IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Crowdfunding for Engineering Startups using Blockchain and Smart Contracts

[1]Jain Darsh NareshKumar, [2]Upadhyay Ankita Ramesh, [3]Nirban Asjad Sajid, [4]Arya Manav SunilKumar , [5] Dr. Vinayak Shinde

[1]Student, [2]Student, [3]Student, [4]Student, [5]Associate Professor
[1]Department of Computer Engineering,
[1]Shree LR Tiwari College of Engineering, Mumbai, India

Abstract : Crowdfunding is a money-raising strategy that began as a way for the general public to donate money to help inventors or startups by helping in funding their projects. The problem with the current websites like Kickstarter is that they do not provide the guarantee that the donor's money goes into good use only and they don't have control over the money they donated. The system of crowdfunding using blockchain and smart contracts technology is proposed in this paper. Through this, The system can provide a safe, secure, and decentralized way for crowdfunding and to make transaction histories more transparent and secure through the use of blockchain technology. Contributors can decide where to invest in terms of the needs of the creator and can acknowledge the requests for money made by the project creators through their votes. The creator of the campaign can only use the money if and only if a minimum number of contributors approve a certain request for the transfer of money. It will make sure the money is used for the necessities of the project/company rather than luxuries. All the transactions would be stored in the form of blocks in the ethereum ledger hence achieving transparency.

IndexTerms **- Blockchain, funding, crowdfunding, startup, smart contracts.**

INTRODUCTION

Crowdfunding is a special type of crowdsourced product that is used as a method for generating funds ie. Crowdfunding seeks little amounts from bulk individuals to fund businesses, creative projects, charities and more. The problem with the current crowdfunding companies is the charging of high fees and several scams happening but implementing it on blockchain will help to avoid these types of problems.

Blockchain is an evolving technology and has the potential of overruling server based systems soon because of the high security and transparency. Websites like Kickstarter are server based and like many other systems might get obsolete as it introduces a lot of security as well as trust flaws which blockchain can reduce by proper implementation. Hence it is very important to create such a system and ensure security and evolution.

Blockchain based crowdfunding has several properties like

- Decentralized Network
- Peer-to-Peer transaction
- Access Equality
- Universal Opportunity

Decentralization and privacy has taken utmost importance today for each individual as well as company. The proposed system will help in achieving privacy, transparency at an individual level. Around the world, cryptocurrency is being utilized and adapted to and hence the system has huge scope to reach individuals as well as help creators of various engineering as well as non-engineering startups. This project will ensure innovation is not hampered and frauds taking place are reduced.

Literature review

One task in the overall project was to determine what types of Crowdfunding systems which use the blockchain technology already existed worldwide. Our particular interest was the capability of these systems to monitor transactions, Transparency within the system, Smart Contract designs and performance and how it reacts in various situations. Also of interest was [3] learning more about use cases of such systems, [4, 5] How crowdfunding involves Smart contracts and Possible cases where system / smart contracts can be exploited, [6] Possible Threats, Opportunities, strengths, weakness of Crowdfunding systems and most importantly [7] the scope of Crowdfunding.

In paper [3] the author proposes that blockchain technology is considered as the most significant invention after the Internet. If the latter connects with people to realize on-line business processes, the former could solve the trust problem by direct networking and use of public-key cryptography. This paper summarizes the most promising use cases of the blockchain technology including cryptocurrency, smart contracts, smart cities, electronic medical records, digital identity, reputation systems, machine-to-machine communication and the Internet of Things. Considering that there is a potential infinite number of use cases

of the blockchain technology, It can be concluded that it has penetrated into all spheres of our life and as a result of its impact on our life

In paper [4] the author conducts a systematic mapping study to collect all research that is relevant to smart contracts from a technical perspective. The actual aim of doing so is to identify the latest research topics and open challenges for future studies in the smart contracts domain. This particular paper focuses on studying, identifying and tackling smart contract issues. The four key issues are identified - codifying, security, privacy and performance issues with the same. This paper [4] presents a few research gaps in smart contract research that need to be addressed in future studies. The identified gaps in research are the lack of studies regarding scalability and performance issues, the lack of studies on deploying smart contracts on various blockchain platforms other than Ethereum, the fewer number of the actual proposed smart contract applications, the lack of studies on illegal activities in smart contracts and the lack of high quality research on smart contracts. These identified gaps could be identified and studied by researchers as future works.

In paper [5], the author provides us with an overview of smart contracts. Smart contract technology is changing traditional industries and business processes. The smart contract is embedded in the blockchain and can automatically execute the terms of the agreement without the intervention of a trusted third party, thereby reducing management and service costs, improving business process efficiency, and reducing risks. Although smart contracts are expected to promote new business processes There is a wave of innovation, but there are still many challenges to be solved. This article introduces a survey on smart contracts. It first launched blockchains and smart contracts. Then it introduces the challenges in smart contracts and the latest technological advances. It also compares typical smart contract platforms, and gives classifications of smart contract applications and some examples. This article indicates the challenges related to smart contracts in various aspects of creating, implementing, executing and terminating smart contracts. Meanwhile, it also discusses the latest advances in addressing these issues. Next, it compares some of the major smart contract platforms. It categorizes smart contract applications and lists some common use cases for each application category.

In Paper [6] the author gives a SWOT analysis of strengths , weaknesses, opportunities and threats of crowdfunding. The strengths of crowdfunding are: 1. A chance to test marketability of the application 2. The accessibility of funds, benefits for the general public, rights to make company's decisions stay in the hands of entrepreneurs completely. Weaknesses include - 1. Administrative and accounting challenges 2. The possibility of ideas being stolen 3.The system has frail investor protection and potential for fraud occurring 4. Crowdfunding is completely internet based, so investors might lack advice and confidence. Identified opportunities include the existence of a niche, information society and positive effects crowdfunding is expected to have on the economy, also, such threats as the risky nature of small business and unsuitable legal restrictions arise. Gaining a deeper understanding about crowdfunding could be useful for entrepreneurs choosing a way to raise capital and investors seeking for different investment opportunities. To conclude , this article analyzes the weaknesses of the system well and hence we can discuss its strengths and weaknesses to evaluate the existing system and see how one can transfer it to the blockchain system while maintaining its integrity and strengths, reducing its weaknesses, and reducing external threats like hacking to a lower level.

In Paper [7] the author briefs us about the potential functioning of the crowdfunding platforms in India, with a limited number of parameters and Campaigns. Crowdfunding is also termed as 'democratic finance', as it does not involve traditional banking middle man. Undoubtedly Crowdfunding, which poses a prodigious potential, is in its early stages. Therefore, it is the need of the hour for the lawmakers to look upon the regulations and give this potential market a strong support system. Crowdfunding Platforms are a great support system for the Fund seekers and Fund Providers, and they have to improve their Competency to be in the mainstream funding in the future.

Limitation of Existing System

1. The user needs to have a good enough internet connection of 1 mbps to interact with the system well.
2. The server has limitations which means in the event of a vast number of users interacting with the portal , the portal might hang or crash or mishandle the transaction.
3. The user needs to have a secure system as well as network while handling transactions as traditional banking systems can be hacked at user side using attacks like MITM.
4. The user is required to have a web browser with javascript enabled.
5. The user will not have transparency of the transactions occurring.
6. The user is required to donate the money through fiat currency like USD or INR which will involve banking systems. This means the users of crypto currencies won't be able to transact on this.
7. The system is bloated with advertisements as well as unnecessary stuff which overwhelms the user.

PROPOSED SYSTEM

In this paper, we propose to make transaction histories more transparent and secure through the use of blockchain technology. Contributors can decide where to invest in terms of the needs of the creator and can acknowledge the requests for money made by the project creators through their votes. The creator of the campaign can only use the money if and only if a minimum number of contributors approve a certain request for the transfer of money. It will make sure the money is used for the necessities of the project/company rather than luxuries.

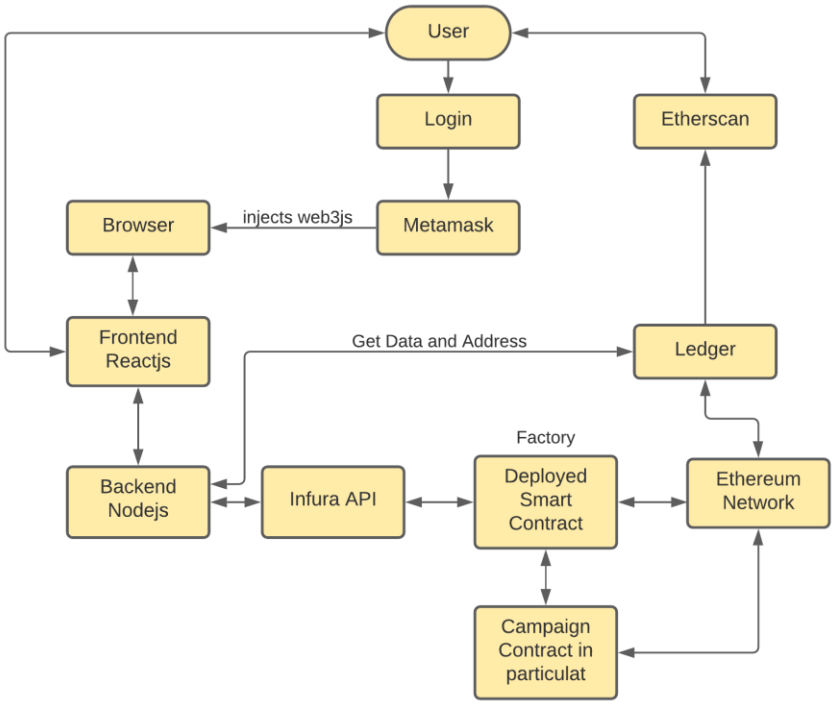

Figure 2.1: System Architecture

The architecture is as shown in the above figure . The website will be built on the base of ReactJS , Nodejs. The smart contract would be drafted and deployed in solidity language. The contract from the solidity language would be converted to ABI code which is in JSON format. This JSON will be parsed to get details like interface for the contract deployment using web3js , INFURA API . This would return a contract address which will be saved in a .env file as a constant. The deployed contract would be then ready to be fetched by the backend and in turn to the frontend for the user. The first block in the chain is known as seed block and it will be the block containing deployed contracts. The system would then be ready to be used by a basic web browser and metamask extension installed as a wallet for Ethereum accounts. Metamask injects the web3js instance into the web browser as well for interaction and would handle each request or transaction as a middleware between the website and the blockchain. This contract will act as an intermediary contract and would be used to deploy the actual campaign contracts since we cannot hand over the raw code to the creator for deployment at their end without ensuring there are no security issues. This contract would store the address for the deployed campaign contracts and would fetch them for the user.

Requirement Analysis

The system will need the following Hardware to use-

1) CPU - Dual Core Processor 2.4ghz
2) Network - Broadband
3) Hard Drive - 1GB
4) Ram-2GB
5) CPU - i3 4th generation
6) Hard drive - 10GB
7) RAM - 4GB

The system will need the following software to use-

1) Metamask (Any version) - A cryptocurrency wallet based on web browser with multiple access modes to conduct transactions from users end like approve request etc
2) Web Browser - Chrome/Brave/Edge/Mozilla - It is used to access the website/portal and interact with it
3) NodeJS - It is used in the system for handling the backend of the system
4) NextJS - This is the frontend and UI of the website which will be available to the users/creators
5) Ganache CLI - This will be used by developers to test the contract by fake ether and creates a test blockchain with accounts.
6) Web3JS @ 1.26 - This will be used to write automated tests to ease the testing phase of contract interaction with ReactJS / UI
7) Mocha - This will be used to write automated tests to ease the testing phase of contract interaction with ReactJS / UI
8) React JS - Frontend framework to build the UI/UX and update asynchronously as interaction happens.
9) Solidity - A language to create , interact and maintain smart contracts with blockchain.

Results and Discussion

The system was successfully implemented on the ethereum rinkeby test network. The solidity programming language is used to implement the system. Initially the Campaign Factory and Campaign file are compiled into bytecode and abi using the Solc solidity compiler. The abi is in JSON format and is used to connect with the front-end in the Bytecode, which will be distributed on the blockchain. The front-end is built with React Js based framework Next Js, Semantic-UI. The user interactive form will be used to make it simple to contribute. The project's originator or management must make a funding request. For the purpose of purchasing some accessories He'll use the request form to make a request. This will be recorded in the blockchain and stored there as blocks of data

If the request is necessary, all investors must approve it. They have the option to refuse the request if this is not the case. After a successful approval the money is transferred to the mentioned account or vendor.

Step 1: Home Screen

The Home page of the project is divided into two sections i.e. Open Campaigns & Create Campaign. Open Campaign is the list of Startups who want to crowd fund their projects, users can find their topic of interest to invest in, and know more about projects available on the platform.

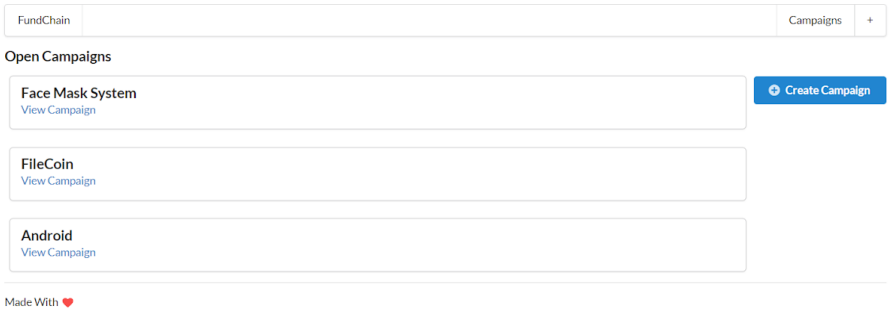

Figure 2.2.1: Home Screen

Step 2: View Campaign

Now after creating the campaign, you can view your created campaign or any other existing Campaign in the Open Campaign section. One can know about details of a campaign by clicking on “view campaign”. The Details include Manager address, Campaign Name, description of campaign, Minimum wei needed to be a contributor, No of approvers, No of request, Remaining Balance / funds. The user will get two options in this screen one is to “view request” and “contribute” .

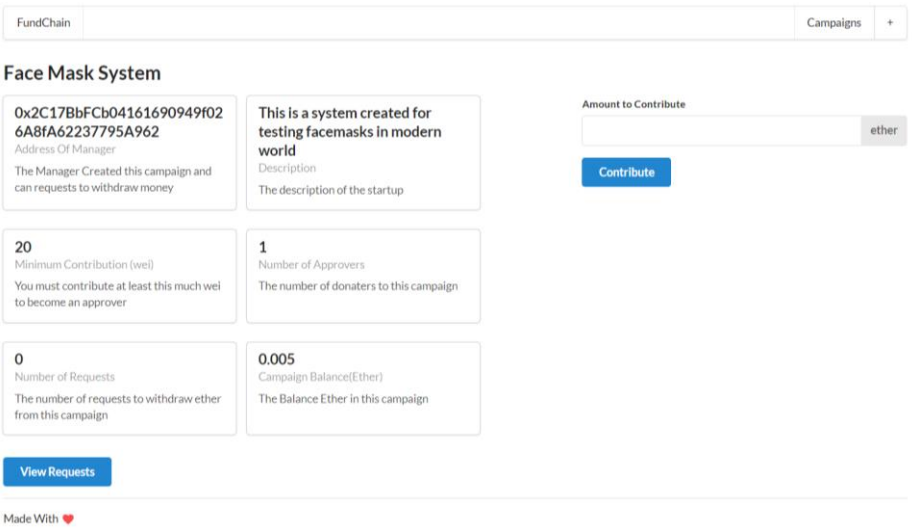

Figure 2.2.2: View Campaign

Step 3: Contributing to Campaign

If one wants to contribute to the campaign then one can click on the “Contribute” button and to be an approver they need to contribute the minimum amount set by the campaign manager. And after successfully becoming the approver He/She can now approve a particular request made by the campaign manager.

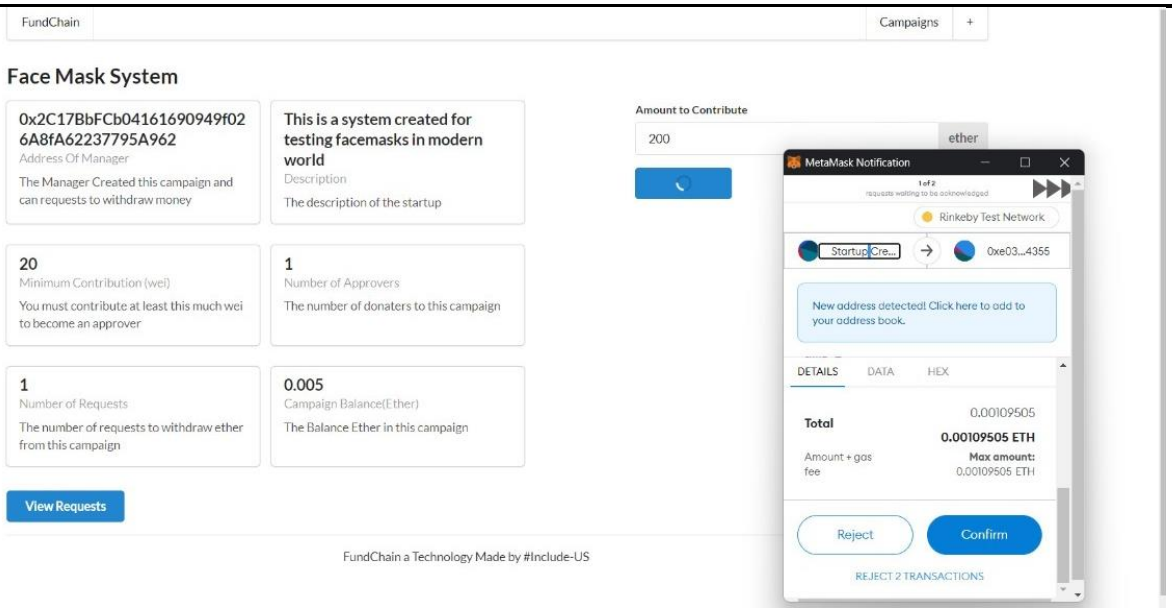

Figure 2.2.3: Contributing to Campaign

Step 4: View Campaign Request

In the view request section one can view the request made by the campaign manager to use funds, only approver of the particular campaign can approve the request, if you're not an approver yet you would try to approve any request then the system will throw an error. Similarly only Campaign Managers can Finalize a request only when the minimum number of approvers had approved the request, if the minimum number is not reached then manager can't finalize the request as it'd thrown an error. If an approver or someone who isn't involved in the campaign can also not finalize any request. The request consists of information like Recipient address, amount requested and the reason for the same.

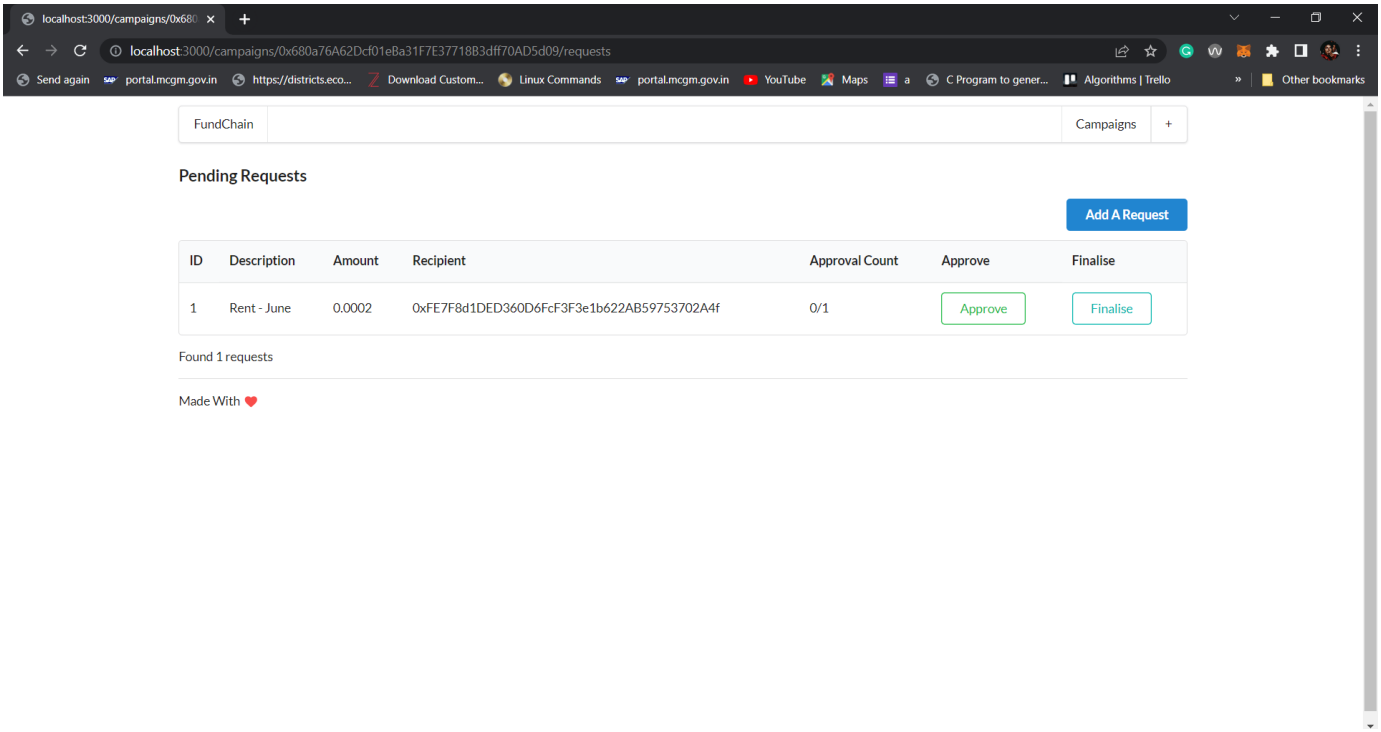

Figure 2.2.4: Campaign Requests

Step 5: Creating a Request

Only Campaign Manager can add requests when needed, no one else in the existing system can add a request. In the Creating request section manager has to tell what he wants to request and a description of it also the amount requested and the recipient Address, as the transaction will be directly sent to the vendor instead of manager.

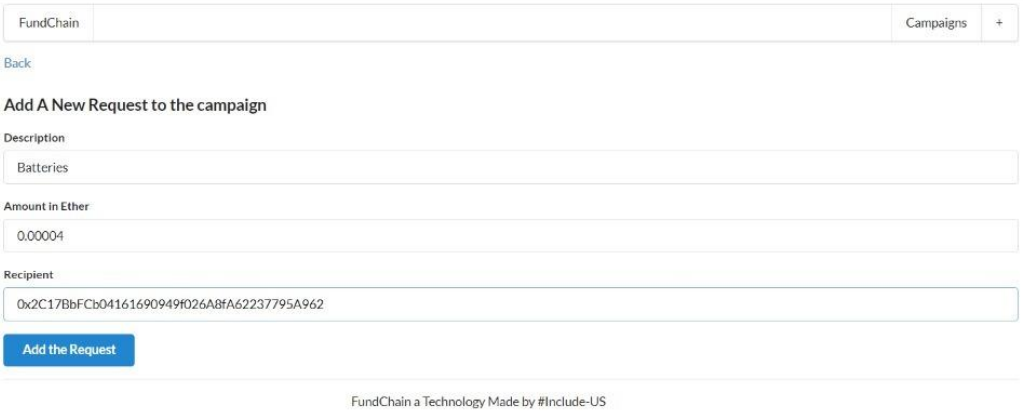

Figure 2.2.5: Create a request

Step 6: Approving Campaign as approver

If an approver feels that the particular requested amount and resources is valid and it's justifiable then He/She can click on approve request to Approve it.

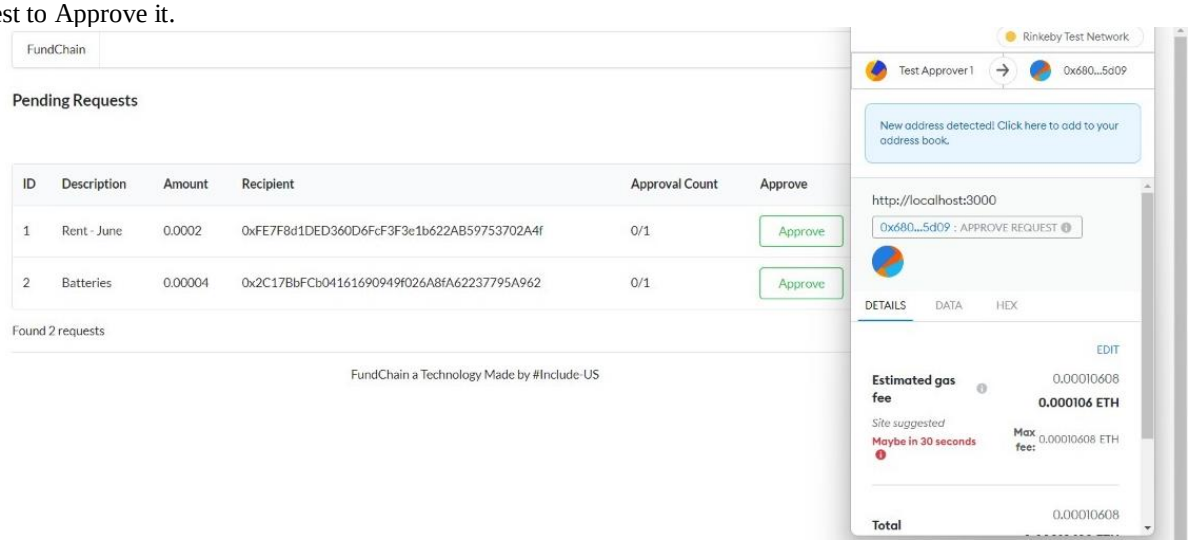

Figure 2.2.6: Approve a request

Step 7: Approver count reaching the minimum requirement

If a request gets a minimum number of approvals then it turns green and is ready to be finalized by the manager.

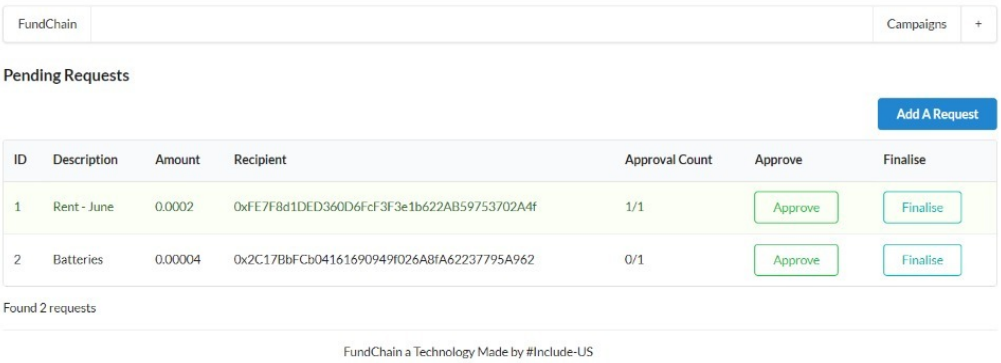

Figure 2.2.7: Request Count reaching its minimum requirement

Step 8: Finalizing request by manager

When a manager clicks on a ‘finalize’ button then the amount requested is transferred to the recipient's metamask wallet.

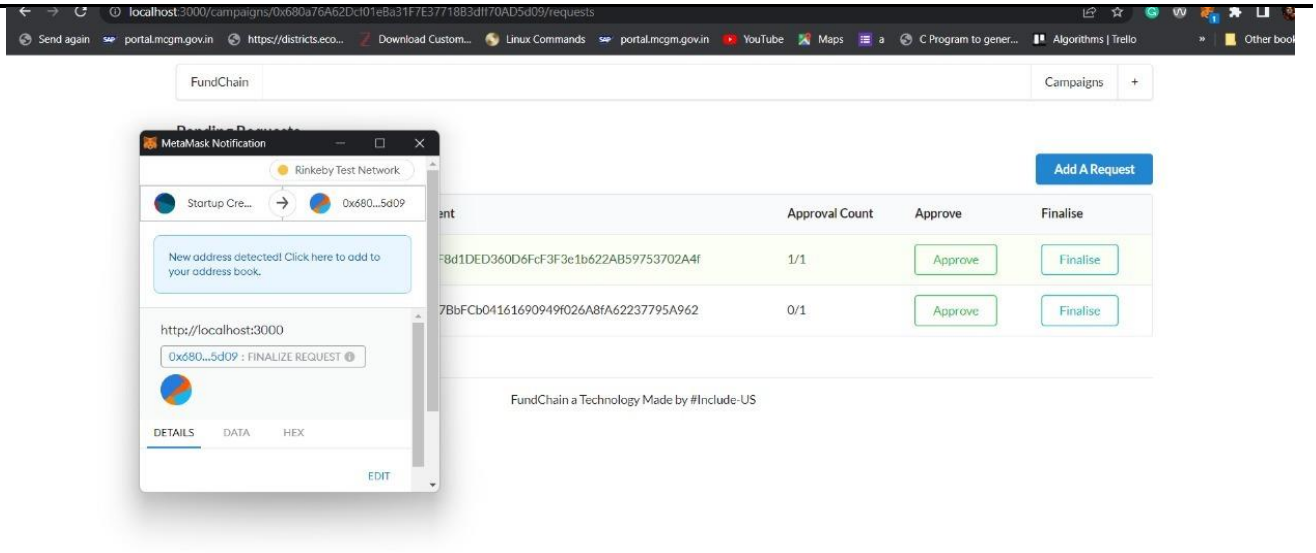

Figure 2.2.8.1: Finalizing a request

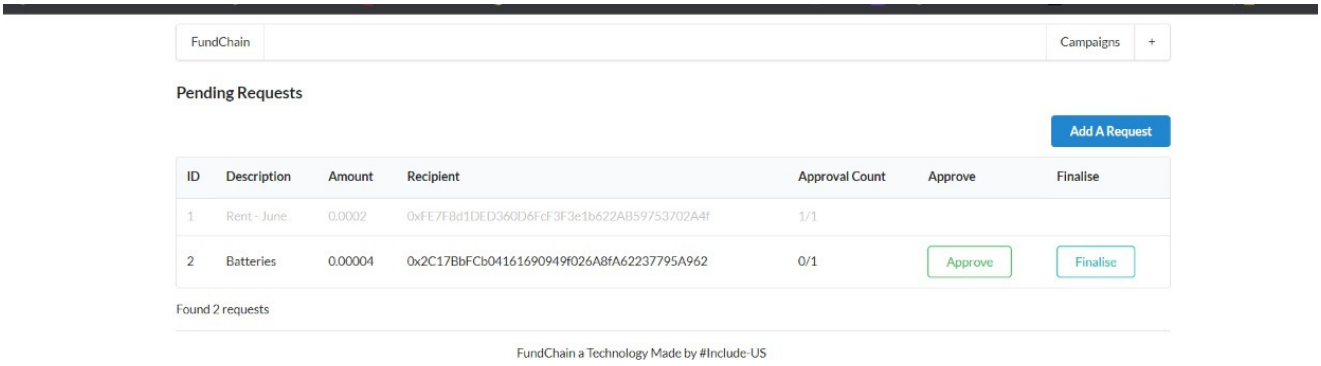

Figure 2.2.8.2: Finalized Request

Figure: 2.2.8.3: After Approving Payment

Step 9: Creating a Campaign

If you want to create your own campaign then you can use the Create Campaign button. In the create campaign section you need to give some basic details about your project like name of the startup, Description of Startup, Minimum amount need to be contributed in wei, then click on create, then you'd be back to the Home screen.

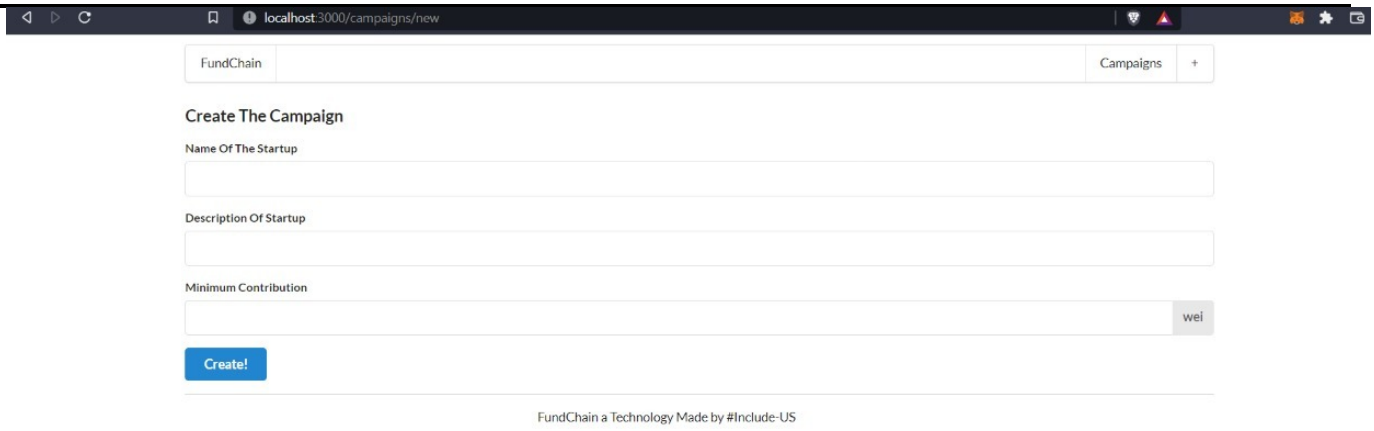

Figure 2.2.9.1 Create a Campaign

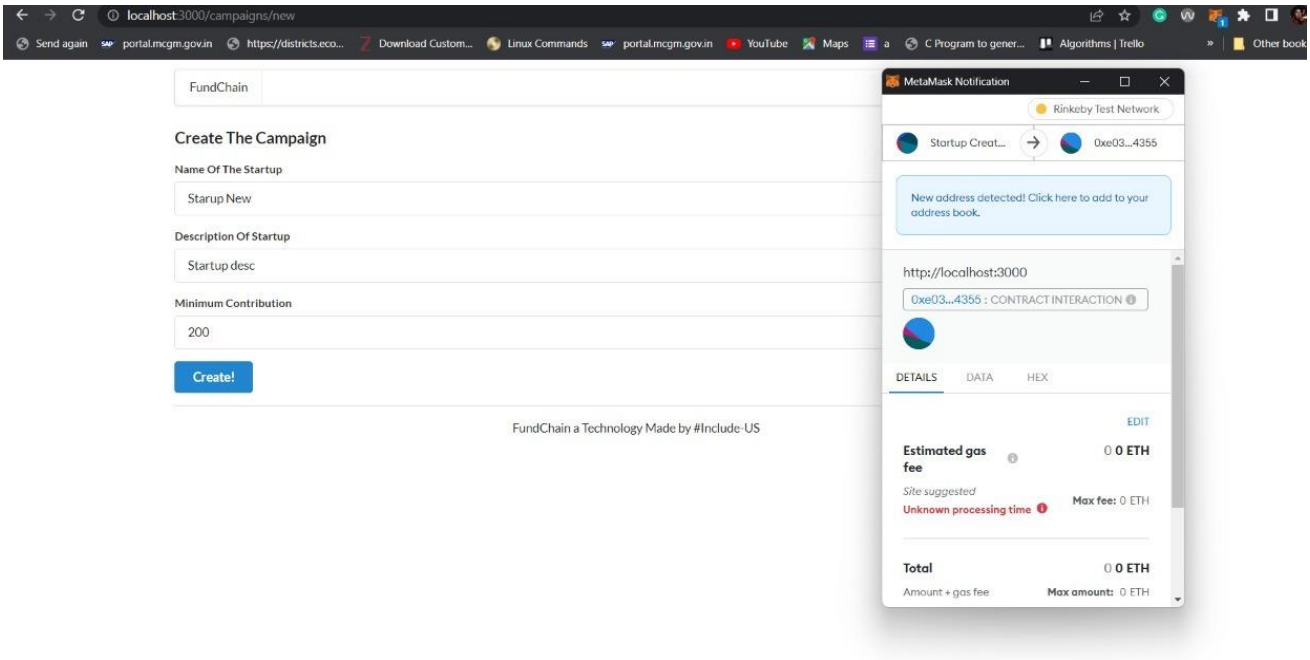

Figure 2.2.9.2: Conforming transaction through Creator account

Conclusion

The system is successfully implemented on a blockchain based application to crowdfund money for engineering startups on an Ethereum ledger. The system successfully deploys a factory and starts a campaign where the caller is set as campaign manager. It allows people to contribute money and marks them as approvers for this campaign while also ensuring each contribution is greater than or equal than a minimum contribution amount. The manager of the campaign can also generate a payment request which will be shown on the requested payment list. Furthermore, the system will check that the appropriate smart contracts have been generated and then finalize the request to transfer funds to the vendor as per the smart contract.

ACKNOWLEDGMENT

We would like to express our deep gratitude to Dr. Vinayak Shinde, our research supervisors, for his patient guidance, enthusiastic encouragement and useful critiques of this research work. We would like to thank Dr. Vinayak Shinde, for his advice and assistance in keeping my progress on schedule. We would also like to extend our thanks to the technicians of the laboratory of the Computer department for their help in offering us the resources in running the program. Finally, we wish to thank our parents for their support and encouragement throughout our study.

REFERENCES

[1] Efanov, Dmitry, and Pavel Roschin. “The All-Pervasiveness of the Blockchain Technology.” Procedia Computer Science, vol. 123, 2018, pp. 116-121.

[2] Alharby, Maher, and Aad van Moorsel. “A Systematic Mapping Study on Current Research Topics in Smart Contracts.” SSRN Electronic Journal, vol. 9, no. 5, 2017, pp. 151-164.

[3] Zibin, Zheng, et al. “An overview on smart contracts: Challenges, advances and platforms.” Future Generation Computer Systems, vol. 105, 2019, pp. 475-491.

[4] Valančienė Loreta, and Sima Jegelevičiūtė. “VALUATION OF CROWDFUNDING: BENEFITS AND DRAWBACKS.” ECONOMICS AND MANAGEMENT, vol. 18, no. 1, 2018, pp. 39-48.

[5] V., Lakshita, et al. "An exploratory study on crowdfunding platforms in india." International Journal of Current Research, vol. 11, no. 1, 2019, pp. 970-972.