A Self-Governing Based Group Life Insurance with Blockchain technology based on Decentralized Finance

Indradhar Paka
1800315C203

Sai Venkat Lakamsani
1800254C203

Kosana Sai Venkata Pavan Kumar
1800230C203

Bollavaram GollaRiteesh Ram Chander
1800206C203

Abstract

The inability of humans to control his surroundings and dependency on others, increases the chance of getting effected. So, Insurance came into existence as a financial support to effected houses, crops, vehicles, and life. A centralized Institute serving the insured is a conventional way of insurance body. But inefficiencies exist as assessment of risk, determining premium, assessment of damage and offering payments is completely controlled centrally. So, a decentralized model involving blockchain which can replace the inefficiencies of centralized institute is proposed and discussed in this paper. This paper will discuss a new way of implementing group life insurance, where group of individuals who are inclined to get insured will build a group of organization and pay their insurance premium to acquire his/her life insured. This corresponding insurance would be claimed by the nominee after successfully validated by Decentralized Autonomous Organization (DAO).

Keywords: Blockchain, Truffle, Ganache, Node, Digital Wallet, Solidity, Decentralized Application

1. Introduction

Human is a social animal, dependent on others in most of the things in daily life. Not only this trust but also his incapability of control over surroundings, increased chance of risk. These unfortunate events sometimes lead to disastrous situations. So, one of the ways to get relief after these incidents could be Insurance. Insurance is offered against damage to one's life, health, house, crops, vehicles etc. in natural calamities, accidents, etc. [1]. Initially, Insurance is provided by centralized institutes working with similar principle as of banks. The centralized institute pools the money collected from insured as premium amounts. This pooled amount is granted to those who bear a financial cost based on the particular risk [2]. The centralized body governing is solely responsible for all transactions like premium payments, pooling of premiums, claims and validation of claims. The control over pooled money centrally in traditional insurance is vulnerable because of single point of control, payout, and failure. Excess charge in premium for employee wages and administrative costs, strategic investments of the funds received as premiums to increase wealth are the few drawbacks of traditional centralized insurance [3]. In the decentralized insurance, the centralized body can be replaced with an efficient, effective, and transparent protocols. So, a blockchain based decentralized insurance could handle the inefficiencies of a centralized organization [4]. The interested people form together a blockchain, a decentralized insurance organization. For every transaction, a new block is added making the transaction immutable. Even though insurance policies and claim procedures are decided by the few individuals and transformed in the form of smart contracts and protocols but during claim, each insurer who is a part of blockchain gets involved in the verification of claims. Typically, the most common DEFI insurances are insuring transactions in blockchain, against the smart contract breaches, crypto wallets etc. [5].

One of the most common options available in policies with a considerable savings component is the possibility to exit (surrender) the contract before maturity and to receive a lump sum (surrender value) reflecting the insured's past contributions to the policy, minus any costs incurred by the company and possibly some charges [6]. The difficulty with insurance contracts is that realistic models pose formidable computational tasks for two main reasons. First, insurance contracts are usually very long term and offer great flexibility in early termination of the contract, meaning that we are faced with multiple exercise dates. Second, a realistic model should consider at least the key drivers of rational surrender decisions, which in the equity-linked case may be quite involved. Incorporating irrational or exogenous factors as well as parameter uncertainty would make the task even more daunting [7].

One can consider blockchain to reward users for their local updates proportional to how many local data points are used. The payment to devices is left to the miner to pay" out-of-pocket", which is not a lasting solution

if miners pay devices more than they are rewarded for blocks. This device reward benefits an honest node; however, this value may be inflated by a malicious node seeking higher reward [8]. And can award incentive considering blockchain mechanism to reward honest participants and penalize dishonest participants. The block wise-BA consensus protocol proposed relies on cryptographically selecting a worker to create a block which is validated by a committee; this method relies on choosing an honest committee, and for the random algorithm to be negligibly close to perfectly random, both issues which may not be true in practice [9]. Also, one can implement Ethereum blockchain of machine learning to reward users for producing trained models for organizers. Given an organizer's published dataset and evaluation function, users compete to produce the first or the best training model that maximizes this evaluation function. One large problem that arises with this system is that all model evaluations are done on the blockchain which yields large gas costs; many users must each pay gas for their models to be evaluated, however only one or two users are paid out. Users needing to pay large gas prices in addition to effort and time into building and training a machine learning [10].

This paper proposes a blockchain based system for providing life insurance to group of people where the members of the group are insured on life by paying premium. Typically, group insurance is opted by a company for all its employees, family for all its members. Here the risk is shared among the members in the group, so the premium amount is reduced compared to the premium if insurance is opted personally [11].

An organization for its employees, family for its members or Close friends would form as a group together by sharing the risk. The members in the group pay their part so to get insured. A model is proposed in this paper, where the group size can be anything more than one. During the payment of premium, nominee details will be requested. All the premium amounts collected from each group are pooled together called Liquidity pool. All the insured in the group are equally righted policy holders but the group head has an additional right as he could apply for the claim on behalf of the members in the group. So, the group head and the nominee of the insured can apply for the claim if life of insured get effected. Whenever an insured appeal for claim, the validation is done in two phases. In first phase of validation, the user uploads all the necessary documents and related images for claim. The peers across the platform irrespective of their group in the blockchain, can vote whether the claim is valid or not. Based on the claim's validity check in the initial phase, the second phase is commenced with DAO's assessors checking the claims validity by reaching the affected insured or nominee physically. Hence the insured could get the claim amount of insured policy if the claim gets validated successfully.

Remaining sections of the paper are organized as follows: Section 2 presents the related literature work and section 4 presents the methodology adopted in this study. Remaining sections of the paper is organized as follows: section 2 presents the related literature work; section 3 presents the proposed system. Section 4 discusses the results of different methodologies for DeFi. Finally, section 5 discusses the conclusion remark and presents the future work

2. Related work

In [12], authors have modelled the blockchain based smart contracts in Insurance sector. In this article the author discussed about the design and working of Etherisc live application. Here Etherisc is a protocol which was used to build smart contracts using Dapps for insurance products. Basically, from the smart contract-based infrastructures Etherisc would be standardizing the syntax for creating insurance products. Also, the third-party data sources would be triggering the smart contracts via APIs like Oracles. Etherisc uses smart contracts to encode the entire insurance workflow like policy pricing, issuance, claims and settlements. According to the author findings some of the Etherisc products are like Social Insurance, Hurricane Guard, Crop Insurance, Flight Delay and Collateral Protection. For the above-mentioned products, each one uses smart contracts which was backed by Etherisc protocol, Ethereum blockchain and third-party APIs to trigger, modify, price, and underwrite the pay-outs. The further understandings of Etherisc protocol were mentioned in the article.

In [13], authors have integrated blockchain technology in the IOT based Insurance. IOT lacks on addressing scalability, privacy, security, and trust management. In case of health insurance in the traditional way or in with centralized platform the patient never knows how much amount paid by the insurance company and date and time of released, Communication is between more than two parties, there is no thrust between the users. So, to overcome these issues author used blockchain technology in it. So here each member of the system will be connected to the blockchain. In that Blockchain network a smart contract was written on the insurance claim and if the condition matches then the related event would be triggered. In the Ethereum platform there are nodes like patient, insurance and the hospital, the smart contract for each of those entities was defined and deployed. Now every transaction would be recorded using the blockchain and that would be shared among all the users, therefore that would be trustworthy.

In [14], authors have introduced UBI (Usage Based Insurance) for vehicles, this scheme calculates insurance premium based on how vehicles are driven. Here UBI uses sensitive driving data to calculate insurance premium but this UBI scheme was decentralized and preserves privacy of user's data. Here the smart contracts serve as insurance company and the drivers would uploading driving data to the blockchain. Also, drivers would be submitting accumulated driving statistics with zero knowledge proof to the smart contract and this proof will be verified and based on that insurance premium will be calculated. In this insurance system three entities were involved like vehicle, blockchain and cloud. In case of vehicle firstly it should be registered in Decentralized UBI(DUBI) and it will be equipped with On-Board Diagnostics device and trip computer, here OBD device will be providing real-time driving data and trip computer process driving data to calculate insurance premium and submits it to the cloud. In case of it could act like an extension of blockchain, it organizes driving data as a Merkle tree the leaf of the Merkle tree corresponds to each data commitment. Here after getting the Merkle root, they could send, it to the blockchain to maintain immutability and integrity. Finally, blockchain which runs smart contracts in DUBI framework, this blockchain is public so there are miners validating to generate a block with consensus algorithm like PoW or PBFT. Moreover, the vehicle will be interacting with the smart contract for registration, premium calculation, and payment. Coming to the security part the author used encryption or zero-knowledge proof techniques to protect the driving data in the cloud storage. Also, to reduce the premium cost the driver may wantedly send forged driving data to the cloud so to overcome this fraud insurance author defined an ideal program called Ideal-DBUI. The further details of the Ideal-DBUI were there in the paper in detail.

In [15], authors have implemented smart contract based on Ethereum blockchain for insurance services. Here in this paper ERC20 standard for the smart contract was implemented, he also created a web interface to sale those tokens. Here firstly Info of loss would be directly sent to the automated claim processing application from the insure. Now with the ensure information the smart contract will be processing their respective business logic; smart contracts will also use additional sources like reports and statistics to calculate loss. Finally, if the claim was approved then the smart contract initiates payment to the insure. Here author used private blockchain to operate backend operations and public blockchain to make automatic payments with existing crypto currencies.

In [16], authors seeked to fill the gap between stable coin design and focused on financial risk as well. Discussed about custodial stable coins (fiat currencies, bonds, or commodities) and non-custodial stable coins (independent of the societal institutions). Basic terminology of non-custodial stable coins (Risk absorbers, stable coin holders, issuance, governance etc.). It discussed the models of non-custodial coins like the Capital structure model (trade-off between debt and equity. Depending on the expectations of agents, they will choose to execute certain actions in the next round), forking model (explore how multiple rounds of agent decisions can affect stability and security of stable coin systems) and dynamic model (time-based pricing, in which businesses set flexible prices for products or services based on current market demands). These models consider attack vectors including governance, data feeds, miners, and deleveraging market feedback effects.

In [17], author analyses the risk involved in the decentralized lending and borrowing. It mainly focusses on the risk associated as the liquidity is less. SAI market was analyzed, and several periods were found which are illiquidity. These were mainly those instances, when more loans were taken in short period of time or lenders withdrawing their share from lending pool. It was shown that, on five occasions, a single transaction was sufficient to change the liquidity over one quarter and in the worst-case single transaction led to change in 95% of available liquidity.

3. Proposed System

This paper is mainly focusing on group insurance. For developing a decentralized application using decentralized finance-based insurance system. We have used ganache for private blockchain, truffle for deploying the smart contracts into the blockchain, metamask digital wallet for connecting the decentralized application with the blockchain. Given in Fig. 1, which illustrates the workflow of the components used in the proposed system.

Fig. 1. Components and technologies used in the proposed system

4. Methodology

The Decentralized application for the proposed system consists of three functions: Enrolling a group, joining a group, Claiming the insurance. As we all know that blockchain is immutable and the blocks created in the blockchain are neither modified nor deleted. With the invention of Bitcoin in 2008, the world was introduced to a new concept, which is now likely to revolutionize the whole of society. It is something that promises to have an impact on every industry, including but not limited to the financial sector, government, media, law, and arts. Some describe blockchain as a revolution, whereas another school of thought believes that it is going to be more evolutionary, and it will take many years before any practical benefits of blockchain reach fruition. This thinking is correct to some extent, but in my opinion, the revolution has already begun [18].

Since 2008, blockchain is implemented in various platforms. One such field where it can be implemented is DeFi. With the help of decentralized finance, we can implement insurance system over decentralized finance in blockchain. So, the smart contract which is written in solidity is deployed into the blockchain with the help of truffle framework. And a digital wallet is used to communicate between the blockchain and decentralized application.

4.1. Smart Contract

The smart contracts which are deployed to the blockchain having some protocols for interaction between the web interface and the blockchain. Every time, when a new operation is performed from the web interface, there is a new block created and mined into the blockchain. So, the three main protocols of the smart contract designed for this system are: Enroll, Join, Claim.

Whenever, a new group or an individual wants to join or enroll in this organization for insurance, this smart contract needs the group size and the address of the digital wallet of the person who is interested in insurance policy. After creating the group, the insured person needs to pay the premium amount. After that, the team is enrolled and will generate the group ID. With the help of group ID, one can join into the group.

If a person wants to join into a group in this organization for insurance, then the person must follow join protocol from the smart contract. the smart contract needs group ID and address of the digital wallet of the person who is

interested in insurance policy. After joining into a group, the insured person needs to pay the premium amount. After the transaction, the person is insured and joined into a group in this organization for insurance.

The amount which is paid from the individuals and groups are received by the smart contract. Now, the smart contract will generate ERC20 tokens to the insured members. The amount is now stored in the liquidity pool. Given in Fig. 2, which illustrates the money flow between, smart contract and the insured person.
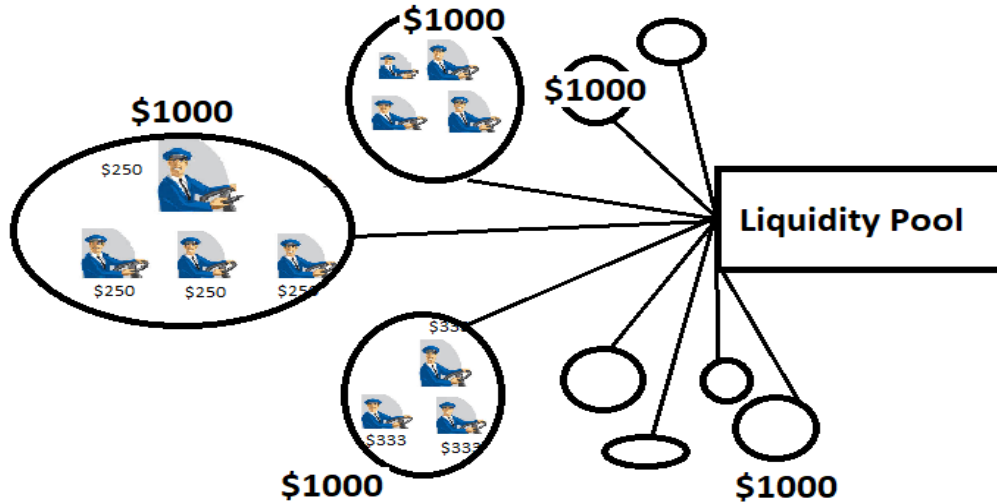
Fig. 2. Money stored into the liquidity pool and ERC tokens are generated

4.2. Web Interface and Digital Wallet

The interaction between the web interface and the smart contract which is deployed into the blockchain is possible with the help of decentralized application and digital wallet. The parameters required for the smart contract protocols are passed through DApp, after successful transaction confirmation from the metamask digital wallet. From the web interface, the insured person provides the group size. After providing the group size, these parameters are then passed to the smart contract which is deployed into the blockchain after the successful transaction from the digital wallet. Given in Fig. 3, which illustrates the process of enrolling a group from the decentralized application. These parameters are passed to the smart contract which is deployed into the blockchain. After the transaction, the person is now insured and will receives an ERC20 token from the smart contract.

Similarly, there is a join protocol for the person to get insured by joining into a group. From the web interface, the insured person provides the group ID. After providing the group ID, these parameters are then passed to the smart contract which is deployed into the blockchain after the successful transaction from the digital wallet. These parameters are passed to the smart contract which is deployed into the blockchain. After the transaction, the person is now insured and will receives an ERC20 token from the smart contract.

Unlike centralized finance, there is no requirement for KYC process and in decentralized finance, the insured person has full authority over fund's custody and DeFi is not accountable for funds and no need to share personal information. At the time of writing this paper, the total value locked in DeFi is 54.02B USD [19]. The only limitation in the decentralized finance is about the faulty code can put funds at risk. To overcome the limitation, the smart contract should be written without any vulnerabilities which are promising to the attackers.
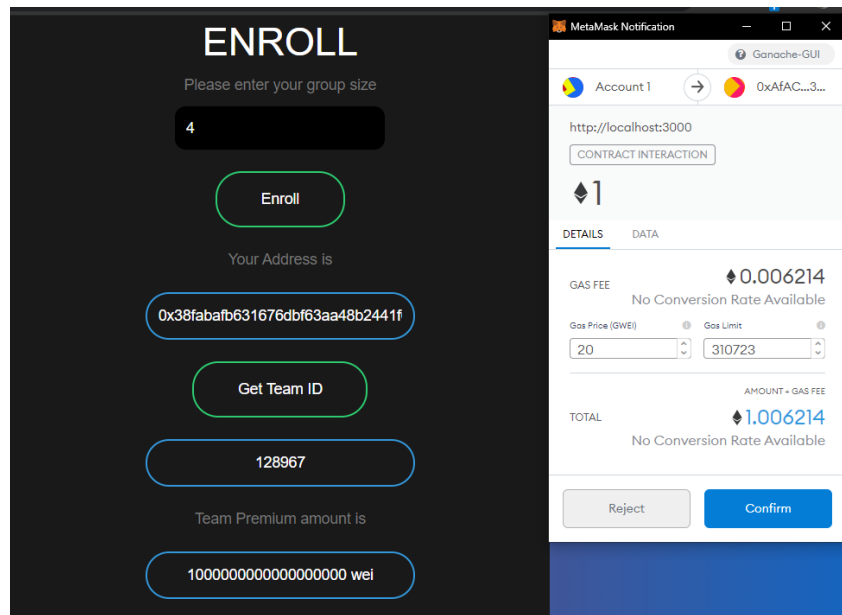
Fig. 3. Accessing enroll protocol of smart contract from web interface

4.3. Claiming the Insurance

At an instance of time, one needs to claim the insurance. It is also known as the request from the insured person for the product which is covered for compensation for damage or loss faced by the insure.

In DeFi scenario, there is an authority named Decentralized Autonomous Organization (DAO) who will validate the claim raised by the insured person. Before DAO investigation there will be a community approval. The insured person, will request the community for approving the insurance claim, based on the reason and proofs uploaded into the web interface. Given in Fig. 4, which illustrates the process of claiming an insurance policy from the decentralized application. After the submission there will be a community approval. A community where, all the insured persons will approve for the claim of insurance or may get rejected if the proofs are invalid. If the community approves for the claim request. Then DAO will investigate and validate the accept or reject the claim request.
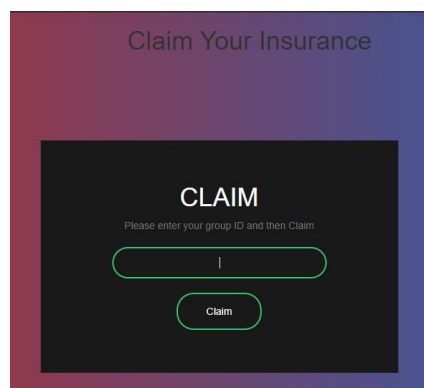

Fig. 4. Claiming the insurance

5. Conclusion

We have developed a decentralized application for insurance system. First, we have created a smart contract and deployed into the local blockchain with the help of truffle framework. For local blockchain we have used Ganache. Then, we have developed a web interface for interacting between smart contract and user. Further we connected the metamask digital wallet with the RPC private network using ganache and injected it to the web interface. This method can also be further developed using public blockchain for higher growth and interaction.

6

Besides, the blockchain shows more promising development in many fields; therefore, we may use and utilize Main network to improve the participation further. And can also involve in expanding many other fields such as: Vehicle insurance, Health insurance, House insurance, Crops insurance, etc.

6. References

[1] Ewold F. Insurance and risk. The Foucault effect: Studies in governmentality. 1991;1972

[2] Greene MR, Trieschmann JS, Gustavson SG. Risk and insurance. College Division, South-Western Publishing Company; 1992 Jan.

[3] Dewatripont M, Maskin E. Credit and efficiency in centralized and decentralized economies. The Review of Economic Studies. 1995 Oct 1;62(4):541-55.

[4] Nofer M, Gomber P, Hinz O, Schiereck D. Blockchain. Business & Information Systems Engineering. 2017 Jun 1;59(3):183-7.

[5] Zetzsche, Dirk A., Douglas W. Arner, and Ross P. Buckley. "Decentralized finance." *Journal of Financial Regulation* 6.2 (2020): 172-203.

[6] M.-O. Albizzati, H. Geman, Interest rate risk management and valuation of the surrender option in life insurance policies, The Journal of Risk andInsurance61(4)(1994)616–637

[7] Bacinello, Anna Rita, Enrico Biffis, and Pietro Millossovich. "Pricing life insurance contracts with early exercise features." *Journal of computational and applied mathematics* 233.1 (2009): 27-35.

[8] H. Kim, J. Park, M. Bennis, and S.-L. Kim. "On-device federated learning via blockchain and its latency analysis", arXiv preprint arXiv:1808.03949, 2018.

[9] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive", Cryptology ePrint Archive, Report 2018/679, 2018

[10] B. Kurtulmus and K. Daniel. "Trustless machine learning contracts;evaluating and exchanging machine learning models on the ethereum blockchain", arXivpreprint arXiv:1802.10185, 2018.

[11] Rejda, George E. *Principles of risk management and insurance*. Pearson Education India, 2011.

[12] Sheth A, Subramanian H. Blockchain and contract theory: modeling smart contracts using insurance markets. Managerial Finance. 2019 May 17.

[13] Mohanta BK, Panda SS, Satapathy U, Jena D, Gountia D. Trustworthy management in decentralized iot application using blockchain. In2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) 2019 Jul 6 (pp. 1-5). IEEE.

[14] Qi H, Wan Z, Guan Z, Cheng X. Scalable Decentralized Privacy-Preserving Usage-based Insurance for Vehicles. IEEE Internet of Things Journal. 2020 Oct 1.

[15] Aleksieva V, Valchanov H, Huliyan A. Application of smart contracts based on Ethereum Blockchain for the purpose of insurance services. In2019 International Conference on Biomedical Innovations and Applications (BIA) 2019 Nov 8 (pp. 1-4). IEEE.

[16] Klages-Mundt A, Harz D, Gudgeon L, Liu JY, Minca A. Stablecoins 2.0: Economic Foundations and Risk-based Models. InProceedings of the 2nd ACM Conference on Advances in Financial Technologies 2020 Oct 21 (pp. 59-79)

[17] Alethio. 2019. Illiquidity and Bank Run Risk in Defi. https: //medium.com/alethio/overlooked-risk-illiquidity-and-bank-runs-oncompound-finance-5d6fc3922d0d

[18] Michael J, Cohn AL, Butcher JR. Blockchain technology. The Journal. 2018 Feb;1(7).

[19] DeFi - The Decentralized Finance Leaderboard at DeFi Pulse. (n.d.). Indradhar. Retrieved May 6, 2021, from https://defipulse.com/