

Application of Smart Contracts in Crowdfunding

Ms. Mini Agarwal
Maharaja Agrasen Institute Of
Technology (Assistant Professor)

GGSIPIU
Delhi, India
mini@mait.ac.in

Anuj Arora
Maharaja Agrasen Institute Of
Technology (CSE)

GGSIPIU
Delhi, India
anujarora0502@gmail.com

Rhythm Jayee
Maharaja Agrasen Institute
of Technology (CSE)

GGSIPIU
Delhi, India
javeerythm8@gmail.com

Jatin Malhotra
Maharaja Agrasen Institute Of
Technology (CSE)

GGSIPIU
Delhi, India
malhotrajatin451@gmail.com

Abstract

Crowd funding is an online money-raising approach that began as a way for people to donate a little amount of money to help inventive people fund their ventures. People may invest in pioneering by using crowdfunding. Businesses can use an intermediate medium or platform to connect with each other. The problem with the present method of crowd financing is through a third-party channel. Don't guarantee the money given by the investor. The project and the investor have no control over the money contributed. This paper offers a blockchain-based crowdfunding infrastructure that can provide a private, secure, and decentralized crowdfunding path. The major goal of this paper is to allow investors to successfully contribute to any project by establishing smart contracts that allow contributors to have control over their money and project creators and investors to effectively make and reserve funds for the project.

I. INTRODUCTION

Crowdfunding is a method of raising funds from a large number of individuals or businesses. Investors can contribute to any project they are interested in, and if the initiative is successful, they can profit [1]. Many crowdfunding sites exist these days, and they accept large sums of money from investors and contributors and then leave them with unfulfilled promises. The traditional manner of dealing with company finance is being disrupted by blockchain-based crowdfunding. In general, when people require money to start a firm, they must first create a strategy, statistical surveys, and models, and then offer their ideas to people or organizations.

Banks, angel capitalists, and venture capital firms were among the subsidized sources. The current crowdfunding concept is based on three types of on-screen characters: the task initiator who offers the idea or venture to be financed, individuals or investors who invest in the idea, and a platform that connects these two characters to make the venture a success. It is used to fund a wide range of start-ups and unique concepts, such as new activities, medical breakthroughs, travel, and social entrepreneurship initiatives

A. Types of crowdfunding

Donation-Based Crowdfunding: There is no financial return to contributors or financial investors in this sort of crowdfunding [2]. This comprises charity, non-governmental organisations (NGOs), disaster relief, and medical assistance.

Crowdfunding based on incentives: In this form, individuals donate to initiatives in exchange for rewards, which might be profit or a product. There are several sites that employ this type of crowdfunding these days.

Equity-Based Crowdfunding: Unlike the previous two types of crowdfunding, this sort of crowdfunding allows you to become a part of the firm by purchasing shares. As a result, investors receive a return on the company's earnings.

B. Present day Crowdfunding

Today, all crowd funding transactions are reliant on a variety of crowdfunding platforms, which require large sums of money from both investors and contributors in order to execute their requests, which may or may not be adequate. Many platforms act as gatekeepers, with rigorous rules and restrictions that make it difficult for both investors and contributors to have a say in the project's success. Having a brilliant concept on a crowd fundraising platform is not a guarantee of success. Users will need a strategy to increase the visibility of their crowdfunding page on search engines and attract new consumers to that project, which would need large spending in advertising alone. Many crowd financing systems do not guarantee that the promises made to contributors will be delivered, and this can be unfair to contributors, causing them to be hesitant to engage in the business and causing project management challenges. Sometimes project managers have watched their entire business fail before they ever had a chance to begin production because when an idea becomes popular on crowdfunding portals, many different business people are inspired and try to produce comparable items, increasing competition.

C. Blockchain

A blockchain is a growing collection of blocks that are linked via encryption. Each block generates the hash using a cryptographic algorithm, the hash of the previous block, the timestamp of when it was created, and value-based information, which is commonly represented as a merkle tree [9]. The information in a block on the blockchain cannot be changed. When the data is recorded, some randomness is added. Without the consent of more than half of the nodes in the blockchain, or 51 percent, a block cannot be modified. It is a shared and irreversible record, and the information contained within it is accessible to each and everyone, making it decentralised. As a result, because there is no need for a central server or trusted authority, blockchain solves the problem of spending more. Proof of Work and Proof of Stake are two methods for securing blockchain. In proof of work, a piece of data called a nonce is generated, which takes a long time and a lot of power and processing. Others, on the other hand, can easily check that the nonce and blocks satisfy specific conditions [3]. Miners compete against one another in proof of work to execute network transactions and earn rewards. Miners put something on the line in proof of stake, and if they mine properly, they will win the reward; otherwise, they will lose the money they put on the line.

A public and a private blockchain are the two most common forms of blockchain. A public blockchain is a network that is accessible to the public and whose rules may be downloaded by anybody. The network is therefore dispersed and decentralised since they may read, publish, or participate in it. A private blockchain allows businesses to use distributed ledger technology without exposing their information to the public. Ethereum is a public blockchain that is a decentralised architecture that is totally independent of anyone and is not bound in any way [10]. It may then be added to the Ethereum blockchain, which cannot be changed by anybody. A smart contract is a computer protocol that enables us to simplify and verify contract fulfilment. These are traceable and irrevocable transactions. In the same manner that a typical contract defines the rules and consequences of an agreement, smart contracts do the same. The solidity programming language was used to create these smart contracts.

D. Crowdfunding using blockchain

Blockchain provides for decentralisation in crowdfunding, which implies that no one platform or set of platforms controls the smart contracts, making them transparent to everyone on the blockchain [4]. It is a peer-to-peer network that collectively follows a protocol for inter-node communication and new block validation, so no one can edit any block without the consent of more than half of the nodes in the blockchain, making it secure and safe. Anyone with internet access may launch a project on the blockchain website, and anyone with internet access can donate to the project. Contributors do not have to be concerned with empty promises, like in traditional crowdfunding. All transactions will be handled by smart contracts, meaning all money will be saved in smart contracts rather than sent to a third party. Blockchain allows project managers and contributors greater latitude, allowing contributors to make fractional contributions to the project.

II. LITERATURE SURVEY

Alexander Backmann [5] has highlighted the distinctions and parallels between traditional fund-raising methods and newer methods. The market for peer-to-peer lending Both fundraising approaches differ greatly in terms of the quantity raised, the screening procedure, and the knowledge gathered for risk management. These studies may clarify whether the outcomes of the new peer-to-peer lending strategy are applicable to the classic fund raising technique or vice versa. This also focuses on traditional fundraising, when the return on investment was quite low and the business typically failed.

According to a study on crowd funding and its consequences in India [2,] crowdsourcing has various advantages over existing methods available to new firms and SMEs. Because crowdfunding is not available to the general public, it is difficult to attract investors to new businesses, but the younger generation is more knowledgeable about crowdfunding, which is a solid starting point for this crowdfunding platform to flourish. This will also enable new companies to reach out to a larger group of investors and financial specialists in order to raise financing.

According to Huasheng Zhu and Zach Zhizhong Zhou [6], blockchain is still an emerging technology in its early stages, with numerous technical and legal difficulties to be addressed before making it available to the public. There is still room for blockchain businesses and market influencers to collaborate and alter the business, use blockchain technology in the market, and propose fresh ideas. They must gain a better knowledge of blockchain innovation, its value, opportunities, and risks. They should be able to successfully progress blockchain applications in the Chinese crowdfunding sector. Through specialised advancement and blockchain applications, monetary proficiency and societal benefits might be realised.

Blockchain, according to Huasheng Zhu and Zach Zhizhong Zhou [6], is still an emerging technology in its early phases, with major technological and legal challenges to overcome before making it available to the public. There is still opportunity for blockchain enterprises and market influencers to collaborate and change the business, apply blockchain technology in the market, and present new ideas. They must learn more about blockchain innovation, including its value, prospects, and hazards. They should be able to effectively advance blockchain applications in China's crowdfunding industry. Financial proficiency and societal advantages may be realised through technological innovation and blockchain applications.

According to the article crowdsourcing and crowdfunding platform employing blockchain and collective intelligence [8], crowdfunding and crowdsourcing are still in their early phases in India. Despite the fact that online crowdfunding is a relatively new concept, the Indian people are yet to embrace it. Regardless of the underlying difficulties, the future of crowdfunding and public support in India will be great. Firm capital and human resources are critical requirements for any business. This is especially noticeable in the case of startups and low-level companies, which often struggle with merging resources. Thus,

the use of blockchain in engineering will aid in the framework's security. The scope of such stages in India is magnificent, but in order for it to be successful, the audience must participate.

III. PROPOSED ARCHITECTURE

Because crowdfunding involves a large number of transactions, it is necessary to handle and document the acts lawfully. As a result, a smart contract is employed, which is a transaction protocol that automatically executes, controls, and documents transactions on behalf of project founders and investors. This article presents a solution that consists of two contracts: one that holds all of the projects and the other that handles the transactions for each project. The primary entities in any crowdfunding platform are the project manager, donors, suppliers, smart contract, expenditure request, and voting system. The crowdfunding process is divided into three sections :

A. Project creation

A project manager starts a new project in the first step by specifying the project's name, description, and minimum commitment to that project. Contributors may then go through all of the available projects on the crowdfunding site and choose which one they wish to give to. To be recognised as contributors, they must make the minimal contribution to the project that the project manager specified when the project was founded. This money is then deposited in the wallet, which the project managers can use, as shown in Fig. 1.

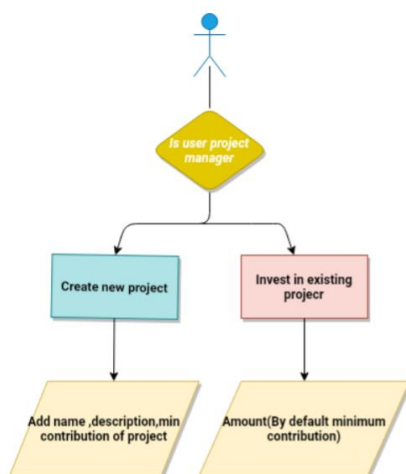


Fig. 1. Creating or contributing to project

B. Spending request

If a project manager wants to spend the money contributed by investors at this stage, they must create a spending request that includes a description of where they intend to spend the money, the total amount they intend to spend, and the address of the vendor who will supply the items required by the project

manager, as shown in Fig. 2.

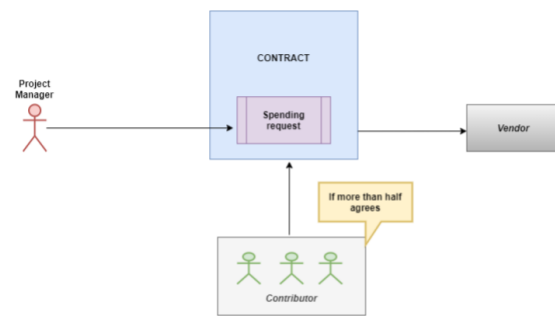


Fig. 2. Voting system ensures money spent is in control of contributors

C. Voting system

The voting system is designed so that only contributors who have invested in that specific project can accept or reject the project managers' expenditure proposals. The voting method also assures that once a contributor votes in favour of a spending request, he or she cannot vote in favour of it again. So, if more than half of the project's contributors agree to the spending request, the funds are delivered to the vendor so that the user can provide the utilities requested by the project manager, and there will be a mechanism in place to protect the project manager's interests if contributors are inactive, the spending request will be processed based on the number of votes cast by all active contributors.

IV. RESULT ANALYSIS AND IMPLEMENTATION

A smart contract written in Solidity language is required to construct the crowdfunding platform. The code is then built and distributed on the Ethereum network using the solidity compiler. To complete all transactions, Metamask, a Chrome browser plugin, is utilised. The following is the procedure for creating a crowd fundraising platform:

Step 1: Make a smart contract.

Step 2: Compile the smart contract in order to receive the bytecode and application binary interface (ABI).

Step 3: Upload bytecode to the Ethereum blockchain.

A. Smart contract creation

It is a software created in the Solidity programming language that handles all transactions automatically.

As illustrated in Fig. 3, the project manager must first construct the project by mentioning its name, description, and the minimal contribution. The user can then create a spending request to spend the money provided by the investors. For this project, authors must include a description of where they intend to spend money, the amount of money they intend to spend, and the address of the vendor who will give some service. If more than half of the investors agree to the expenditure request, the project manager has the authority to transmit the funds to the vendor's address. The vendor will then offer the service required

by the project manager.

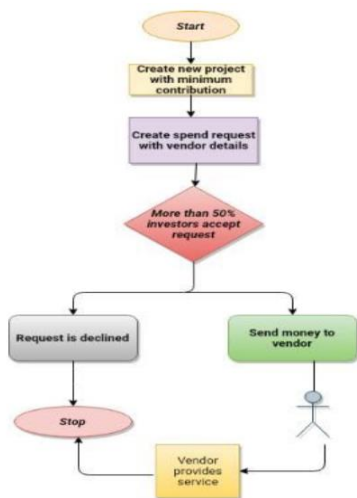


Fig. 3. Flow chart of project manager

If the investor is interested, it is displayed in Fig. 4. If a project is mentioned on a crowdfunding site, They may participate in the initiative by making a little contribution which the project manager has set while creating the project. Then this money is added to the wallet assigned for the specific project. After that the contributor can either accept the spending request sent by the project manager or decline.

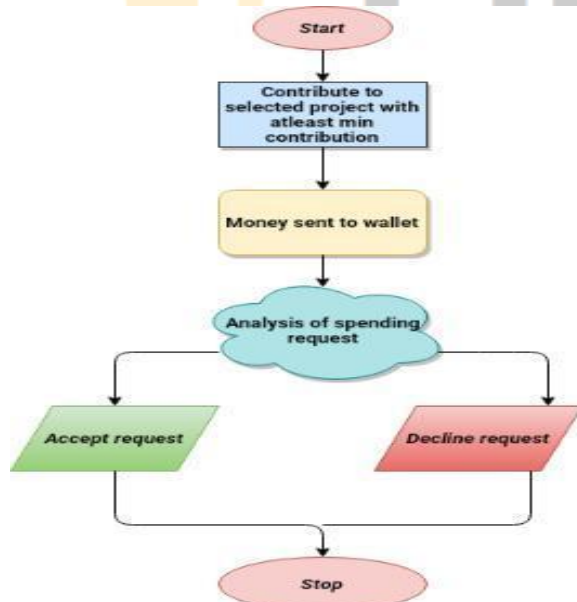


Fig. 4. Flow chart of investor

B. Compilation and Deployment

The smart contract is compiled using the solidity compiler. This gives bytecode and application binary interface as out-put. Bytecode is then deployed to ethereum blockchain and application binary interface is used to interact with smart contract. Bytecode is a hexadecimal representation of the compiled

contract which can only be understood by Ethereum Virtual Machine(EVM).

The bytecode obtained from the compilation can be deployed to either rinkeby test network, ropsten test network or ethereum live network. After deploying they return the address

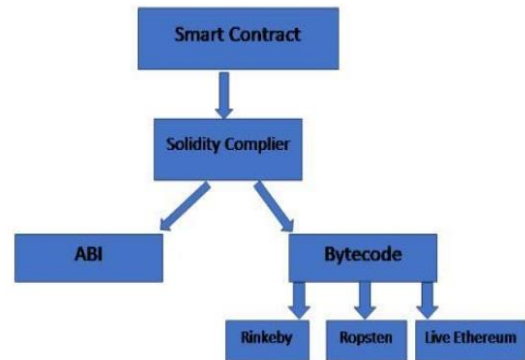


Fig. 5. Compilation and deployment of smart contract

where the smart contract is deployed using which the user can make the transactions.

C. Result Analysis

When a user wants to create a new project then the user can do it by pressing this button. It consists of the name of the project, description of the project and the minimum contribution to the project as shown in Fig. 6.

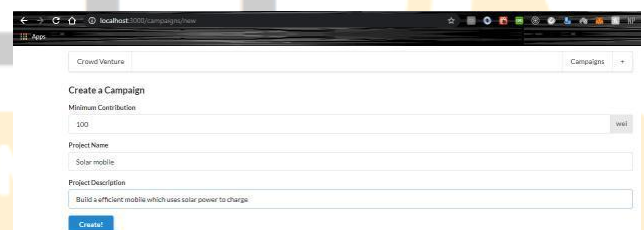


Fig. 6. Creation of venture

Here the list of all current projects are shown with their name, description and the address of project manager as shown in Fig. 7.



Fig. 7. List of all the projects

Contribute form contains the form to contribute to a particular project with minimum contribution. If the user gives a minimum contribution, the user is added as a contributor to that project and rendered back to the home page as shown in Fig. 8.

Request form is created by the project manager to request money to spend. It consists of the description of request, value

in ether and address of vendor as shown in Fig. 9.

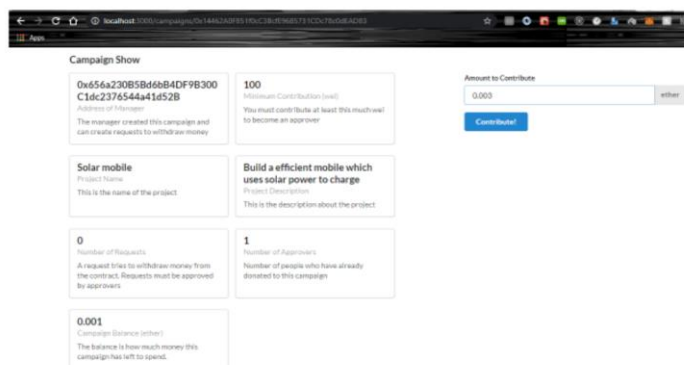


Fig. 8. Contribute to the project



Fig. 9. Creating request

This is the list of requests made by the project manager which contains an accept button which will increase the number of counts as shown in Fig. 10.

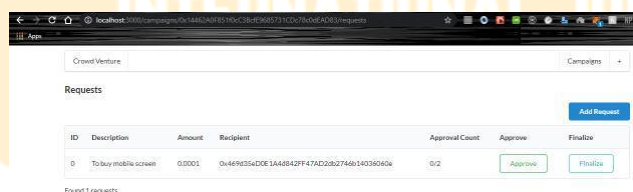


Fig. 10. List of request and voting system

When the request accepted is more than half, then the request will turn green indicating that the request is accepted by the majority of contributors as shown in Fig. 11.



Fig. 11. Acceptance of request

Money can be delivered to the vendor once the majority of donors accept, as illustrated in Fig. 12.



Fig. 12. Sending money to vendor

V. CONCLUSION

Finally, it is argued that blockchain-based crowdfunding is a relatively new notion in the ICT community. So far, the solidity code for the campaign contract has been successfully developed and built using the solidity compiler. The solidity compiler produces bytecode, and the interface was published onto the Ethereum network using metamask. Following the deployment of the project, a decentralised web app with a frontend for starting a new project, contributing to an existing project, generating a new request, accepting a request, and finishing a request is established. At the moment, the blockchain use in crowdfunding is still in its early stages, with several legal and specialist difficulties to be resolved.

With the advancement of blockchain technology, our suggested work has a bright future and plenty of room for progress and evolution. In the future, the planned research activity can move forward in a more straightforward and secure manner for all proposals.

REFERENCES

- [1] <https://www.investopedia.com/terms/c/crowdfunding.asp>
- [2] Prinsha K, "A Study on Crowd Funding and its Implications in India ParipeX," Indian Journal Of Research, Vol: 5, 1 January 2016.
- [3] Arthur Gervais, Ghassan O. Karame, Karl Wust, Vasileios Glykantzis, "Hubert Ritzdorf, and Srdjan Capkun, "A Study on Crowd Funding and its Implications in India ParipeX," In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery, New York, NY, USA, 2016.
- [4] <https://due.com/blog/a-new-era-of-crowdfunding-blockchain>
- [5] Bachmann, Alexander Becker, Alexander Buerckner, Daniel Hilker, Michel Kock, Frank Lehmann, Mark Tiburtius, Phillip Funk, Burkhardt, "Online Peer-to-Peer Lending–A Literature," Online Peer-to-Peer Lending–A Literature. Journal of Internet Banking and Commerce, 2011.
- [6] Zhu, H., Zhou, Z.Z. "Analysis and outlook of applications of blockchain technology to equity crowdfunding in China," Financ Innov, 2016.

[7] Gebert, Michael, "Application of blockchain technology in crowdfunding," New European.

[8] Dhokley, Er Gupta, Saurabh Pawar, Ganesh Shaikh, Abrar, "Crowdsourcing and Crowdfunding Platform using Blockchain and Collective Intelligence," International Journal of Computer Sciences and Engineering, 2016.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564, 2017

