Funding Application for Start-ups with Blockchain Approach

Mitali Markande[1], Rahul Dagade[2]

[1,2]*Computer Engineering Department, Smt. Kashibai Navale College of Engineering, Pune, India*

---***---

Abstract - *There are numerous applications available nowadays that allow start-ups to raise funding for the development of their product. The concept of crowdfunding is that the founder of a start-up comes up with a brand new product that has to be produced. The creation of the product necessitates the expenditure of funds for a variety of resources such as vendors, workers, and so on. The founder of the start-up, or the person who came up with the idea, registers with the fund-raising application and creates a new campaign. Investors can contribute to the various campaigns that are registered on the application. In exchange, the contributors will be rewarded at a later date based on the success of the start-up in which they have invested. The first problem with the previously mentioned crowdsourcing strategy is that the campaign creator/idea person retains complete ownership of the funds raised. He has complete control over how he spends the funds. In actuality, start-ups have an extremely low success rate. When a start-up fails, the backers who provided money lose their money and receive nothing in return. The second risk is that the campaign's founder may be a con artist who will take all of the money and flee. These are the most common and serious issues that arise on the fundraising platform. A smart contract can be constructed using a blockchain-based approach for a fundraising application that controls where the idea person can spend the money. Donors to the campaign no longer contribute money directly to the person who came up with the idea. They send money to a smart contract on the Ethereum blockchain. This contract contains code that specifies which resources are eligible to receive funds from the campaign. The use of blockchain technology in fundraising makes it more reliable, transparent, trustworthy, and decentralised.*

Key Words*:* Blockchain, Ethereum, Smart Contact, Backers, Crowd funding, Start-up

1. INTRODUCTION

A. Blockchain

Satoshi Nakamoto initially described blockchain technology in his article "Bitcoin: A Peer-to-Peer Electronic Cash System," which established the mathematical underpinning for the bitcoin cryptocurrency [8]. Not only is blockchain technology at the heart of all cryptocurrencies, but it has also found widespread use in the traditional financial sector. It also allowed new uses, such as smart contracts, to emerge. Nakamoto's solution to the difficulty of creating trust in a distributed system was the blockchain. The difficulty of developing a distributed storage of time stamped documents in which no party can tamper with the data or the timestamps without being detected.

In its most basic form, blockchain is a growing list of documents, known as blocks, that are connected together using encryption. Blockchain is a database that keeps track of all transactions that have ever occurred. Transactions are data units that include the transaction details as well as a timestamp. Both can be represented as numbers or strings on a computer. A blockchain can be thought of as a table with three columns: the first column holds the transaction's date, the second column stores the transaction's data, and the third column stores a hash of the current transaction plus its details and the prior transaction's hash. The hashing process is a key part of assuring blockchain immutability. The meta-information from the preceding block's hash output is always incorporated into the hashing data of the current block. This connection in the hashing system makes the chain "tough, unbreakable" - it's difficult to control or erase information once it's been approved and added to the blockchain, because if that were attempted, the subsequent blocks in the chain would reject the attempted change (as their hashes wouldn't be valid). As a result, if information is changed, the blockchain will crash, and the cause will be obvious. This property isn't found in traditional data sets, where data can be easily tampered with or removed.

B. Smart Contract

Smart contracts are lines of code recorded on a blockchain that run automatically when certain terms and circumstances are met. They are, at their most basic level, programmes that run as they were designed to run by the individuals who created them [7]. The blockchain, together with smart contracts, appears to be a strong contender for developing a more dependable, transparent, and trusted decentralised fundraising platform.

C. Crowdfunding

In a nutshell, the crowdfunding method is as follows:

1. On the fund-raising platform, the start-up owner establishes a new project/campaign.

2. Backers, also known as investors, can donate money to a variety of campaigns on the site.

3. In return, donors will be rewarded at a later date based on the success rate of the start-up in which they invested.

4. The money goes to the campaign creator only if the minimum funding target is attained. When this requirement is met, the fundraiser programme sends the funds to the campaign creator.

5. The campaign creator creates the product and distributes prizes to donors [4].
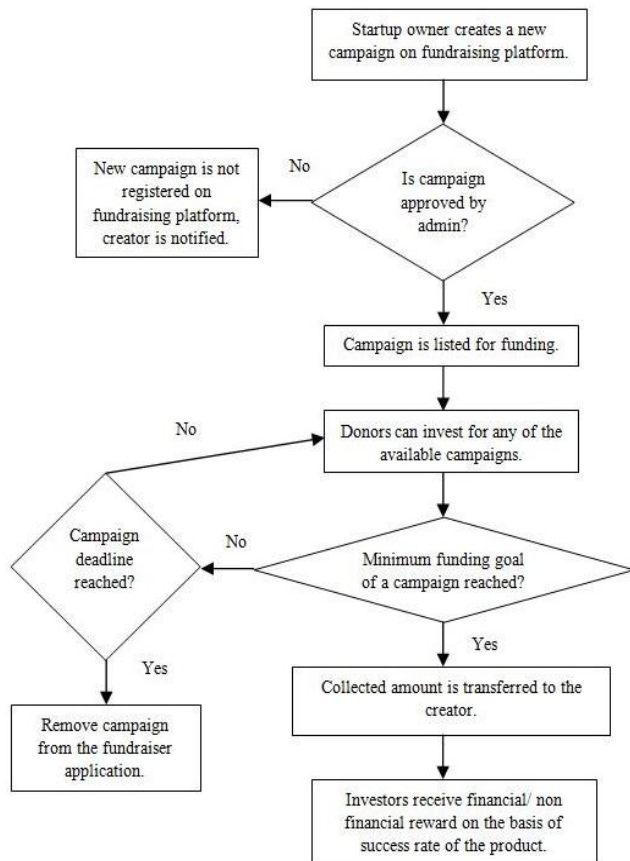

Fig -1: Crowdfunding Process

The basic architecture of a blockchain-based crowdfunding platform is depicted in Figure 3. The application has three sorts of users: admin, startup creator, and contributor. The registered campaign might be approved or rejected by the administrator. On the app, the startup creator starts a new campaign and assigns milestones to it. Money can be donated to any of the available campaigns by contributors. Smart contracts are used in blockchain-based architecture to decide whether to approve or deny spending requests. When the founder of a startup has to pay for a resource or vendor, he submits a spending request. This spending request is approved by contributors. Only money is transferred to the vendor/resource if more than half of the donors approve the expenditure request. Compiled smart contract is deployed on the ethereum network. Users interact with the deployed contract via ethereum wallet such as metamask [1].
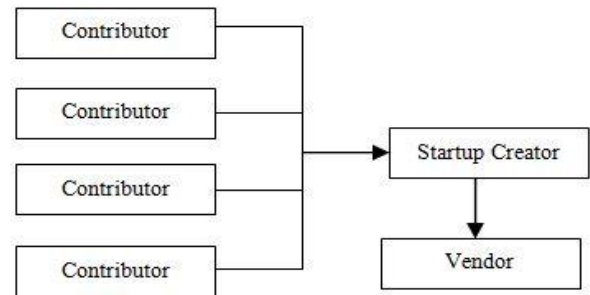

Fig -2: Traditional crowdfunding approach involves direct transfer of amount from start-up creator to vendor
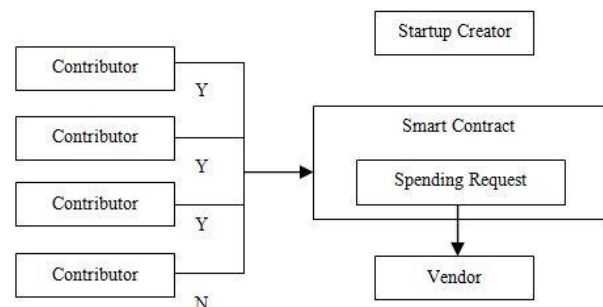

Fig -3: Role of smart contract to monitor each transaction

1. LITERATURE SURVEY

The paper [1] 'Towards Venturing Crowdfunding using Smart Contracts in Blockchain' addresses the creation and testing of a prototype blockchain-based fund raising application as a smart contract for the Ethereum network using Ethereum wallets - metamask and the Solidity language. According to this method, a product owner establishes a new project in the first step by providing the details of the idea products offered by the startup creator. He establishes a minimum donation amount as well as a minimum fundraising target. All open campaigns are visible to contributors, who can donate accordingly. To spend money on any resource, the product owner creates a spending request, detailing the resource and the amount. For each of the spending requests, the next stage voting system records the votes of donors who have registered for the campaign. The product owner can only proceed to pay for the resource if more than half of the contributors agree to the expenditure request.

The paper [2] 'Applying Ethereum Smart Contracts to Blockchain-Based Crowdfunding System to Increase Trust and Information Symmetry' attempts to solve the problem of information asymmetry in crowdfunding platforms, in which different stakeholders receive different information. To earn investors' trust, the system design incorporates more

transparent transactions. As a development platform, the Ethereum blockchain is employed. Traditional and blockchain-based approaches to crowdfunding platform deployment are contrasted on the basis of factors such as transaction transparency, CRUD operations, transaction speed, and information symmetry. It claims that in a blockchain-based approach, transaction transparency is higher because each transaction is recorded in the blockchain network, and once a block is inserted, no one can change it, whereas in a traditional approach, there is no guarantee that once data is inserted in the database, no one can change it. The traditional technique enables all create, read, update, and delete operations, but the blockchain-based solution just supports creation and read actions, lowering the trust factor. Because the data in the block is immutable, information symmetry is stronger in the blockchain-based approach, whereas in the traditional approach, data may be changed more easily, resulting in less information symmetry. Although the blockchain-based technique is advantageous in the above-mentioned characteristics, the traditional system has a faster transaction time.

The paper [3] 'BitFund: A blockchain-based crowd funding platform for future smart and connected nation' explains how to set up a secure, ethereum smart contract based crowdfunding system that employs a bidding approach and an iterative auction algorithm that allows developers to vary their bid amounts over iterations to improve their chances of winning. This method eliminates the need for manual negotiations between investors and developers for any of the project's characteristics.

Four types of crowdfunding are explored in the study 'Blockchain-Based Crowdfunding' [4]: donation-based, reward-based, crowdinvesting, and crowdlending. Table 2 summarizes the many categories.

Table -1: Related work

Aim	Methodology
To implement and test a sample blockchain based funding application as a smart contract for the Ethereum network using the Ethereum wallets and the Solidity language. [1]	Uses blockchain-based peer-to-peer technology. 1. As a development platform and blockchain network, the Ethereum ecosystem is favoured. 2.Solidity, a programming language that combines C++ and JavaScript, is used to create smart contracts. Project Creation, Spending Request Creation, and Voting System are the three key components of application design.
To build ethereum smart contract based crowdfunding platform which improves information symmetry	Traditional and blockchain-based approaches to crowdfunding platform deployment are contrasted on the basis of factors such as transaction transparency, CRUD operations,
of the system by enabling transparency in the transactions. Compare blockchain based approach with the traditional approach for crowdfunding. [2]	transaction speed, and information symmetry. 1.Transparency of transactions is higher in a blockchain-based approach because each transaction is recorded in the blockchain network, and once a block is inserted, no one can change it, whereas in a traditional approach, there is no guarantee that once data is inserted in the database, no one can change it. 2. A blockchain-based system only allows for create and read operations, but a traditional approach allows for all create, read, update, and delete operations, lowering trust. 3. Information symmetry is higher in a blockchain-based system because data in the block is immutable, but data can be changed more easily in a traditional approach, resulting in less information symmetry. 4.While the blockchain-based strategy is advantageous in the above-mentioned characteristics, the old approach has a faster transaction speed.
To build a unique and secure crowdfunding platform based on blockchain and ethereum smart contract. Make use of iterative auction algorithm. Eliminate the need for any mutual negotiation between investors and developers for the project parameters. [3]	The following are the high-level steps that are involved: 1.A new project is being added to the decentralised crowdfunding platform by an investor. 2.The timestamp, project specifications, and estimated cost, time, and developer reputation are all contained in a block. 3.The block is sent to all nodes in the developer's network, and they begin bidding for the project based on time, cost, support duration, and votes. 4.The auctioning algorithms are operated by the smart contract, which looks for the best developer for the project. 5.The block has been accepted and validated. 6.The block is added to the blockchain and connected to the blocks that came before it.
To give brief overview of blockchain technology. [7]	Important step taken to establish trust in distributed systems is that - blockchain provides a distributed trust mechanism: multiple parties keep a record of transactions, and every party can verify that the order and timestamps of the transactions haven't been tampered with.

Table -2: Types of crowdfunding

Type	Description
Donation-Based	Investors don't get any benefit. They simply donate to feel good about helping the project or because they believe in the cause. This type of crowdfunding platform acts as intermediary for charity and NGOs.
Reward-Based	Investors receive free sample product for supporting the idea. The main motive behind this type of crowdfunding is to feel good about having the name in the list of contributors.
Crowdinvesting	Investors get equity shares as return of investment.
Crowdlending	This type of crowdfunding is also called as "Peer-To-Peer lending", "Loan-Based lending". In this type, borrower i.e. the product owner takes loan from the investors at fix interest rate.

3. MOTIVATION

The key objectives of this research are to:

a. Gain a better understanding of the crowdfunding lifecycle.

b. Issues that frequently arise in financing applications.

c. Concentrating on implementation aspects in order to develop a blockchain-based funding application that overcomes the constraints of old methods.

The Fundraiser application serves as a great platform for start-up founders to pitch their idea to a group of contributors and get funding to construct their product. However, the primary flaw in this strategy is that it gives the campaign creator / start-up creator "complete control of the money." The donors are not involved in the decision-making process for which resource the idea person can spend money on. As a result, the start-up's failure or success is entirely dependent on the decision-making of the idea person. In practise, the success rate of a start-up is extremely low, and failure results in significant financial loss for donors who receive nothing in return.

Our main goal is to concentrate on implementation and to create a blockchain-based funding system that eliminates single-person decision-making, ownership of gathered funds, and involves investors in deciding whether or not to approve each resource spending request. The Ethereum environment is recommended as the development platform in this study. The smart contract controls the money that the idea person can spend.

4. IMPLEMENTATION

Implementation of blockchain based crowdfunding platform involves following steps –

1. Smart Contract Design and Implementation –
It is a code written in solidity programming language.
Two smart contracts are implemented –

a. Campaign Factory – It is responsible for deploying new instances of campaign on ethereum test network and storing the resulting address, providing list of addresses of all the deployed campaigns. Table 3 lists the contract's variables, whereas Table 4 lists the contract's functionalities.
b. Campaign – It has responsibility to manage all the functionalities related to single campaign instance. Table 5, 6 lists the contract's variables, whereas Table 7 lists the contract's functionalities.

Table -3: Campaign Factory Contract – Variables

Variable Name	Data Type	Description
deployedCampaigns	address[]	The address of all deployed campaigns.

Table -4: Campaign Factory Contract – Functions

Functions	Description
createCampaign	Deploys a new instance of a campaign and stores the resulting address.
getDeployedCampaigns	Returns a list of all deployed campaigns.

Table -5: Campaign Contract – Variables

Variable Name	Data Type	Description
manager	address	The address of the person who is in charge of this campaign.
minimumContribution	uint	Minimum contribution required to consider a contributor as approver.
approvers	mapping	List of each investor's ethereum wallet addresses who has contributed to the campaign.
requests	Request[]	List of requests that the manager has created.

Table -6: Campaign Contract – Request Structure

description	string	Purpose of request
amount	uint	Ether to transfer
recipient	address	Who gets the money
complete	bool	Whether the request is done
approvals	mapping	Track who has voted
approvalCount	uint	Track number of approvals

Table -7: Campaign Contract – Functions

Functions	Description
Campaign constructor	Constructor function that sets the minimum contribution and the manager of the campaign.
Contribute	Called when someone wants to donate money to the campaign and become an 'approver'.
createRequest	Called by manager to create a new spending request.
approveRequest	Called by each contributor to approve a spending request.
finalizeRequest	After a request has gotten enough approvals, the manager can call this to get money sent to the vendor.

2. Smart Contract Compilation –

Smart contract is compiled using solidity compiler to generate the bytecode. Bytecode is a hexadecimal representation of a built contract that only the Ethereum Virtual Machine can understand (EVM).
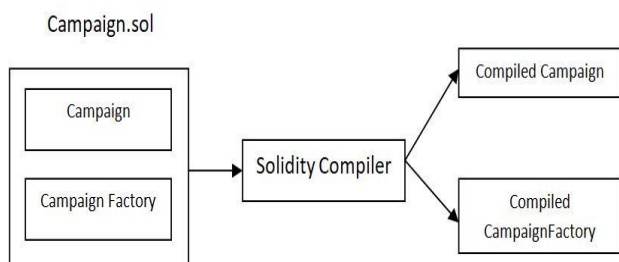

Fig -4: Smart contract compilation process

3. Deployment –

Bytecode generated for each of the smart contract – CampaignFactory and Campaign is deployed to the ethereum test network – rinkeby test network. In this process deployment script makes use of truffle/hdwallet-provider - HD Wallet-enabled Web3 provider.

4. Interaction with deployed contracts via user interface –

User interface built using Semantic react ui, next.js and ethereum wallet – Metamask which is a browser extension allows end user to interact with the contracts deployed on the rinkeby test network.

5. CONCLUSION

Traditional crowdfunding platforms lack in reliability and trustworthiness. This work presents, funding application for start-ups with blockchain approach which addresses these issues. The use of blockchain technology in fundraising makes it more reliable, transparent, trustworthy, secure and decentralised.

A. *Reliable, Transparent, Trustworthy*

The use of a blockchain-based solution enables the creation of a smart contract that monitors and controls every transaction made by the product owner. To spend money on any resource, the product owner must first file a spending request, detailing the resource and the amount. The voting mechanism records donor votes for each spending request. The product owner can only proceed to pay for the resource if more than half of the contributors agree to the expenditure request. As a result of this method, investors are involved in all transactions, making the crowdfunding platform more transparent, trustworthy and reliable. No one can change or delete a block once it has been added to the blockchain, making the application more secure.

B. *Secure, Decentralised*

A blockchain is a decentralised database that is shared among computer network nodes. It's difficult to control or erase information once it's been approved and added to the blockchain, because if that were attempted, the subsequent blocks in the chain would reject the attempted change (as their hashes wouldn't be valid). As a result, if information is changed, the blockchain will crash, and the cause will be obvious. This property isn't found in traditional data sets, where data can be easily tampered with or removed. No one can change or delete a block once it has been added to the blockchain, which makes the application more secure.

Blockchain technology holds a lot of promise, but it may not realize its full potential in its current state. There has to be a coordinated effort in core blockchain technology

research to improve its features and support for complicated apps that can run on the network.

6. FUTURE SCOPE

The developed prototype of a blockchain-based crowdfunding application is deployed on the ethereum test network - rinkeby network in this work, which does not use real crypto currency. The application can be deployed to the production environment in the future. Genuine crypto currency can be invested in innovative start-ups by real investors.

REFERENCES

[1] Yadav, Nikhil; V, Sarasvathi, "Venturing Crowdfunding using Smart Contracts in Blockchain" , Third International Conference on Smart Systems and Inventive Technology (ICSSIT), IEEE, 2020.

[2] Abdul Halim Syed Abdul Rahman, "Applying Ethereum Smart Contracts to Blockchain-Based Crowdfunding System to Increase Trust and Information Symmetry", 7th International Conference on Computer Technology Applications (ICCTA 2021), ACM, 2021.

[3] Vikas Hassija,Vinay Chamola,Sherali Zeadally, "BitFund: A blockchain-based crowd funding platform for future smart and connected nation.", Sustainable Cities and Society, Volume – 60, ELSEVIER, September 2020.

[4] Rosa Righi, R. da, Alberti, A. M., & Singh, M. , "Blockchain-Based Crowdfunding",Blockchain Technology for Industry 4.0. Blockchain Technologies, Springer, 2020.

[5] Ine´s Alegre, Melina Moleskis, "Beyond Financial Motivations in Crowdfunding: A Systematic Literature Review of Donations and Rewards", International Society for Third-Sector Research, Springer, 2019.

[6] Francesco Paolo Appioa, Daniele Leoneb, Federico Plataniac, Francesco Schiavoneb, "Why are rewards not delivered on time in rewards-based crowdfunding campaigns? An empirical exploration", Technological Forecasting & Social Change, ELSEVIER, 2020.

[7] Alaa Hamid Mohammed, Alaa Amjed Abdulateef, Ihsan Amjad Abdulateef, "Hyperledger, Ethereum and Blockchain Technology: A Short Overview", 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), IEEE, 2021.

[8] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system",[Online].Available:https://bitcoin.org/bitcoin.pdf.

[9] Viren Patil, Vasvi Gupta, Rohini Sarode, "Blockchain-Based Crowdfunding Application", Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) IEEE, 2021.