SMART TIME LOCK WALLET INTEGRATED WITH VOTING SYSTEM

Madhav Mohanakrishnan[*1], Mir Faizaan Sajjad[2], Vaibhav[3], Nithin Shankar[4] & Neha Tyagi[5]

[*1,2,3&4]Computer Science Engineering, Amity University, Uttar Pradesh, India

[5]Associate Professor, Department of Computer Science & Engineering, Amity University, Noida Uttar Pradesh, India

Abstract:

Today more than ever, blockchain technology is an emerging technology and its applications are widely used. With its smart contract features, Ethereum in particular opens the door to novel concepts that may be implemented in a distributed, unchangeable, and trustless manner. Over the past few years, interest in blockchain has been growing at a tremendous rate, since the technology allows us to solve a lot of problems. It is advisable to create a separate blockchain-based application for the needs of each company. Today, its development is not complete without smart contracts Ethereum. The use of this technology has several advantages: perfect protection against fraud, improved trust between partners, and much more. In this paper, two different applications of blockchain are used inorder to secure funds and preserve the trust of investors. Solidity was applied as the scripting language throughout this development. With the emergence of the startup industry and the ongoing bloom of entrepreneurs, there has also been an increase in public funded projects. Most of the time, these projects possess the vital flaw, that the usage of the funds given by the investors is often unrecorded and unregulated. By suggesting a method that can accurately regulate and see the usage of funds, this application aims to resolve this ongoing issue. Time lock wallets, which store funds until a certain time period and a voting system, which requires majority in order to pass a decision, are pattered for the application. This project has been able to safely protect the funds of the investors as well as come up with further applications caused by the culmination of the two ideas

Keywords: Time lock wallet, voting system, Blockchain.
DOI: 10.24297/j.cims.2023.5.20

1. Introduction

Entrepreneurship, also the latest fad on the planet has been causing an uproar across the globe, from auto driving cars, to rockets that launch till the moon. With the ever-growing number of entrepreneurs, the funding of said projects also grows, with many owners, unable to gather funds by themselves, the reliance for capital often is put on the public's shoulders. This reliance, causes public to give funds in return for shares or better returns, but this process is often done

over editable means. Hence the usage of blockchain is most optimal in this case, with the usage of the smart time wallet along with the integration of a voting system, the funds will be transferred to safe, secure and non-editable means

2. Literature Survey

Since this is an unique approach to tackling problems in the actual world, research on the subject isn't readily available. The privacy and security of any company are today's top priorities. Digital internet transactions involving money or coins also required a particular level of protection, and not just before the transaction was broadcast [1]. Although the cost of cybercrime doubled between 2013 and 2015, a sizable amount of it remains uncovered. According to a Gartner research, by 2019 the cost of cybercrime is predicted to exceed $2 trillion[2]. At the IBM Security Summit, IBM CEO Ginni Rometty declared that cybercrime poses the biggest danger to all businesses worldwide[3]. Because of the novelty of the concept and the unknown aspects of the blockchain, there is a wealth of untapped potential for the future of banking and secure transactions that deter cybercrime. We seek to analyse the potential barriers and usability difficulties that could prevent the widespread adoption of five programmes (i.e., wallets) that are used to handle coins because cryptocurrency is the most successful use of blockchain. We look at typical usability problems with desktop and mobile-based wallets using the analytical cognitive walk-through usability assessment approach. Our findings show that neither wallet performs the essential duties well, which may be greatly improved [4]. The concept of "smart contracts," or computer protocols intended to immediately enable, verify, and impose the negotiating process and implementation of digital agreements without the need for centralised authorities, has been revived by the fast evolution of cryptocurrencies and the blockchain technology that underpins them, in recent years. Smart contracts have been incorporated into popular blockchain-based development platforms like Ethereum and Hyperledger. They have a wide range of possible application areas in the globalised era and intelligent industries, such as financial services, managerial staff, healthcare, and the Internet of Things, among othersHowever, smart contracts are still in their infancy, and significant technological hurdles including security and privacy concerns require more investigation. A broad group of players in the [5th production model supply goods and services to people or organisations. For instance, among the various types of crowdsourcing, crowdfunding has grown to be a popular method of communal fundraising. Crowdfunding is a method wherein a number of people pool their little contributions or investments to promote the creation of new initiatives in exchange for gifts or other forms of recognition. Traditional crowdsourcing is built on a centralized computer where requesters publish jobs on a central server or platform. This centralised approach now faces a number of difficulties including high cost, single point of failure, and insecurity.. In light of this, blockchain is viewed as a promising solution that promises to address the aforementioned issues by removing the single point of failure, improving transparency, and enforcing regulations through smart contracts [g]. In order to establish a secure system for crowdsourcing platforms, this article makes use of a variety of applications,

including time wallet and voting systems. It also seeks to identify potential future uses for the integration of the two blockchain subtopics.

3. Design And Implementation

This paper revolves around a seven-stage methodology as indicated in Fig.1

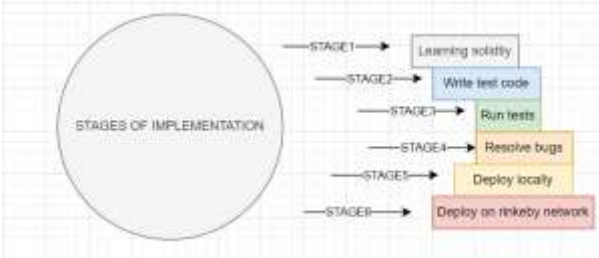

Fig.1 Methodology

Initial writing of hands on code is done on the remix ide, which supports solidity, as well as real time testing of code , using the javascript vm, furthermore the remix ide also supports the connecting of different wallets to it.

Fig.2 Initial code written on Remix IDE

Using the solidity 0.4.17 version , code was written in an easy and comprehendible format in the remix IDE. Furthermore real life testing of the code was done with the help of a metamask account which was created with the sole purpose of real life testing of the contract.

Fig.3 Metamask wallet

Test networks such as Rinkeby was used to prevent any loss of funds, that can be caused due to the transaction fees in the main network. The temporary Ethereum required to complete creation as well as testing of the contract is obtained with faucets that provide them across the Internet. After writing the code, the process of deploying begins. Firstly, it makes sure that the code is compiled without any errors, that is done through auto checking in the remix IDE. Then the code is tested with the remix IDE, with the function buttons that come in the UI, after compilation. Next comes the step of deploying it in the network, this involves usage of writing the code in a local IDE. Furthermore, the code is then tested using mocha and then hosted using ganache into the main network. Mocha is a testing framework used to test the code, it requires the bytecode, which is pushed out after the compiling of the code, the bytecode along with the interface is then used in testing. Both the processes of testing and deploying the voting system contract as well as the smart time lock wallet is done simultaneously. The publication also talks about shifting of testing networks from Rinkeby, as the protocol along with Ropsten and Kovan are in queue to be discontinued due to the protocol changes of the main Ethereum network. Truffle is the wallet provider that was used in the code, inorder to deploy the contract locally.

We have moved from the Rinkeby to Goerli, thereby allowing to develop on the Ethereum test networks. The UI has also been created using HTML, JavaScript and CSS , thereby allowing the User to interact with the Contracts.

4. Review And Results

Succeeding the completion of code tests, were written and run and after several removal and adjusting of bugs, as well as different test cases, using the describe , 'before each' and 'it' keywords which all ran test cases which used accounts given by the truffle wallet , inorder to send money into the contract, as well as to see if the money can be taken out from the wallet.

Fig.4 Testing for voting contract

The following figure shows the deploying of the voting contract, the first lines show the deployment of the of the contract on a local network created using a truffle wallet. Further lines

also show the pneumonic keys as well as the endpoint, the pneumonic key is changed for privacy reasons in the following figure.

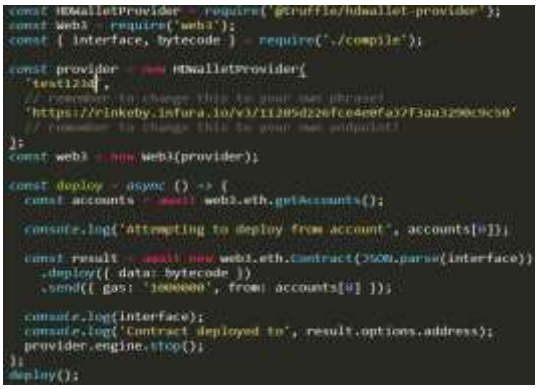

Fig.5 Deploying voting contract

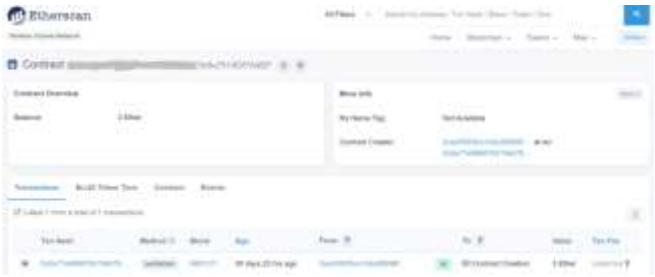

Fig.6 Contract on etherscan

The following figure shows the usage of the function to send money from contract to the manger of the contract

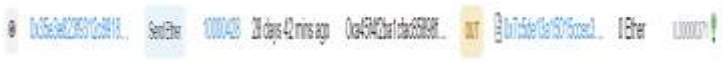

Fig 7. Send money function proof on etherscan

Figure 8 shows the transaction details of the send money function

Fig 8 Send Money Function

The following figure shows the testing of the smart time lock wallet in the remix ide, this includes testing of functions such as setting a time period for locking of the funds

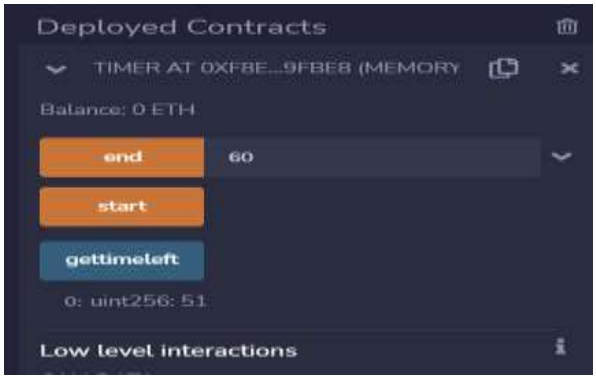

Fig 9. Testing of start, end and gettimeleft functions

The following figure shows the UI , which allows the creation of campaigns

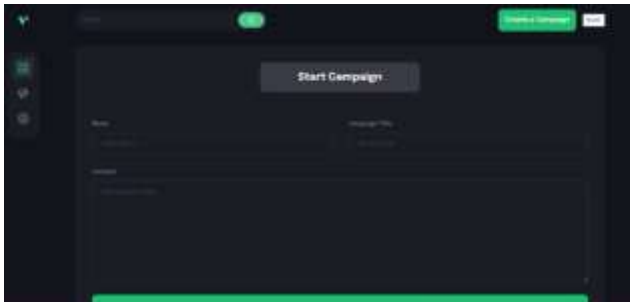

Fig 10. UI for Creating Campaign

The following figure shows the message shown to campaign creators when requests for fund release, saying that funds will only be released if the investors agree to do so.

Fig 11. Message for Release of Funds

5. Conclusion

This paper was designed to show the capabilities of the smart time lock wallet which is integrated with a voting system across different aspects of the community. The goal of this paper is to show the working and the abilities of the wallet in terms of fundraising projects. This study aims to safeguard the investors funds, from being stolen by owners of programs. There is an increase in startup ideas across the world over the last few years, and so has the stories of owners embezzling funds from investors. Protecting investors funds and trust is of utmost importance in any projects life. Blockchain, and its applications such as time wallets were used in

the application. Voting system which includes transfer of funds only on majority approval of investors is one of the two centers of the project. The time lock wallet and its integration with the voting system provides maximum security of the funds while the project moves forward. The additional decision for sending the funds directly to third party service owner, also increases the security of the investors funds.

6. Future Prospects

By using the funds into DeFi, the investors will also be welcomed into the world of lending and borrowing using crypto, thus allowing people to keep with the latest application of web3 and the future of banking. It will also include hosting on the main network, once proper capital funds can be secured, and pipelines concept will be introduced to the same, thereby enabling CI/CD .

References

1.]. A. G. Khan, A. H. Zahid, M. Hussain and U. Riaz, "Security Of Cryptocurrency Using Hardware Wallet And QR Code," 2019 International Conference on Innovative Computing (ICIC), 2019, pp. 1-10, doi: 10.1109/ICIC48496.2019.8966739.
2. 2019, [online] Available: http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#768e4f293bb0.
3. IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World, [online] Available: http://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-inthe-world/#16ff2faf3548.
4. Moniruzzaman, M., Chowdhury, F., Ferdous, M.S. (2020). Examining Usability Issues in Blockchain-Based Cryptocurrency Wallets. In: Bhuiyan, T., Rahman, M.M., Ali, M.A. (eds) Cyber Security and Computer Science. ICONCS 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 325. Springer, Cham. https://doi.org/10.1007/978-3-030-52856-0_50
5. S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F. -Y. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266-2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.
6. Khan, S.N., Loukil, F., Ghedira-Guegan, C. et al. Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-Peer Netw. Appl. 14, 2901–2925 (2021). https://doi.org/10.1007/s12083-021-01127-0.