Blockchain Technology in Health Inusrance – Integration of 8 Stake Holders

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

Abstract— Blockchain is a progressive innovation technology that is impacting several domains, especially in the area of FinTech. The Health Insurance Company involves a number of stake holders for effective completion of various activities. All these stakeholders work in silo, there by data becomes dirty and may lead to errors as it moves from one stake holder to others. There are a considerable number of cases of fraud that goes undetected and measures to prevent fraud appears to be a distant goal. Insurance companies are incurring huge losses because of such errors due to unclean data and undetected frauds. Moreover consumers are loosing control over their own data. This leads to disintegration of trust between Insuree and Insured. Current system lacks transparency, takes lot of time for claim processing, settlement and underwriting process.

Our framework is built using blockchain technology induces Trust and Transparency. It also provides efficiency and security that enables the information to be controlled by the policy owner. Smart contracts are used for claim management there by increasing the speed of claim settlement process and decreases the administrative costs and provides an error and fraud free solution. Ethereum is used for developing the framework, which is open source premissionless blockchain framework.

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

1 Introduction

Satoshi Nakamoto[3] proposed bitcoin in 2009, which is decentralized cryptocurrency which works on public ledger and it is distributed across the nodes, there is no central authority involved for validation of transactions and validation is done based on the consensus algorithms which provides high guarantee that transactions cant be altered once it is committed to blockchain.

Nukala. Poorna Viswanadha Sravan, M.Tech(cs), SSSIHL. Email: poorna.sravan@gmail.com.

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

Satya Sai Mudigonda, Department of Mathematics and Computer Science in Sri Sathya Sai Institute of Higher Learning, Puttaparthi,India.
Email:satyasaibabamudigonda@sssihl.edu.in

Phani Krishna Kandala M.sc, M.Tech, is currently Assistant Vice President in Swiss Re. Visiting Faculty Sri Sathya Sai Institute of Higher Learning, Puttaparthi, India. Email: kandala.phanikrishna@gmail.com.

As the blockchain technology is evolving many cryptocurriences like Litecoin[4], Ripple[5], Ethereum[6] have attained huge success. Many consensus mechanisms are proposed for managing the ledger: Proof-of-work[7], Proof-ofstake[8,16],proof-of-activity[10],practical Byzantine faulttolerance[11] other consensus mechanisms[13-14].

Blockchain is a distributed ledger which works on the peer-to-peer network for recording the transactions. All the transactions that are committed in the blockchain are immutable, comparing to traditional databases, rules of the transaction are fixed to itself using the smart contracts. Smart contracts have the rules which are agreed by participants in the distributed ledger. Distributed ledger has 3 components a) Consensus Algorithm b) Shared Ledger c) Nodes in the network. All the transactions that are occurring in the network will be grouped into blocks and then added to the chain in chronological order.

Hashing technique is used for entangling the blocks which prevents changes to a particular block[1]. Every block has a pointer which points to its previous block and it is associated with a time stamp. Once the transactions are recorded in the blockchain it is Immutable, this characterstic of blockchain helps to prevent double spending, records can't be tampered and transactions are protected from the attackers [2]. Consensus mechanism is used for validation of transactions that are happening, thereby avoiding the trust on centralized authority or third party. Contracting parties can track their assets and agreements without any 3rd party or centralized verification process.

Every transaction that is committed by a node will be signed and then broadcasted to a network. Signing a transaction by the private key provides authenticity and

integrity of the transaction. The Important fact is only a valid user with the private key can sign the transaction and if others try to intrude they get an error because the information results in the failure of decoding. Blocks have set of transactions with a time-stamp, these blocks are broadcasted in the network where the validation nodes check whether all the valid transactions are present in the block if it is valid then it is added to blockchain else it is discarded. Thus network nodes play a crucial role as validators and the full node has the full copy of the blockchain ledger[20,21,22].

Transactions occurred in the network and considered legitimate by the network are chronologically arranged and packed to a time-stamped blocks by certain nodes, those are called miners. In different frameworks, different consensus mechanisms are available like proof-of-stake or proof-ofwork. The selection of data type and miners is incorporated into the block by the type of consensus protocol chosen. The blocks are then broadcasted to the network, validation nodes verify whether the received block has legitimate transactions and that it references the previous block in the chain by using the corresponding hash. If both requirements are met, the block will be added to the blockchain by the nodes. Otherwise block is discarded. This is the role of nodes in the network. Since the blockchain network is a P2P network, a node can be regarded as a peer when it starts to connect and communicate with other nodes in the network, along these lines the proper name would be a peer-node. In laymans term, the computer that has a complete copy of the full blockchain ledger and operates on that is called as a full node[33,34].

Each node maintains the copy of the ledger and the transactions that are committed to chain depends on the consensus algorithm. Major advantages of using this technology are as follows[16]

1. Redundancy Transactions are bundled into blocks.Once the block is validated it is written to the chain which will be immutable. Creation of new block is done only after the completion of the previous block.
2. No central authority is involved.
3. Various business rules are encoded into a smart contract which helps for automation of various tasks.
4. Prevents single point of failure as the ledger copy is replicated across the nodes.

Huge amount of data is getting generated in the modern world which leads the industry to take business decisions according to the data they receive. As there is a lot of middlemen involved in passing information from one agent to other agents in the Health Insurance industry there is a possibility of human error and fraud which leads insurance industry to incur huge losses. With Blockchain technology, we can avoid the middle man and can make the entire system decentralized, transparent thereby making the entire claim management system in a friction-free way.

Policyholder avails the services from the hospital and the data is scattered across the service providers and all service providers work in a silo, because of which policyholders lose access to their data and they are not able to get the ownership of their data[19].

In Health Insurance claim management, there are hospital, pharmacy, emergency, TPA(Third Party Authorisation), policyholder, Regulator, Insurance Company are the various stakeholders involved in claim processing. Health Insurance Industry is about handling the claims and managing the risks which have a lot of financial transactions daily. This leads the Health Insurance company vulnerable to some of the following: Attacks on system, fraudulent transactions, data becomes dirty as it passes from one stakeholder to other stakeholders, Security of the policyholder information. As this domain is highly complex with many business rules and a lot of stakeholders involved the claim handling becomes tedious and time taking which demands a lot of processing and settlement time. And there is no control of the medical information to the respective policyholder.

Storing the financial transactions and ownership of the data of policyholders are the fundamental core part in coverage of claim operations. Existing methods are noticeably complicated, fragmented data across stakeholders suffer from lack of a standard. Reconciling the data across stakeholders for claim settlement is a tedious job and demands a lot of time for the same, there is the probability of duplication of data which leads to high cost.

Business rules are coded into the smart contract[15] which represents the contractual agreement. Parties involved in the contract structures the relation between them efficiently without any ambiguity of words in self-execution fashion. We have implemented the framework on ethereum blockchain and different smart contracts have been implemented for different stakeholders involved in the entire chain. With Smart contract customer experience, claim time can be reduced and operational cost will be decreased.

Our Framework focuses on getting all the stakeholders into one single platform thereby sharing information across the stakeholders become easy and drives the efficiency in claim processing and other activities in the Health Insurance Company, as a consequence it brings the structural change in the current working system of Health Insurance. Our work also addresses on Transparency, Security of Medical records of policyholder, Reduction in Claim settlement time and decreasing the administrative cost, avoid's middle man, human errors and fraud, detailed description is given in the Table-1.

A. Ethereum

Vitalik Buterin in 2013 designed Ethereum, which facilitates to build the decentralized applications on top of the blockchain. Currency in Ethereum is called Ether. Transactions and computation fees called gas have to be paid and the amount of gas depends on the computation type. Consensus mechanism in Ethereum is Proof of Work. Solidity is the language which helps to build decentralized applications that are Turing complete.

Each account is an object with 20 unique byte address.

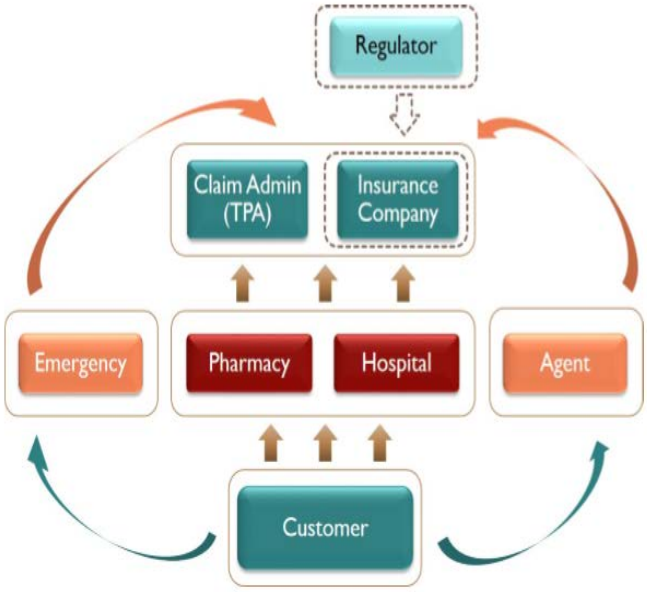


Figure 1. Current System of Stake Holders In Health Insurance

	contracts thereby increasing the pace of settlement time.

Table I

Accounts in Ethereum are 2 types Externally Owned Account which work with a private key and Contract account, that is generated on uploading the contract code into blockchain. EOAs are meant for signing transactions to produce messages and it doesnt contain any code.

2. CHALLENGES IN CURRENT HEALTH INSURANCE SYSTEM

Insurance company incurs a lot of administrative costs to figure out the claims of the policyholder that are claiming by different service providers in favor of the policyholder. A lot of time human involvement is required to find out whether it is fraud or genuine. This also consumes a lot of time for processing and settling the claim. As the data arises from different stakeholders where all stakeholders are operated in silos as shown in Figure 1, thereby data gets fragmented and becomes dirty and may prone to human errors and fraud, legacy models may slow down the process of claim settlement.

In the current system, all the data will be stored in the centralized system and it will be controlled by central authority, there is possibility of changing the records, forgery, an omission of information and reversing transaction without past information, thereby creating a lack of trust and transparency to the policyholder's data [25], which can be addressed using blockchain.

Insurance providers lack behind the patient data because of the involvement of various stakeholders, there is a possibility of ending up in assigning inappropriate funds to the policyholders which lead to customer dissatisfaction.

Current system runs with a lot of paperwork which may lead to manipulation of data at different stakeholder's level, thereby creating a huge loss to insurance companies.

Security of policy holder's medical data is the biggest disadvantage, because policyholder does not have control over his data, and he may not be able to access his records as and when required. And the policyholder has to wait a lot, for settling the claim. This procedure may take from 17-20 days to months. For both Insurer and Insuree Trust, Transparency, security of the data, creates the gap in visibility that leads to error/fraud.

Some other areas that affecting Health Insurance Company [24]:

1. Verification and process delays.
2. Unstructured data capturing in account.
3. Claims settlement including premium payments.
4. Operational cost.
5. Poor user engagement.
6. Lack of trust between Insuree and Insured.
7. Risk aversion and delayed processing time.

Stakeholders we considered in this paper are the Insurance company, Agent, Policyholder, Hospital, Pharmacy, Emergency, Third party Administration. Currently, all these stakeholders work in a silo and communicates across themselves depends on the services needed. Time taken to settle the claim in this scenario is large because of the involvement of the various middle man across the entire Insurance chain [37]. Policyholders do not have much control over there information and lack of transparency exists because of the business model and organizational structure, a lot of interactions in this system is done using the brokers. During 2015 Digital Life Design conference in Munich, Christof Mascher, Allianz chief operating officer said [23]

"How to get to a higher frequency of interaction with customers was always a big challenge for insurers. The digital age has brought us countless opportunities and frequent touch points. Now it is up to us to understand the devices and the customer's diverse ecosystems, so we can tailor our offer and reach out to them".

Main activities in the Health Insurance Company are Underwriting, Claims Process and Management.

A. Underwriting

Risk selection is one of the most important constituent in an insurance cycle. Underwriting department in an (re)insurance company mainly performs the quantitative and qualitative assessment of risk with the support from other departments (Example: Actuarial). They would assess the risk based on their experience, market conditions. Each underwriter has some capacity within which to accept or reject the risk being insured.

B. Claim Process and Management

Claim unit comes to play once the risk arises for enabling the timely payment of the client. This procedure includes loads of examination and due constancy to possibly distinguish fake cases and guarantee the Insurance company isn't paying more than anticipated. Multiple claims

payment as requested by the policyholder is one challenge in the Insurance industry because there is practically zero coordinated effort in sharing data among them.

Claims processing improves the reputation of the Insurance company and the trust of the customer. Claim processing has 3 stages: a) Claim Submission b)Loss Adjustment by Insurance Company and other stakeholders c)Claim Approval and payment. Around $ 800 billion per year is the loss incurred by the Insurance sector for paying the fraudulent claims which are generally about 20% of the aggregate claims annually paid [28]. Currently, the claim settlement is done through assessors [29] which increases the turn around time. The same claim settlement can be done in real time through smart-contract by imbibing the business rules into it.

3. NEED OF BLOCKCHAIN TECHNOLOGY IN HEALTH INSURANCE SYSTEM

With blockchain technology policyholder is assured about the control of their data because of the public-private key cryptography and blockchain characteristics. Through smart contracts business processes are automated and other characteristics like robustness, Immutability of Data, Encryption, Transparency, Data redundancy are achieved. This helps the Health Insurance company for fair pricing and it also reduces the number of false positives in surveillance of transactions and helps in fraud prevention[9]. The entire procedure is transparent and avoids a lot of middle agents and the claim settlement time will come down because of the smart contract [26] [27].

In claim processing, Health Insurance company acts like intermediate for paying the claims according to the services that are availed by the policyholder. In the current system, the claim processing takes on an average 17-18 days to settle a claim and claims may not be processed automatically. Blockchain records the set of transactions that are coming from different stakeholders can help the Insurance company to identify fraud during the claim-processing.

It also helps to record the documents, ownership proof etc, by different stakeholders in the Insurance chain and link them to their digital identity. Stakeholders will not be able to modify the information that was inserted by other parties, because of this dis-intermediation will lead to lower costs. Trust between the Insurance company and policyholder is ensured because of the blockchain characteristics, as it removes a lot of middle man.

The main feature of this technology is to track the transactions in a decentralized way, thereby avoiding fraud and counterfeiting [17]. Trustworthy transactions are supported by this technology without any human monitor and control [18]. This technology helps to prevent fraud through AML (Anti Money Laundering) procedures. Some of the studies [30-32] suggest that using blockchain rather than with central databases, it helps the various stakes holders to validate the transaction and reduce the current challenges in the industry.

4. BLOCKCHAIN BASED FRAMEWORK FOR HEALTH INSURANCE

The activities that are involved in the Health Insurance company are encoded into smart contracts and deployed the same in Ethereum Blockchain for storing the results and transaction executions. Some of the terms in blockchain are as follows:

A. Transactions

Transactions are considered as an exchange of information between different stakeholders in the entire insurance chain. In Health Insurance scenario transactions are Underwriting, Processing claim, Claim Settlement etc.,

B. Proposers

Proposers initiate and submit transactions to the Blockchain.Allstakeholderscanbeconsideredasproposers.

C. Validator's

Validator's role is to validate whether the incoming transaction to be included in the Blockchain or not and this validation is done based on the rules that are coded in the smart contract and the consensus mechanisms. In Ethereum framework they are called as miners.

D. Block

Each block will be validated by the set of nodes involved in the network using the consensus mechanism, depending on the type of consensus algorithm (maximum voting whether to add a particular block to chain) block will be added to the chain.

Integration of all the stakeholders into one single platform as shown in Figure 2 using the blockchain will cut down the administration cost and it also solves the issue of transparency and security of the data. Policyholders has the access to their data because of the public-private key cryptographic concept. All the stakeholders are able to access the data because of the smart contract [12]. Accessing the data and performing a set of transactions in the chain depends on the kind of role the stakeholder has and this is done based on the role-based authentication using a smart contract.

Different contracts are defined in this framework because of the involvment of various stake holders and each transaction will be validated by the set of nodes using the proof of work consensus mechanism.

The ability of blockchain helps to improve customers experience and automate premium payment. Information can be stored in distributed ledger thereby reducing the turn around time in finishing the underwriting process, this is achieved through smart contract. Policy holder can pay the monthly premium using the Escrow concept in Ethereum.

Policyholders contract is encoded with the policy hold-

er's coverage information. Refunding and processing the claim requests are major areas where customer focuses and the involvement of experts in insurance industry plays a role whether to pay the requested claim amount or not. This varies according to the policies and the services entitled under those policies. Protection of policy holder's data is an important aspect in underwriting and also the rules that govern for settling the claims. A lot of information will be generated from the stakeholders in the form of medical records, pharmacy bills etc., which has a lot of sensitive information and some of the records may not be in digital form. Claims settlement is done based on the rules defined in the policy contract. Claim adjusters and doctors in Health Insurance company investigate whether the claim amount should be paid or not depending on the reports that are submitted by different stakeholders on behalf of the policyholder. Blockchain helps to build all these rules in the smart contract, thereby achieving the transparency, decentralization, and security as shown in figure 3. Whenever a transaction occurs if it is satisfied by the set of rules that are encoded in the smart contract, all such transactions will be written to the blockchain.

5. BLOCKHCHAIN ARCHITECTURE FOR HEALTH INSURANCE COMPANY

Our model implements the different functionalities that are done by the Health Insurance Company through smart contracts, and executing these contracts in Ethereum Blockchain, for contracts execution and storing the results.

Figure2. Stake Holders in Health Insurance with Blockchain

Figure3. High-Level view of Claim Processing through smart contracts.

A. Members involved in the Health Insurance

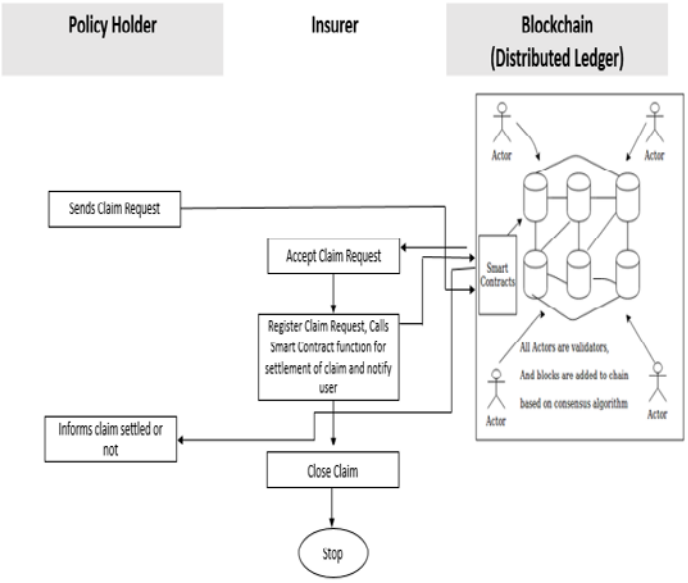
Primary member in the Health Insurance is Policy Holder who will be covered by Insurance Company by taking the Insurance Policy and paying the premium amount for the same and submitting the claims and receiving the refund for the same.

"Agent" acts as the mediator between Insurance Company and the Insured, role of agent ends by submitting the new policy holder's details to the insurance company and paying the premium amount on behalf of the customer.

"Insurance Company" modifies the cap for various fields of the details of the policyholder which are submitted by the agent, underwriting process will be done only by the Insurance Company. Insurance Company handles claim requests and also adjusts the claimed amount to be paid, with the help of claim adjusters and physicians.

"TPA"(Third Party Authorization) can be seen as outsourcing the claim processing administration, premium collections, and other administrative activities.

"Policy Holder" can see only his details and his agent information, and all the past history, he does not have the right to interfere at the services that are being done by the Insurance Company or other stakeholders in the Insurance Chain.



Role of "Emergency" stakeholder is to admit the patient in case of emergency and treat for the same and submit the amount to the insurance company on behalf of the policyholder. Insurance company validates whether the claimed amount should be paid to the hospital that treated Emergency.

"Pharmacy" provides the medicines as prescribed by the

doctor to the policyholder, and claims the pharmacy amount to Insurance Company on behalf of the policyholder.

"Regulator" mainly work with insurers to protect policyholdersinterestsandtheyensurebyenforcingtheregulations to insurance companies, setting sanctions and educating the policyholders. Their role is important in both promoting the industry growth and good governance.

B. Components involved in Model

The model has a distributed Ethereum blockchain B which logs the execution results of all transactions and also maintains the Insurance contracts, Authentication contracts and transaction results of all stakeholders in the chain. Nodes who involved in the verification of transaction validates whether the transactions that happen across the chain will be added to the chain or not based on the rules that are encoded in the smart contract. Entire functionalities of the Health Insurance company will be driven in Blockchain using the Smart Contracts.

C. Registration of Stake Holders

All the stakeholders involved in the chain will have an Externally Owned Account which is issued by Insurance Company through eth.createAccount(). Each stakeholder will have one public key and associated private key and also defined with a certain roles and services as shown in algorithm 1. Identity verification and authentication process are done in a decentralized way which is done using smart contract[36].

D. Proposed Model

Health Insurance company does a lot of transactions and different functionalities across the stakeholders. Transactions that happens across stakeholders will differ and these will be validated by the different smart contracts, whose business rules are encoded for the same. All the valid transactions are added to the Blockchain by using the consensus protocol. Blockchain maintains each transaction execution thereby ensuring that the client will not falsely accuse the Insurance company in case of any discrepancies that happens for his Health Insurance Data or delay in Claim Processing mechanism as shown in Figure 4.

Each contract (SC) can be accessed only by certain stakeholders. We are referring to the attributes of the stakeholders including policyholder and policy details as objects. Structure of all these things is defined during the instantiation of the smart contract. We have a function f that creates accepts the inputs of the details of the policyholder during underwriting and function f generates the composite keys (private key, public key). The public key will help to retrieve the details of the user information in the future.

Storing the data in Blockchain is very costly, we have used IPFS(InterPlanetary File System) for the storage. It is content addressable and in case of failure in a particular node, other nodes will be able to provide necessary information. By inserting the data in IPFS it generates a hash for the same, using the public key of Insurance Company or Third Party Authorization or other stakeholders, the generated hash will be encrypted. Respective stakeholders view the request by decrypting the same.

By recording the transactions on blockchain at every stage in the life cycle from the time of taking a policy and other activities that are done by various stakeholders to particular policyholder in Insurance Company, the immutability nature of Blockchain helps to trace the details thus delivers a degree of simplicity in underwriting procedure and has the capacity to lessen the fraud. This will lead to a decrease in transactional cost and trustless computations. Massive aspects of underwriting procedure, claims and billing administration are completely automated.

Algorithm1: Adding Stake Holders and their Roles

1. **Input:** userAddress, Role is passed to a function in Smart Contract
   //(only Insurance Company can add to contract)
   Adduser(address userAddress, String Role)
   onlyOwner
2. Mapping (address => uint) public userAddressList;
3. StakeHolders[] public Roles_List;
4. Check whether the above passed address is already present in the contract.
   //check userAddress in userAddressList
5. uint id= userAddressList[userAddress];
6. **if(id == 0)**
   // userAddress not present in the contract, so add
   Add userAddress to user Roles_List as follows.
   Roles_List[userAddress]= StakeHolder({Address: userAddress, From: TimeStamp, role: Role});
   //write this to event
   StakeHolderAdded(userAddress,Role);
   else
   User is already registered with certain role.

E. Validation of New Policy

In the process of issuing new policy, Insurance company has to validate with certain check list whether the new policy holder is eligible for the type of policy he choose,once all the conditions in checklist is verified corresponding clients policy-id will be created as described in algorithm 3.

F. Retrieving the details of the stake holders

Policy details can be retrieved by either an Insurance Agent or policyholder. Policyholder passes session key to Insurance Agent (ida) for accessing certain details. On expiration of session key, that can't be used anymore and any changes that are done by the agent will be recorded only if it is duly signed and authenticated by the policyholder.

The Insurance Company can see what all hospitals and pharmacies are enrolled with their company and it also can view the number of patients that are availing the services from the enrolled hospitals, pharmacies, these will be done using the public key of the hospitals, pharmacies.

G. Processing the Claims

In Proposed framework we have considered some stakeholders(Emergency, Hospital, Pharmacy, Policyholder) who had done service to the policyholders, those are eligible for receiving the refund for same. All these stakeholders send a transaction request to the Insurance Company or TPA(Third Party Authorization). As TPA acts as outsourcing for the Insurance Company it also does the claim settlement. Policy Holder has to sign a message using the private key for the request. Insurance Company decrypts the message using the Elliptic curve cryptography function ecrecover(). If the decrypted address is present in the Blockchain, then smart contract validates how much amount has to be paid and the same will be transferred to the respective accounts of the stakeholders(Pharmacy, Emergency, Hospital) as described in the algorithm 2. Nodes in the network run the consensus algorithm and append the transaction to blockchain if it is valid. Detailed description of the claim processing smart contract is shown in the Figure 5.

Signed Message:
0x2bd417da8309df910acfa85ec45038ed5358d991ca4539fd55dc4126cb128a087476c71e65b72adb0d0ef9474939d32eca0854e3937b3b0d9b8ce738dd7975191A.

Figure 6 shows how the policy owner signs. The signed message will be send as (64,64,4) bits to smart contract, smart contract decrypts using ecrecover.

Ethers will be transferred to the stake holders who have claimed on behalf of the policy holder from Insurance Comapany or Third Party Authorization and the entire claim processing is done through Smart Contract, all the transactions are Immutable and transparent as shown in figure 7.

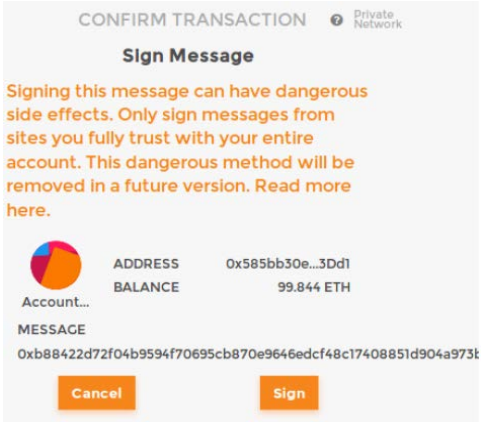


Figure 6. Sign made by policy owner

Algorithm 3: Validation of New Policy

1. **Input:** Pass the customer/policy holder Id_C, agent Id_A to a function in smart contract.
2. Queries the Blockchain with Id_C,Id_A.
3. If both exists in Blockchain

    Functions in Smart Contract has a checklist which cross-checks some of the fields like client premium amount with policy premium amount etc.,

    If all the details of customer satisfies the checklist then

        return $O_{client's\text{-}policy\text{-}id}$;// Client's policy-id

    else

        return "Policy can't be Sanctioned";

Algorithm2: Processing the claim

Input: $id_{private\_Key\_client}$,message,$O_{client's\text{-}policy\text{-}id}$

1. signedKey -> f($id_{private\_Key\_client}$,message);
2. pass the signed message as (64,64,4) bits to smart contract.
3. Smart contract decrypts the signed message using ecrecover(Elliptic curve cryptography function)

    returns ecrecover(message,r,s,v); //$id_{client\_publicID}$

4. If $id_{Public ID\_client}$,$O_{client's\text{-}policy\text{-}id}$ exists in Blockchain **then**

        if claimedAmount <= reimbursementp **then**

        //Deduction of amount will be taken care by

        //the ether wallet and transfers the amount

        //to recipent

        TransferAmount($id_{Hospital\_publicID}$,Number of Ethers);

        End

    else

        rejectclaim(idH,public);

    end

end

Figure 7. Immutable Transactions

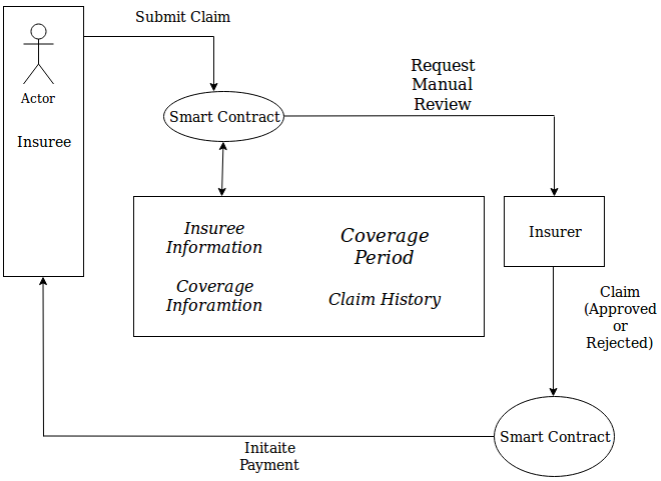


Figure 5. Claim Processing

H. Authentication based on the Stakeholders Role

Authentication mechanism helps to define the control principle over data and other activities. As Health Insurance industry involves a lot of stakeholders and set of roles are defined for each of them. The smart contract is encoded with the set of rules about the role of stakeholders in the Health Insurance chain, this helps to represent the authenticated and endorsed relationship between each stakeholder and helps to verify the ownership of roles. Each stake holders role is unique and it defines the access eligibility of specific services, every user has a role and every role has a service in the Insurance chain[34].

Digital certificates can be a solution for role-based authentication, but these require a public key infrastructure(PKI).PKI could be insecure and costly for maintenance[35]. We have defined a smart contract, which does the verification of user roles in a secure manner without any centralization, all the relevant information of stakeholders are encoded in the smart contract and deployed on blockchain, thus allows transparency in the roles and also maintains the anonymity of the users and this serves as, point of synchronization for various service providers to check their deserted roles.

Authentication-Response protocol is used for verifying whether the user owns certain services or not. Every stakeholder owns an External Owned Account(EOA) which will be issued by the Insurance Company. As and when request comes from a certain user for service(EOA.upublickey) is passed to role-based contract whether u.EOA has a particular service. Role-based contract responses back saying Response as (ServicesAvailable) and provides access to the services accordingly.

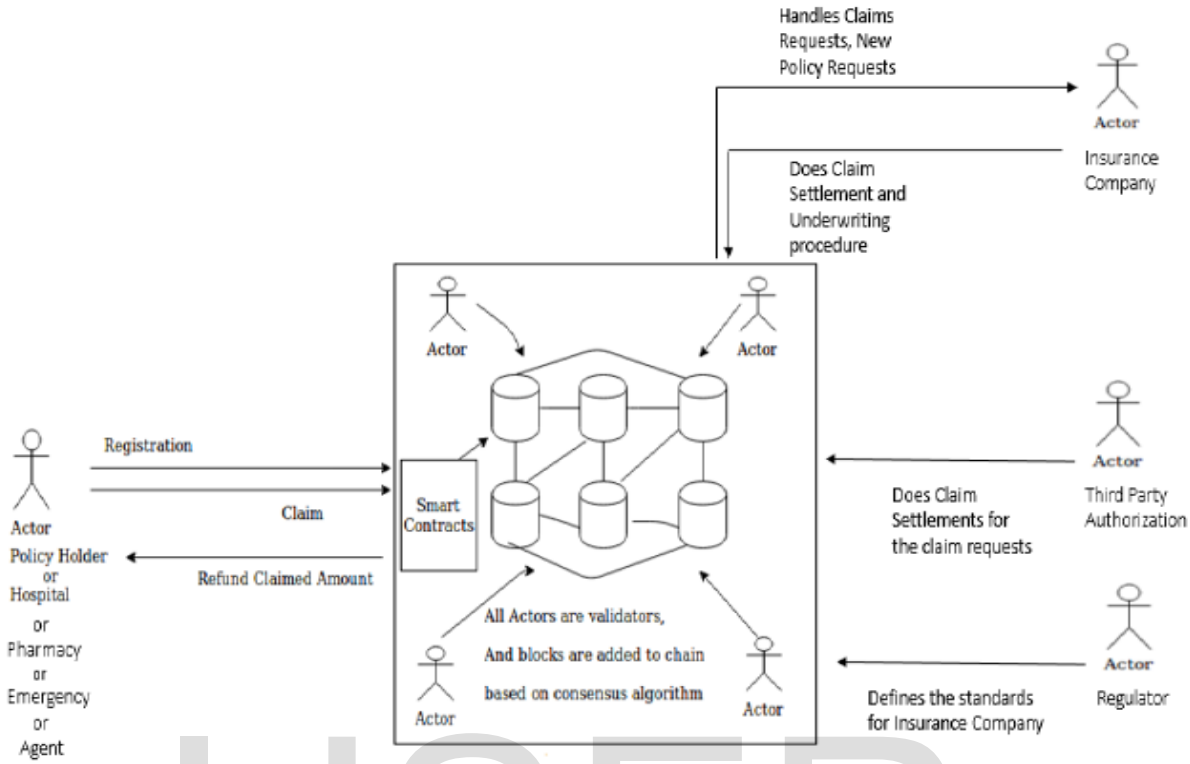


Figure 4. Stake Holders in Health Insuance connected through Blockchain

The protocol does the following tasks
1. Declares the user role.
2. Responding to the user query for accessing the services.
3. Responding to the verification of the user.

A stakeholder can access the service's iff there is role r. Service providing contract always communicates with the role assigned contract to figure out whether the service has to be given for a request or not according to the output of the role-based contract. This authentication of roles has the following properties:
1. The insurance company can issue roles to the stakeholders.Example- Duration of the role etc.
2. Role issuing authority can modify the roles in a transparent manner.
3. Authority has the right to cancel certain roles if necessary.
4. Services for the stakeholder will be identified based on Authentication-Response protocol.
5. Every action that is performed in the roles is transparent. Stakeholder can't perform an action on behalf of other stakeholders in Health Insurance Chain.

The above mechanism achieves transparency because all the activities are done using Smart Contract and these are reflected in Ethereum Blockchain and on the events log of Smart Contract.

I. Off-chain Storage

As the massive transactions happen in the Health insurance industry daily, there is need to store the information, storing the details of policyholders and medical reports on blockchain is very costly Example- $ 76,000/GB, A kilobyte is thus 640k gas according to the yellow paper[33].In order to overcome this issue, we have used IPFS(InterPlanetary File System).

IPFS is a distributed file system, resulted from the peer-topeer systems like BitTorrent, SFS, DHTs. There is no single point of failure and it is content addressable, there is no privilege for any nodes in IPFS. Data stored in IPFS can be communicated/added/retrieved using TCP, TOR, Bluetooth no centralized authority involved. Similar to hash table IPFS also implements a distributed hash table which provides a mechanism of (Key, Value), nodes that are participating can retrieve the value using the key.

Hashing a piece of data generates the content address, this address is hashed again to generate the key name. Hashes begin with Qm, it is multihash, means hash itself specifies the length of hash and hash function from the starting 2 bytes of multihash.

6 Prototype and Experiments

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.Proposed Framework had been tested wih 3 nodes. Confirmation time for transactions has been computed with different number of nodes in the network and the same are added to the blockchain using 3 node setup as shown in figure 8. Different types of health records with different sizes are uploaded for claiming the amount as the proof of services that are availed by policy holder,and records are uploaded in IPFS for storage, figure 9 shows the gas consumption for different types of records according to their memory sizes.

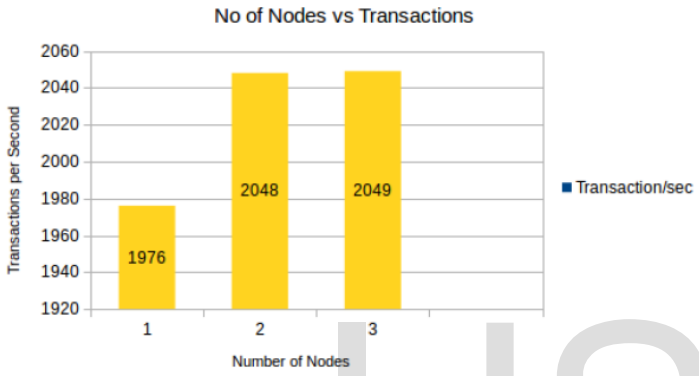


Figure 8. Number of transactions per second

7 CONCLUSION AND FUTURE WORK

We proposed a working framework of blockchain providing totally decentralized environment to handle large number of transactions with the characteristic's of

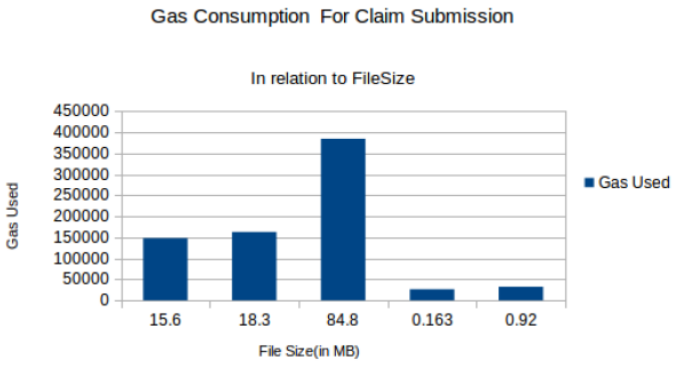


Figure 9. Gas Consumption

transparency and data integrity, Immutability. Our future work involves integrating Blockchain and Deep Learning to create Deep Chains. They ensure that model receives the appropriate data from authenticated sources, which can be used for training and making right level of business decisions. Interoperability is one of the essential feature for blockchains to share information across, we will be developing a protocol to share the information between R3 Corda[38] and Ethereum Blockchains. 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.

ACKNOWLEDGMENT

Our work is dedicated to Bhagawan Sri Sathya Sai Baba, Founder Chancellor of Sri Sathya Sai Institute of Higher Learning. We acknowledge Adarsh Saraf from IBM Research, Bengaluru, India.

REFERENCES

[1] C. Sillaber and B. Walt, Life Cycle of Smart Contracts in Blockchain Ecosystems, 51 Datenschutz und DatensicherheitDuD, vol. 41, no. 8, pp. 497500, 2017.

[2] B. Notheisen, J. B. Cholewa, and A. P. Shanmugam, Trading Real-World Assets on Blockchain: An Application of Trust-Free Transaction Systems in the Market for Lemons,Bus. Inf. Syst. Eng., vol. 59, no. 6, pp. 425440, 2017.

[3] Nakamoto S, Bitcoin: A peer-to-peer electronic cash system, IEEE Access, vol. 4, pp. 22922303

[4] Litecoin, Available: https://litecoin.org

[5] Schwartz D, Youngs N, and Britto A, The Ripple Protocol Consensus Algorithm, Available: https://ripple.com/files/ripple consensus whitepaper.pdf

[6] Wood G, Ethereum: A secure decentralised generalised transaction ledger, Ethereum project yellow paper 151:132, 2014.

[7] Dwork C, and Naor M, Pricing via processing or combatting junk mail, Annual International Cryptology Conference, pp.139147. Berlin: Springer,1992.

[8] King S, and Nadal S, Ppcoin: Peer-to-peer crypto-currency with proof-of-stake, Self-published paper, August-2012.

[9] N.P.V.Sravan, Pallav Kumar Baruah, Sathya Sai, Phani Krishna K, Use of Blockchain Technology in integrating Heath Insurance Company and Hospital, International Journal of Scientific Engineering Research, Volume 9, Issue 10,October-2018

[10] Bentov I, Lee C, Mizrahi A, Rosenfeld M, Proof of activity Extending bitcoins proof of work via proof of stake, Proceedings of the ACM SIGMETRICS 2014 Workshop on Economics of Networked Systems, NetEcon. 2, 2014.

[11] Castro M, Liskov B, Practical Byzantine Fault Tolerance, OSDI 99:173186, 1999.

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

[13] CryptoManiac, NovaCoin. Available: https://github.com/ novacoin-project/novacoin/wiki/Proof-of-stake

[14] Bentov I, Lee C, Mizrahi A, Rosenfeld M, Proof of activity Extending bitcoins proof of work via proof of stake, SIGMETRICS Perform. Eval. Rev.42(3):34-37, 2014.

[15] Buterin V, A NEXT GENERATION SMART CONTRACT DECENTRALIZED APPLICATION PLATFORM

[16] M. Friedlmaier, A. Tumasjan, I. M. Welpe, Disrupting Industries With Blockchain:The Industry, Venture Capital Funding, and Regional Distribution of Blockchain Ventures, Proceedings of the 51st Annual Hawaii International Conference on System Sciences (HICSS), January 2018.

[17] Vasilis Kostakis, Chris Giotitsas, The Political Economy of Bitcoin,TripleC: Communication, Capitalism Critique. Open Access Journal for a Global Sustainable Information Society, 12(2):431440,2014.

[18] J.Leon Zhao,Shaokun Fan,and JiaqiYan, Overview of business innovations and research opportunities in blockchain and introduction to the special issue, Financial Innovation,2(1):28,2016.

[19] Health Information and the Law, "Who owns medial records: 50 state comparison," 2015.Available: http://www.healthinfolaw.org

[20] Zheng Z, Xie S, Dai H, Chen X, Wang H, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Boston, MA, USA, 1114 December 2017; pp. 557564.

[21] Greenspan G, Blockchains Vs Centralized Databases, Available: https://www.multichain.com/blog/2016/03/blockchains-vscentralized- databases/

[22] Lewis A, A Gentle Introduction to Blockchain Technology. Bits on Blocks, Available: https://bitsonblocks.net/2015/09/09/gentle-introduction-blockchaintechnology/

[23] Allianz SE, "Digitalization: 'We need to tailor our offer to the new customer' - Press — Allianz", Available: https://www.allianz.com/en/press/news/company/pointofview=150123-we-need-to-tailor-our-offer.html

[24] Bernardo Nicoletti, The Future of FinTech: Integrating Finance and Technology in Financial Services - Bernardo Nicoletti-Google Books

[25] M. Mainelli and M. Smith, Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers(aka blockchain technology), J. Financ.Perspect., vol. 3, no. 3 Winter, pp. 3869, 2015.

[26] J.T. Lorenz, B. Mnstermann, M. Higginson, P. B. Olesen, N. Bohlken, and V. Ricciardi, Blockchain in insurance opportunity or threat?,McKinsey Co.,no.July, pp. 19, 2016.

[27] T.T.Kuo, H.E.Kim, and L.Ohno-Machado, Blockchain distributed ledger technologies for biomedical and health care applications, Journal of the American Medical Informatics Association, Volume 24, Issue 6, 1 November 2017.

[28] W. Nowiski and M. Kozma, How Can Blockchain Technology Disrupt the Existing Business Models?, Entrepreneurial Business Economic Review, vol. 5, no. 3, pp. 173188, 2017.

[29] F. Lamberti, V. Gatteschi, C. Demartini, C. Pranteda, and V. Santamaria , Blockchain or not blockchain, that is the question of the insurance and other sectors, IT Prof,2017.

[30] R. Hans, H. Zuber, A. Rizk, and R. Steinmetz, Blockchain and Smart Contracts:Disruptive Technologies for the Insurance Market, AMCIS 2017,August, pp. 110, 2017.

[31] 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

[32] A. Deshpande, K. Stewart, L. Lepetit, and S. Gunashekar, Overview Report Distributed Ledger Technologies / Blockchain: Challenges, opportunities and the prospects for standards, Br. Stand. Inst., no. May, p. 82, 2017

[33] DR. Gavin Wood, Founder: ETHEREUM ETHCORE, "ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER"

[34] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, Role-based access control models, IEEE Computer, vol. 29, no. 2, pp. 3847, 1996.

[35] R. Charette, DigiNotar certificate authority breach crashes e-government in The Netherlands, IEEE Spectrum 2011.

[36] Wallet based authentication. Avaliable: http://zeltsinger.com/2017/04/14/the-ethereum-signaturevalidation-app/

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

[38] Corda Platform: http://www.corda.net/