INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD ISSN: 2455-0620 Volume - 6, Issue - 5, May – 2020
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value: 86.87 Impact Factor: 6.497
Received Date: 07/05/2020 Acceptance Date: 20/05/2020 Publication Date: 31/05/2020

Life Insurance and Death Claim Management leveraging Blockchain

[1]Hazim Shaikh, [2]Omkar Dhamdhere, [3]Rahul Bhole
[1]Student, [2]Student, [3]Asst.Professor
[1, 2, 3] Information Technology Department,
[1, 2, 3]Zeal College of Engineering and Research, Pune, India
Email - [1]hazim.shaikh2919@gmail.com, [2]odhamdhere@gmail.com, [3]rahul.bhole@zealeducation.com

Abstract: *The insurance sector is heavily dependent on multiple processes for transacting parties for beginning, preserving and closing diverse kinds of policies. The major concerns are the time required and security of transaction processing and payment settlement. Blockchain innovation which was initially created as an unchanging dispersed record for recognizing twofold spending of cryptographic forms of money is presently progressively utilized in various FinTech (Financial Technology) frameworks to attempt profitability and security necessities. The application of Blockchain in FinTech processing requires a profound understanding of the basic mechanisms of industry. Smart contracts help us in automating the interactions between the Blockchain system and the traditional transaction system. In this paper, we are focusing on designing an effective method to use Blockchain enabled platform for transactions of insurance sector. We will discuss the primary design necessities, design suggestions and convert different insurance related processes into smart contracts. In order to evaluate the performance of our system and the security of the proposed design, comprehensive experiments are performed.*

Key Words: *Blockchain framework, smart contracts and transaction processing.*

1. INTRODUCTION:

Blockchain technology offers a unique way to build secure distributed systems. At first planned as a framework administration to identify twofold use on digital currency frameworks, blockchain is broadly Pertinent to numerous business applications where certainty is required among disseminated parties. At a high level, a blockchain is a distributed ledger system carried out by several users, each of whom stores a local copy of the ledger. Certain consensus protocols involving all participants achieve consistency of the ledger. Depending on the trust model, blockchain systems can choose from a wide range of consensus protocols. A combination of cryptographic primitives and a clear distribution of the ledger ensure that the ledger is immutable. The main purpose of the blockchain-based insurance industry solution is: (a) automating the insurance processes like customer authentication to claim settlement, (b) facilitating fraud prevention and detection using distributed and decentralized repositories , (c) making client data secure and accessible to authorized parties only, and (d) allowing regulators and auditors to detect suspicious patterns of transaction and market behaviour.

2. LITERATURE REVIEW:

Marko Vukolic [1] et.al state that current blockchain stages, particularly the ongoing permissioned frameworks, have structural confinements: brilliant contracts run successively, all hub executes every single shrewd contract, accord conventions are hard-coded, the trust model is static what's more, not adaptable, and non-determinism in shrewd agreement execution presents difficult issues. Defeating these confinements is basic for refining both valuable properties of blockchains, for example, classification and consistency, also as their non-useful properties, for example, execution and adaptability. We talk about how these constraints work with the early blockchain platform which were similar to the Hyperledger fabric blockchain framework and how a restructure and engineering of the Hyperledger fabric would impact these constraints and the framework as a whole.

C.D.Clack [2] et.al introducing advanced Contract Templates support lawfully enforceable keen agreements, utilizing operational parameters to associate legitimate understandings to institutionalized code. In this paper, we investigate the structure scene of potential arrangements for capacity and transmission of keen legitimate understandings. We distinguish fundamental prerequisites and portray various key plan choices, from which we visualize future advancement of institutionalized organizations for defining and controlling brilliant legitimate understandings. This gives a fundamental advance towards supporting industry selection of lawfully enforceable brilliant agreements.

K. Christidis and M. Devetsikiotis[3] proposed that inspired by the ongoing hype around blockchains, we speculate whether it can give go toe to toe with Internet Of Things (IOT). Blockchains enable to establish communication between different individuals who don’t trust each other. We log how blockchain works and investigate astute arguments like the computerization of forms and the contents of the blockchain. We move into how IOT and blockchain work together: 1) Encourages a division of administrations and resources encouraging the development of a business management center between gadgets and 2) helps us to robotize a few real, repetitive work processes cryptographically and unequivocally. In addition, we posed other matters which should be taken into account prior to sending a blockchain in an IOT setting: from quality security to the usual evaluation of the system-swapped digital resources. We make arrangements and workarounds in every relevant place. Our conclusion is that the combination of blockchain and IOT is revolutionary and in addition will open up new opportunities to enhance for future projects in the area of distributed blockchain.

Indranil Nath [4] states that receiving a typical Blockchain could make a step change in claims taking care of being progressively effective and streamlined, bringing about an improved client experience. Such a methodology could likewise lessen further, if not so much counteract, extortion if character the board was likewise authorized on the Blockchain – implying that culprits could never again crash for money, or abuse the present difficulties of sharing information except if their techniques for clouding personalities turned out to be essentially increasingly refined despite the fact that many may be doubtful that anybody will give a decentralized power a chance to oversee characters, Fraught with hazard. A typical case dealing with stage would in any case make it workable for person guarantors to go after clients, offering a scope of items and costs by ethicalness of the savvy contracts they set up. In addition, a Blockchain could permit the business overall to streamline its handling and offer a superior client experience for clients who need to make a case. At the same time, putting away claims and client data on a Blockchain would chop down false action – it would unquestionably make it a lot harder for crooks to endeavour to guarantee more than once, if not veil their personalities. For sure, in numerous regards, with ventures like the IFB now since quite a while ago settled, the general protection industry faces a littler social and hierarchical slope to climb than does banking and different areas.

Wenting Li et.al [5] introducing the blockchain rises as a creative apparatus that has the potential to emphatically affect the manner in which we plan a number of online applications today. From multiple points of view, the blockchain innovation is, be that as it may, at present not develop enough to cook for mechanical models. In particular, existing Byzantine tolerant consent based blockchain organizations can just scale to a predetermined number of hubs. These frameworks commonly require that all exchanges (and their request for execution) are freely accessible to all hubs in the framework, which comes at chances with regular information sharing practices in the business, Furthermore, keeps an incorporated controller from administering the full blockchain Framework. In this system, we propose novel blockchain engineering formulated explicitly to satisfy modern guidelines. Our proposition use the idea of satellite chains that can secretly run diverse accord conventions in parallel—along these lines extensively boosting the versatility premises of the framework. Our answer likewise represents a "hands-off" controller that administers the whole system, upholds explicit arrangements by methods for keen agreements.

H. Watanabe et.al [6] proposed another instrument for verifying a blockchain applied to contracts the board. A major issue in contracts the board is that breakdown in coin costs will not fill in as discouragement against assaults when utilizing the proof of-stake strategy. To settle this, we devised another consensus technique using a rating of legitimacy and depicted a half blockchain created by using this new strategy and verifying the stake. We additionally demonstrated an assault on the half and half blockchain and uncovered the likelihood of its being finished. Subjects for our future work incorporate explaining the system so as to execute it on a real cryptographic money.

F. Lamberti et.al [7] introducing blockchain is an intriguing issue and has been considered by media as a leap forward innovation. In this system, we gave some specialized foundation to see how this innovation functions, and underlined its focal points/weaknesses by additionally exhibiting a survey of potential applications. Specifically, we took the perspective of an expert researching whether blockchain could be worth of venture, and centred the field of research to protection, an area where blockchain could either establish the frameworks for new procedures/benefits or speak to a danger, due to its ability to expel (existing) go-betweens. We broke down conceivable use cases and responded to key inquiries to recognize whether a blockchain is as a matter of fact required or in the case of existing advances will get the job done. Subsequently, we discovered a few territories where blockchain could bring immense advantages, changing additionally the manner in which procedures are actualized, also, others where advantages could be less troublesome or where practically identical results could be accomplished additionally with conventional frameworks.

Christian Cachin [8] proposed that A blockchain is best understood in the state machine model, where the operator maintains certain conditions and customers carry out certain activities that alter the state and generate returns. A blockchain copies a ' trustful ' storage administration via a suitable convention managed by Internet-associated hubs. The administration speaks to or makes an advantage, where all hubs have some stake. The hubs share the common purpose of handling the administration, but do not trust each other more. In a "permission less" blockchain, for example, the one fundamental the Bitcoin cryptographic money, anybody can work a hub and take an interest through spending CPU cycles.

L. S. Sankar et.al [9] states that Blockchain is an immutable, open and distributed file. The foundation of the blockchain is the Consensus protocol. They determine how a blockchain works. With new conceivable findings in blockchain technology, scientists are quick to find an improved Byzantine Convention on accommodating agreements. Making a worldwide accord convention or fitting a cross-stage attachment and play programming application for execution of different agreement conventions are thoughts of tremendous intrigue. Excellent Consensus Protocol (SCP) is viewed as a worldwide agreement convention and vows to be Byzantine Fault Tolerant (BFT) by carrying with it the idea of majority cuts and united byzantine adaptation to non-critical failure. This current agreement's working and its examination with different conventions that were prior proposed are broke down here. In addition, Hyperledger is an open-source venture of the Linux Foundation that includes updating the idea of earth-to-earth Byzantine adaptation to internal failure and also a stage where different agreement conventions and blockchain applications can be sent in a fitting and play way. This paper focuses on the dissection of these previously proposed agreements and their achievability and ability to fulfil the criteria they propose.

H. Sukhwani, et.al [10] states that while blockchain arrange brings huge advantages, there are fears whether their presentation would coordinate up with the standard IT frameworks. This system expects to explore whether the agreement procedure utilizing Practical Byzantine Fault Tolerance (PBFT) could be an exhibition bottleneck for systems with an enormous number of friends. We model the PBFT agreement process utilizing Stochastic Reward Nets (SRN) to figure the interim to finish agreement for systems up to 100 companions. We make a blockchain arrange utilizing IBM Bluemix administration, running a generation grade IoT application and utilize the information to parameterize and approve our models. We too direct affectability examination over an assortment of framework parameters furthermore, look at the presentation of bigger systems.

3. METHOD:

Our model proposes using blockchain based distributed platform for insurance processes, we propose to use smart contracts for transaction processing and storing of the results. The proposal for an insurance usage blockchain scheme provides for a thin grain inspection by showing the distinctive arrangement between supporters in each brilliant agreement. To imitate the current insurance policies which require multiple set of endorsers, we will be creating a different set of Smart contracts for every policy provided by the firm. We will be using hyper ledger fabric to implement our blockchain based insurance management framework. Considerable amount of experiments will be conducted on the system with different set of parameters to check the efficiency of the system while extensively scaling the system to measure its robustness. We will also test the relation between system dormancy or idleness with the system size and structure

3.1. Entities in the model:

Primary entities in the model are – the Client, who is being covered by an insurance policies or requests claim settlement or is the benefactor of policy funds, and the vendor, who is responsible for communicating with the blockchain framework for client requests and authentication. A vendor can handle multiple clients

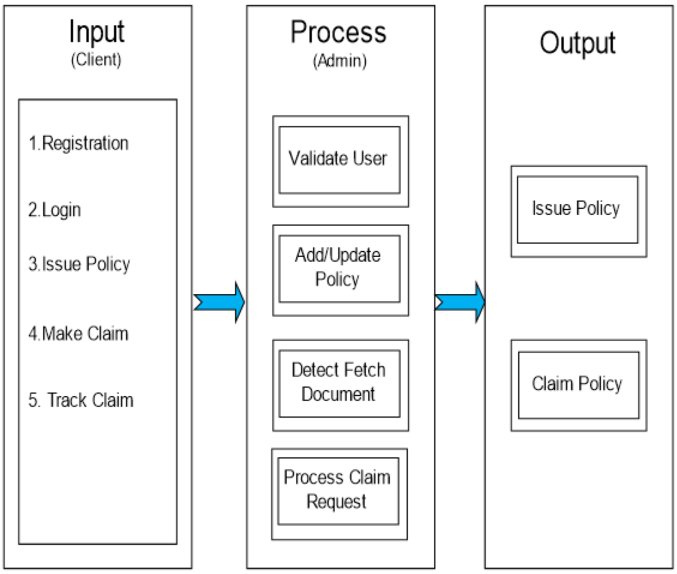


Figure 1. System Flow

4. ALGORITHM:

4.1 Hashing Algorithm:

A hashing algorithm is a cryptographic hash function. It is a mathematical algorithm that maps data of arbitrary size to a hash of a fixed size. It's designed to be a one-way function, infeasible to invert. However, in recent years several hashing algorithms have been compromised. This happened to MD5, for example — a widely known hash function designed to be a cryptographic hash function, which is now so easy to reverse — that we could only use for verifying data against unintentional corruption. It's easy to figure out what the ideal cryptographic hash function should be like:

- It should be fast to compute the hash value for any kind of data;
- It should be impossible to regenerate a message from its hash value (brute force attack as the only option);
- It should avoid hash collisions; each message has its own hash;
- Every change to a message, even the smallest one, should change the hash value completely. It's called the avalanche effect.

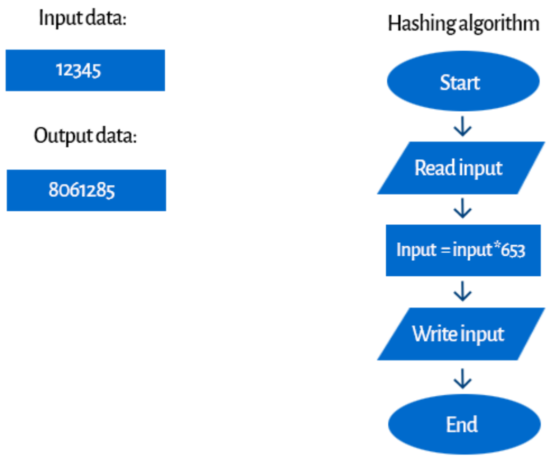


Figure 2. Hashing Algorithm

4.2 BlockChain

Let's study the Blockchain architecture by understanding its various components:

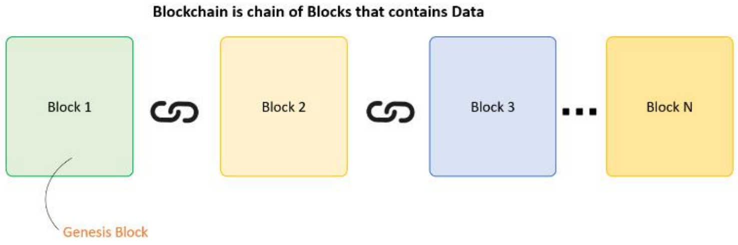


Figure 3. BlockChain

What is a Blockchain?

A BlockChain is a chain of blocks which contain information. The data which is stored inside a block depends on the type of blockchain. For Example, A Bitcoin Block contains information about the Sender, Receiver, and number of bitcoins to be transferred. The first block in the chain is called the Genesis block. Each new block in the chain is linked to the previous block.

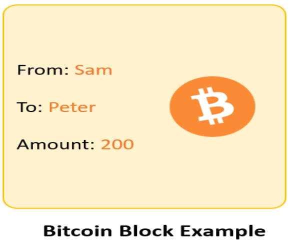


Figure 4. Bitcoin Example

Understanding SHA256 – Hash

A block also has a hash. A can be understood as a fingerprint which is unique to each block. It identifies a block and all of its contents, and it's always unique, just like a fingerprint. So once a block is created, any change inside the block will cause the hash to change.

Therefore, the hash is very useful when you want to detect changes to intersections. If the fingerprint of a block changes, it does not remain the same block.

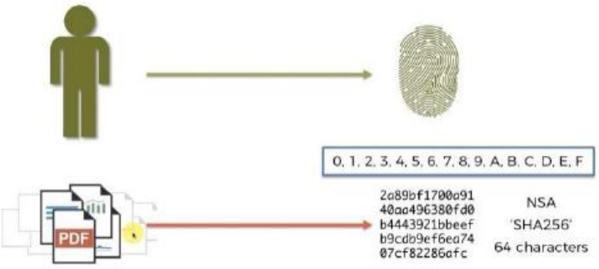


Fig. 4.2.3. SHA256

Each Block has

- Data
- Hash
- Hash of the previous block

Consider following example, where we have a chain of 3 blocks. The 1st block has no predecessor. Hence, it does not contain has the previous block. Block 2 contains a hash of block 1. While block 3 contains Hash of block 2.

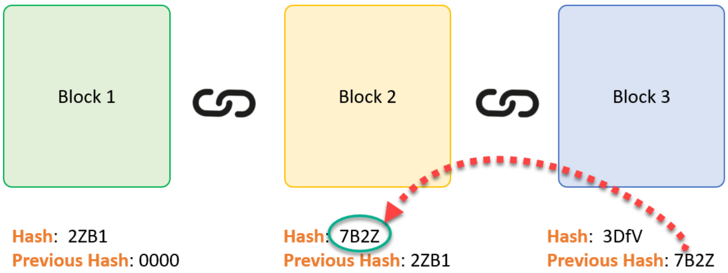


Fig. 4.2.4. Hash Check

Hence, all blocks are containing hashes of previous blocks. This is the technique that makes a blockchain so secure. Let's see how it works -

Assume an attacker is able to change the data present in the Block 2. Correspondingly, the Hash of the Block also changes. But, Block 3 still contains the old Hash of the Block 2. This makes Block 3, and all succeeding blocks invalid as they do not have correct hash the previous block.

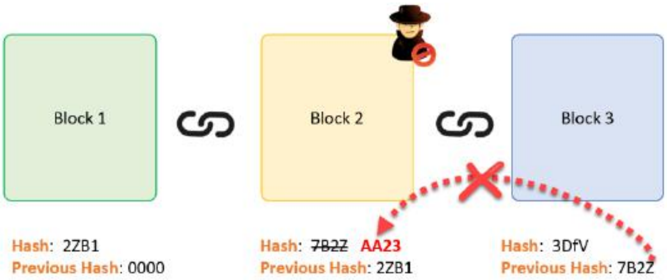


Fig. 4.2.5. Tampered Hash Detection

Therefore, changing a single block can quickly make all following blocks invalid.

4.3 Proof of Work

Hashes are an excellent mechanism to prevent tempering but computers these days are high-speed and can calculate hundreds of thousands of hashes per second. In a matter of few minutes, an attacker can tamper with a block, and then recalculate all the hashes of other blocks to make the blockchain valid again.

To avoid the issue, blockchain uses the concept of Proof-of-Work. It is a mechanism which slows down the creation of the new blocks.

A proof-of-work is a computational problem that takes certain to effort to solve. But the time required to verify the results of the computational problem is very less compared to the effort it takes to solve the computational problem itself.

In case of Bitcoin, it takes almost 10 minutes to calculate the required proof-of-work to add a new block to the chain. Considering our example, if a hacker wants to change data in Block 2, he would need to perform proof of work (which would take 10 minutes) and only then make changes in Block 3 and all the succeeding blocks.

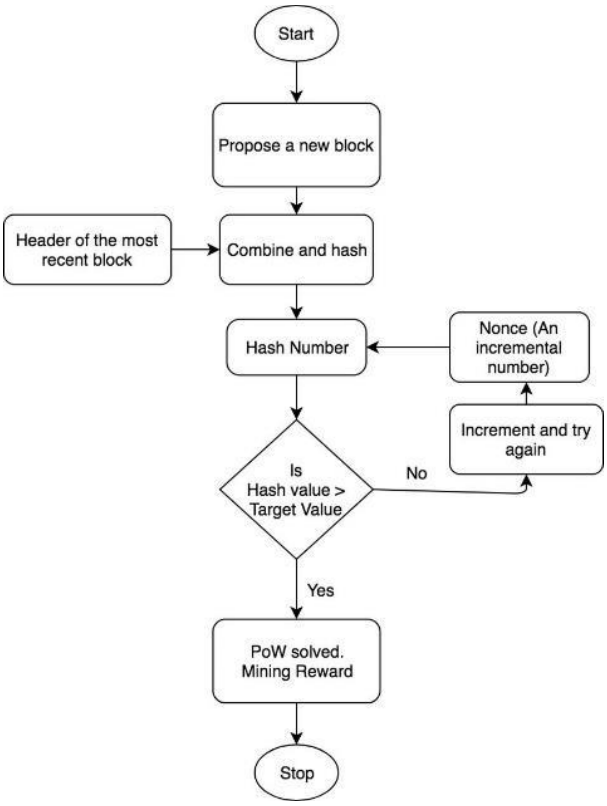
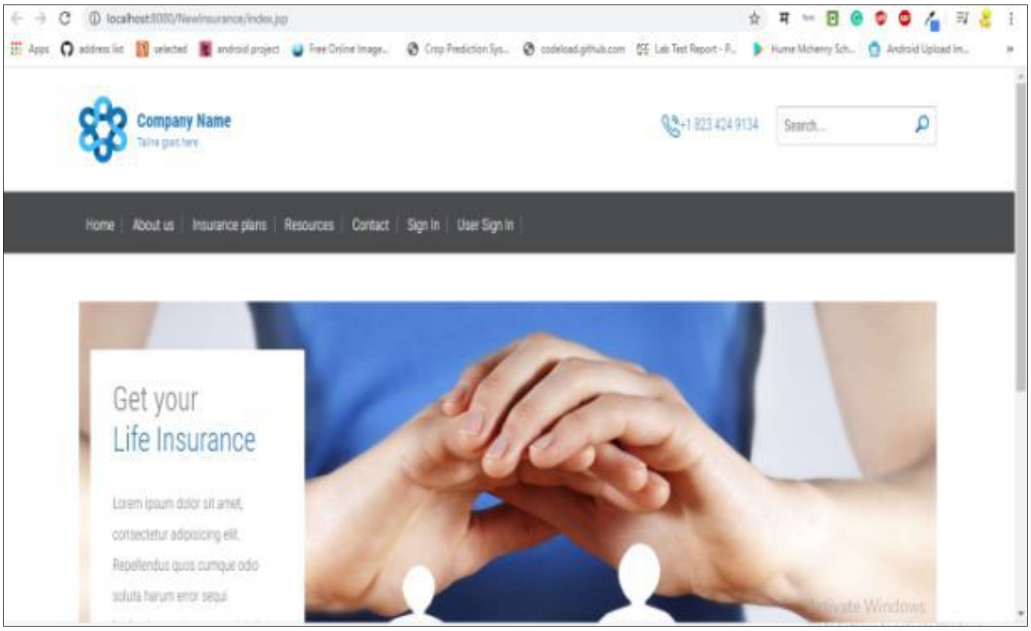

Start
Propose a new block
Header of the most recent block
Combine and hash
Hash Number
Nonce (An incremental number)
Increment and try again
Is Hash value > Target Value
No
Yes
PoW solved. Mining Reward
Stop

Fig 4.3. Proof of Work Block diagram

5. RESULT:

In our System we have handled health insurance using Blockchain and result is given below.

Screenshots:



Get your
Life Insurance

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Repellendus quos cumque odio soluta harum error sequi

Fig. Home Screen

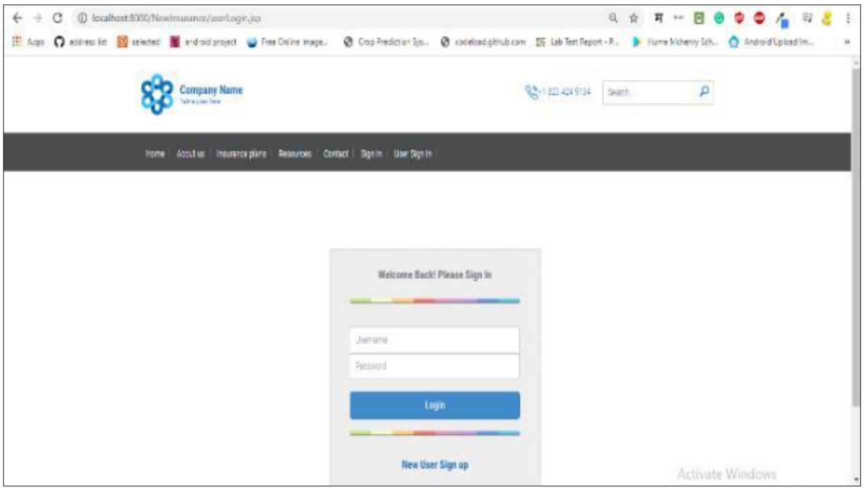

Company Name
Home | About us | Insurance plans | Resources | Contact | Sign in | User Sign In
Welcome Back! Please Sign In
Username
Password
Login
New User Sign up

Fig. User Login Screen

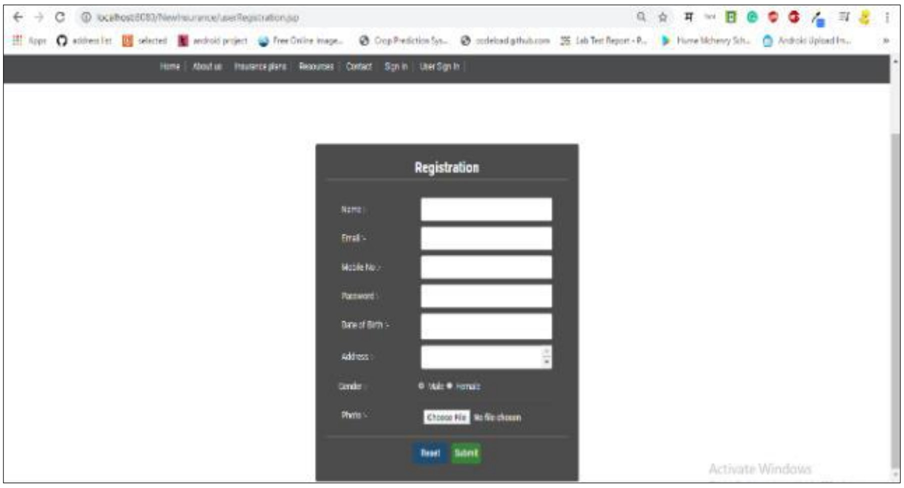


Fig. User Register Screen

6. CONCLUSION:

Our model proposes using blockchain based distributed platform for insurance processes, we propose to use smart contracts for transaction processing. Experiments will be conducted on the system with different set of parameters to check the efficiency of the system and the network latency while extensively scaling the system to measure its robustness. The database though not encrypted currently, can be encrypted on multiple level to get finer control on the database processes. Smart contract has its own array of supportive partners in our proposed model and can be extended even to the transaction level so that we can assign individual endorsement partners to each transaction.

ACKNOWLEDGEMENT:

This paper has been worked as a paper on Blockchain and smart contracts. The authors would like to thank the faculty members of college for their constructive criticism and detailed comments.

REFERENCES:

Journal Papers:

1. Marko Vukolic, “Rethinking permissioned blockchains,” in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, ser. BCC ’17. New York, NY, USA: ACM, 2017.
2. C. D. Clack, V. A. Bakshi, and L. Braine, “Smart contract templates: essential requirements and design options,” arXiv preprint arXiv: 1612.04496, 2016.
3. K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.

4. Indranil Nath, “Data exchange platform to fight insurance fraud on blockchain,” in 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW), Dec 2016, pp. 821–825.
5. Christian Cachin, “Architecture of the hyperledger blockchain fabric,” IBM Research - Zurich CH-8803 Ruschlikon, Switzerland 2016.
6. H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, “Blockchain contract: Securing a blockchain applied to smart contracts,” in Consumer Electronics (ICCE), 2016 IEEE International Conference on. IEEE, 2016, pp. 467–468.
7. 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 Professional, vol. PP, no. 99, pp. 1–1, 2017.
8. Christian Cachin, “Architecture of the hyperledger blockchain fabric,” IBM Research - Zurich CH-8803 Ruschlikon, Switzerland 2016.
9. L. S. Sankar, M. Sindhu, and M. Sethumadhavan, “Survey of consensus protocols on blockchain applications,” in 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Jan 2017, pp. 1–5.
10. H. Sukhwani, J. M. Martnez, X. Chang, K. S. Trivedi, and A. Rindos, “Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric),” in 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), Sept 2017, pp. 253–255.
11. O. Dhamdhere, H. Shaikh, “Survey paper on life insurance and death claim settlement using blockchain,” in 2019 journal of the gujarat research society, vol 21 no. 16,2019.