IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Blockchain Based Crowdfunding Platform usingEthereum

Sheetal Phatangare
Department of Computer Engineering,
Vishwakarma Institute of Technology,
Pune, India
sheetal.phatangare@
vit.edu

Sahil Patil
Department of Computer Engineering,
Vishwakarma Institute of Technology,
Pune, India
sahil.patil20@vit.edu

Shivendra
Patil
Department of Computer Engineering,
Vishwakarma Institute of Technology,
Pune, India
shivrendra.patil20@
vit.edu

Yadnesh Patil
Department of Computer Engineering
Vishwakarma Institute of Technology,
Pune, India
yadnesh.patil20@vit.ed
u

Praharsh
churi
Department of Computer Engineering
Vishwakarma Institute of Technology,
Pune, India
praharsh.chur20@vit.
edu

***Abstract* - At first, blockchain was solely utilised as the basis for cryptocurrencies, but as time goes on, we are witnessing the adoption of this brand-new, rising technology across a range of businesses. Blockchain is anticipated to be used by the majority of technology as an effective method of conducting online transactions in the future. One application for blockchain technology is in crowdfunding sites. The biggest problem with the current global crowdfunding industry is that campaigns are not regulated and some of them have proven to be fake. Additionally, some projects have been considerably delayed in their completion. By integrating Smart contracts into the crowdfunding platform, enabling the contracts to be fully automated, eliminating fraud, and other concerns, this project aims to address them.**

Keywords— Blockchain, crowdfunding, Ethereum; smart contracts, metamask.

I. INTRODUCTION

Blockchain technologies are the best platforms for fund-raising efforts since they can represent value as blockchain - enabled assets. Investors can quickly support new projects in a safe and effective way. Crowdfunding on the blockchain canhelp to accelerate the investment process and reduce time to market. Additionally, the procedure is made accessible to many sorts of investors, allowing them to access the fund-raising process. Due to such elements, blockchain-based crowdfunding may be an efficient way to finance insurance policies. Transparency is another additional benefit of using blockchain technology. Owners of cyber-insurance policies (and other interested parties) may have unrestricted access to immutably stored data, such as details on premiums, claims, or profits. Transparency encourages equality and trust, which improves public's opinion of the cyber-insurance industry, which is frequently portrayed as untrustworthy.

Crowdfunding is the practice of collecting money for a project or campaign through a group of people rather than through established entities such as banks or loan providers. Crowdfunding, as defined by Freedman and Nutting [8], is a way of supporting or capitalising a well-known organisation by obtaining numerous little contributions using an internet funding platform. Contributors, the crowdfunding platform, and project management made up the core group of participants in the crowdfunding campaign.

The main advantage of crowdfunding is that it can increase the necessary funds in a short period of time. This is because many people these days use the Internet and social media, which means that the project owner can reach out to the public in a small amount of time through these networks. Furthermore, because it is more difficult to obtain loans from banks or other shareholders, many project creators have turned to crowdfunding to raise funds for theirprojects. This occurs because most loans take a long time to process. According to some studies, there are non-financial benefits to crowdfunding.

Crowd funders, for example, can provide valuable participation and responses to the project while also increasing publicity and public awareness of the company. According to Schlueter [4] there are two primary benefits to crowdfunding. The first advantage is that crowdfunding allows for better competitions between inventors and funders from all over the world. The second advantage is that investors have access to additional details during the project's early stages. This data is extremely valuable to investors and may increase their desire to invest in such crowdfunding projects.

Moreover, despite their numerous advantages, crowdfunding platforms have numerous flaws that must be addressed. Fraud cases have been one of the major issues in conventional crowdfunding platforms. According to studies, online crowdfunding exposes contributors to fraud because traditional legal and reputational security measures may not work. Researchers have identified the following crowdfunding issues: 1) the rewardsare significantly delayed 2) After an unmet delivery date, campaign organizers stop communicating with their backers

for more than six months, or 3) the promised product isnever delivered, and the backers are not fully refunded.

By incorporating smart contracts into a crowdsourcing system, we can establish a contract that will hold onto a contributor's funds until a specific deadline or objective is achieved. Depending on the conclusion, the money will either be handed to the project owners or safely returned to the contributors.

II. Literature Survey

A literature survey was done by surveying research papers. The limitations and knowledge gained from the papers will help us to create a better system. It include the limitations of the existing work and briefly explain how our ideas are advantageous over the existing ones.

Applications of Blockchain in Crowdfunding Zhao Hongjiang et al [12] presented The Applications of Blockchain Technology in Crowdfunding, proposing the idea of combining Blockchain technology with Crowdfunding which can provide efficiency and ensure security by eliminating other intermediary Crowdfunding platforms. The usage of blockchain technology in crowdfunding might be the foundational technology to address the majority of the apparent difficulties of current crowdfunding contracts over the other technologies. Crowdfunding contracts are conducted online using a variety of technologies. The use of blockchain technology in crowdfunding contracts might offer the much-needed remedy to the problems associated with abuse, trust, and secrecy in the industry.

Blockchain Based Crowdfunding Md Nazmus Saadat et al [15] proposed a Blockchain based crowdfunding system where the fundraisers will receive money from the blockchain based on the voting approval of the investors. The fundraiser can create the campaign and the investors can contribute to the campaign. In order to specify how the funds raised will be utilised, the fundraisers may also create requests. The donors cast a vote for or against the request, determining whether the costs are appropriated. Money will be paid to the vendors in the form of ether if it is authorised by the majority of supporters. A smart contract is used to do this, and it will handle the ether transaction between fundraisers, investors, and vendors. The system has a network connection to Ethereum. Users' transactions are encouraged in this system via the use of a proof-of-authority blockchain called the Rinkeby network.

Venturing Crowdfunding Using Smart Contracts Page 6 Vikas Hasijja [16] proposed Venturing crowdfunding using Smart Contracts in Blockchain, a base paper which speaks about the advantages of integrating crowdfunding technique with blockchain. It first explains about the different types of crowdfunding and then why crowdfunding using Blockchain stands out from the other types of crowdfunding. Crowdfunding is a way of raising money from a large number of individual investors. The investors who invest in a campaign can gain their profit if that campaign gets successful. But still in certain crowdfunding platforms, they receive money from investors and run away with a chunk of money. In order to build trust between the investors and the platforms, a Smart contract is introduced. And the Smart contract automates the transactions which removes the need for a manager to handle this process. Blockchain thus solves the problem of spending more on a campaign as there is no need for any central or trusted authority. Due to the decentralised nature of blockchain, no one can manage smart contracts, which makes them transparent to all users. Each phase of the project may have a different number of expenditure requests created by the campaign owner. Each expenditure proposal can be supported by a majority vote of the investors. Therefore, the developers will receive the funds promised in the expenditure proposal. A spending proposal is approved if it receives the votes of the majority of the donors. If not, the budgetary proposal will have to wait. Thus, a campaign may effectively launch its items when all expenditure requirements have been fulfilled.

Crowd-funding Campaigns With Machine Learning An increasing number of new entrepreneurs use online crowd-funding for funding their start-ups. Different factors have been examined through which campaign success can be measured (pledged amount vs. goal, number of backers), and thus distinct factors and features that determine campaign success. The aim of this work was to define the success factors for crowd-funding campaigns by using artificial intelligence (AI) techniques, such as machine learning which was proposed by Lorenzo Grassi [1]. Kickstarter website is an online platform for crowdfunding and has datasets over thousands of campaigns. The investigated influencing factors were classified into three different categories (descriptive, financial and linguistic). The descriptive category includes data that describe aspects of the campaign itself, such as the length of the campaign's funding round, the number of updates the campaign posted, the weekday it launched, the category that it was a part of, and the number of comments made on the campaign. Additionally, they have examined two different parameters of success as dependent variables. The Feature extraction process drops the unnecessary features which are not related to the campaign success. The predictor model was found to predict campaign success with high performance.

Long-term Study of Crowdfunding Platform: Predicting Project Success and Fundraising Amount Most of the research papers are based on Kickstarter platform because it is the biggest crowdfunding site. But there is no research paper studying the entire data yet.

Crystals – Kyber Page 7/34 CRYSTALS - Kyber, a CCA-secure module-lattice-based KEM that introduces the Kyber Lattice-based Cryptography approach, was suggested by Joppe Bos et al [4]. Kyber is a collection of post-quantum cryptographic primitives centred on a key-encapsulation mechanism (KEM) that is based on module lattice hardness hypotheses. By using a modified version of the Fujisaki-Okamoto transform, a CCAsecure KEM was built and a public-key encryption strategy that is CPA-secure was presented. The new construction's key and ciphertext sizes are roughly half that of the old one, the KEM provides CCA rather than just passive security, and the security is based on a more flexible and broad lattice problem.

Noninteractive Zero Knowledge Proof System Zero Knowledge Proof, according to Hasnan Baber [3], is a crucial area of computational complexity theory and cryptography. There is only one message transmitted from the prover to the verifier in the Zero Knowledge Proof (ZKP) system. The method proposed in this work takes use of cryptographic techniques to enable several parties to validate the veracity of a piece of information without having to reveal the data that makes it up. a group of technologies that make it possible to verify information without revealing the supporting evidence. This paper covers and analyses the fundamental ideas of the noninteractive zero knowledge proof system in detail, and it also provides a summary of the research advancements made by this system.

III. BLOCKCHAIN AND SMART CONTRACT

The widespread adoption of blockchain technology is a result of its capacity to offer security and transparency. Blockchain stores transaction histories using a distributed ledger. In this scenario, updating records is done by consensus, which necessitates the consent of all nodes, and all network members share the same documentation rather than having individual copies. Additionally, because data is stored across a network of computers rather than on a single server, blockchain offers greater security. Blockchain has the potential to remove errors and spot fraudulent conduct since it

can provide a public record across numerous untrusted parties.By offering a thorough history record, a decentralized digital repository can independently check the legitimacy of clients, policies, and transactions (such as claims). As a result, insurers would be able to spot transactions that were repeated or involved dubious parties. First-movers in the insurance industry are already looking at using blockchain to reduce fraud and the dangers involved in cross-border transactions and currency exchanges. In specialised reinsurance and insurance markets, wherein insurers are usually far from the end customers, blockchain may be utilised to reduce the enormous inefficiency, gaps, and errors brought on by poor data quality in both the front and backend offices.

The blockchain's smart contract technology enables the specification of business logic for transactions, allowing for everything from keeping track of who owns what assets to carrying out intricate and self-enforcing operations. Some examples of the benefits that smart contracts and blockchain can provide are the automatic transfer of assets and the processing of claims. The Ethereum blockchain [9] presently offers the most support for the development of smart contracts. The Ethereum Virtual Machine, a straightforward stack-based Turing complete 256-bit virtual machine, executes smart contracts (EVM). Solidity is a popular scripting language with a burgeoning ecosystem for creating smart contracts. There are two sorts of accounts in Ethereum: externally owned accounts and contract accounts. Ether serves as the cryptocurrency's basic unit of measure. A user is often connected to an externally owned account, which is made up of a special public-private key pair. In contrast, a contract instead of a single private key controls a contract account. Externally held accounts are used to createand sign transactions. A contract account or an externally held account may be the recipient of the transaction. The goal of the transaction in the first scenario is to transfer ether between users. While in the latter scenario, the transaction causes a smart contract function to be executed. Transactions also include a gas limit and a gas price; the gasprice is used to convert the transaction's gas use into ethers. The sender's account will be charged with these ethers as transaction fees.Let's take the purchase of a home as an illustration of a "enhanced asset transfer." A mortgage lender must confirm during the purchasing process that both the buyer and the seller of the property being sold have the legal right to sell it. For titles with prior liens on them, the current process cantake weeks. All of the property data can be recorded on a blockchain, which allows this process to be completed quickly and at a significant cost savings. The information kept in a blockchain can easily show whether the seller still owns the property and hasn't already sold it, as well as any debts that may be attached to it [10]. The middlemen's job in transaction processing is handled by blockchain technology .

A smart insurance contract for travel insurance is a further example of "automated claim processing." Without using a claims department to confirm the loss, an automated payout to customers who purchased insurance can be made after the airline reports a cancellation of a covered flight. The insured can be spared the inconvenience of making a claim and waiting for payment to be made as a result of this. The insurer is spared the inconvenience of having to investigate the claim [10].

Cyber-insurance involves a variety of criteria that are not simply stated, and since the purpose of insurers is typically to pay policyholders as little as possible, this dissatisfies consumers who do not have sufficient insurance knowledge or expertise. Customers, on the other hand, could submit false claims, tell lies, and cheat to receive the reward. With the use of smart contracts, the problems of false claims by policyholders and underpayments by insurers can be easily avoided if the policies are written as codes and performed without human interference as well as in a decentralized manner.

IV. METHODOLOGY

Pseudo Code:

```
CrowdFactory contract{
    Create event and define state variables
    function for total Published Projects{
        return publishedProjs.length;
    }
    function for creating Project{
        Defined state variables
        initialize Crowdfunding Project contract
        pass arguments from constructor function

        push project address
        call event for Project creation
    }
}

Crowdfunding contract{
    Defined state variables
    set the address where amount to be transfered
    add event
    Mapping values using constructor

    Donation function
    function for Donation{
        if goal amount is achieved, it closes the project
        wallet address of donar will be recorded
        total amount raised calculated
    }
}
```

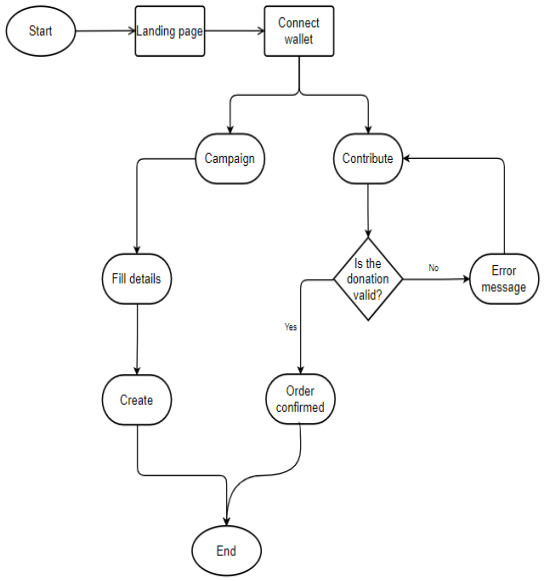

Fig. 1 Flow of execution

V. PROPOSED MODEL FOR DECENTRALIZED CROWDFUNDING

Most of the existing crowdfunding platforms are dependent on a small number of key institutions. These centralized organizations oversee the entire project allocation procedure and keep track of all project-related paperwork. When shared with an organization, such information that is confidential runs the danger of being leaked. In order to connect developers and investors, the central organizations impose a steep fee. We can keep all private papers on a single chain using blockchain. Using cryptographic hash functions, the documents can be hashed such that only the necessary participants can access them.Both presenting the ideas to potential investors and soliciting bids from developers are free of charge. The data on the chain can be verified by anyone, and once the data has been committed, no attacker can change it.

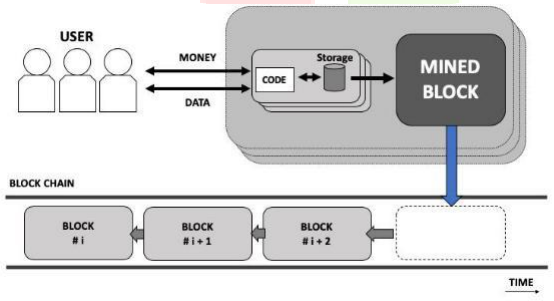

Figure 2: Smart Contract System [17]

A. *Block*

To prevent tampering, all transactions or agreements are kept in a series of blocks that are linked together. All final obligations from the winning developer and investor are saved on the blockchain as a smart contract. Each block consists of a cryptographic hash value, the transaction's timestamp, transaction information, and the prior block's hash value. The total number of transactions contained within a block is determined by the size of the transaction and the previously defined size of a block. Because of the use of cryptographic hashing and hash chaining, it is difficult for a malicious user to tamper with the information that has already been devoted to the chain.

Everybody on the system can investigate committed transactions based on permissions, but no one can alter the transaction data. When the shareholder submits the project request, the first block is created. The requested specifications are included in the block, including the requirement specification, deadline limitations, cost constraints, and expected assistance period. Following block validation, the developer nodes receive the block. The bid results, as well as the finalised parameters in terms of cost, time, and support duration, are recorded in the chain's blocks as the developers continue to submit bids for the requested project.

B. *Digital Identity*

In most cases, symmetric key cryptography involves two people communicating with one another using a single shared secret key. It is challenging to keep a secret key between each group of network participants in an open peer-to-peer network where everyone on the network can connect with everyone else. As a result, we employ asymmetric key cryptography for digital signatures and key creation. In our suggested approach, we employ the Elliptic Curve Digital Signature Algorithm (ECDSA). When a new user (who might be either an investor or a developer) joins the bitfund network, the ECDSA technique is used to produce both a private key and a public key. To begin with, the user must be aware of his private key in order to send any communications or sign any transactions.A huge random number is generated using a random number generator and used as the private key d. With the use of point multiplication and the equation Q(X; y) = d G(X; y), the public key may be calculated from the random private key. Here, the domain parameter is G(x, y), and Q(x, y) serves as the user's public key. The public key is disclosed to all intended users in order to verify the signed transaction, while the private key is kept secret from all users and used to digitally sign transactions. A user's digital identity is formed whenever they want to participate in the decentralized crowdfunding model, either as investors or developers. Developers use their digital identities for all transactions linked to project request submission by investors and iterative bids by developers to win the project.

C. *Consensus Algorithm*

We create a network model with numerous project developers, financiers, and investors. The investors put forward the project in which they are interested, along with the Software Requirement Specification (SRS) document, the anticipated time, cost, and length of maintenance neededonce the product is deployed.

Developers that are interested in the project submit bids with details about the time, money, and maintenance assistance they can offer. The nodes can come to an understanding through consensus. The transaction cannot bechanged later after it has been put to the block. It must first be confirmed. In a conventional approach, outside parties like crowdfunding platforms see to it that each developer is confirmed. A peer-to-peer system lacks a centralized controlling entity. To check the validity of the data being fed into the network by the nodes, distributed systems use a variety of consensus procedures. To come to an agreement regarding the developers' veracity, we employ the Proof of Virtual Voting (POVV) technique. The conventional real voting algorithms have scalability restrictions in terms ofthe number of nodes, despite being the best for achieving a final consensus. Though highly scalable in terms of the number of nodes, the proof-of-work mechanism used by bitcoin never achieves a definitive consensus, making it a probabilistic and randomized protocol. In contrast to genericvoting algorithms,

the proposed POVV method gives the votes to the developers based on mathematical calculations rather than message forwarding. As opposed to the standard systems' time complexity of O(n2) or O(n3), the POVV algorithm operates with a time complexity of O(1). A developer receives a favorable vote from the network each time he or she completes a project. It should be emphasized that winning an iteration does not guarantee success on a project. In the subsequent part, we go over the specifics of the bidding procedure. The number of votes that each developer has received is used to determine their merit. The developer's vote is taken into account as an input parameter in addition to the disparities between the investor and developer's bids in terms of time, cost, and support duration. A high vote will increase the likelihood that the developer will win the bid.

D. Digital Signature

Every transaction has the investor's and the developer's digital signatures attached to prevent non-repudiation. The transaction is digitally signed using the private key created in the previous section, and the other intended users can verify it using the public key. Every bid submitted by Journal Pre-proof the developer must be digitally signed by him or her because any bid throughout the auctioning process could end up being the winning one. Once the developer has won the auction, he or she must digitally sign the winning bid with their private key in order to accept it. This stops the developers from submitting just irrational bid prices in an effort to win the auction.

VI. INTEGRATION OF BLOCKCHAIN AND CROWD FUNDING

The possibility for blockchain technology to change the Investors' knowledge about equity-based crowdfunding. In centralised crowdfunding, documents like contracts, shareholder lists, and other sorts of information are stored on a platform, and only a select group of users has access to them. It's exclusively accessible to a select few people. The security of data and information will be improved by blockchain crowdfunding technology's anti-tampering, anti-fraud, and decentralised ledger system features. The time-consuming process of signing various documents, postage problems, registration, authorization, and certification will all be made easier by blockchain. Due to the secure and universal accessibility of investors' rights, this feature may increase the platform's reach. A digital or smart contract secures and recognisesthe privileges of investors across the globe.

Blockchain technology's transparency can help the crowdfunding platform build credibility and trust with donors and fundraisers. The effectiveness of the advertising and the platform itself depends on how trustworthy the crowdfunding platform is. Blockchain technology will entirely eliminate the problem of duplicated payment records since each equity transfer will be uniquely and once recorded.

Blockchain technology can be used to enhance crowdfunding. It might switch to a decentralised platform that manages the money from donors and, if the effort is successful, sends the funds to the fundraiser or returns the contribution to donors, rather than a platform that collects donations and allocates them to campaign runners. The trust problem that many brand-new crowdfunding sites may experience is now resolved.

At conferences for the Bitcoin sector, crowdfunding frequently comes up, and experts are worried about its veracity. Crowdfunding is regularly criticised for breaking securities laws in various ways, and critics typically lament the lack of a reasonable process for doing it where one truly holds a stake inside the underlying company. Crowdfunding platforms like Swarm provide non-monetary incentives like instant access to apps, memberships, freebies, and other non-monetary incentives to address problems with equity-based crowdfunding. However, this can be misleading even though, in many cases, the marketing still seems to be selling assets

VII. RESULTS

This project has given a significant outcomes which includes a simple and easy to use user interface. Using the Ethereum wallet, its easy to do transaction as well.

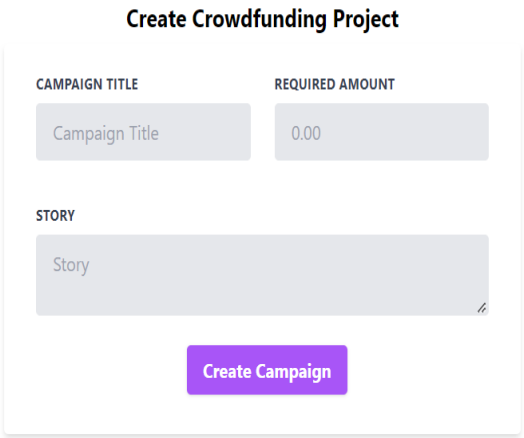

Fig. 3 User Interface

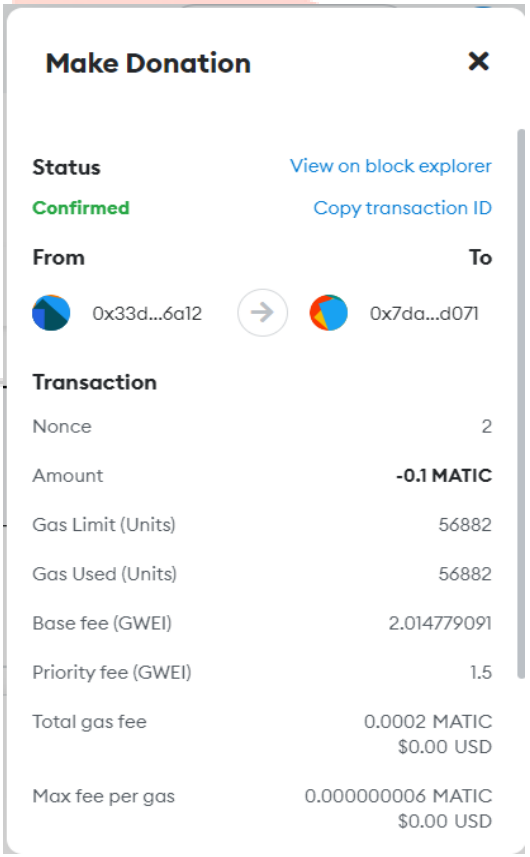

Fig. 4 Transaction Details

Using this interface, the user can donate the funds to the organization who have started the crowdfunding platform. By entering funds in the field available, the amount entered gets verified by the details entered in the smart contract. If the smart contract allows, the request for confirmation of transaction can be seen in the interface of the metamask wallet and can be confirmed and rejected based on user's choice. After confirmation amount gets deducted from user's account and credit can be seen in the account of organization who has created this platform. The target amount and current amount raised is also shown on thescreen.

Funds Raised for various Projects

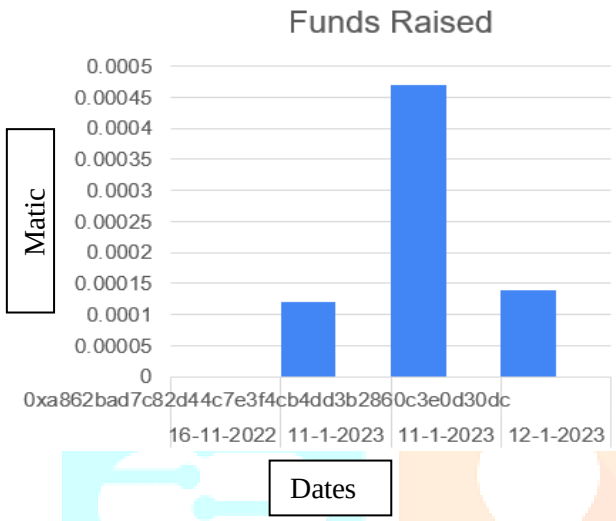

Fig.5 Funds raised by user 1

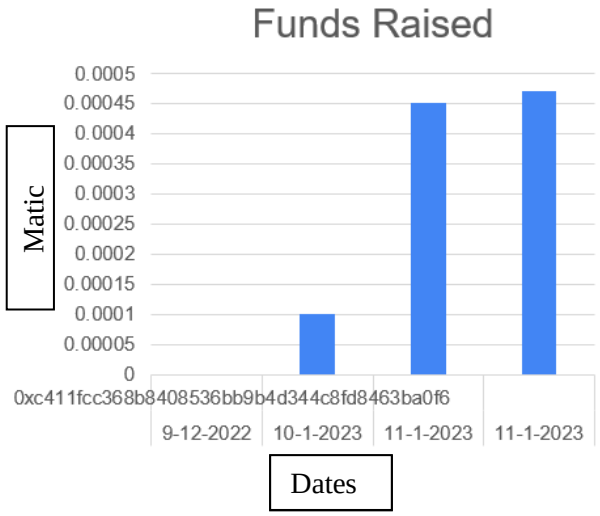

Fig.6 Funds raised by user 2

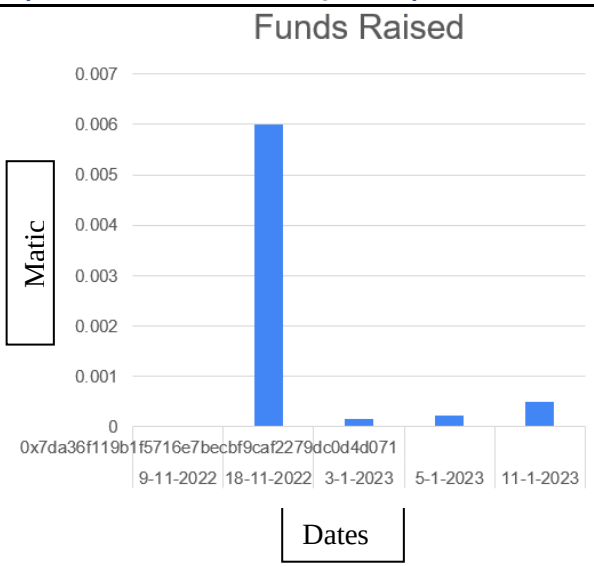

Fig. 7 Funds raised by user 3

VIII. CONCLUSION

Transactions become more transparent when blockchain technology is included into a crowdfunding platform. Users may feel more comfortable making donations to a campaign as a result. Contributors may benefit from knowing how their money is being used thanks to the usage of smart contracts on expenditure requests. With the help of this platform built on the blockchain, transaction transparency may be preserved. Users who make financial contributions can be sure that their funds are in good hands. This platform offers a history of all transactions together with the addresses of the accounts that are making donations and receiving payments, eliminating the chance of fraud as well.

IX. ACKNOWLEDGEMENT

Without the assistance of our mentor Sheetal Phatangare, of the Vishwakarma Institute of Technology in Pune, this project model and article would not have been possible. We were successful in completing this prototype system due to the active involvement of every teammate. Finally, we would want to express our gratitude to the university and institute for providing this opportunity and for their unwavering support.

X. REFERENCES

[1] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. Poseidon: "A new hash function for zero-knowledge proof systems. In USENIX Security Symposium, 2021".

[2] Constantine Xipolitopoulos, Maria Nefeli Nikiforos, Maria Malakopoulou, and Adamantia Pateli. "Success factors for crowd-funding campaigns with machine learning techniques. 09 2020".

[3] Hasnan Baber. "Blockchain-Based Crowdfunding, pages 117–130. 01 2020".

[4] Crystals - kyber: "A cca-secure module-lattice-based kem. In 2018 IEEE European Symposium on Security and Privacy (EuroSP)"

[5] T. Dannberg, 'Advantages and disadvantages with crowdfunding : - and who are the users?', Dissertation, 2017.

[6] Schlueter, M. (2015). Underlying Benefits and Drawbacks of Crowdfunding from the Perspective of Entrepreneurs in Germany. In: 5th IBA Bachelor Thesis Conference. [online] Enschede: University of Twente.

[7] Freedman, D. M. and Nutting, M. R. (2015). The Foundations of Online Crowdfunding. In Equity Crowdfunding for Investors (eds D. M. Freedman and M. R. Nutting).

[8] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1–32, 2014.

[9] Ramos, J., & James, S. (2014). Crowdfunding and the Role of Managers in Ensuring the Sustainability of Crowdfunding.

[10] Macht, Stephanie and Weatherston, Jamie (2014) The Benefits of Online Crowdfunding for Fund-Seeking Business Ventures. Strategic Change, 23 (1-2). pp. 1-14. ISSN 10861718.

[11] Schwienbacher, Armin and Larralde, Benjamin, Crowdfunding of Small Entrepreneurial Ventures (September 28, 2010). HANDBOOK OF ENTREPRENEURIAL FINANCE, Oxford University Press, Forthcoming.

[12] Hongjiang Zhao and Cephas Coffie. "The applications of blockchain technology in crowdfunding contract. SSRN Electronic Journal, 01 2010".

[13] Cumming, Douglas J. and Hornuf, Lars and Karami, Moein and Schweizer, Denis, Disentangling Crowdfunding from Fraudfunding.

[14] "Blockchain: An insurance focus - milliman insight,"

[15] Md. Nazmus Saadat, "Blockchain based crowdfunding systems in Malaysian Perspective"

[16] Vikas Hasijja, "BitFund: A Blockchain-based Crowd Funding Platform for Future Smart and Connected Nation"

[17] Mark Renier M. Bailon, Lawrence Materum, **International Roaming Services Optimization Using Private Blockchain and Smart Contracts**, International Journal of Advanced Trends in Computer Science and Engineering, vol 8, no.3, pp. 544 - 550, 2019.

[18] Iman Vikilinia, "Crowdfunding the Insurance of a Cyber-Product Using Blockchain"