

# Blockchain Based Crowdfunding Using Ethereum Smart Contract

*Dipali Pawar*<sup>1</sup>, *Ruhinaaz Shaikh*<sup>2</sup>, *Sanket Sangle*<sup>2</sup>, *Siddhesh Wankhede*<sup>2</sup>, *Aditya Muley*<sup>2</sup>

<sup>1</sup>Assistant Professor, Department of Computer Engineering, Savitribai Phule Pune University, Pune, India.

<sup>2</sup>Students, Zeal College of Engineering and Research (ZCOER), Pune, Maharashtra, India.

Corresponding Author: [wankhedesiddhesh@gmail.com](mailto:wankhedesiddhesh@gmail.com)

**Abstract:** - Crowdfunding or Crowdsourcing is an online fundraising system that began as a way for society to allocate small sums of money to assist innovative individuals, start-ups, NGOs, and charitable organizations in funding their activities. Nowadays, crowdfunding mostly raises funds for business start-ups because it is relatively inexpensive and simple. Crowdfunding uses social media and crowdfunding websites to connect organisations, entrepreneurs, and charitable causes with investors and donors so they can collaborate. By widening the pool of investors beyond the typical circle of owners, relatives, and venture capitalists, crowdfunding has the potential to boost entrepreneurship and non-profitable projects. The first issue with the aforementioned crowdsourcing approach is that the individual who came up with the campaign/idea still owns the whole sum of money received. He has total discretion over how he uses the money. Start-ups actually have a very low success rate. The investors who made contributions lose their funds and receive nothing in return when a start-up fails. The second concern is that the initiator of the campaign can be a swindler who will steal the entire sum and flee. One solution to the above-mentioned problems is to introduce transparency and security in the crowdfunding system. Blockchain technology aids in the development of a decentralised user network where transactions are tracked in an open distributed ledger. These characteristics of blockchain make it possible for many apps to run on a private, secure, and decentralised platform. A smart contract can be constructed using a blockchain-based approach for a crowdfunding application which would set up the protocols for the application and the investors have to send their contribution to the smart-contract in the form of ethers. This makes the process of fundraising more reliable, transparent, trustworthy, and decentralised.

**Key Words:** *Food security, Crowdfunding, Blockchain, Ethereum, Smart Contract, Decentralized, Investors.*

## I. INTRODUCTION

Crowdfunding (CF) is a general phrase that means obtaining funds, typically in small amounts, from a vast population

known as the crowd in order to support a business initiative, cause, loan, or other financial necessity via the designated platform. It uses typical online platforms such as Kickstarter, Indiegogo or Republic. Crowdfunding provides an easy way to find cash for innovative project ideas. The problem with the current crowdfunding companies is that they are charging high fees and sometimes there were scams that took place. Implementing a crowdfunding strategy in blockchain will help to avoid these types of problems.[2] The blockchain is an immutable ledger that keeps records of every transaction. It uses peer to peer network in which all the system are acting as a client as well as server and all the records are stored on every node. All the transactions are stored in the blockchain with the help of a Smart Contract. We can avoid the problems faced in a traditional crowdfunding system and develop a reliable

Manuscript revised May 04, 2023; accepted May 05, 2023. Date of publication May 07, 2023.

This paper available online at [www.ijprse.com](http://www.ijprse.com)

ISSN (Online): 2582-7898; SJIF: 5.59

application by incorporating blockchain into our application where every transaction is being stored on the blockchain. Actualizing a crowdfunding procedure in blockchain will assist with staying away from scams and transaction fees. By consolidating Peer to Peer shrewd agreement for crowdfunding eliminates the customary transaction charges and platform expenses typically connected with other crowdfunding stages, for example, Kickstarter. The target of our undertaking is to make a solid application with the goal that each ground breaking thought gets life. We have planned a crowdfunding site which is a blockchain based website.[1] We give a simple to utilize interface for everybody to make and post their thoughts on this application. These thoughts at that point become public to everybody. Any individual who wishes to help their thoughts can contribute. Every one of these cycles are done in an intuitive way.

Blockchain is fairly new technology, there are only few studies and researches available on the internet. Blockchain can be characterized as a distributed database of records of all transactions that have been executed and shared among interest members. The attributes of blockchain incorporates decentralization of information, persistency, anonymity and auditability.[10] There are two primary parts in blockchain framework, which are transaction and block. Transaction speaks to the activity set off by the member, while the block is a collection of information recording the transaction and other related subtleties, for example, the right sequence, timestamp of creation, and so on. The transaction records, or blocks, in a blockchain are connected together cryptographically, delivering them tamper proof. This implies each block that have been embedded can't be changed or erased. To achieve reliability, blockchain uses consensus algorithms.

### 1.1 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. 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.

### 1.2 Ethereum

Ethereum is an open-source public distributed computing platform and operating system based on blockchain technology first used by Bitcoin. Ethereum extends the usefulness on Blockchain well beyond cryptocurrencies by making the blockchain programmable according to developer's needs. It was proposed by a cryptocurrency researcher Vitalik Buterin in his whitepaper published in the year 2013, where he states the intention of

Ethereum is to provide, "a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that are used to encode arbitrary state transition functions" [7]. These features make it the apt choice for building truly decentralized applications similar to this project and many other decentralized applications (dApps).

Although Ethereum blockchain is much more advanced and intricate, it is still based on the same principles as Bitcoin's. Ethereum similar to Bitcoin also uses a proof-of-work algorithm run by a peer – to – peer distributed network to find consensus on the current state of the system, with the miners being rewarded in Ether (crypto currency used by Ethereum network). Network gets transactions from users distributed across the globe and the proof of work algorithm at regular intervals determines a sequence of those transactions to be included in the next block in the blockchain. Every new block

added to the chain determines the state of the system. The block creation time in case of Ethereum averages around 14 seconds while that of Bitcoin averages around 10 minutes, both operate on the same set of core principles of blockchain.

### 1.3 Smart Contracts

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.

It is a self – executing contract with the terms of the contract between the buyer and the seller directly written into lines of code.

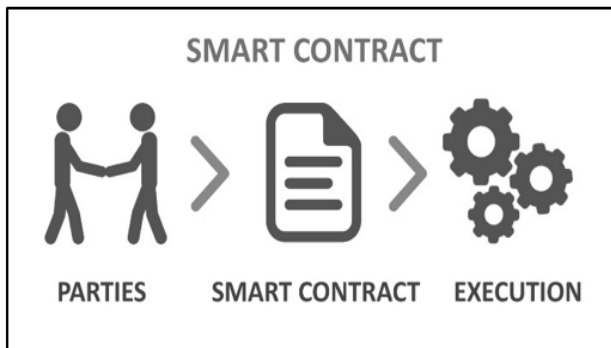


Fig.1. What is Smart Contract

### 1.4 Crowdfunding

In a nutshell, the crowdfunding method is as follows:

- On the fund-raising platform, the start-up owner establishes a new project/campaign.
- Backers, also known as investors, can donate money to a variety of campaigns on the site.
- In return, donors will be rewarded at a later date based on the success rate of the start-up in which they invested.
- When the minimum funding target is reached, the decision whether to approve the campaign or not goes to the investors. Voting occurs and if more than 50% of the investors will approve of the campaign then the fund-raiser will receive the money otherwise the campaign is terminated.
- If successful, the campaign creator creates the product and distributes prizes to donors.[6]

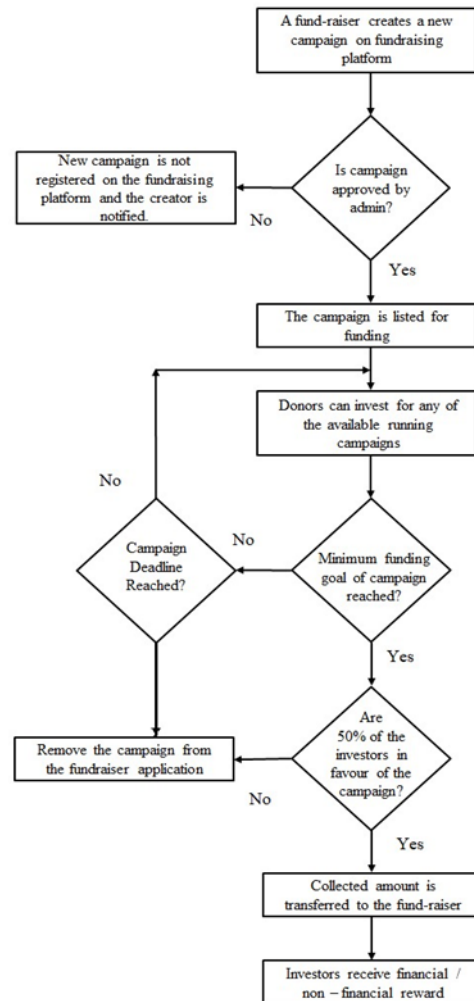


Fig.2. Crowdfunding Process

## II. ARCHITECTURE OF CROWD - FUNDING

The basic architecture of a blockchain based crowdfunding platform is depicted in Figure 3. The application has three sorts of users: admin, fundraiser, and donor. The registered campaign might be approved or rejected by the administrator. On the app, the fundraiser starts a new campaign and assigns milestones to it. Money can be donated to any of the available campaigns by contributors/donors. Smart contracts are used in blockchain-based architecture to decide whether to approve or deny spending requests. When the founder of a fundraiser has to pay for a resource, he submits a spending request. This spending request is approved by contributors. Only money is transferred to the recipient 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.

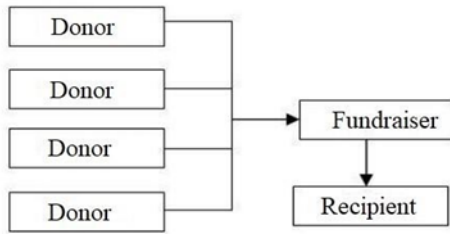


Fig.2. Traditional crowdfunding approach involves direct transfer of amount from startup creator to vendor.

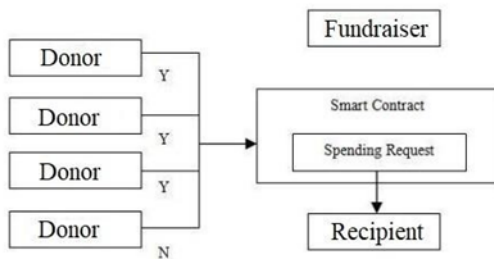


Fig.3. Role of smart contract to monitor each transaction

The smart contracts written for crowdfunding dAapp tie the whole platform together and make it work by controlling the flow of business logic. Even though they do not contain any of the bulk data, the business model they define and transactions that change the business logic flow are how this system of crowdfunding

can work in a peer-to-peer manner, without central control. Crowdfunding dapp is divided into various activates a user can perform in the platform. Anyone who lands on the platform can browse through all the campaigns listed and explore more about each campaign. The application extensively uses JavaScript libraries to build the user interface, handle user inputs and communicate with Ethereum network. The application is built on model view controller architecture so that there is clear distinction on each layer's responsibilities.

### III. WHY BLOCKCHAIN BASED CROWDFUNDING

Online crowdfunding enables people to raise funds for their project. People who are interested in a project can donate by making an online transaction. The donated money goes to the

project manager, which he uses to complete the project or to make a product. This existing method of online crowdfunding has a major drawback. It does not allow contributors to have control over the money they have contributed. Since in the existing method the project manager has all the control over the money contributed, he can very easily perform malicious activities.

Here we address this problem faced by the existing online crowdfunding platforms by using Ethereum network and smart contract. The development of Blockchain technology has allowed businesses to build decentralized models. It has derived new methods to conduct transactions and make agreements. One of the technologies that propose an alternative to the traditional model is the smart contract. A smart contract is similar to a contract in the physical world, but it is digital and represented by a tiny computer program stored in a blockchain. These smart contracts can be used to implement logic.[5] A method has been proposed here that uses smart contract to manage all the activities performed in a crowdfunding campaign. The proposed method has been implemented and its various features are tested by funding campaigns on Rinkeby test network.

## IV. MODULE DESCRIPTION

### 4.1 Modules Description

The system has been designed in the form of three modules namely Creating a Campaign, Contributing a Campaign and Withdrawal of Funds.

### 4.2 Creating a Campaign

In a couple of minutes, anyone may start a campaign, much as in the real world or on other crowdfunding platforms. An Ethereum-based smart contract will keep track of the campaign data, ensuring that it cannot be tampered with. A few basic fields must be filled out in order to create a campaign. The creator of the campaign must provide the campaign name and a few sentences describing it. The campaign creator must determine the minimum donation amount and the target amount required for the campaign. [7] The campaign creator is required to submit the image URL. It is preferable to produce a campaign-related graphic. The contributor cannot contribute less than the minimum contribution amount once it has been set. The most crucial point is that the campaign creator must connect their Ethereum wallet before starting a campaign. If they do not have an Ethereum wallet or have not connected their Ethereum wallet through Metamask, they will not be able to build a campaign.

### 4.3 Contributing a Campaign

Users can share campaigns they have made, and anyone can contribute to them after they have been created. When a contributor clicks on a campaign from the main page, he is taken to the campaign contribution page. The name and description of the campaign, the minimum amount of contribution set by the campaign creator, the campaign creator wallet address, the number of requests so far given, the number of approvers or contributors who have contributed so far to the campaign, and the status of the fund collected will all be displayed on that page. If the contributor does not connect his Ethereum wallet using meta mask, the person will not be able to contribute to the campaign. Before contributing to the campaign, the contributor can view the campaign withdrawal requests. The funds will be sent to the campaign address rather than to the campaign founder, making the procedure more efficient and anti-fraudulent.

### 4.4 Withdrawal of Funds

The Creator of a Campaign can propose how the funds should be spent in the form of a Withdrawal Request. Anyone in need of funds for the same campaign cause can submit a withdrawal request using the site. They must present a valid reason for the requested amount. They should submit the address of their Ethereum wallet. The withdrawal request page has a table with columns such as request Id, withdrawal description, amount needed, recipient wallet address, approval count, and finalize. [3] The approvers can decide whether or not to provide funds for the requests that have been submitted, as well as examine the request description. The request can potentially be denied by the approvers. Without the consent of approvers, funds cannot be withdrawn. The desired amount can be deposited into the recipient wallet once all approvers have authorized and finalized.

## V. CONCLUSION

Implementation of blockchain technology to crowdfunding platform provide more transparent transactions. As a result, users can feel more confident when they want to donate to a campaign. The application of smart contract on spending request also can help contributors to know how their money are being spent. The purpose of a smart contract-based solution is to enable secure way of crowd funding by ensuring that the money donated by the investors is safe and also each and every step taken in the start-up with help of donated money involves investor's opinion i.e. whenever the campaign creator wants to spend the money he/she has to make a spending request where

the purpose of using the money, to whom the money is being sent(vendor) and the amount needed should be mentioned. The main advantage of using the smart contract is the concept of blockchain that it is resilient against many threats. Also, it provides many features like improved reliability, faster and efficient operation.

## REFERENCES

- [1]. Sharma, A., Sharma, P., Goel, N., Singh, R., & Singh, A. R. (2022). Block Chain-Based Crowd Funding Using Ethereum. *International Research Journal of Engineering and Technology*.
- [2]. Gupta, R., Yadav, M., & Dhankar, U. (2022). Crowdfunding using Ethereum Blockchain. *International Journal for Research in Applied Science and Engineering Technology*, 10(5), 3386–3390.
- [3]. Markande, M., & Dagade, R. (2022). Funding Application for Start-ups with Blockchain Approach. *International Research Journal of Engineering and Technology*.
- [4]. Senthamil Selvi, R., B, P. D., & Professor, A. (2022). Crowdfunding Platform Using Blockchain Technology.
- [5]. Purushotham, I., Singh, J., Sajith, K. P., Jamwal, K., Kumar, S., & Mohamadi Begum, Y. (2022). Crowdfunding dApp: Block chain based fundraising protocol.
- [6]. Benila, M. S., Ajay, V., Hrishikesh, K., & Karthick, R. (2019). Crowd Funding using Blockchain. *GRD Journals-Global Research and Development Journal for Engineering*, 4.
- [7]. Nazmus Saadat, M., Halim, S. A., Osman, H., Nassr, R. M., & Zuhairi, M. F. (2019). Blockchain based crowdfunding systems. *Indonesian Journal of Electrical Engineering and Computer Science*, 15(1), 409–413.
- [8]. Hassija, V., Chamola, V., & Zeadally, S. (2020). BitFund: A blockchain-based crowd funding platform for future smart and connected nation. *Sustainable Cities and Society*, 60.
- [9]. Choudary, A. D. (n.d.). Role of Blockchain Technology in Crowdfunding (*International Banking and Finance*).
- [10]. Hongjiang, Z., & Coffie, C. P. K. (n.d.). The Applications of Blockchain Technology in Crowdfunding Contract.