WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Blockchain Based Crowdfunding

Medha Kulkarni[1], Pratik Tayade[2], Gaurav Patil[3], Ashutosh Yadav[4], Vivek Lone[5]

[1]Faculty of IT- Department, VPPCOE
[2,3,4,5]Student of IT- Department, VPPCOE

ABSTRACT –

Currently, there are multitudinous operations available that allow launch- ups to raise backing for the development of their product through the conception of crowdfunding. This involves the author of a launch- up registering with a fundraising operation and creating a new crusade, which investors can contribute to in exchange for prices grounded on the success of the launch- up. still, this traditional crowdfunding strategy has some downsides. For case, the crusade creator retains complete power and control over the finances raised, and there's a threat that the author may be a con artist who'll take all the plutocrat and run. also, start- ups have a low success rate, meaning that investors who give plutocrat may end up losing their investment.

To address these issues, blockchain technology can be employed to produce a more dependable, transparent, secure, and decentralized fundraising platform. A smart contract can be programmed to control where the idea person can spend the finances, and benefactors can shoot their benefactions to the smart contract on the Polygon blockchain rather of directly to the crusade creator. The smart contract can also release finances in stages as the design progresses, with the crusade creator needed to give substantiation of progress or reach certain mileposts before entering the coming tranche of backing. This can help to help fraud and increase translucency and trust between the crusade creator and the benefactors. likewise, since blockchain is a decentralized technology, a blockchain- grounded crowdfunding platform can exclude interposers and reduce costs associated with traditional fundraising styles.

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

1. INTRODUCTION

Blockchain

Satoshi Nakamoto first introduced blockchain technology in his article "Bitcoin: A Peer-to-Peer Electronic Cash System," which established the foundational principles for the bitcoin cryptocurrency [8]. Today, blockchain technology is not only the backbone of all cryptocurrencies but also finds widespread application in the traditional financial sector. The innovation of blockchain also paved the way for new uses, such as smart contracts. Nakamoto's solution to the challenge of establishing trust in a distributed system was the blockchain, which enables the creation of a distributed storage of time-stamped documents that cannot be tampered with by any party without detection.

At its core, blockchain is a growing list of records, called blocks, that are linked together using encryption. The blockchain serves as a database that records all transactions that have ever occurred. Transactions are data units that consist of transaction details and a timestamp, represented as numbers or strings on a computer. A blockchain can be visualized as a table with three columns: the first column records the date of the transaction, the second column stores the transaction data, and the third column records a hash of the current transaction and its details, as well as the hash of the prior transaction. The hashing process plays a vital role in ensuring the immutability of the blockchain. The output of the previous block's hash is always integrated into the current block's hashing data, creating a "tough, unbreakable" chain that is challenging to manipulate or erase information once it has been approved and added to the blockchain. Any attempts to alter the data in a block would be rejected by subsequent blocks in the chain since their hashes would no longer be valid. As a result, if any changes are made, the blockchain would fail, and the cause would be immediately apparent. This feature distinguishes blockchain from traditional data sets, which can be readily tampered with or removed.

Smart Contract

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

Crowdfunding

In a nutshell, the crowdfunding system is as follows:

The start-up owner establishes a new project/campaign on the fundraising platform.

The start-up owner establishes a new project/campaign on the fundraising platform.

The start-up owner establishes a new project/campaign on the fundraising platform.

Money goes to campaign creators only if the minimum funding goal is met. When this requirement is met, the fundraiser program sends the funds to the campaign creator..

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

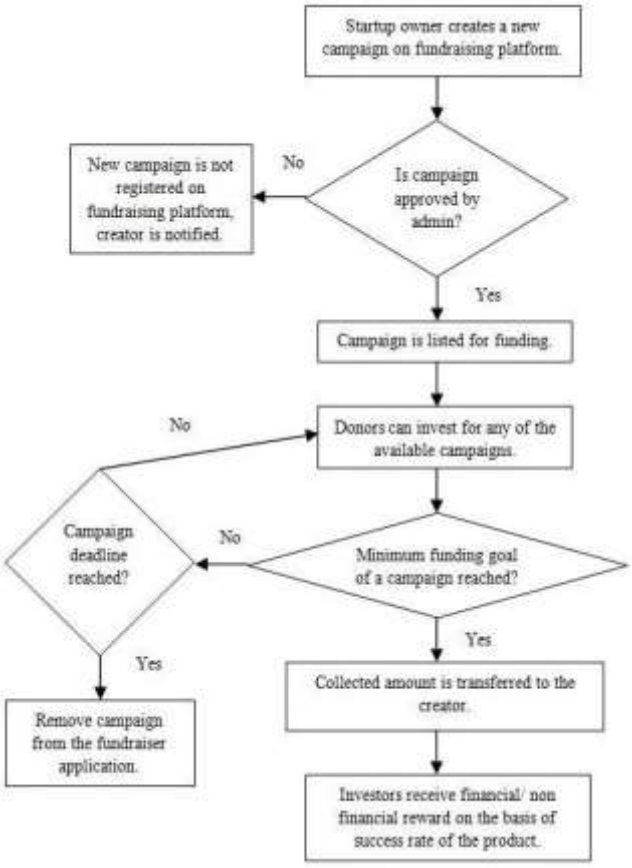


Fig -1: Crowdfunding Process

The diagram in Figure 3 shows the basic structure of a crowdfunding platform based on blockchain technology. This platform has three categories of users namely admin, startup creator and contributor. The administrator has the power to approve or reject campaigns submitted for registration. The startup creator is responsible for launching a new campaign and assigning milestones to it. Contributors can donate funds to any campaign of their choice. The blockchain architecture uses smart contracts to determine whether to approve or reject spending requests. If a startup founder needs to pay a vendor or resource, they need to submit a spend request that requires contributor approval. Payment will only be made to vendors or sources if more than 50% of donors approve the request. The compiled smart contract is deployed on the Polygon network and users can access it through a Polygon wallet such as Metamask [1].

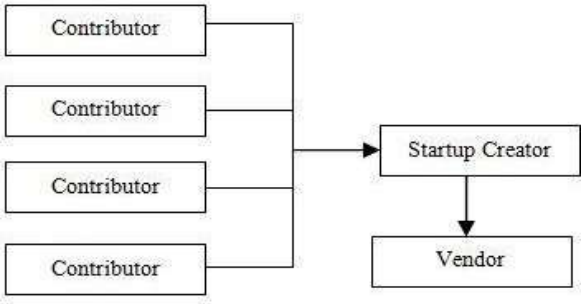


Fig -2: The traditional crowdfunding approach involves a direct transfer of the amount from the start-up creator to the seller

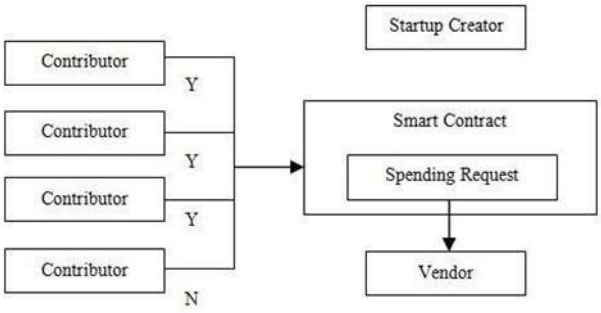


Fig -3 The role of a smart contract to monitor each of them transaction

2. LITERATURE SURVEY

The article [1] describes the development and testing of a prototype blockchain-based fundraising application using smart contracts for the Polygon network, using Polygon wallets and the Solidity language. The Product Owner creates a new project and sets a minimum donation amount and fundraising goal. Contributors can contribute to visible campaigns and spending requests can be made by the product owner, which requires the approval of more than half of the donors through a voting system to continue paying for the resource. The platform is transparent and secure thanks to the use of blockchain technology.

The article [2] "Applying Polygon 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 gain investor confidence, the system design includes more transparent transactions..

The paper compares the deployment of crowdfunding platforms using traditional and blockchain- grounded approaches, with a focus on the Polygon blockchain as the development platform. It highlights several factors similar as sale translucency, smut operations, sale speed, and information harmony. In a blockchain- grounded approach, sale translucency is advanced as every sale is recorded on the blockchain network, and formerly a block is fitted , it can not be changed. In discrepancy, in a traditional approach, there's no guarantee that formerly data is fitted into the database, it can not be changed.

The traditional approach allows for all CRUD operations, while the blockchain-based approach only supports creation and read actions, reducing the trust factor. As the data in the block is immutable, information symmetry is stronger in the blockchain-based approach, while in the traditional approach, data can be changed easily, resulting in less information symmetry. Despite the advantages of the blockchain-based approach, the traditional system has a faster transaction time..

The paper [3] presents a blockchain-based crowdfunding platform called BitFund, which uses Polygon smart contracts and a bidding approach with an iterative auction algorithm. This method allows developers to vary their bid amounts over iterations, improving their chances of winning without the need for manual negotiations with investors. The platform is secure and eliminates the need for negotiations on project characteristics.

The study in [4], titled "Blockchain-Based Crowdfunding," explores four types of crowdfunding: donation-based, reward-based, crowdinvesting, and crowdlending. Table 2 summarizes the various categories.

Table -1: Related work

Aim	Methodology
To implement and test a sample blockchain based funding application as a smart contract for the Polygon network using the Polygon wallets and the Solidity language. [1]	Uses blockchain-based peer-to-peer technology. As a development platform and blockchain network, the Polygon ecosystem is favoured. 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 Polygon smart contract based crowdfunding platform which improves information symmetry system by enabling transaction transparency Compare blockchain based approach with the traditional approach for crowdfunding. [2]	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. Transaction transparency is higher in the blockchain based approach because every transaction is recorded in the blockchain network and once the block is entered, no one can change it, while in the traditional approach there is no guarantee that once the data is entered into the database, no one can change it cannot change. Blockchain-based system allows only create and read operations, but the traditional approach allows all create, read, update and delete operations, which reduces trust. Information symmetry is higher in a blockchain-based system because the data in the block is immutable, but the data can be changed more easily with the traditional approach, resulting in less information symmetry. While the blockchain-based strategy is advantageous in the above characteristics, the old approach has a higher transaction speed.
To build a unique and secure blockchain-based crowdfunding platform and Ethereum smart contract. Use an iterative auction algorithm. There is no need for any mutual negotiation between investors and developers about project parameters. [3]	These are the following high-level steps: 1. An investor adds a new project to the decentralized crowdfunding platform. 2. Timestamp, project specification and estimated cost, time and reputation of the developer are contained in the block. 3. The block is sent to all nodes in the developer's network and they start bidding on the project based on time, cost, duration of support and votes. 4. Auction algorithms are operated by a smart contract that searches for the best developer for the project. 5. The block has been received and verified. 6. The block is added to the blockchain and connected to the blocks that came following it.
Give a brief overview of blockchain technology. [7]	An important step to creating trust in distributed systems is that blockchain provides a mechanism of distributed trust: multiple parties keep records of transactions, and each party can verify that the order and timestamps of transactions have not been tampered with.

Table -2: Types of crowdfunding

Type	**Description**
Donation-Based	Investors do not receive any benefits based on the donation. They simply donate because they feel good about helping the project or because they believe in the cause. This type of crowdfunding platform acts as an intermediary for charities and NGOs.
Reward-Based	Reward-based investors receive a free sample product to back the idea. The main motive of this type of crowdfunding is the good feeling of placing a name in the list of contributors.
Crowdinvesting	Investors receive shares as a return on investment.
Crowdlending	This type of crowdfunding is also called "Peer-To-Peer lending", "Loan-Based lending". In this type, the borrower, i.e. the owner of the product, takes a loan from investors at a fixed interest rate.

3. MOTIVATION

The main objects of this exploration are to understand the crowdfunding lifecycle, address common issues in backing operations, and develop a blockchain- grounded backing system that eliminates the limitations of traditional styles. While the Fundraiser operation is a useful platform for launch-up authors, it has the excrescence of giving complete control of the finances to the crusade creator. This approach doesn't involve benefactors in the decision- making process regarding the use of finances, and the success or failure of the launch- up depends entirely on the crusade creator's decision-timber. To address this, the exploration aims to produce a blockchain- grounded backing system on the Polygon platform that involves investors in the

decision- making process and eliminates single- person decision- timber and power of finances. The smart contract controls the spending of finances by the crusade creator.

4. IMPLEMENTATION

Perpetration of blockchain grounded crowdfunding platform involves following way —

1. *Design and Implementation of Smart Contracts* –

It is a piece of code created in the computer language Solidity. There are two smart contracts in use:

a) Campaign Factory –

Campaign Factory, which provides a catalog of addresses for all deployed campaigns, is in charge of deploying new instances of campaigns on the Polygon test network and storing the resulting address. The contract's variables are listed in Table 3, and its features are listed in Table 4.

b) Campaign –

It is in charge of overseeing all operations pertaining to a particular campaign instance. The contract's variables are listed in Tables 5, 6, and 7, while its capabilities are listed in Table 7.

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 campaign instance and saves the resulting address.
getDeployedCampaigns	Returns a list of all deployed campaigns.

Table -5: Campaign Contract – Variables

VariableName	**DataType**	**Description**
Manager	Address	The address of the person who is in charge of this campaign.
Minimum contribution	Unit	The minimum contribution required for a contributor to be considered an approver.
Approvers	Mapping	List of ethereum wallet addresses of every investor who contributed to the campaign.
Requests	Request[]	A list of requests that themanager 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	A constructor function that sets the minimum contribution and the campaign manager.
Contribute	It is called when someone wants to donate money to a campaign and become an "endorser".

createRequest	A manager called to create a new spend 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.

1. *Smart Contract Compilation* –

The smart contract is compiled using the solidity compiler to generate bytecode. The bytecode is a hexadecimal representation of the assembled contract that only the Polygon Virtual Machine (EVM) understands..

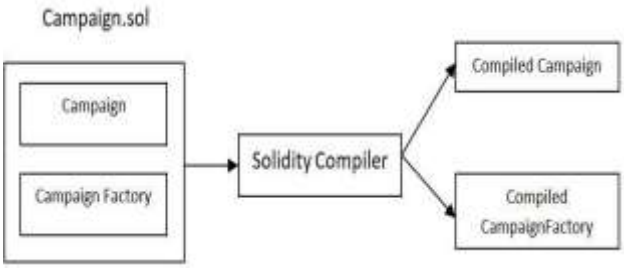


Fig -4: Smart contract compilation process

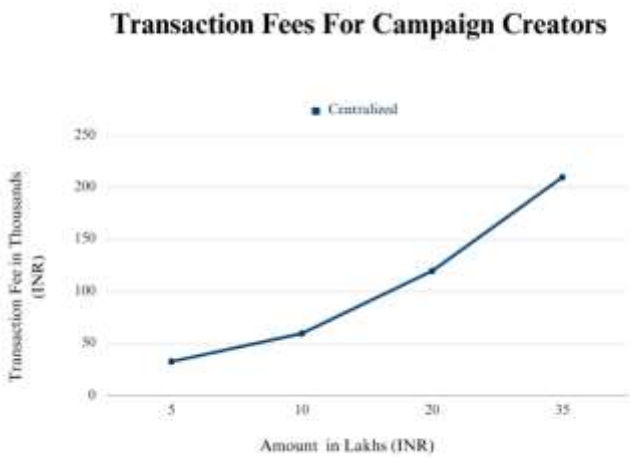
2. *Deployment* –

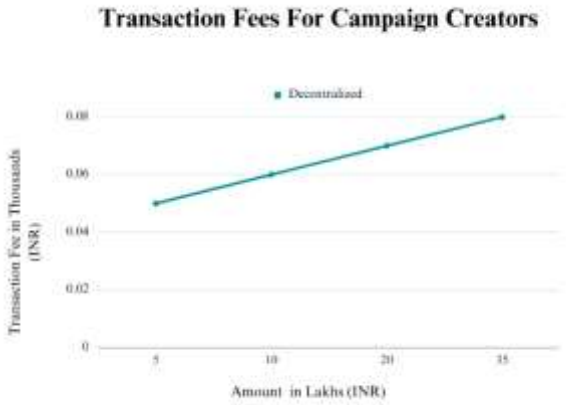
Bytecode generated for each of the smart contract – CampaignFactory and Campaign is deployed to the Polygon test network – matic test network. In this process, the implementation script uses the truffle/hdwallet provider - a Web3 provider with HD Wallet support.

3. *Interacting with deployed contracts via the user interface* –

The user interface for the blockchain-based crowdfunding platform is developed using Semantic React UI, Next.js, and the Polygon wallet Metamask. Metamask is a browser extension that enables end-users to interact with the smart contracts deployed on the Matic test network. The Semantic React UI framework is used to create a responsive and user-friendly interface for contributors to browse and select campaigns, donate funds, and vote on spending requests. Next.js is used as the front-end framework to provide server-side rendering, allowing for better performance and SEO optimization. The integration with Metamask enables secure and easy-to-use interaction with the blockchain network.

5. RESULTS





COMPARISON CHART

FEATURES	TRADITIONAL	DECENTRALIZED
Cost	Approx. 10-12% of transactions	Only Gas Fees = 0.0256-0.03302 matic
Transparency	No, everything is in database	Yes, everything is available onchain
Payment Processing Fees	3-5%	0.5-1%
Security	Traditional Security systems	Backed By Blockchains Security

6. CONCLUSION

A blockchain-based crowdfunding platform can offer greater dependability and credibility in comparison to conventional crowdfunding platforms by making use of the intrinsic characteristics of blockchain technology, such as immutability, decentralization, and transparency. All transactions in a blockchain-based system are recorded on the blockchain, making them transparent and immutable. This reduces the need for middlemen and fosters greater participant confidence. Smart contracts can also be used to automate fundraising procedures and impose terms and conditions, which improves security and lowers the possibility of fraud.

A. Reliable, Transparent, Trustworthy

A smart contract can be developed using a blockchain-based solution to track and manage each trade the product owner makes. The product proprietor must submit a spending request outlining the resource and the budget before spending any money on it. For each spending proposal, the voting system tracks the votes from donors. If more than half of the contributors consent to the expenditure request, the product owner can only move forward with paying for the resource. This approach involves investors in every transaction, which increases the crowdsourcing platform's transparency, dependability, and reliability. Once a block is put to the blockchain, it cannot be altered or removed, which increases the security of the application.

B. Secure, Decentralised

A decentralized database shared by computer network components is known as a blockchain. Once data has been accepted and added to the blockchain, it can be challenging to control or remove it because, if you tried, the following blocks in the chain would refuse the change (because their hashes wouldn't match). The blockchain will crash as a consequence of information change, and the reason why will be clear. Traditional data sets, where data can be readily changed or removed, do not have this property. Once a block is added to the blockchain, it cannot be altered or removed by anyone, making the application more private.

Although blockchain technology shows great promise, its present form may prevent it from reaching its full potential. To enhance its capabilities and provide support for complex apps that can operate on the network, core blockchain technology research must be coordinated.

7. FUTURE SCOPE

In this work, a blockchain-based crowdsourcing prototype that does not utilize actual cryptocurrency is installed on the Matic network, a Polygon test network. Future deployments of the program to the production environment are possible. Real investors can use genuine cryptocurrency to fund creative start-ups.

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 Polygon 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, Polygon 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.