SOFTWARE ENGINEERING PROJECT REPORT

COURSE SLOT: A1 slot

PROJECT TITLE: MAKING AN APPLICATION FOR TRANSFERRING CRYPTOCURRENCIES THROUGH SMART CONTRACTS

PROJECT ASSOCIATES:

Anchit Agarwal [Reg. No. 19BCE2279]

Prithish Samanta[Reg. No. 19BCE2261]

UNDER THE GUIDANCE OF

Dr. DEEBAK BD

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

1. Objective

The main objective of our project is to understand the working of smart contracts in blockchain and where it can be implemented. In our project we have focused on money transferring and insurance. Over the past three months we have tried to learn the basics of smart contracts, how to code them and deploy them in an ethereum network. For our project we have made a basic Application for Transferring Cryptocurrencies through Smart Contracts. This application helps us to transfer Ethereum coins to tokens and vice versa. This is done with the help of tools like MetaMask extension, Ganache, Solidity programming, Truffle, etc. We have also followed a particular paper and some its referenced materials for our project. Our base paper is "Application of Smart Contracts based on Ethereum Blockchain for the Purpose of Insurance Services" which talks about the use of blockchain and cryptocurrency in the insurance sector. The above paper has also used the same tools and ERC20 token standard for creating and running the smart contracts on the Ethereum Blockchain.

2. Problem addressed

1. Type Of Research

The following research is a Qualitative type of research.

2. Problems Addressed by the Paper

In classical insurance services the insurer must complete a number of documents and provide evidence of the value of the loss. On top of that the involvement of the broker brings additional delays and costs. Sometimes the sources of information are biased, often requiring the insurer to contact additional sources. Fraud activity is possible if the loss assessment is done without exchanging information between insurers and the processing of the claim is subjective and not automated. Also there is the issue of transparency.

3. Prior research

The above research paper aims to further digitize the sector of insurance. It wants to get rid of the old conventional methods by implementing a new version of it which uses blockchain and smart contracts.

The original process of claiming insurance is as follows: In the beginning the person requesting for insurance(call him A), should inform the loss and apply to claim his money against the insurer. The above step happens through a broker, who takes the additional information / proof from person A and sends them to the insurer. The verification process takes place and after this is done, the loss is quantified and the additional info is requested if it's needed. Then the total loss amount is stated to the insurer and the amount is given to him.

We can digitize this by using blockchain, which will get rid of the middle men. By getting rid of the middle men they will be able to speeden up the process of applying for insurance and getting their money. In this approach a smart contract is used to calculate the losses, by using statistics and past reports. It also initiates the payment of the money, once the claim is approved.

The authors have referred to a few papers and documentation(eg:- documentation of coding in solidity) for writing his paper. Most of the papers they have referred to do not explain the practical aspect of the project. They mainly talk about blockchain and smart contracts, it's uses, advantages and disadvantages and the benefits and problems of implementing them in the insurance sector.

One of the referred Papers was "Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?" by Valentina Gatteschi, Fabrizio Lamberti, Claudio Demartini, Chiara Pranteda and Víctor Santamaría. The above paper has analysed the importance of blockchain and smart contracts. It talks about the benefits of implementing smart contracts in the field of insurance, but it does not talk about the practical/ implementation of this. The base paper does add this information too and they have implemented the model using solidity.

Another paper referenced by the Base Paper is “IEEE Standard for the General Process of Cryptocurrency Payment” by the Blockchain Standards Committee. It also shows only the theoretical aspect of implementing blockchain in the payment process but it doesn’t talk about the practical part. Prior papers do not show how exactly web applications work with ethereum smart contracts. This paper mentions about ganache server which is used to connect to the blockchain network for development purposes, truffle suite which acts like a database for smart contracts and meta mask to make our browser to a blockchain browser and connection of smart contracts to frontend of any website using web3.js.

Our paper says there can be reduction of frauds by using blockchain technology. But it does not state how the frauds can be fought using the given technology. The paper “Application of Smart Contracts based on Ethereum Blockchain for the Purpose of Insurance Services” by Veneta Aleksieva, Hristo Valchanov, Anton Huliyan talks about the aspect of fighting fraud using the blockchain technology. The base paper could have elaborated a bit more on this topic by referring to this paper.

4. Significance

Contribution to the insurance industry.

The problem with the classical insurance services is that the insurer must complete a lot of documents and provide evidence of the value of the loss. On top of that the involvement of the broker brings additional delays and costs. Sometimes the sources of information are biased, often requiring the insurer to contact additional sources. Fraud activity is possible if the loss assessment is done without exchanging information between insurers and the processing of the claim is subjective and not automated.

This can be changed if we apply the idea given in this paper. In the paper, the middle men, i.e. different insurers, are replaced with smart contracts automation. Hence, it solves the problem of miscommunication, speedens the insurance process and decreases the corruption between insurers. As we increase automation, frauds decrease automatically, and also with the introduction of decentralisation the transparency increases. Claim submission becomes more simplified, faster and more accurate as the need

for a claims agent is now eliminated. The logic used in smart contracts is made such that there is no need for a loss adjuster now to review every loss personally. He/she now has a list of origin of losses helping him/her to identify patterns in fraud attempts. Lastly, the use of intermediary claims agents is also not needed as payment of loss is calculated automatically by the code of smart contracts.

The problem that is addressed by the above article is indeed an important one. It is a fact that the benefits of blockchain technology can be used in the field of insurance to improve customer satisfaction in processing of claims for correction, for reducing the operational costs, for authenticating through signed transactions from a blockchain address and for the calculation of Insurance premium, risk assessment and fraud prevention.

5. Introduction, Literature Review and Methodology

Installation:- Install Ganache, truffle-suite, node js and npm.

Writing Smart Contracts For Buying and Selling Tokens:- Create two events, for purchasing tokens and selling the tokens. Both the events will have parameters for account, token, amount and rate. Create a function to buy the tokens. Declare the token amount as unsigned and initialize it with the value of the number of ethers to transfer using the rate b/w ether and token. Make sure that the balance of that address is greater than the ethers you want to transfer. Transfer that token amount to the address of that account. Use the transfer function to transfer the token amount.Create a function to sell the tokens. Declare the ether amount as unsigned and initialize it with the value of the number of tokens to transfer divided or multiplied according to the conversion rate.

Make sure that the balance of tokens of that address is greater than or equal to the ether amount. Before transferring ether, we have to specify both the addresses and the amount. For this we use the TransferFrom function from the Token.sol file readily made by the ERC20 website.

Connecting this application to the backend of our website. We can connect these ERC20 token functions using a library of javascript called web3.js. It gives us a set of predefined functions which we can use to connect.

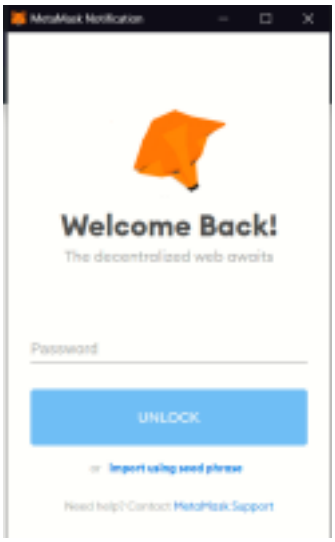
Running this blockchain application on the browser: In order to actually deploy our smart contracts, we need to store a local copy of blockchain on our machine, but since we are at the development phase, we just need to download the browser extension meta mask which connects the blockchain with the ethereum. It can perform sending and receiving ERC20 tokens and ethers.

Appropriateness of this methodology: According to the paper, the results of the experiments show that the proposed solution is giving accurate results wrt managing automatic payments on already approved claims for loss.

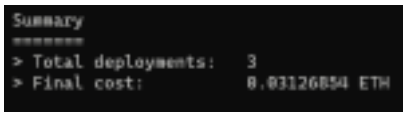
Screenshots which prove that this methodology works:

To show that this app connects to metamask.

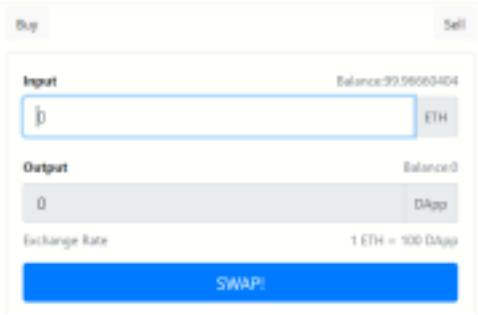
This comes when we start our application.



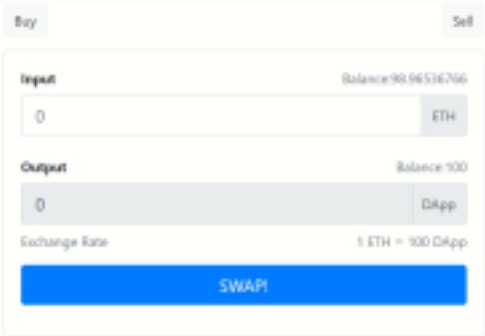
Proof that our smart contracts are deployed



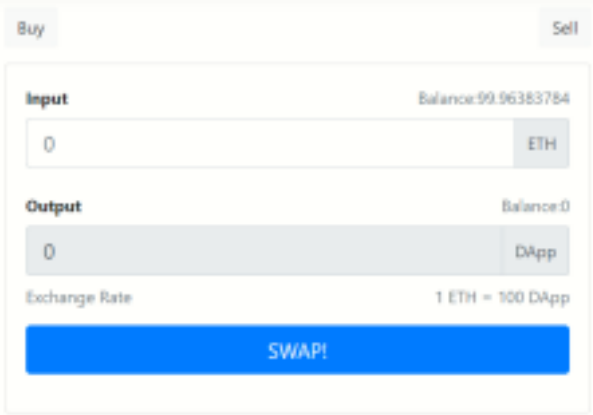
Initial balance



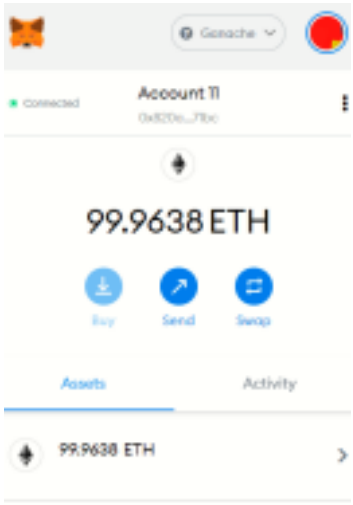
After buying 100 Dapp tokens



After selling 100 Dapp tokens



Status of our account on meta mask



Status of our account on ganache

ADDRESS	BALANCE
0x820aB6aE0DcfAab7A29025E98495640BBa1B71bc	99.96 ETH

Possible problems with the methods used: It's not likely that users will be comfortable using blockchain browser extensions like Meta Mask, etc. 70% of the users use mobile phones to view their accounts. In order to access his/her own account, he/she will have to download the app of meta mask or other various blockchain extensions which decreases the convenience and increases the complexity. Ethereum blockchain surely does increase the security, reduces the documents etc, but not many people can understand this change and due to the above 2 reasons may not use it.

Statistical model

Sources of data for study:

- Ethereum Homestead Documentation, https://ethereum.org/en.
- Solidity documentation http://solidity.readthedocs.io/en/develop/

6. Contributions

1. Contributions by the Authors

The authors have analyzed the possibilities of using blockchain technologies in the field of insurance services. They have presented few of the advantages of such solutions over the classical ways of insurance. They were able to showcase an easy connection of websites with its backend as smart contracts, connecting with the frontend through ganache servers, deploying smart contracts to the network using truffle suite and using meta mask to connect everything to the browser. The authors have successfully implemented the application, as far as automatic payments with already approved loss claims is concerned.

2. Our Contributions

We have contributed equally for making the documents and for creating the website.

Anchit Agarwal, 19BCE2279: Did some of the documentation, and was responsible for the frontend of the web application (shown during implementation), contributed in finding materials for ERC20 functions, and using them in the implementation of the project.

Prithish Samanta, 19BCE2261: Also did some of the documentation work, and was responsible for writing the smart contracts along with team member's help. Did some research on the tools used for the project and helped in implementing it. Researched and came up with the idea of using ERC20 tokens.

7. Further research

Possible areas in which the research can be extended.

Insurance services provide non refundable payments i.e. once paid, not given back. For these types of payments the paper uses ERC20 tokens rather than using those tokens which are used for infungible transactions for example ERC721. We can also include the idea of individual identification using the above mentioned tech stack.

Potential research questions.

Firstly, in a blockchain network, the identity of a person should not be revealed, as only a public key is our identity. So, how would this type of blockchain based application perform well on checking the identity of a person who is doing a fraud.

Secondly, how do we achieve full decentralisation? As there has to be someone who will decide the rules. The math is done by the smart contracts, but what formula to use has to be decided by some authority. So, how can an insurance company be one hundred percent decentralised?

8. References

1. “Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?” by Valentina Gatteschi, Fabrizio Lamberti, Claudio Demartini, Chiara Pranteda and Víctor Santamaría.
2. “IEEE Standard for General Process of Cryptocurrency Payment” by the Blockchain Standards Committee.

3. “Application of Smart Contracts based on Ethereum Blockchain for the Purpose of Insurance Services” by Veneta Aleksieva, Hristo Valchanov, Anton Huliyan. 4. Ethereum Homestead Documentation, http://www.ethdocs.org/en/

5. Solidity Documentation, http://solidity.readthedocs.io/en/develop/introduction-to-smart-contracts.html
6. Blockchain as a Service, https://cryptoapis.io/products/baas/
7. The Blockchain Insurance Industry Initiative, https://b3i.tech/home.html 8. MAERSK, https://www.maersk.com/