

Crowd Funding using Blockchain

Suryansh Jaiswal, Rudrendra Bahadur Singh, Suraj Yadav, Vishal Kumar
*Department of Computer Science and Engineering,
Babu Banarasi Das Institute of Technology and Management, Lucknow, India*

ABSTRACT

Crowd financing is an internet fundraising approach that started as a way for the general public to give modest sums of money to assist creative people fund their projects. Individuals can invest in entrepreneurial start-ups via crowdsourcing through an intermediary, such as a broker-dealer. The problem with the present sites is that they do not offer a Donor Guarantee Policy, and they have no control over the funds they have contributed. The purpose of this article is to suggest the use of blockchain technology for crowdfunding. We can provide a safe, secure, and transparent crowdfunding platform as a result of this. This paper's goal is to build interactive forms for campaign creation, contribution, and request approval so that campaign creators and donors may easily establish and support campaigns. The money that was sent to the donor may be tracked. All transactions will be recorded and stored in a block on the Blockchain.

Keywords- Crowdfunding, Blockchain, Campaign, Smart Contracts, Request-Approval, Consensus

INTRODUCTION

The blockchain is a decentralised digital ledger that keeps track of all transactions. Because it is a distributed system, every node in the decentralised network stores all of the records. Smart Contracts are Ethereum-based programs that operate on the blockchain.

The Ethereum Virtual Machine is used to operate all Smart Contracts. Crowdfunding makes it simple to raise funds for new project ideas. The issue with today's crowdfunding organisations is that they charge exorbitant fees, and fraud does occur sometimes. Avoiding these issues can be as simple as using a blockchain-based crowdfunding campaign.

Traditional transaction costs and platform fees generally associated with other crowdfunding sites, such as Kickstarter, are eliminated by using Peer to Peer smart contracts for crowdfunding.

Our project's goal is to develop a dependable application that will allow every fresh concept to come to reality. We created a crowdfunding platform that is built on the blockchain. On this programme, we give an easy-to-use interface for anyone to generate and share their ideas. These ideas are then made available to the whole audience. Anyone who wants to support their ideals is welcome to do so. All of these procedures are carried out in a collaborative manner.

PROPOSED SYSTEM

The problem with the current method is that firms charge both the donor and the consumer a high fee. The project is developing since there is no track of the money records, transparency, or contact between the investor and the user. When it comes to crowdfunding with existing businesses, the major issue is trust. None of these organisations provide a donor guarantee policy. - Lacks Transparency

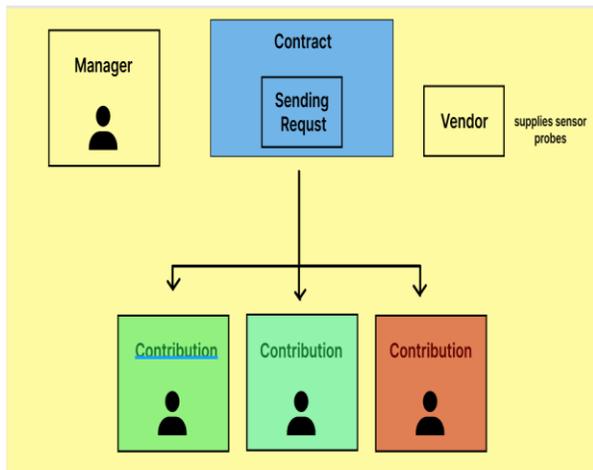
- High Charges
- Donor guarantee policy not available
- No track of Records

The campaign developers will put their project ideas in the campaign, and interested individuals will pay funds to the project concept, according to the provided system. Where it differs from traditional crowdfunding is that all funds are now held in digital currencies such as ether. All ether coins will be logged in the blockchain and kept track of. In this scenario, blockchain is an immutable ledger. The money that has been provided is under the hands of the Donor. The donor has complete control over the money they invested thanks to the Request approval module. Only if two out of every three investors must agree to the founders' desire. The Trust is created by delegating power over invested funds.

- Trust
- Control Over Money
- No Charges
- Donor Guarantee Policy
- All Transactions are Recorded
- Money is Stored Securely

SYSTEM IMPLEMENTATION

Solidity is used to install contracts on the blockchain platform, hence all contract code is written in that language. The Campaign Factory is created, which includes all of the source code needed to launch new campaigns across the network. New campaigns can be designed with the help of campaign factory. A one-time gas fee is required whenever a campaign factory is deployed, and it is a relatively tiny sum. The new Campaign is initially developed by providing the project's Idea, the project's Minimum Contribution, and a full description of the initiative. A block is created and added to the blockchain when a new campaign is created. Figure 1 depicts the system's architecture.

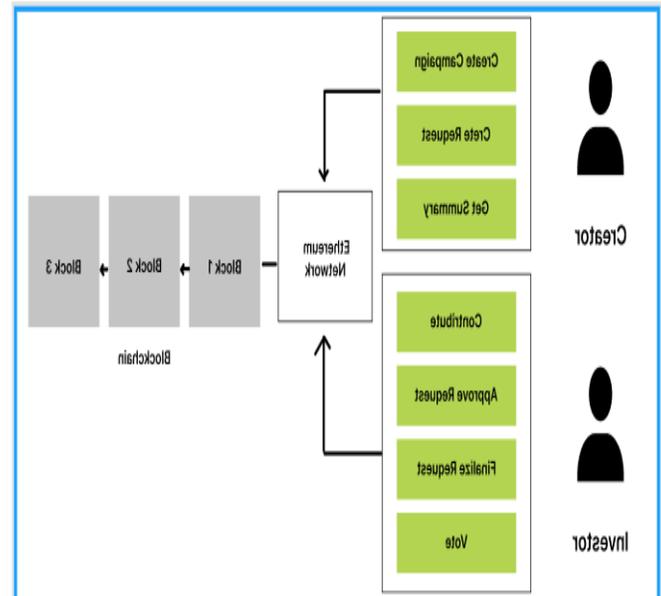


The solidity programming language is used to implement the suggested system. The Campaign Factory and Campaign file are compiled into bytecode and abi using the Sol solidity compiler. The abi is in JSON format and is used to connect with the front-end in the Bytecode, which will be distributed on the blockchain. React.Js, Next.Js, and Semantic-UI are used to create the front-end. The user interactive form will be utilised to make it simple to contribute. The project's developer or management will ask for funds to purchase some accessories. He'll use the request form to make a request. This will be recorded in the blockchain and stored there. If the request is necessary, all investors must approve it. They have the option to refuse the request if this is not the case. The request will be confirmed once all of the investors have voted; a minimum of 1/2th of the investors must approve the request. The money will be transferred to the vendor if it meets the requirements.

METHODOLOGY

A. Overview

Crowdfunding and cryptocurrency are both hot topics on the internet, and they go hand in hand. One possibility for reducing the challenges that arise in crowdfunding is to employ blockchain technology. The contract specifies that all funds will be deposited into the pool. The money will be sent to the beneficiary after the request satisfies the given criteria. The working model is shown in Figure 2. Ethereum is an open-source, public, blockchain-based distributed platform and operating system that supports smart contracts. It's a modified Bitcoin that uses transaction-based state changes. The Ethereum platform generates and uses Ether, which is a cryptocurrency. The Ethereum Virtual Machine (EVM), a decentralised operating system, allows an application to run on public nodes.



B. Blockchain

The blockchain is derived from the Bitcoin, which was created by unknown individuals. The Blockchain is a set of blocks that are continually expanding records. Each Block is connected to the next, and cryptography was used to secure them. Integrity, decentralisation, immutability, security, and anonymity are all properties of blockchain. There are three different types of blockchains: Bitcoin and Ethereum are examples of public blockchains; Hyperledger and Ripple are examples of consortium blockchains; and private blockchains are examples of private blockchains

C. Peer to Peer

The Peer to Peer (P2P) mechanism is a critical component of how blockchain operates. Every node in the network is connected to the blockchain. This implies that information saved on blockchain cannot be lost or erased since doing so would need the destruction of every node on the network, which is impossible.

D. Consensus Protocol

In blockchain technology, the consensus protocol is the most critical. The Blockchain consensus process is what keeps all of the nodes' blocks in sync with one other. The term 'consensus' refers to the requirement for all nodes to agree on the same state of the blockchain. The consensus process allows the blockchain to be updated every minute (depending on the network) and assures that each block is correct. The consensus protocol's goal is to ensure that all nodes utilise and follow the same chain.

E. Proof of Work

Many cryptocurrencies employ proof of work (abbreviated to PoW) as a consensus process. Mining is the name given to this operation, and miners are the nodes that make up the network. The Proof of Work is a mathematical issue that needs a significant amount of effort to solve. The only way to address the problem is for each node in the network to go through the procedure via trial and error. A miner will keep trying different unique values until he or she finds one that works. The miner who succeeds in solving the problem will add the next block to the chain, validating all transactions within it and getting the reward linked with it. The block is depicted in Figure 4.

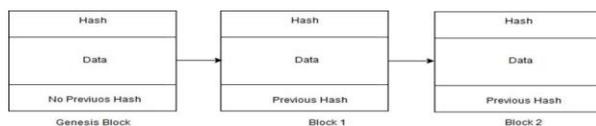


Fig. 3: Blockchain

Block #12345
Timestamp: 1519156432
Nonce: 125376
Transactions: 0x2446f1fd773fbb9f080e674b60c6a033c7ed7 0xe084fe4397a8aa889df50f85a6f400f0eb1b7
Prev hash: 00007851A8D01E4
Hash: 0000DAB128901AC

Fig. Illustration of

F. Modules

- 1) Campaign Creation
- 2) Create Request Module
- 3) Request Approval Module
- 4) Finalize Module

1) Campaign Creation

Making an instance of the Campaign factory creates a new campaign. To build a new campaign, the user will utilise the user interface to access the campaign factory. We must supply a campaign title, a minimum donation, and a campaign description in order to establish a campaign. A specified quantity of gas charge is required for each transaction to be processed. As a result, when the user selects the "Create" button, a new campaign with gas fees will be established. The transaction will be completed in 15 to 30 seconds, and a new block with the contract address will be added to the blockchain. The campaign will appear on the home page after it has been established. It may be interacted with by both the user and the donor. To start a new campaign, the contract's create campaign function is used. An E-Wallet or account is necessary to manage the transactions associated with the campaign once it has been created and posted to the blockchain. Because every update to the blockchain requires payment of a charge in order for the transaction to be legal, this cost is referred to as the gas fee. The Create Campaign Module is shown in Figure 4.

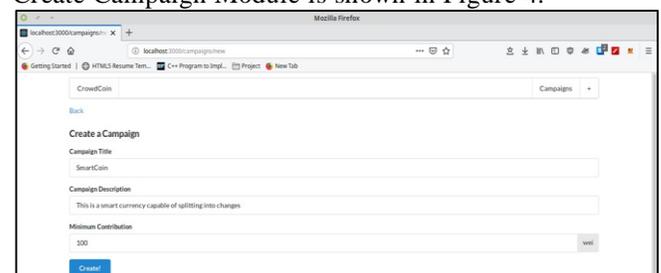
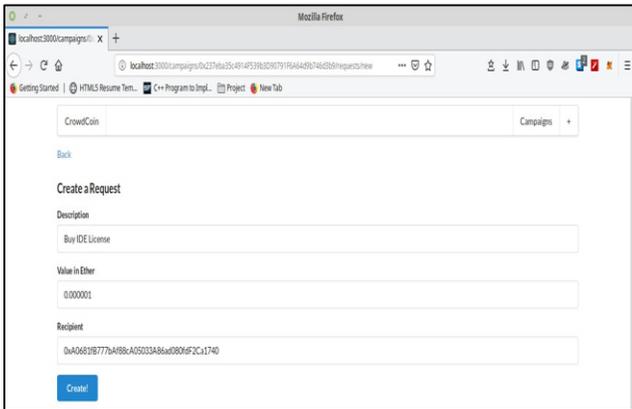


Fig. 4: Create Campaign

2) Create Request Module

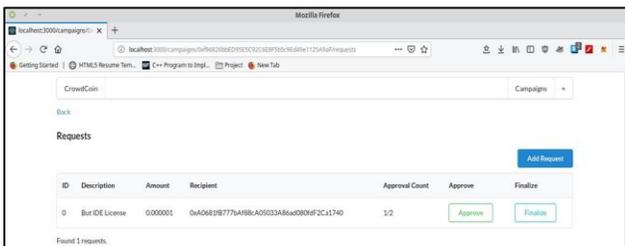
Donors will give and contribute to a new campaign when it has been created. The user cannot use the money directly; instead, they must submit a request for usage. For example, if the user wants to purchase something for the project, he must first write a purchase request that includes all of the necessary information as well as the vendor's address. The transaction will then be completed, and a block will be added to the blockchain. He is unable to spend the funds immediately since doing so would expose him to the numerous frauds that have plagued several crowdfunding platforms. Figure 5 illustrates how to make a request.



FigCreate

3) Request-Approval Module

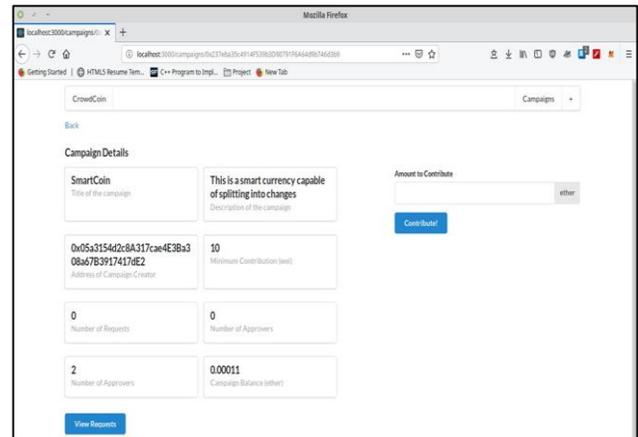
The developer of the campaign will submit a request for funds to purchase accessories or other items with documentation. The developer will then notify all investors that he or she has to spend some money. As a result, if the investor desires, he must approve the proposal. For each investor, only one approval is allowed. All investors should vote at a certain time. The approval of all requests will be recorded and stored in the block. The investor will not be able to grant consent again after then. The Request-Approval Module is depicted in Figure 6.



FigApproval

4) Finalize Module

All of the approvals were recorded when the Investor voted. If the approval exceeds the stated criterion, such as two-thirds, the funds will be instantly sent to the Vendor to whom the creator must send. The blockchain stores all of the transactions. The author should include specific information about the seller as well as the address to which money should be sent. The campaign detail and summary will be displayed when the money has been transferred. The comprehensive description of the campaign is shown in Figure 7.



FigCampaign

CONCLUSION

The use of blockchain in crowdfunding is a novel notion to the community. We've taken that into account and built this software to be simple enough for even the most inexperienced user to use. However, the storey does not finish here. With the advancement of blockchain technology and the introduction of initial coin offerings (ICOs), our application has a bright future and plenty of room for innovation and evolution. The world is still adapting to Blockchain and Cryptocurrencies, and Ethereum-based Dapps will take a few years longer to gain popularity and recognition from the community. In this context, a Blockchain-based crowdfunding application is a difficult notion for everyone to grasp. We've taken that into account and built this software to be simple enough for even the most inexperienced user to use. But the storey doesn't end there. With the advancement of blockchain technology and the introduction of initial coin offerings (ICOs), our application has a bright future and plenty of room for innovation and evolution. Through our crowdfunding

application, we hope to make it even simpler and safer for all ideas to come to life in the future.

REFERENCES

- [1] Shuai Wang, Liwei Ouyang, Yong Yuan, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends", IEEE Trans. on Sys. Man and Cybernetics, Feb 2019, 2168-2232.
- [2] Yong Yuan, Fei-Yue Wang, "Blockchain and Cryptocurrencies: Model, Techniques, and Applications", IEEE Trans. on Sys. Man and Cybernetics, Sep 2018, 2168-2232.
- [3] Bhabendu Kumar Mohanta, Soumyashree S Panda, Debasish Jena, "An Overview of Smart Contract and Use Cases in Blockchain Technology", 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Oct 2018, 978-1-5386-4430-0.
- [4] Yi-Hui Chen, Shih-Hsin Chen, Iuon-Chang Lin, "Blockchain based smart contract for bidding system", 2018 IEEE International Conference on Applied System Invention (ICASI), Apr 2018, 978-1-5386-4342-6.
- [5] X. Wang, X. H. Zheng, X. Z. Zhang, K. Zeng, F.-Y. Wang, "Analysis of cyber interactive behaviors using artificial community and computational experiments", IEEE Trans. Syst. Man Cybern. Syst., Jun. 2017, 995-1006.
- [6] F.-Y. Wang, Y. Yuan, X. Wang, R. Qin, "Societies 5.0: A new paradigm for computational social systems research", IEEE Trans. Comput. Social Syst., Mar. 2018, 2168-2232.
- [7] Vitalik Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform" [Online]. Available: <https://github.com/ethereum/wiki/wiki/White-Paper>. [8] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system", [Online]. Available: <https://bitcoin.org/bitcoin.pdf>.