all the nodes involved in the consensus should agree upon the request that has come.

As there is no central authority involved, there is no middle-man involvement in processing data and taking actions accordingly. These results in non-reversible transactions and no need to trust the parties involved in the transaction. People should trust the system and the code. All transactions are grouped and stored in blockchain. The sender broadcasts the transaction in the P2P network when a new transaction is created. Transactions are not confirmed as it arrives, because as nodes acquire the transaction, they run consensus algorithm for validating it and holds it in their transactional pools. Validation of transactions involves running the predefined tests about the structure and the parameters.

As operations of Health Insurance Industry involves lot of business rules, smart contracts will be encoded with these rules[3],[4] for writing the ongoing transactions to the blockchain. Policy holders who had registered with company, Service provider (Hospital) for treating patients with valid health cards, Claims made by the Hospital/Policy holder and receiving the refunds for same, all these are written in smart contracts. This distributed ledger will avoid transactions, if the transaction violates the rules that are defined in the smart contract. Current Health Insurance system needs lot of interactions manually for transaction process which leads to dirtiness of the data or slow process because of the involvement of various stakeholders which leads to long time for payment. This current system puts the industry in tough challenges for detection of fraud claim[4], all these can be handled using smart contracts based on distributed ledger[5],[6].

This paper addresses the Transparency, Data level Security, handling the drawbacks of the current insurance system by using blockchain technology as a solution ([7]). By using blockchain technology in health insurance, a) provides solution for speeding up and automating the business process in Health Insurance like registration of new policy holder and assigning roles for various stakeholders in the Health Insurance Industry, b) Making client data confidential and accessible to authenticated parties [8], c) Triggers were made to higher authenticated authorities in the organisation for detection of transactions that are suspicious, d) Reducing the lengthy time and costs involved in claim settlement.

Our proposed design handles the efficient approach for the transactions related to Health Insurance are done using Blockchain technology. The framework has been developed on Ethereum, a permissionless blockchain framework.

Paper is organised as follows

1. Introduction
2. Current Health Insurance System.
3. Need of Blockchain Technology to replace current Health Insurance System.
4. Technical challenges with Blockchain.
5. System architecture for Health Insurance Framework.
6. Prototype and experiments
7. Conclusion

2. CURRENT HEALTH INSURANCE SYSTEM

Health insurance is insurance that covers the whole or a part of the risk of a person incurring medical expenses. By estimating the overall risk of health care and health system expenses over the risk pool, an insurer can develop a routine finance structure, such as a monthly premium, to provide the money to pay for the healthcare benefits specified in the insurance agreement. The benefit is administered by a central organization such as a government agency, private business. A health insurance policy is a contract between the insurance provider and a policyholder. A Contract could be annual, monthly. The type and amount of health care costs that will be covered by the health insurance provider are specified in writing.

2.1 Pain Points in Current System

1. It is tedious to maintain the patient information. Insurance providers do not have access to whole facts of the patient data which ends up in assigning wrong policies and increases in costs of processing.
2. Whole insurance industry operates among diverse stakeholders like policyholders, doctors, and hospitals etc., Because of the involvement of various stakeholders the complete flow of claim operates independently thereby increases the difficulty in sharing records.
3. Lot of time and administrative costs involved in processing insurance claims because of diverse stakeholders, which leads to customer dissatisfaction.
4. Involvement of paperwork involved in the current environment and there is a possibility of manipulating details at every stage which incurs a huge loss to the insurance industry. There is a possibility of data getting dirty and wrong.
5. Customer/Policy holder information stored on central server can lead to theft of the information and there is a lack of security.

3. NEED OF BLOCKCHAIN TECHNOLOGY TO REPLACE CURRENT HEALTH INSURANCE SYSTEM

3.1 Advantages that Blockchain Promises for the above issues

Blockchain transforms the insurance industry, by decreasing the amount of time and operational cost for processing claims.

Features of blockchain like accessibility, immutability, transparency, automated execution of transactions and being the distributed ledger among all the peers in blockchain network make all the issues resolved. Patient owns his/her medical information and can share the information as per needs without depending on any central agency, this is done using the blockchain peer-to-peer network. Role-based authentication has been implemented to provide access to the various stakeholders depending on their roles and the information is stored in blockchain thereby avoiding identity theft. Improves the claim settlement in real time by processing or denying claims easier and faster which will be done by rules in the smart contract, which improves trust factor.

This technology improves the operational efficiency, prevents fraud and helps bring transparency in the complex world of insurance business.

Policy Contract defines rules for policy holder's coverage. Processing the claims and refunding the same are the key customer focus areas where expertise is needed for adjusting the claims or the investigators for negotiating and settling the claims. This differs depending on the type of policy and the kind of services provided by Hospital and other entities in-

cluding regulators. Consumer protection issues are important aspects within the underwriting, and settlement of claim process, the rules, i.e. the rules-based claims processing. During the claim processing several documents originating from several stakeholders (Policy holder, Hospital, Insurance Company etc..) containing sensitive data is used and some of which may not be available in digital format. Settlement of claims is done based on the regulations governed by the policy contract. This leads claim processor to apply rules and take decisions before the claim is paid. This goes into building incentive models to enable groups to decide which claims should be paid out and which should not be paid. In Health Insurance claims adjusters and doctors have to investigate whether the claimed amount should be paid for such illness and these are done based on analysis made on the medical reports submitted by the policyholder or hospital. Blockchain could help to building all these features into the smart contract and enable Insurance Companies to achieve the transparency, security, decentralization. All transactions written to Blockchain are visible to all, shared across multiple locations and impossible to alter or delete.

Current process takes 17-18 days for claim settlement, with blockchain all this can be done in real time.

4. TECHNICAL CHALLENGES WITH BLOCKCHAIN

Currently all over the world there are lot of blockchains and cryptocurrencies. Identifying all of these options and establishing communication across the blockchains are the biggest issue. Many industries are focusing on the creation and use of more proprietary blockchain for the business problems. Blockchain does not solve the data standardization issue, but provides a platform for sharing data in real-time on trusted network. This is achieved using the interoperability across the different applications in the same frame work using the IPFS.

4.1 Interoperability across Smart Contracts

Interoperability provides sharing of information and transactions across diversified blockchain systems. User can send information from his blockchain to other blockchain where the user will have ability to read and interact respectively. In Health Insurance as there are a lot of stakeholders involved all of them work independently so sharing information is limited. This problem is overcome with IPFS. All the networks will be connected using the same system of files through InterPlanetary File System which is peer-to-peer distributed system. It is content addressable and there is no single point of failure.

In our case hospital claims for refund which is deployed in a separate smart contract, and insurance company validates the claim for request which is deployed in other smart contract. In order to pass the data between these 2 different contracts in the same frame work, the data will be put in IPFS. When a data is put on the IPFS it generates a hash for that content, using the public key of the insurance company the IPFS hash will be encrypted. Insurance company decrypts the same using its private key for viewing the claim request which includes medical reports as well. Applying IPFS to store medical informa-

tion would mean no trust requirement between providers and no single point of failure to prevent patients from accessing their medical records.

4.2 Authentication of Stake Holders in Blockchain

Smart contract potentially solves the data access issue, providing access to right information at right time and this mechanism describes the control principle over the access. In insurance industry every stakeholder is described with the access control relation. The relevant information of user-role is in a smart contract deployed on a blockchain and to employ a challenge-response authentication protocol for verifying if a user owns an asserted role. Ethereum protocols and cryptography make the proposed system suitable for the authentication of roles. After creating the Smart contract, insurance company deploys the SC on the Ethereum blockchain under a corresponding smart contract address (SC.EA). Details about the SC can be accessed by checking the SC and the information of the user role will be stored on blockchain.

5. SYSTEM ARCHITECTURE FOR HEALTH INSURANCE FRAMEWORK BETWEEN HOSPITAL AND HEALTH INSURANCE COMPANY

We investigated how to effectively realize the Blockchain technology mechanism in the Health Insurance Industry for Claim processing and achieve the same in real time with more transparency and decentralized way. Smart contracts were used and the same were placed in the distributed ledger (blockchain platform), for storing the result. Methods in smart contracts handles the requests that were made by the stake holders.

5.1 Core Members of the Proposed Model

Insurance Company covers the Policy Holder, Hospital (Service Provider to policy holder), new policy requests, claim submissions and receiving the refund for same. The Hospital may claim the insurance company for treating the patient so the payment can be done to either of the entities.

5.2 Various Components in the Model

Access to the data depends upon the roles which are automated by smart contract. A distributed ledger records the execution results of all transactions. Authentication and user access are based on cryptographic algorithms.

The framework uses smart contracts that drives the transactions. All smart contract has its own defined rules, of which addition of transactions to blockchain depends. Nodes validate a transaction by running the consensus depending on the result of the validation block will be added accordingly to Health Insurance blockchain.

5.3 Registration

Various stake holders should have a minimum of one main account like [EOA] or the account can be created by the Insur-

ance company using the `eth.createAccount()` which generates the key pair for joining the network. All the accounts are indexed by their addresses which are derived from his/her own public key. In our scenario, the identity management and authentication are done in a decentralized way and smart contract handles this[9].

5.4 Insurance Model

The scenario where main transactions are standard of insurance operations like client registration, claim submission by

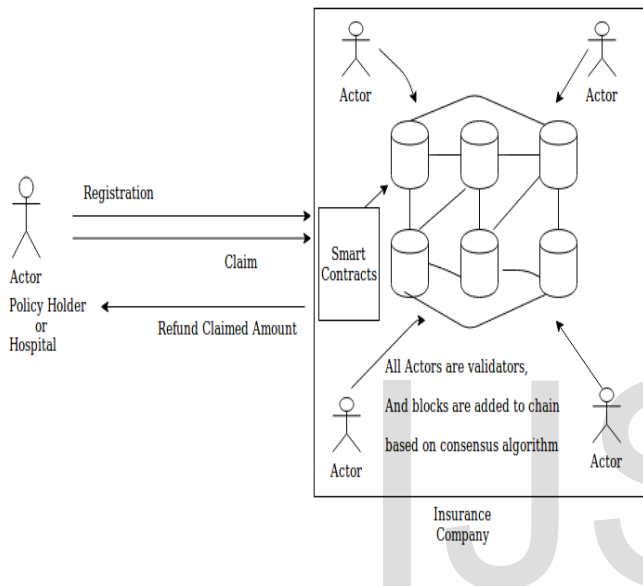


Figure 1. Health Insurance Blockchain Framework

either policy-holder or Hospital, processing of refunds etc. The characteristics of blockchain ensures that policy-holders do not blame insurance company falsely for the service company provides because all the transactions are transparent and tamper proof. Figure 1 depicts the proposed framework workflow.

A transaction that occurs should satisfy the rules which are governed by the smart contract if it failing to satisfy then that transaction will be put in the uncle block for some time, after a certain period that transaction will be removed. The term object refers to the attributes of the client or the policy. Rules are coded in smart contract, and any transaction that occurs should satisfy the rules, if it fails to satisfy, then that transaction will be put in the uncle block for some time, after a certain period that transaction will be removed.

5.5 Retrieval of Policy Holder Details

Retrieval of client details can be done by either an insurance agent or the owner of the policy. The user needs to pass a session key to the insurance agent (ida) to access certain details. Once session gets expired that key can't be used any more. Any changes to policy information that are made during that session by the insurance agent will not be recorded until it is signed by the owner of the policy.

5.5 Claim Processing

The proposed model of blockchain network has, client (policyholder/hospital) sends a transaction to Insurance Company. Smart contract executes the claims request accordingly as shown in Figure 2. Hospital bills will be paid by the insurance company for a valid policyholder. Policy Holder has to sign a message using his/her private key for the claim. The insurance company will decrypt the same using the `ecrecover()` which is Elliptic curve cryptography function. If the retrieved address is present in the blockchain, then smart contract validates how much amount has to be paid and transfers the ethers to the account of Hospital. The peer nodes run the Proof of work consensus and appends the transaction's to blockchain if they are valid.

Signed Message: 0x2bd417da8309df910acfa85ec45038ed5358d991ca4539fd55dc4126cb128a087476c71e65b72adb0d0ef9474939d32eca0754e3937b3b0d9b8ce738dd7975191b.

This signed message (Figure 3) will be passed as (64,64,4) bits to smart contract, and smart contract decrypts using `ecrecover(hash value, r, v, s)`.

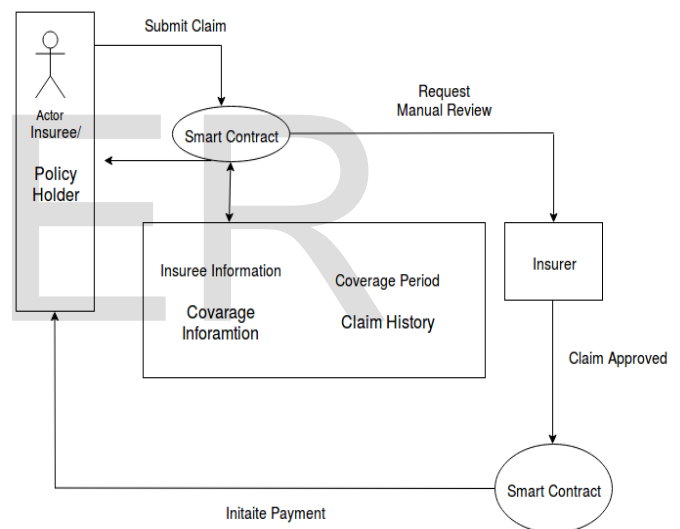


Figure 2. Claim Processing

GAS USED	GAS LIMIT	MINED ON	BLOCK HASH
27088	6721975	2018-09-26 09:05:26	0x54d209c5296edc43fbc20fdb19b65c5ac30cef52388537ecf90cebc461ac917
TX HASH			
0x6d699a92eb01f3a3df9602edbf36315c9af79636428a27218fde6ba884c63688			
FROM ADDRESS			
0x5850b30ef8c332235154824528177a1810f730d1			
TO CONTRACT ADDRESS			
0x32085f83095ec2641ba6893f83fe97C68eE15A			
GAS USED	VALUE		
27088	0		

Figure 4. Immutable Transactions

Transferring ethers to hospital account accordingly with the consent of policyholder. All this happens in a smart contract and all the transactions are transparent and Immutable with cryptographic techniques Figure 4.

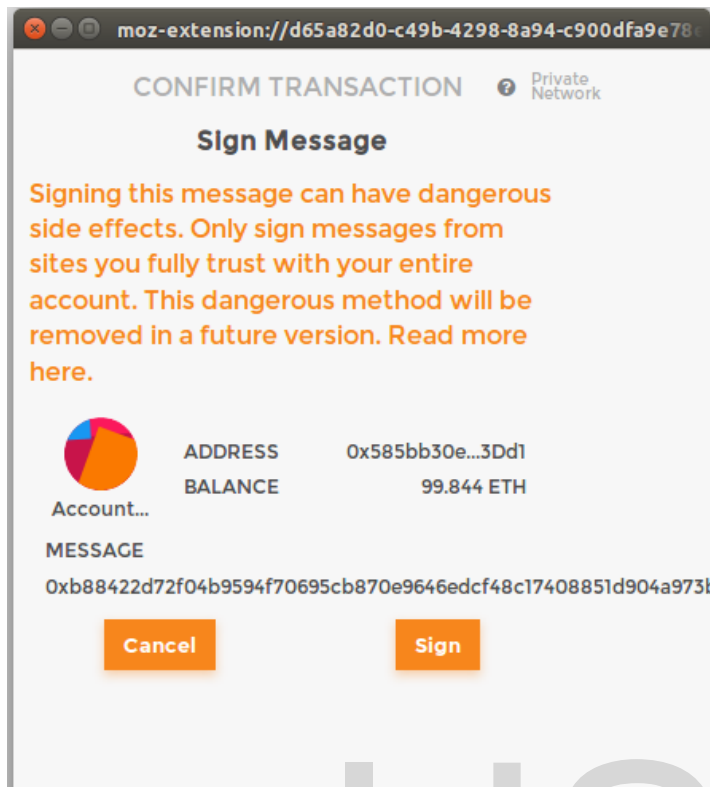


Figure 3. Sign made by Policy Owner

6 PROTOTYPE AND EXPERIMENTS

In our set up we have tested with 3 nodes for the proposed Health Insurance Framework. Ethereum Blockchain was used and contracts were written in solidity v4.0.31. The experiments were carried out on a system with a quad core Intel i5 processor and 15.6 GB RAM, running Ubuntu 16.04 (64 bit), Lan speed 15 Mbps. We computed the confirmation time of transactions with different number of peer nodes in the network.

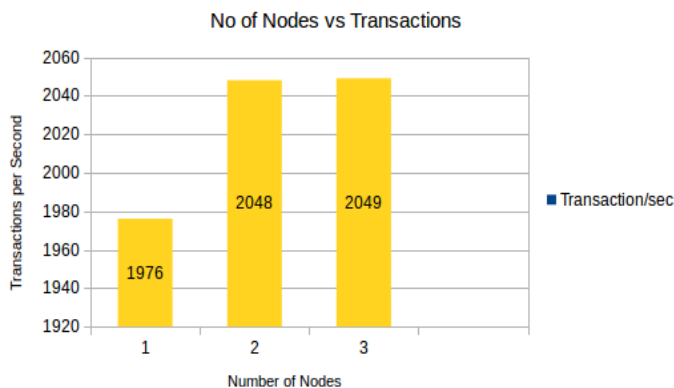


Figure 5. Number of Transactions per second

Figure 5 shows the Number of transactions per second that are written Blockchain using 3 node setup. Figure 6 shows the gas consumption for claim submission.

Different networks in ethereum had given different con-

firmation time for validation of transactions and the same with different smart contracts in the framework.

7 CONCLUSION

We proposed a working model of blockchain based framework to provide, totally decentralized environment to handle big data with the characteristic's of transparency and data integrity.

While implementing our framework we used the concept of interoperability across different applications in same frame

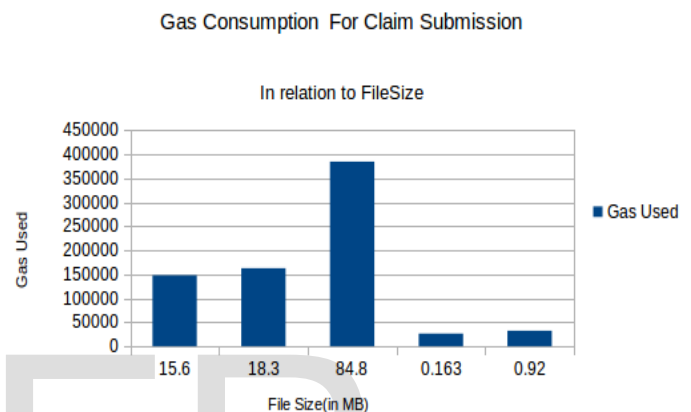


Figure 6. Gas Consumption

work using the IPFS.

In Future, we will be developing and evaluating our prototype by implementing the same model in R3 Corda[10] platform. Interoperability protocol will be developed to establish the communication across the frameworks of Ethereum and R3 Corda platforms. A study will be done by comparing the outcomes with respect to Ethereum and Corda to check the latency, throughput and tps. This enables evaluating the varying tradeoff between frameworks.

8 REFERENCES

- [1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
- [2] Vukolic and Marko, Rethinking permissioned blockchains, in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, ser. BCC 17 New York, NY, USA: ACM, 2017.
- [3] K. Christidis and M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access, vol. 4, pp. 22922303, 2016
- [4] C. D. Clack, V. A. Bakshi, and L. Braine, Smart contract templates: essential requirements and design options, arXiv preprint arXiv:1612.04496, 2016

[5] I.Nath, Data exchange platform to fight insurance fraud on blockchain, IEEE 16th International Conference on Data Mining Workshops(ICDMW),pp.821825, 2016

[6] H.Watanabe, S.Fujimura, A.Nakadaira, Y.Miyazaki, A.Akutsu, and J.Kishigami, Blockchain contract: Securing a blockchain applied to smart contracts,IEEE International Conference in Consumer Electronics,pp. 467468, 2016

[7] Mayank Raikwar, Subhra Mazumdar, Sushmita Ruj, Sourav Sen Gupta, Anupam Chattopadhyay, and Kwok-Yan Lam A Blockchain Framework for Insurance,IEEE 978-1-5386-3662-6/18, 2018

[8] Ason Paul Cruz, Yuichi Kaji Role Based Access Control Using Smart Contract, IEEE Access 10.1109/ACCESS.2018.2812844., 2018 January

[9] Wallet based authentication.Available:
<http://zeltzinger.com/2017/04/14/the-ethereum-signaturevalidation-app/>

[10] Corda Platform: <http://www.corda.net/>

IJSER