Grenze International Journal of Engineering and Technology, Jan Issue

Crowdfunding System based on Blockchain

Rashmi Jain[1], Hrushikesh Panchabuddhe[2], Amaan Ranapurwala[3], Aniruddha Kate[4] Atharva Gaikwad[5], Harsh Maroo[6] and Yash Mishra[7]
[1-7]Department of Computer Science and Engineering, S.B. Jain Institute of Technology, Management and Research, Nagpur
Email: rashmijain@sbjit.edu.in, hrushikeshpanchabudhe@sbjit.edu.in, amaanr.csed19@sbjit.edu.in, aniruddhak.csed19@sbjit.edu.in ,atharvag.csea19@sbjit.edu.in, harshm.csed19@sbjit.edu.in, yashm.csed19@sbjit.edu.in

***Abstract*— Blockchain was first only utilized to support cryptocurrencies, but as time passes, more and more industries are embracing this new technology. Several other crypto currencies started to emerge piecemeal from bitcoin. With the use of blockchain technology and smart contracts, Defy Systems increases the power of websites. Blockchain is expected to be used as an efficient method of conducting online transactions as technology matures. One of the diligences to which blockchain technology may be applied is crowdfunding sites. A brand-new and cutting-edge method for funding many kinds of bets is crowdfunding, in which the bets' individual writers can ask for money. With the advent of the internet and social media, new platforms emerged. For charitable organizations and business owners looking to grow their wealth, the internet and social media are crucial. In this study, it is proposed as a cutting-edge hybrid blockchain crowdsourcing platform called CrypFunds to further explore the benefits of merging blockchain and crowdsourcing. Cryptocurrency donations, whether they are made to a political party or an association, are frequently accepted in the Contributions in cryptocurrencies can give organizations access to a new group of implicit philanthropists who would rather give via blockchain than some of the more conventional methods that might enable them to avoid capital gains taxes.**

***Index Terms*— Blockchain, Solidity, Web3, Web3.eth, Goerli testnet, Infura, Next.js, React.js, Crowdfunding, donation, Web development**

I. INTRODUCTION

Crowdfunding has become a popular means of gathering funds for various projects, causes, and individuals in need, and its usage has surged in response to the COVID-19 pandemic. Crowdfunding enables people or organizations to request support from a broad audience through accessible and user-friendly platforms. This method of fundraising can be especially effective for small-scale initiatives and social movements that lack access to traditional sources of funding. However, the success of a crowdfunding campaign is dependent on various factors such as campaign quality, supporter network size, and overall economic conditions. To maximize the chances of success, it's essential to have a well-defined plan and strategy in place

The objective was to address the primary issues with the existing crowdfunding platforms, which include:

As the amount of funds being transferred electronically grows larger, the need for heightened security measures becomes increasingly crucial. Although stringent protocols such as symmetric encryption are in place to ensure safe and secure e-payments, they are still vulnerable to hacking. In contrast, blockchain technology has yet to be compromised, which makes it a highly secure option for protecting large sums of money.

Crowdfunding scams have become prevalent and pose a serious threat, as it's often challenging to track the

Grenze ID: 01.GIJET.10.1.308

utilization of funds. To tackle this issue, the project aims to introduce complete transparency in the flow of funds at every stage of the process. By doing so, it can eliminate any chance of financial misuse and assure donors that their money is being utilized appropriately.
Country-specific crowdfunding platforms can create barriers for people in other countries who wish to contribute to campaigns. By leveraging blockchain technology, individuals from anywhere in the world can conveniently participate in crowdfunding campaigns, enabling a more global and inclusive fundraising approach.
While blockchain technology was initially developed as a foundation for cryptocurrency, it has now emerged as a versatile and innovative technology that is being adopted across various industries. Blockchain technology is expected to be widely adopted across various industries in the future, particularly for online transactions due to its efficiency.
Crowdfunding platforms are one such area where blockchain can be leveraged.
The prevailing issue with crowdfunding globally is that campaigns are largely unregulated, leading to fraudulent activities. Additionally, some campaigns fail to deliver their promises, resulting in significant project delays. The goal of this project is to address the issues with crowdfunding by integrating Ethereum smart contracts into the platform. This approach enables automated execution of contracts, which helps to prevent fraudulent activities and ensures timely completion of projects.
The Goals would be to combine the advantages of blockchain, and formalize a decentralized funding framework named CrypFunds, to design a Payment gateway that supports multiple currencies, Creating Progress meter to easily track campaign progress, Providing Secure mobile options to best reach your audience.

II. Literature Survey

Maryani, A. S. Perbangsa and T. Udiono, "The Model of Web-based Crowdfunding Platform," 2020 International Conference on Information Management and Technology (ICIMTech), 2020. Crowdfunding allows people to invest with a joint scheme on a project or business that is not included in the stock exchange list. With a joint scheme, investors can buy a portion of project or business ownership with a relatively small nominal purchase. However, investors need tools to facilitate the search and purchase of projects or businesses that match their character. This research is intended to design a Web-based Crowdfunding Platform model that suits the needs of investors. This study uses the questionnaire method to obtain investor information requirements data. As for model designing, this study employed the Object-Oriented Analysis and Design (OOAD) method, and used notation from the Unified Modeling Language (UML) standard. The result of this study is a Web based Crowdfunding Platform model that facilitates investors to choose and arrange investment portfolios that are appropriate to their preferences
V. Patil, V. Gupta and R. Sarode, "Blockchain-Based Crowdfunding Application," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2021. Initially, blockchain is only used as a foundation of cryptocurrency, but today, we can see the rise of this new emerging technology are being implemented in many industries. In the future, most technologies around the world are expected to use blockchain as an efficient way to make online transactions. One of the areas that blockchain technologies can be applied is crowdfunding platforms. The most common problem with current crowdfunding scene in around the world including is that the campaigns are not regulated and some of the crowd-funding campaign turned out to be fraud. Besides, the completion of some projects also was significantly delayed. This project aims to solve these problems by applying Ethereum smart contracts to the crowdfunding site to that the contracts will be fully automatically executed, thus preventing frauds and ensuring that the projects can be delivered within duration given.
Abel's Eileen G., Marilyn Domas White and Karla Hahn. "A user-based design process for Web sites." OCLC Syst. Serv. 15 (1998): 35-44. This paper reports on Phase II of a two-part project to identify and implement user-based design criteria in World Wide Web sites. The test site is a Web page for the academic business community. As an alternative to existing, largely ad hoc design processes, the authors developed a user-based design process, gathering user input at three different times in the process. Delineating this four-stage process (information-gathering; development; test and evaluation; and implementation) is a major focus of the paper. In addition to explaining the process in detail, the paper reports on the second stage of this process, which involves operationalizing definitions of the criteria and translating the criteria into Web page features and, to some extent, on the evaluation activities undertaken during Stage 3. Already reported are the results of Stage 1, which gathered user criteria for evaluating Web sites through a focus group session.
N. Agrawal, R. Ananthanarayanan, R. Gupta, S. Joshi, R. Krishnapuram and S. Negi, "EShopMonitor: A Web content monitoring tool. Data presented on commerce sites runs into thousands of pages, and is typically delivered from multiple back-end sources. This makes it difficult to identify incorrect, anomalous, or interesting data such

as $9.99 air fares, missing links, drastic changes in prices and addition of new products or promotions. We describe a system that monitors Web sites automatically and generates various types of reports so that the content of the site can be monitored, and the quality maintained. The solution designed and implemented by us consists of a site crawler that crawls dynamic pages, an information miner that learns to extract useful information from the pages based on examples provided by the user, and a reporter that can be configured by the user to answer specific queries. The tool can also be used for identifying price trends and new products or promotions at competitor sites. A pilot run of the tool has been successfully completed at the ibm.com site.
L. Liu, C. Pu and W. Han, "XWRAP: an XML-enabled wrapper construction system for Web information sources," Proceedings of 16th International Conference on Data Engineering The paper describes the methodology and the software development of XWRAP, an XML-enabled wrapper construction system for semi-automatic generation of wrapper programs. By XML enabled we mean that the metadata about information content that are implicit in the original Web pages will be extracted and encoded explicitly as XML tags in the wrapped documents. In addition, the query-based content filtering process is performed against the XML documents.
The XWRAP wrapper generation framework has three distinct features. First, it explicitly separates tasks of building wrappers that are specific to a Web source from the tasks that are repetitive for any source and uses a component library to provide basic building blocks for wrapper programs. Second, it provides a user-friendly interface program to allow wrapper developers to generate their wrapper code with a few mouse clicks. Third and most importantly, we introduce and develop a two-phase code generation framework.

III. Block Chain

Blockchain is a technology that uses a decentralized, distributed ledger to store records of transactions and data in a secure and open manner. The blockchain network is maintained and transactions are validated by all participants who each have a copy of the blockchain, without any central authority or point of control. The technology is secure as changing one block in the chain would entail modifying every following block, which is impossible.
The concept of blockchain-like systems was proposed as early as 1982 by David Chaum, and further work on a chain of blocks that was cryptographically secured was conducted in 1991 by Stuart Haber and W. Scott Stornetta. The blockchain structure consists of interconnected blocks, each containing a collection of transactions or other pieces of information that are independently validated by the network's nodes. All participants in the network have access to the distributed ledger and its unalterable record of transactions.
All network participants have access to a distributed ledger and its unchangeable record of transactions. When a transaction takes place, it is recorded as a block of data containing various details, including who initiated the transaction, what was exchanged, when and where it happened, and the amount involved. These blocks are interconnected to form a chain of data that secures the sequence and timing of transactions, preventing any block from being modified. The addition of each new block enhances the verification of previous blocks and the overall blockchain, making it tamper-evident and guaranteeing immutability. Blockchain has a wide range of potential applications beyond finance, such as supply chain management, voting systems, and identity verification.

A. History of Blockchain

David Chaum proposed a blockchain-like system in his thesis in 1982, and in 1991, Stuart Haber and W. Scott Stornetta described a chain of blocks that were cryptographically secured to prevent tampering with document timestamps. The design was improved in 1992 by Haber, Stornetta, and David Bayer, who introduced Merkle trees to aggregate multiple document certificates into a single block. Since 1995, The New York Times has been issuing document certificates through Surety, a firm that uses blockchain technology.

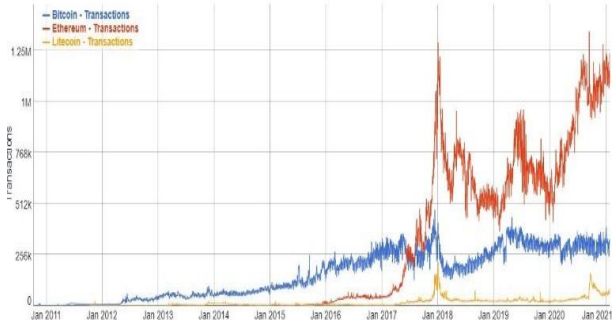

Fig 1. Bitcoin, Ethereum and Litecoin transactions per day (January 2011 – January 2021)

B. Structure and Design of Blockchain

A decentralized network of peers and a distributed timestamp server independently manage a blockchain database. This type of system is able to provide strong security measures due to the collaborative efforts of participants who have a shared interest. Once deployed, a blockchain database ensures that digital assets cannot be endlessly reproduced, and eliminates double-spending by verifying that each unit of value has been transmitted only once. This technology is commonly referred to as a means of exchanging value. Furthermore, a properly constructed blockchain can be used to establish ownership rights, as it creates a record that documents the offer and acceptance of a trade agreement.

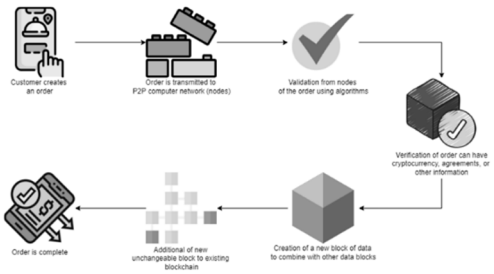

Fig 2. Blockchain Model

Fig 3. The primary chain, depicted in black, comprises the longest sequence of blocks from the genesis block in green to the current block. Any blocks that are not part of the primary chain are known as orphan blocks, shown in purple.

C. Key Elements of Blockchain

a. Distributed ledger technology

The entire network can access the distributed ledger and its unalterable record of transactions. By utilizing this shared ledger, there is no need for redundant record-keeping, which is commonly found in traditional corporate networks.

b. Immutable records

After a transaction has been included in the shared ledger, it cannot be modified or tampered with by any participant. If there is an error in a transaction record, it can only be rectified by adding a new transaction to the ledger, and as a result, both the incorrect and corrected transactions will be viewable.

c. Smart contracts

On a blockchain, a collection of directions known as a smart contract is stored and executed automatically to facilitate transactions. These contracts can establish conditions for the transfer of corporate bonds, define the amount required for purchasing travel insurance, and have many other applications.

D. Working of Blockchain

a. As each transaction occurs, it is recorded as a "block" of data

These transactions demonstrate the transfer of a physical or digital asset, which can include tangible items like products or intangible assets such as intellectual property. The data block on the blockchain can record a variety of information, including the identity of parties involved, the type of asset being transferred, the time and location of the transfer, the quantity or amount of the asset, and even additional details like the temperature or condition of a product during shipment.

b. Each block is connected to the ones before and after it

As an asset is transferred or changes ownership, the data is recorded in a chain of blocks. This creates a sequential record of transactions with exact times and order. The blocks are interlinked in a secure manner to prevent any alteration or insertion of a block between two existing ones.

c. Transactions are blocked together in an irreversible chain: a blockchain

The integrity of the blockchain is fortified with each new block, resulting in a tamper-evident system with an immutable nature. This eliminates the potential for malicious parties to interfere with the data, generating a ledger of transactions that you and other members of the network can rely on.

IV. PROPOSED WORK

There are two modules, Admin and Donators\Fundraisers. Investors needs to fill in details like description of campaign, target amount and minimum contribution. This detail is registered on the network along with the campaign. Only Admin can withdraw funds to the desired wallet when the finds requirements are met and consciences are passed. The flow shifts smoothly between the investors\donators which has been shown in fig 4.

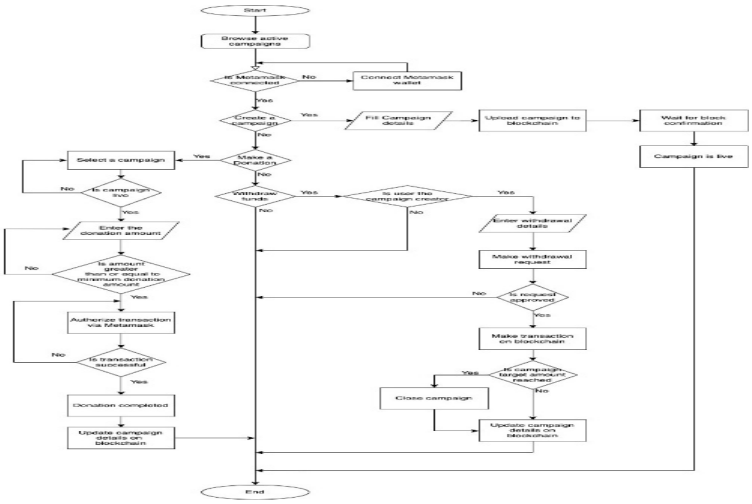

Fig. 4. Flowchart for CrypFunds

V. FUNCTIONAL MODULES

There are multiple functional modules that play their own in the system parts:

1) *Campaign Creators*: These are the users who have created a Campaign.
2) *Contributors & Approvers*: Contributors are the users who contribute and fund the campaigns. Approvers are Contributors who have contributed more than the Minimum Contribution, and they can approve the withdrawal requests.
3) *Creating a Campaign*: Similar to real-world crowdfunding and other crowdfunding platforms, it is possible for anyone to create a campaign on this platform within a matter of minutes. The information regarding the campaign is managed by a smart contract based on Ethereum, ensuring that it remains immutable and cannot be modified.
4) *Contributing to a Campaign*: Once a campaign has been created, users can share the campaign and anybody can contribute to the campaign. The funds will go to the address of the campaign and not to the creator of the campaign, thus making the process more efficient and anti-fraudulent.
5) *Withdrawal of Funds*: The person who initiates a fundraising campaign can suggest a Withdrawal Request specifying how the funds should be used. People who donate an amount greater than a certain threshold are considered as approvers and have the ability to accept or reject the request. Approval from at least 50% of approvers is required to withdraw the funds.

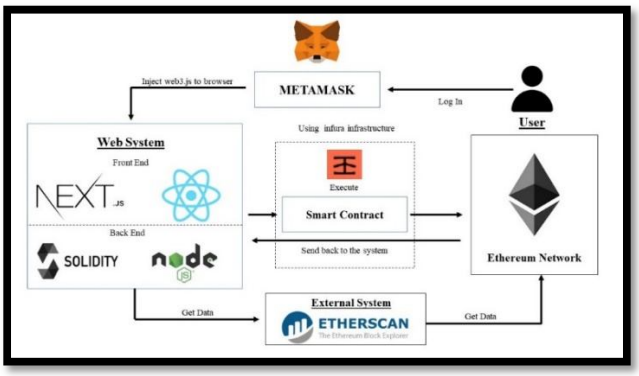

Fig. 5. System Architecture of CrypFunds

VI. RESULT

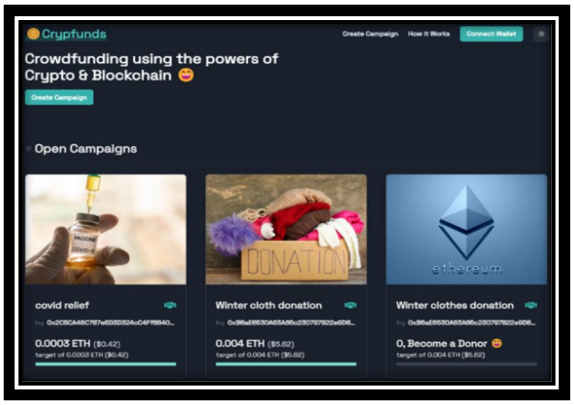

Fig. 6. Home Page

This is the home page of the website. It contains hyperlinks to various sections of the website such as Active Campaign, how it works and Create Campaign. User can continue as a guest if they don't want to connect wallet and authorize to the app. This is the homepage of the app and it also has information about current campaigns in brief. This helps new user to see all the running campaigns on the blockchain based decentralized Crowd funding app. There is also step by step demonstration of how app works in a section of this page. This page also has a hyperlink button which takes user to the new campaign page where user can create his own campaign.

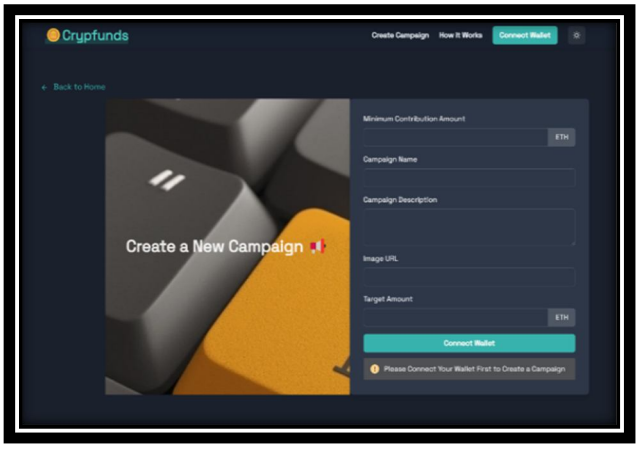

Fig.7. Create Campaign Page

This is the Create Campaign page of the website where in user can create his own campaign for raising funds and it will be run on blockchain. User needs to connect his metamask wallet to authorize his wallet address with the website in order to further proceed with creation of the campaign. User needs to enter following details in order to create campaign:

- Minimum contribution allowed
- Campaign Name
- Campaign Description
- Target Amount

In fig 8. you can see all the details related to the campaign such as the total amount of money collected, how many people have contributed and more are displayed. It also shows the minimum contribution, number of donators. The page also has a functionality of showing the user how much progress has been made in the campaign for the user to get the better idea of the campaign. After seeing all the details user can verify the can finally donate to the campaign with the desired amount in ether.

There is also an option to check the withdrawal requests that are already in place and new ones can also be created.

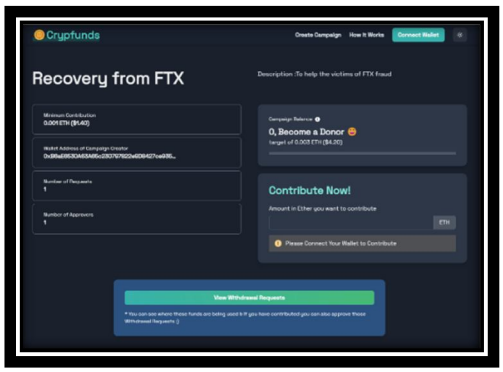

Fig.8. Campaign Page

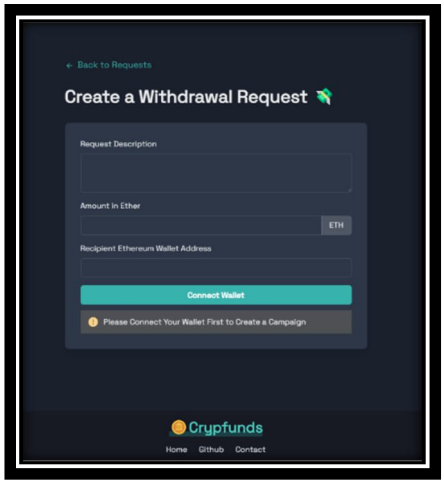

Fig 9. Withdrawal Request Form

By this Form the admin of a particular campaign can create a withdrawal requesting, that he/she be using some particular amount of money for a cause. User has to mention his wallet address. The validation of the wallet address is done with the admin wallet address. User has to specify the description, as in the purpose of the campaign.

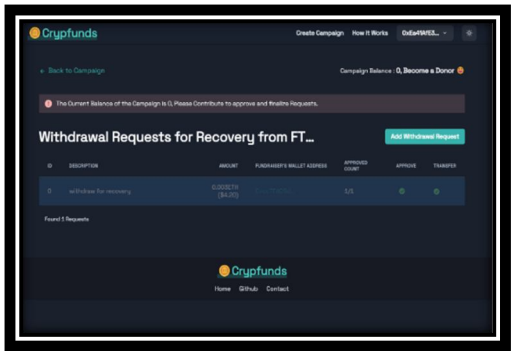

Fig 10. Withdrawal Requests

In Fig 10, you can see the no of withdrawal request that are opened by the admin. This project has used the consciences algo where if the majority of the contributors accept the request, then only the admin can receive the amount requested. All the requests that are made are shown on this page to maintain the transparency of the projects and campaigns. The amount won't be transferred unless it's been verified by minimum number of votes and those votes can also be tracked.

In Fig 11, Wallet is connected to the website and now it can handle all the transactions. The metamask integration with the projects works as expected and user has to switch the network to testnet in order to test the project. For development purposes have used Ethereum testnet.

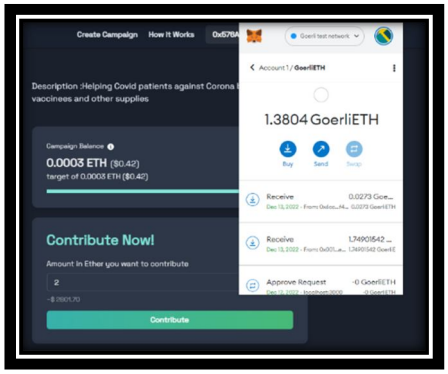

Fig 11. Integration of Wallet

VII. Application

Decentralization: Block-chain is decentralized; thus, it doesn't depend on any other platforms to generate money. To begin with, there are no longer any regulations to follow, any project may be made visible and supported if investors choose to do so, and by doing away with fees, crowdsourcing becomes more affordable for creators.
Access Equity: Asset tokenization is a key component of blockchain's equity or ownership distribution system. For instance, a person who intends to grant tiny ownership stakes in the company and develop a number of new goods with the incoming money. This might provide a whole new universe of opportunities.
Universal Opportunity: Anyone with an internet connection can contribute to projects based on blockchain, allowing every initiative to receive funding.
Flexible Options: Utilizing asset tokenization on the blockchain gives creators and business owners more freedom. Asset tokens typically have their own currency so that businesses may employ experts and advertisements.
Peer-to-Peer: The use of a peer-to-peer network facilitates the exchange of cryptocurrency, which can be beneficial for investors and contribute to overall excitement surrounding the process.

VIII. Conclusion

The project is fully designed as a platform in which proper engineering knowledge has been applied. Conventional crowdfunding methods have long suffered from lack of transparency and fraud; with help of problem analysis, it was seen that it is an avoidable problem, and implemented a solution that can do away with these long-standing problems with help of modern tools usage such as solidity and web3. The project is applied with algorithms and knowledge to analyze the social problems in crowdfunding and provide a modern engineering solution. Then designed the application in two modules, investigated the available application to find out the new solutions and updates. The aim to have a transparent, anti-fraudulent, decentralized platform and environment has been achieved to a great extent. The project is implemented with proper team work and industry level standards have been maintained. This project has covered the weak points of general crowdfunding platforms to provide transparency to the process of crowdfunding and build trust among society by ethical practices and transparency, so that they may contribute their wealth to good ethical causes without fear of fraud.

References

[1] Li, Ming & Weng, Jian & Yang, Anjia & Lu, Wei & Zhang, Yue & Hou, Lin & Jia-Nan, Liu & Xiang, Yang & Deng, Robert. (2018). CrowdBC: A Blockchain-Based Decentralized Framework for Crowdsourcing. IEEE Transactions on Parallel and Distributed Systems. PP. 1-1. 10.1109/TPDS.2018.2881735.
[2] S. Zhu, Z. Cai, H. Hu, Y. Li and W. Li, "zkCrowd: A Hybrid Blockchain-Based Crowdsourcing Platform," in IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4196-4205, June 2020, doi: 10.1109/TII.2019.2941735.
[3] S. Wang, A. F. Taha, J. Wang, K. Kvaternik and A. Hahn, "Energy Crowdsourcing and Peer-to-Peer Energy Trading in Blockchain-Enabled Smart Grids," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 8, pp. 1612-1623, Aug. 2019, doi: 10.1109/TSMC.2019.2916565.
[4] Maryani, A. S. Perbangsa and T. Udiono, "The Model of Web-based Crowdfunding Platform," 2020 International Conference on Information Management and Technology (ICIMTech), 2020, pp. 957-961, doi: 10.1109/ICIMTech50083.2020.9211136.
[5] Hassija, Vikas & Chamola, Vinay & Zeadally, Sherali. (2020). BitFund: A Blockchain-based Crowd Funding Platform for Future Smart and Connected Nation. Sustainable Cities and Society. 60. 102145. 10.1016/j.scs.2020.102145.

[6] DeVries, Peter. (2016). An Analysis of Cryptocurrency, Bitcoin, and the Future. International Journal of Business Management and Commerce. Vol. 1. Pages 1-9.
[7] Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.
[8] Vujičić, Dejan & Jagodic, Dijana & Ranđić, Siniša. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. 1-6. 10.1109/INFOTEH.2018.8345547.
[9] Hewa, Tharaka & Hu, Yining & Liyanage, Madhusanka & Kanhare, Salil & Ylianttila, Mika. (2021). Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research. IEEE Access. 10.1109/ACCESS.2021.3068178.