iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.53967

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

Medtrust - A Decentralized Model for Medical Crowdfunding Based on Smart Contract Using Etherium

Dr Nirmal K Raja[1], Dr Prem Sankar C[2], Mrs. Anurgaha K R[3], Mrs. Divya Jose[4], Mrs. Gadha M M[5], Mrs. Aswathy P[6], Mr. Sreejesh R[7]

[1]*Principal -ICCSCEM Thrissur*

[2]*Professor,* [3, 4, 5, 6]*Asst. Proff,* [7]*Student, Computer Science & Engineering*

Abstract: ***Trust and Transparency is a great challenge that the current world encounter when coming with systems that really matters the day to day life. When it comes to financial systems, the requirement becomes stronger. The paper suggests the implementation of a medical crowdfunding system incorporating trust and transparency with blockchain. With decentralized approach. The paper explains implementation of a Crowdfunding system based on blockchain using smart contract. The Paper explains the architecture, implementation and Test cases that been used and a study of the how the model solves the issue of trust. The system is been tested and deployed with hardhat framework over sepolia Test Network.***

Keywords: Trust and Transparency, Sepolia Network, Hardhat, Blockchain, Smart contact,

I. INTRODUCTION

Trust and Transparency is a most crucial problem that need to be addressed when working with systems that make impact. The technology that we use try to most simple and yet complicated question of the Trust and Transparency in the real life. The need of trust and transparency is been more crucial when the system is based on financial transaction. The Proposed Project model is trying to solve the issue in medical crowdfunding in an innovative and modern approach. Crowdfunding is a method of raising founds through online medium for addressing a challenge. The agenda of hosting a crowdfunding campaign could be Anywhere between a solving a social impact problem to raising fund for a project, education or even entertainment. Medical Crowdfunding is the crowdfunding is a crowdfunding when the agenda of the organizers of the campaign to raise the fund to save a life or to meet a medical expense. The main issue with medical crowdfunding is the lack of trust and transparency over the campaigns. [7][3] The Proposed Model explains how the implemented solution address the challenges of trust and transparency in medical crowdfunding using blockchain. A detailed explanation of existing system along with problem statement is been attached.

A. Existing System

In the section we will be discussing about the existing system and how the solution been implemented now address the problem. As of now there are a lot of platforms that host medical crowdfunding some of such platforms are general in purpose. That suggest these platforms are designed such a way that it promotes both the medical as non-medical crowdfunding. The other kind of systems in the category is platforms that are designed exclusively for medical crowdfunding. Even though the working of the both systems works on same basis. The Organizer could host the campaign with the required funds that he needs to raise and start the campaign. The Campaign is been hosted in the platform for free even though a large cap of the money that been raised is been taken by the platform, this could be 6 to 25 percentage of the total money raised. And is a great gap and due to that sometime even the contributors contribute the campaign for but due to the platform charges the money is still been lack of. This is how the existing systems work.

B. Problem Statement

In the section the existing problem statement is been described. The great challenge with the existing architecture is the lack of trust and transparency over the campaigns that been done. The main challenges that include,

1) Lack of Transparency and Trust

The great challenge of the current application is the lack of trust and transparency over the system.

The issue is due to anyone could able to host the campaign and receive funds and there is no sufficient mechanism to validate the campaigns or validate the fund transfer. The system also doesn't ensure that these campaigns can either be genuine or not. There should be an efficient mechanism to host the campaigns and validate the transaction

2) Lack of Financial Trackability

Another challenge of the existing system is the lack of possibilities for an efficient financial tracking. Even a lot of agencies point out the usage of online based crowdfunding establishments for illegal and anti-social/National elements to raise the funds. But due to an efficient system that is been lack of financial trackability the issue still is been unresolved. An efficient system should be able to track the source as well as the destination of the all transactions that been availed in the particular platform with an ease of public verifiability.

3) Challanges with Security

Another next challenge of the systems is the thread of security. Most of the systems is been built on a centralized architecture where the attacker has the target vector to push the attack on. Due to the centralised mechanism the chances of the insider frauds are also high in these kinds of systems.

These are the challenges that needed to be addressed in the case of developing a model for a crowdfunding platform.

II. LITERATURE REVIEWS

In the section various models that been implemented prior are been discussed. Various relevant concepts are been considered from these models for the further development of the application.

A. Blockchain – Based Crowdfunding a Trust Building model

Blockchain – Based Crowdfunding a Trust Building model is a model based of crowdfunding deployment that been proposed by the authors to overcome the limitations and challenges in the traditional crowdfunding approach. The work points out that in the traditional model of centralized architecture. The challenges that the work is been pointing out is the data leaks and risk of security due to lack of cryptographically secured mechanism and attacks like DDOS (Distributed Denial of Service) that the platforms need to address with

The paper also points out the challenge that a centralized system poses in case of insider crimes like modifying the records from internally. The proposed system suggests a decentralisation of the crowdfunding platform with blockchain network that will not only reduce the challenges also it will provide better security and risk mitigation in case of attack. The proposed work is been tested over the Rinkeby test network with running multiple campaigns at same time. The proposed work suggest how it addressed various challenges and also provide a detailed approach on how the solution solve the challenges is been detailed discussed. [1]

B. Blockchain – Based Crowdfunding Application

Blockchain – Based Crowdfunding Application is a model proposed to implement a decentralized crowdfunding application based on blockchain. The advandage of this platform is the platform is been governed by the smart contracts. Smart Contracts are codes run on blockchain network. The smart contracts are autonomous codes that will be executed automatically. The application provides a 3 person view of the entire system encountered as smart contract powered admin portal, a page for investor and a page for the client to run the campaign. Through the campaign page the clients could be able to host the campaigns where through the campaign pages the investors could invest in the campaigns.

The core approach that been used here is that the instead of the funds get entirely transferred to the user the funds is been taken in hold by the smart contract and is only been transferred when the particular campaign meets some milestones. This is a way that the scam over the networks could be reduced. In the case the campaign is failed to meet the milestones in a deadline manner or the scam is been detected the funds could be reverted back. This is a kind of approach that been used by the platform for a better implementation. [2]

C. Decentralised Crowdfunding Platform Using Smart Contract

The research work "Decentralised Crowdfunding Platform Using Smart Contract "is a decentralised crowdfunding platform that been developed in proposal to the alternative of the centralized platforms of crowdfunding platforms.

The proposed application is a decentralized crowdfunding platform based on blockchain that runs with smart contract on blockchain network. The application proposes 2 major suggestions in the model of crowdfunding.

1) KYC Based Verification

The model proposes a KYC Based verification system where the projects and the campaigns that host on the network need to do the mandatory KYC (Know Your Customer) Procedure before it been published in the main network. The KYC Documents verification provides a much more authenticity even though it doesn't make it completely immutable since fraud paper works could bypass the system.

2) Votin Based approach

Another approach that the system is taking considered is a decentralised voting-based approach. In the system the fund transfer is based on an approach of voting. The investors could be able to get a chance based on the share of the investment and a voting would be done and that particular voting would decide whether the funds should be transferred or not. If the kind of voting is able to secure a 50 % or more only then a fund transfer is been initiated. [3]

D. FarmFund: A Blockchain Based Crowdfunding Application for Farmers

FarmFund is a Blockchain based crowdfunding application for farmers proposed in the paper. In the paper the problem that they are looking to solve is the issue that the farmers face when they require founds. In the system the credit Score of the farmers is been integrated with the system and with the better credit score the investors would be able to invest in the better option available. This is how the trust is been implemented in the Platform. They are using a plasma based distributed ledger technology to the transparent transaction of funds. In the Work they had also set some preconditions for the algorithm of the credit condition and corresponding actions on the credit They Implemented the entire project using Ethereum Solidity to provide smart contract service and Front end is been done using React and to implement side chain they used Provable which reduce gas cost and improve scalability [4]

E. LikeStarter : A Smart-Contract based Social DAO For Crowdfunding

Social Media are a now a days a great medium to share the information. In the current scenario Social media is been used to sharing the life as well as contents related to their works and sometime skilled or some core areas where a smaller number of peoples are there, which mainly include arts forms. LikeStarter is a Project proposed by integrating the social media element and Crowdfunding element. Which will be hosted over ethernet network which will become a Decentralized application.

Unlike Familiar Crowdfunding application like Kickstarter and Twitch the LikeStarter uses blockchain network and Ethereum Based crypto transactions makes it a distributed publicly verifiable system where each and every transaction. The integration of social media along the application make it more trust worthy.[5]

III. PROPOSED SYSTEM

A. Propsed System Archtecture

This section provides an overview of the proposed architecture for the system in the sector. While there are existing implementations for online crowdfunding, the primary issue with these systems lies in the lack of trust and transparency in the campaigns hosted on the network. Additionally, security concerns arise due to the centralized nature of these solutions. There are also uncertainties regarding the cryptographic methods and encryption techniques employed in current implementations.

To address these challenges, the project model suggests a dynamic approach by leveraging a decentralized solution. This involves developing a Decentralized Application (DAO) that operates on the Ethereum framework. By adopting a decentralized approach, the project aims to mitigate concerns such as organizational immunity and provide public accessibility to the ledger through Distributed Ledger Technology (DLT). This innovative crowdfunding model aims to enhance trust and transparency in the process.

The Trust and Transparency is been achieved through 2 independent elements or modules working along with the main application in the main network. The Trust is been made by the integrated social media part and the transparency is been implemented using Etherscan API Where the transaction sources and the transactions of the profile is publicly available With the Implementation of the project a much more efficient model can be implemented in the aspect of crowdfunding. Which can bring a notable impact in this area Figure 3.1 is a diagrammatic representation of the proposed model in the entire model the core is the process where the process is been coordinated.

In the process the data from the Transaction Part where the actual transaction is been taking place and API is been placed for Transaction and Profile Validation. Which Ensure the Transparency Part Social Media/Blog is a Single Integrated entity which bring the trust over the campaigns are also been integrated to the same network

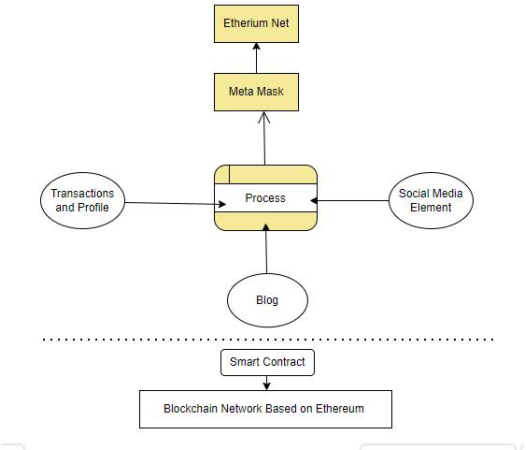


Fig 3.1: Overview of Proposed Model

The Figure 3:2 Shows how the trust and transparency elements is been integrated in the Application. The crowdfunding application is been connected with 2 interfaces which includes Meta Mask Account Manager and Social Media-Blog Element.

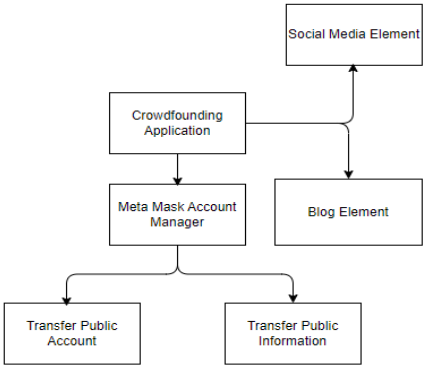


Fig 3.2: Trust and Transparency Element

The integration of the Social Media-Blog Element is aimed at ensuring trust within the system. Trust is established through posts made by the campaign runner, which are required to be related to the campaign. These posts are designed to be immutable, meaning they cannot be deleted or edited at a later stage. The inclusion of social media enhances the authenticity of the campaign, making it more convenient for individuals who wish to transfer or invest funds in a particular campaign. It also allows for easy access to previous records and activities, further bolstering trust. The Metamask profile management is integrated into the core application to promote transparency. Transparency is achieved through two main aspects: transaction transparency and profile transparency associated with those transactions.

The Profile Transaction refers to the comprehensive information associated with a profile, including the profile's creation date and the transactions that have taken place within the profile. To use the application, a public Metamask profile is mandatory, allowing the public to verify the data and ensure that the profile has not been involved in any spam or unlawful activities. Transaction transparency is a sub-module within the broader transparency framework. This component ensures that transactions are directly sent to the intended recipient, eliminating the common practice of receiving transactions in an organization's account and then redistributing them. This practice has been susceptible to a significant amount of fraud. The proposed model aims to enhance transparency and build a trustworthy network, providing a more robust framework for crowdfunding.

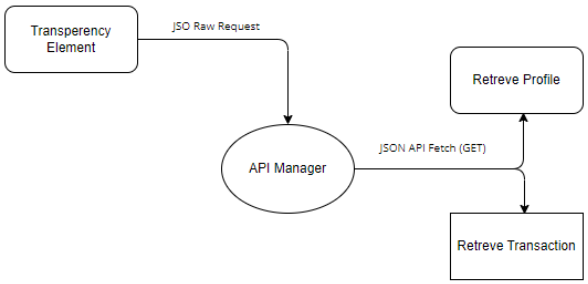


Fig 3:3 API For Transparency

Figure 3.3 provides an overview of the implemented API for transparency. The central component is the Transparency Manager, which serves as the main module responsible for handling all functionalities related to transparency. The Main module writes data to the API Manager using the JSON format. The data is sent via an API designed with the assistance of the Postman Tool. The API Manager is responsible for sorting and sending data requests to the appropriate functions. It has access to two main functionalities: Retrieve Profile and Retrieve Transaction. The Retrieve Profile function allows users to view profile information and validate the authenticity of the profile used for the campaign. On the other hand, the Retrieve Transaction function retrieves data related to transfers or transactions, including information about the sender, recipient, and other relevant details

To facilitate these API calls, the implementation utilizes the Etherscan Public API. This allows for publicly verifiable record management using Etherscan, a trusted platform in the Ethereum ecosystem.

Figure 3.4 illustrates the implementation of the API for the trust element in the proposed model and demonstrates how the implementation is carried out within specific functionalities. The Profile Manager serves as the responsible entity for ensuring trust. It sends data to the API Manager of the Profile Manager, where the request is analysed and the data is retrieved.

The API Manager has access to the social media-blog element on the platform. It fetches the data and presents it to the user, allowing them to assess the validity of the campaign. The integration of social media serves the purpose of campaign validation. The data related to social media and blog posts is stored in a blockchain network, ensuring its immutability and preventing any modifications or deletions. Users can also track the records of their own posts, which enables them to make informed judgments about the credibility of the campaign they are running on the platform. The primary objective of this integration is to establish a need for continuous follow-up and transparency.

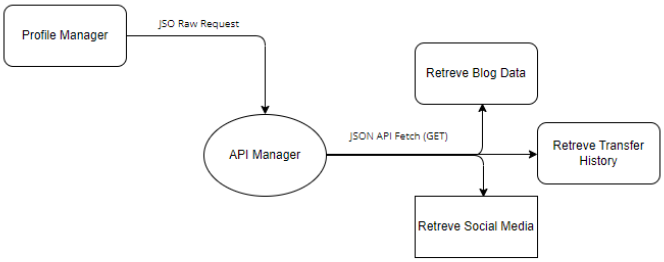


Fig 3:4 API For Trust

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations. The Entire thing is been ran over blockchain network based on Ethereum with the help of smart contract. The smart contract enables the application to be hosted over the blockchain and run seamlessly. The profile is been connected with Metamask which is an online digital valet which digitally store and enable the transaction over peer to peer networks which is been connected to the ethernet main network.

B. Implementaion Details

The Implementation details could be briefly detailed as

1) Core Crowdfunding Application

The Core Element of the project is the crowdfunding core application. It is been developed by React Application with Hardhat powered blockchain element. The entire system is been divided to 4 Native elements as follows

a) Create Campaign
b) Campaign Details
c) Campaign Support/Backing
d) Campaign List

The Create Campaign Part start with the Code Snippet described The code appears to a route configuration for a React Router. It specifies that when the URL path matches"/create-campaign", the corresponding component" CreateCampaign " should be rendered. The Page Create-Campaign is designed to push new campaigns to the Network. The Networks are been pushed to the Network and Been Added to the network using Blockchain Test Network updates on the form is been handled using the function deployed

The Function Handle Donation is doing the Donation Backing In the Project the Function deals a donate Function which will be responsible the donation. Since the function need to be executed to do the transaction the function is been written on the Script Execution

Campaign Details is been used to Fetch the Details of the Campaign on the Platform it is been implemented using Multiple Modules which is been linked with Transpercy and Trust

The getCampaigns function you provided is an asynchronous function that interacts with a smart contract to retrieve campaign data. It expects that the contract object has a call method that can be used to call the getCampaigns method on the contract.Inside the function, it awaits the result of calling contract.call("getCampaigns") and assigns it to the campaigns variable. The assumption is that this call returns an array of campaign objects.

The function then maps over the campaigns array using the map function and creates a new array called parsedCampaigns. For each campaign in the original array, it extracts specific properties such as owner, title, description, target, deadline, amountCollected, image, and pId.It uses ethers.utils.formatEther to format the target and amountCollected values from BigNumber to a more human-readable format in Ether. It also converts deadline to a number using toNumber().The code snippet renders the DisplayCampaigns component with specific props, including the title, loading state, and campaign data. These props provide customization and flexibility to the component, allowing it to display the campaign data effectively and handle loading states appropriately

2) Social Media Element

The Social Media Element is been Implemented here to bring the trust in the campaigns and each data pushed to the Element is been stored forever. The Lens Protocol is been using here to implement the Social Media element. Moralis is a development platform that provides various tools and utilities for building applications on blockchain networks. By importing the Moralis object, the code gains access to functionalities such as authentication, data querying, and smart contract interaction, enabling seamless integration with the Moralis server

Although the exact specifics of the query and the client object aren't visible in the provided snippet, it suggests that the query aims to acquire profile-related information.The subsequent line of code employs the Moralis library's start method to commence the Moralis server. The method accepts an object containing an apiKey property, which likely retrieves the Moralis API key from an environment variable (env.MORALISAPIKEY). This key is crucial for server communication with Moralis.

In summary, the getServerSideProps function performs two main tasks: it queries a GraphQL API (client.query) to retrieve profile-related data, and it utilizes the Moralis library to fetch NFTs associated with an Ethereum account. This data is likely used to generate the initial props for a Next.js page component, which will be rendered on the serverside.

3) API With Etherscan Network

The API (Application Programming Interface) serves as a communication bridge between different software applications, allowing them to interact and exchange data. In the context of the proposed model, an API implementation is utilized to enhance transparency and trust. Specifically, the implementation involves integrating the Etherscan API.

The Etherscan API provides a way to interact with the Ethereum blockchain and retrieve relevant information. To access the Etherscan API, an API key is required, which authenticates the requests made to the API. The API offers various endpoint URLs for different functionalities, such as retrieving account balances, transaction history, token transfers, and contract details.

Public API Provided by etherscan is been used in the project to deploy the Trust and Transparency part. The Proposed model uses API to fetch the profile and transaction information from the etherscan network. This information could be crossmatched prior to send the funds to a certain campaign.

IV. RESULTS AND FUTURE SCOPE

A. *Results And Conclusion*

The proposed system you described is a crowdfunding model that incorporates trust and transparency features. It includes a dedicated module to implement these functionalities. Additionally, the entire application will run on the blockchain, specifically the Ethereum framework. By utilizing blockchain technology, the system becomes decentralized, offering improved efficiency and security. The integration of Distributed Ledger Technology (DLT) further enhances the decentralization aspect of the system, reducing the reliance on centralized authorization-based networks.

Running the crowdfunding model on the Ethereum blockchain provides several benefits. Firstly, it ensures transparency by maintaining a public ledger of all transactions and activities. This transparency helps build trust among participants as they can verify the authenticity and integrity of the information. Additionally, since the blockchain is immutable, once a transaction is recorded, it cannot be altered or tampered with, further enhancing the system's transparency and trustworthiness.

Moreover, using a decentralized application (DApp) architecture brings greater efficiency to the crowdfunding process. With a decentralized network, there is no single point of failure or bottleneck, reducing the risk of system downtime or data loss. The distributed nature of the blockchain ensures that transactions can be processed quickly and securely, eliminating the need for intermediaries and reducing associated costs.

The model provides much more efficient way of peer to peer transaction than the existing solutions of Crowdfunding provides since it uses cryptocurrency and can be proceeded without the help of an 3rd party banking services. And with the running on Blockchain network the application will have a high up time that of the traditional as well as it would be have better security advancements. The model proposed is a great intact in light of integrating trust and transparency in the crowdfunding.

In Summary a model of incorporating trust and transparency is been developed and Implemented. The System is also able to provide much security and been deployed in a decentralized manner , Makes it a model that could be more sustainable in terms of a cyber-attack.

B. *Future Scope*

The model could be used as a base model for further development of crowdfunding platforms from a point of view of integrating trust and transparency. The same platform could also be used to integrating various enhancements in financial sectors which includes concepts like programmed currency and CBDC (Central Bank Digital Currency). The security provided with the blockchain network along with the internal security measurements could make the application more sustainable in further

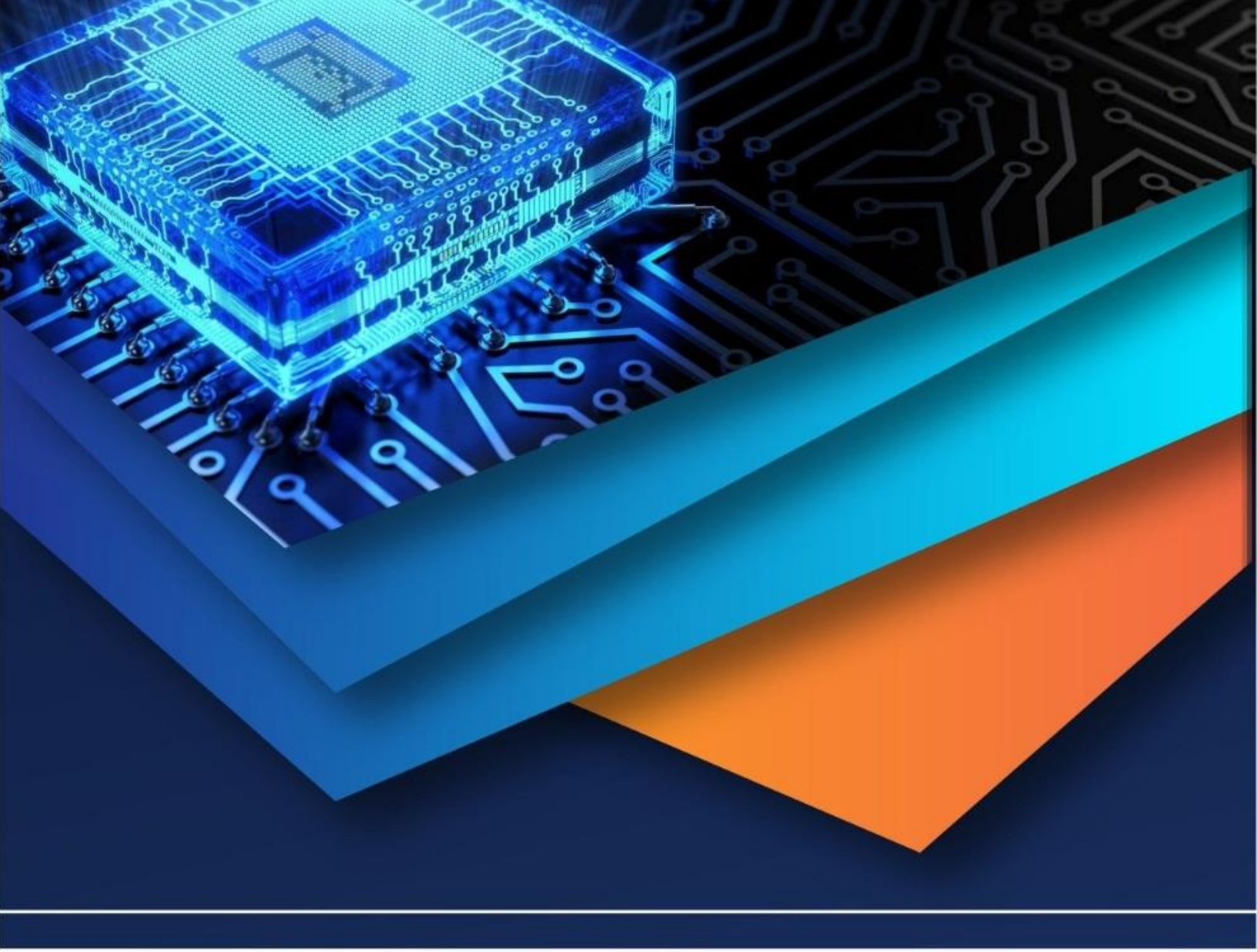
V. ACKNOWLEDGMENT

We would like to recognize all the researches who worked with the team. We also want to recognize Contributions of Saru S, Archana V S, Anaswara Narayanan, Vinaya P B, Akshay Kumar C R and Druvika S Nair throughout the Project. We also want to acknowledge our sincere thanks to all our Friends, On Teaching Staff and Colleagues of ICCS Family and APJAKTU University

REFERENCES

[1] Sayyam Gadha,Akash Dhuri ,Denish Jain ,Smita Bansod and Dhanshree Toardmalee “Blockchain -Based Crowdfunding :A Trust Bulding Model” 2021 AIMV IEEE
[2] Viren Patil,Vasvi Gupta and Rohini Sarode Blockchain Based Crowdfunding Application 5th International Conference on I SMAC
[3] Umit Cali,Ugar Halden,Marthe Fogstad Dynage and Alekshandra Sasa on Blockchain -Enabled Equity Crowdfunding for Energy Storage Investment
[4] Sujaritha M,Shumugapriya S,Arun Bharath S,Indrajith K,Haritharam S “Decentralised Crowdfounding Platform Using Smart Contract”
[5] Rashmitha S,Sanjay H A,K Aditya Shastry,Jaya Shree Lakshmi K FarmFund – A Blockchain Based Crowdfunding App For Farmers,2021
[6] Mirko Zichichi, Michele Contu, Stefano Ferretti, Gabriele D’AngeloM. Titile “ LikeStarter : A Smart Contract Based Social DAO For Corwdfunding”,2022
[7] Mithsara W.K.M., Jinasena T.M.K.K ,” Blockchain-based Distributed Secure Crowdfunding and Decision-Making Platform for Large-scale Business Projects in Public and Private Sectors” Vol 4,No 5 2020 Europian Modersn Studies Journal
[8] Tittled “Fundraising Portal using Smart Contracts in Blockchain using Group Signatures” M. V. Ranjith Kumar, Arpit Shukla, Saket Agarwal International Journal of Engineering and Advanced Technology (IJEAT)ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020
[9] “Research On the Application Model of Public Welfare Crowdfunding Based On Blockchain Technology “ Work by Ye Fan,Chen Ao,Liang Jingren ,2021 2nd Intenrational Confernece on E Comerence and Internet Technology(ECIT)

[10] Md Ratul Amim,Megat F Zuhairi Titile" Crowdfunding Smart Contract Security and Challenges" ,IJCSE Vol 2 No 1 Feb 2021
[11] Tharaka Mawanane Hewa ,Yining Hu,Madhusanka Liyanage,Salil S. Kanhare4,And Mika Ylianttila Paper Tittled "Survey on Blockchain-Based Smart Contracts:Technical Aspects and Future Research" IEEE Acess 2021
[12] Security, Performance, and Applications of Smart Contracts: A Systematic Survey Sara Rouhani And Ralph Deters,IEEE Acess 2019
[13] A Massive Analysis of Ethereum Smart Contracts Empirical Study and Code Metrics by Andrea Pinna,Simona Ibba1,Gavina Baralla,Roberto Tonelli And Michele Marchesi
[14] Etherscan (etherscan.io) And Docs



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY