Introduction to LifeBlocks: A Blockchain based Insurance Platform

Shikhar Bhatt, Sumit Hotchandani, Kailash Raj Gaur and Sumedha Sirsikar
Maharashtra Institute of Technology, Pune, MH, India

Keywords: Blockchain, Insurance, Ethereum, Encryption, Cryptography, Smart Contract, IPFS.

Abstract: In India, the insurance sector is rife with inefficiencies. The entire process, from buying an insurance policy to settling claims, has numerous stumbling blocks. Blockchain is considered as a disruptive technology that could revolutionize and bring huge benefits to the insurance sector. It can be can be a game-changer, making the entire insurance process simpler, secure and efficient. Through this paper, we are proposing a blockchain based system "LifeBlocks" to solve various problems in the insurance sector. The paper talks about the problems in the current insurance process and how our system overcomes these problems. The paper discusses the four major use-cases of the system along with technologies like Parity Ethereum, InterPlanetary File System (IPFS) and Smart Contracts used to develop our insurance platform.

1 INTRODUCTION

Blockchain(Nakamoto, 2008) is a distributed ledger of records. It provides security by cryptographically storing the data. It is inherently permanent and immutable i.e. once recorded, data on the blockchain can not be changed retroactively. Involved parties can view all the data(transactions) ensuring transparency in the system. Blockchain supports smart contracts(Buterin, 2013)(Waltl et al., 2019) which are programmable logic that self-execute once predetermined conditions are met without the need for third-party intervention. Blockchain technology offers a novel way for constructing secure distributed systems. Initially designed as a system service for detecting double spending in cryptocurrency systems, blockchain is widely applicable to many business applications where there is a requirement of trust among distributed parties.

A blockchain is maintained by a set of nodes which do not fully trust each other. Nodes in the blockchain agree on time-stamped ordered set of blocks, each containing multiple transactions, thus the blockchain can be viewed as a log of ordered transactions. This log of transactions is called a ledger. The nodes keep replicas of this ledger and agree on an execution order of transactions. Whenever there is a transaction, it is broadcasted to the other nodes in the network and added to the pool of un-verified transactions. One of the nodes verifies the transaction by solving a random cryptographic puzzle and then broadcasts the solution. Other nodes act as validators and check if the solution is correct or not. If correct then the transaction is included in the ledger else reverted. This is the basic life-cycle of a blockchain transaction.

"LifeBlocks" aims to create a streamlined and efficient healthcare system by leveraging the blockchain technology. With blockchain already being a cryptographically secured platform and other applied cryptographic algorithms for secure file management and sharing makes the system robust and helps maintain integrity in the system. In addition, the tamper-proof nature compels the entire process of insurance to be efficient.

The paper is organized as follows: In section II, we describe the current landscape of health insurance in India, and how digital disruption can be key in it's evolution. Section III describes in detail our approach to the problem - various components in the system and how they improve the insurance process. Section IV covers all the important technologies used and their importance in the system. Section V concludes the paper with possible future work for our system.

2 CURRENT LANDSCAPE OF HEALTH INSURANCE

The right to health care is an essential and universally agreed upon human right. This basic human right has been kept out of the reach of the common man due to escalating costs and unavailability of quality medical services. Health insurance has emerged as an alternative to finance health care in light of these concerns. Health insurance is a contract between an

Bhatt, S., Hotchandani, S., Gaur, K. and Sirsikar, S.
Introduction to LifeBlocks: A Blockchain based Insurance Platform.
DOI: 10.5220/0009854000770081
In *Proceedings of the 17th International Joint Conference on e-Business and Telecommunications (ICETE 2020) - DCNET, OPTICS, SIGMAP and WINSYS*, pages 77-81
ISBN: 978-989-758-445-9

individual or group and an organization, wherein the organization provides the buyer health care coverage in exchange for a fixed amount known as "premium", which is decided based on a myriad number of factors.(Anita, 2008)

Health insurance refers to a wide variety of policies. These range from policies that cover the cost of doctors and hospitals to those that meet a specific need, such as paying for long term care. Health insurance in India is one of the fastest growing industries. Although there is a wide scope for growth, the sector is currently under-performing compared to other developed and emerging countries, especially when it comes to key performance indicators like insurance penetration and density. Penetration defined as ratio of insurance premium paid over GDP of the country is 3.69% in India compared to 5.62% in other emerging Asian economies and 6.13% in the rest of the world as of 2017. (Majumdar et al., 2019) Density indicates the coverage of a country's population i.e. the ratio of total insurance premium paid to the total population of the country. India's insurance density of USD 73 in 2017 lagged considerably behind the global average of USD 650 and USD 360 of other Asian economies. (Majumdar et al., 2019)

Insurance (Raikwar et al., 2018) providers recognize the advantages of technology in other industries and along with other stakeholders are making well-thought investments in leveraging technology to drive better customer experience, faster closure of claims and ease of buying insurance policies. The insurance sector has been a late adopter of technology but is now witnessing disruption. With adoption of AI and chat bots, insurance companies are able to provide round the clock customer support and the data being collected helps them understand the market better and launch more user-friendly products. As a result, the industry is experiencing a new era of growth in an increasingly competitive space.

The evolution of India's insurance sector holds great promise for both customers and the entities that operate within the industry. Disruption will likely continue and will result in the creation of many innovative companies and transformative services.

3 PROPOSED SYSTEM

This section talks about the four major use-cases of our system as mentioned- Identity Management, Electronic Health Records Upload and Sharing, Policy Servicing and Claim Settlement. Subsequently, each use-case is discussed in detail.

3.1 Identity Management

For any system to be used by the customers, it must have a mechanism to seamlessly on-board them. If we look at any ordinary system, the user signs-up using a unique user-name and password and further uses it to log into the system. As our system "LifeBlocks" uses the blockchain technology, the process of user on-boarding is quite different.

The users of our system are divided into three categories- customers, hospitals and insurance companies. The registration process for all the three categories of users is similar with only minor changes in the details to be provided at the time of registration. The registration process comprises of two steps:

1. *Creating an Ethereum Account*

   This step is same for all categories of user. To create an ethereum account, our system uses a browser extension called Metamask. The user needs to download the extension on their web-browser. After the Metamask extension is successfully installed, the user just needs to follow the steps directed by the Metamask to create an ethereum account. The users will be given a pass-phrase for the created account which they need to save or store it safely. This pass-phrase can be used to recover the ethereum account.

2. *Sign-up on the Portal*

   This step varies slightly for different users. For a customer, they need to provide their Aadhaar number and a One-Time-Password is sent to the customer's mobile number linked with their Aadhaar. If all details are valid, the customer is registered and can avail the services on our platform. For a hospital or an insurance company, they need to provide the Unique Identifier and the secret key provided to them by the government. The rest of the process is same as that of a customer. A mapping between the user's Aadhaar number and their ethereum address is made in the smart contract, when the registration process is completed successfully.

For all users, the process of registration also involves the generation of a PGP key-pair in which the private key is encrypted by the seed-phrase provided by the user in the registration form. This encrypted PGP key-pair is stored on the IPFS (Benet, 2014) and the subsequent IPFS address generated for the key-file is stored in the smart contract i.e. on the blockchain. This process is completely automated and the user need not worry about any of the related processes. They just need to remember the seed-phrase which is required to decrypt the PGP private key.

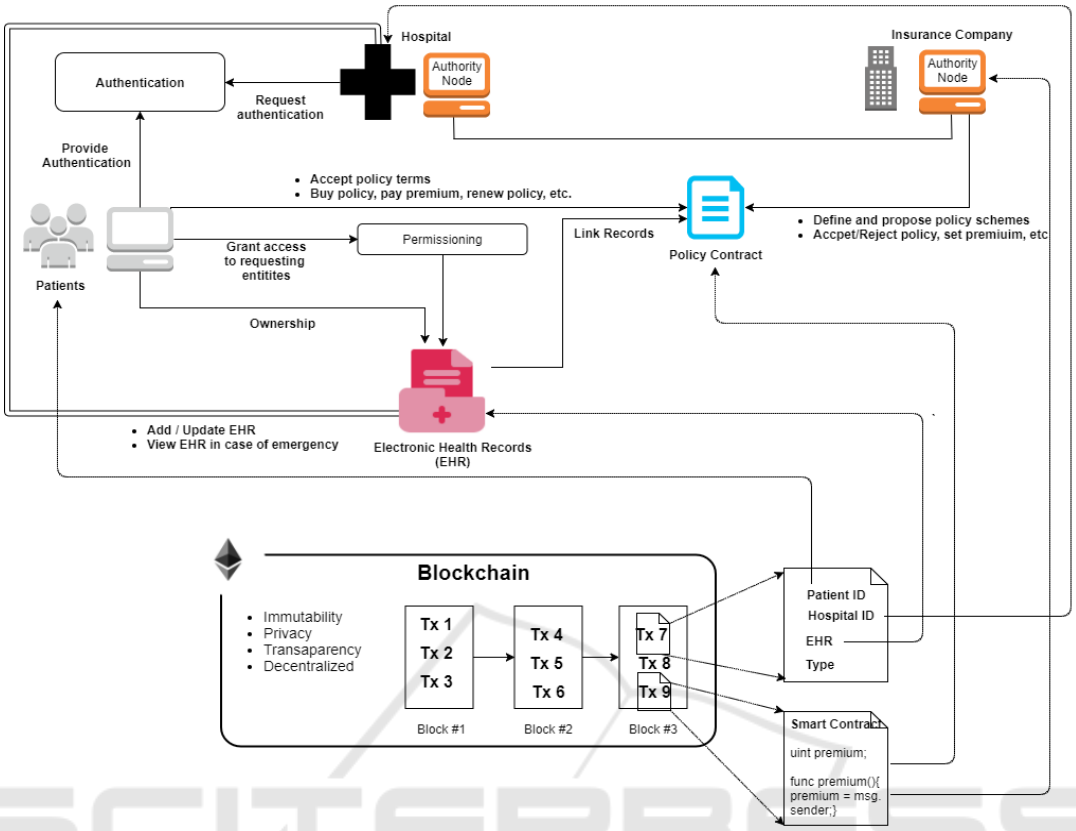

Figure 1: System Architecture.

Such an identity management system gives people the freedom to create self-sovereign and encrypted digital identities, hence replacing the need for creating multiple usernames and passwords.

3.2 Electronic Health Records Upload and Sharing

Today, there are inefficiencies in the management of health records. The patients have no control over their medical records. Since most of the medical records are paper-based, it's difficult for the patients to keep track of their medical history.
The following steps explain the process of medical record management i.e. record upload and sharing:

1. *Record Upload*
   This process begins when a customer/patient goes to a hospital. The medical records generated are uploaded by the hospital on a distributed file storage system built using InterPlanetary File System(IPFS) (Benet, 2014) and the hash-key of the address generated is stored in smart contract. The records are processed before being stored on IPFS. For each record a unique symmetric "master" key is generated using which the record is encrypted. This master key is encrypted with the user's PGP public key(generated at the time of registration). The encrypted record is stored on the IPFS. The generated hash-key of the record's IPFS address and the encrypted master key are stored in the smart contract along with the record's other details. Since the record's master key can only be decrypted with the patient's PGP private key, only patients have access to their medical records. The end users of the system i.e. patients and hospitals are abstracted from all the technical intricacies involved in the encryption and decryption process.
2. *Record Sharing*
   The customer securely shares the symmetric key of the record with the recipient(hospital/insurance company) of their choice. The record's symmetric key is first decrypted with the user's PGP private key. The decrypted symmetric key is then re-encrypted using the hospital's or insurance company's PGP public key. This newly encrypted symmetric key is stored in the smart contract. The recipient can view the user's medical record

by decrypting it with the symmetric key, which can be un-locked using their own PGP private key.

Our system manages the inefficiencies prevalent in the current system by cryptographically securing the medical records which gives users complete control over their records. These medical records are electronically stored on the blockchain allowing users to easily track their medical history and access them anytime and anywhere.

3.3 Policy Servicing

Policy Servicing includes applying for an insurance policy, paying premiums and handling the various stages of the insurance policy life-cycle. Initially, the insurance company deploys policy scheme contracts. The user can view all the different policy schemes deployed by various by multiple insurance companies. The user can apply for only one insurance policy at a time and a new smart contract is deployed for the same. This new smart contract stores necessary details like the buyer, seller and coverage information of the insurance policy. While applying, the customers have to share certain medical records with the insurance company. The insurance company can either accept or reject the application. If the application is accepted the state of the policy contract created remains as *APPLIED* else it is set to as *DEFUNCT*. If policy accepted and customer pays the premium the state of the policy is set to *ACTIVE*. Further, the state of the policy may change based on the duration of the policy. It may go in to *GRACE*, *LAPSE*, *INACTIVE* or in the *DEFUNCT* state.

3.4 Claim Settlement

This is the most important use-case of our system. The entire process of claim settlement is automated. In our system, in case of a claim-able event, for example an accident, the hospital uploads the medical bills and records tagged as claim-able. The smart contract checks if the patient has any health insurance policy or not. If yes, the uploaded bill and records are analyzed and checked against the conditions defined in the contract. Based on the analysis, the amount to be given to the patient against the health insurance policy is calculated. The amount is then automatically sent to the patient's ethereum account by the insurance company. All the above discussed processes are automated, saving precious time of all the involved parties.

4 TECHNOLOGIES USED

4.1 Ethereum

Ethereum (Buterin, 2013)(BLO, reum) is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications. It is basically a peer-to-peer network of virtual machines that any developer can use to run distributed applications(DAPPs). These computer programs could be anything, but the network is optimized to carry out rules that mechanically execute when certain conditions are met, like a contract. Ethereum uses its own decentralized public blockchain to cryptographically store, execute, and protect these contracts.

4.2 Parity

It is an open-source software for building the decentralized Web. Parity develops cutting-edge blockchain technologies to foster innovations. Parity Ethereum provides the core infrastructure essential for the speedy and reliable services. It uses Proof of Authority consensus protocol. It provides clean, modular code base for easy customization along with minimal memory and storage footprint. The decision to use Parity was due to it's use of the Proof of Authority consensus mechanism that allows only one node to verify a particular transaction and other just validate it. This would provide a more close and controlled system but one with a much faster transaction rate.

4.3 Inter-Planetary File System (IPFS)

InterPlanetary File System (Benet, 2014) (IPFS) is a protocol and network designed to create a content-addressable, peer-to-peer method of storing and sharing hypermedia in a distributed file system. In other words, IPFS is a distributed file system that seeks to connect all computing devices with the same system of files. In a way, this is similar to the original aim of the Web, but IPFS is actually more similar to a single BitTorrent swarm exchanging git objects. Instead of referring to objects (pics, articles, videos) by which server they are stored on, IPFS refers to everything by the hash on the file. The idea is while retrieving a file, IPFS will ask the entire network about that particular file which corresponds to that particular hash and a node on IPFS that does can return the file allowing you to access it. The mechanism is to take a file, hash it cryptographically so it ends up with a very small and secure representation of the file which en-

sures that someone can not just come up with another file that has the same hash.

IPFS is the perfect distributed file storage solution as it meshes in seamlessly with the Blockchain architecture. Through it's decentralized architecture and built-in data redundancy, IPFS ensures fault-tolerance and low-cost file distribution. The immutable nature of data on IPFS is necessary when dealing with sensitive documents like medical and insurance records.

4.4 Smart Contracts

Smart contracts (Buterin, 2013)(Waltl et al., 2019) are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism. They render transactions traceable, transparent, and irreversible.

5 CONCLUSION/FUTURE WORK

The paper proposes a blockchain based model for implementing a complete insurance process - from buying an insurance policy to settling claims. The medical records are securely stored with an access-based mechanism that ensures privacy and gives the record-owner complete control over their medical records. This approach ensures that none of the records, be it medical or insurance, are lost or tampered with, maintaining integrity in the system. Having insurance policies as smart contracts that can trigger payouts based on pre-defined parameters would help facilitate faster claim settlement, thus building a more customer-centric ecosystem. This model not only benefits customers but also the insurance companies by allowing them to directly market and sell insurance policies as smart contracts, thereby reducing operational costs of the company by cutting down on the middlemen involved in the current system.

Complex policy conditions, like intricacies of diseases covered, when introduced in our proposed system might lead to complications at the time of settling claims, thereby delaying the process. In order to support fully automated claim settlements in the future, a more robust system design with deeper domain knowledge is required. Running computational analysis on a blockchain ledger is a strenuous task due to scalability and data retrieval problems in the current Blockchain ecosystem. As the Blockchain community continually looks to address these issues, the system would then allow governments to detect and predict disease patterns and help pharmacies in medical inventory management.

REFERENCES

(https://blockgeeks.com/guides/ethereum/).

Anita, J. (2008). *Emerging Health Insurance in India – An overview*. 10th Global Conference of Actuaries.

Benet, J. (2014). *IPFS - Content Addressed, Versioned, P2P File System*.

Buterin, V. (2013). *A Next-Generation Smart Contract and Decentralized Application Platform*.

Majumdar, A., Chatterjee, S., Gupta, R., and Rawat, C. S. (2019). *Competing in a new age of insurance: How India is adopting emerging technologies*. PwC.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Raikwar, M., Mazumdar, S., Ruj, S., Gupta, S. S., Chattopadhyay, A., and Lam, K.-Y. (2018). *A Blockchain Framework for Insurance Processes*. 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS).

Waltl, B., Sillaber, C., Gallersdörfer, U., and Matthes, F. (2019). *Blockchains and Smart Contracts: A Threat for the Legal Industry?* Business Transformation through Blockchain, Cham: Springer International Publishing, pp. 287-15.