International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

CrowdFund: CrowdFunding Decentralized Implementation on Ethereum Blockchain

Sukhvinder Singh Bamber *[1]

Submitted: 03/11/2022 **Accepted:** 01/02/2023

Abstract: The Ethereum blockchain platform's decentralised application (DAPP) called crowdfunding enables users to donate money for causes they care deeply concerned about. We can ensure that contributors engage in low-risk backing of emerging ventures and venture capitalists by leveraging blockchain and verifying their transactions and securing the sensitive data. More global supporters can be attracted by creators, which makes it simpler for them to raise significant sums of money quickly. There are a number of projects in the blockchain realm right now. Individuals or small dispersed teams who want to raise funding by issuing tokens have built on this platform to attract the potential contributors. The concept of raising funds through a crowdfunding site is simplified. With the help of global assistance of the public who may be interested to contribute in the campaign for a monetary incentive so that it is beneficial to the contributor as well as the creator and the cause for which the crowdfunding DAPP is being made.

Keywords: *CrowdFund, Blockchain, Ethereum Virtual Machine, Consensus, MetaMask, DAPP.*

1. Introduction

Philanthropy has become more open and transparent as a result of the growth of Internet technology, which has increased the number of avenues via which individuals can obtain information. Numerous issues with philanthropy have been revealed [1]. During a natural or man-made disaster, supplies and money are donated. The everyday administration of philanthropic resources, however, is confusing. Both the willingness to give and the amount given decreased as a result of these conditions. Crowdfunding-online has emerged as a new avenue for the netizens to support causes related to public welfare.Raising certain amount of money in more or less required amount from a sizable (manageable) group of netizens known as crowd for supporting a certain cause, project (business), medical emergency, loan or a financial need via chosen platform is CrowdFunding [2]. There are several instances of unknown individuals or businesses receiving funding from others on the basis of social connections on the enabling platforms like: Twitch, Patreon, IndieGoGo, and Kickstarter [3].However, blockchain technologies have fundamentally altered how we view the Internet. More precisely, the blockchain has fundamentally changed how we think about finances, communication trust, and even revived the idea of digital democracy [4]. Many of the principles in the "hyper-connected and trusted world" vision were already becoming widely accepted notions, but the blockchain has provided the instruments for their quick implementation without the need for a third party (thanks to smart contracts) [3]. Thus, the Blockchain has been enabling technologyfor the rapid development of decentralized currencies and smart contracts (Digital Contracts – self executing). Also, the Blockchain is the building block for the Smart Property (Intelligent assets those can be managed via Internet).

1 Computer Science & Engineering, University Institute of Engineering & Technology, Punjab University SSG Regional Centre, Hoshiarpur, Punjab, India.
ORCID ID : 0000-0002-1749-2940
** Corresponding Author Email:ss.bamber@pu.ac.in*

In this paper, we introduce CrowdFund, a social networking platform that allows users to fundraise for other users using a straightforward web Dapp created on top of the Ethereum blockchain. Through the use of smart contracts, CrowdFund makes it simple for anyone with a project to raise money from the public. The word "something" in this sentence suggests that any financial need, loan, project – business, emergency can be popularized and promoted by a user using the CrowdFund website. A decentralised online service called CrowdFund uses smart contracts to handle and regulate money.

2. Literature Survey

In previous papers we have seen that people who want to raise funds for a cause, visit the crowdfunding DAPPs and give all the details about the cause and create a campaign. After that people who are interested in the cause can help the creator by donating funds to the campaign, and in return the creator will issue some tokens in return to the investors so that when the purpose of the campaign is completed, the investors can use the tokens as some kind of perks given by the creator.

2.1. Blockchain

A distributed, duplicated digital ledger which manages each and every transaction that is executed over Internet / Intranet makes up a Blockchain. Every block of a chain consists of multiple transactions and the ledger of each participant is updated with the copy of every new transaction executing in the Blockchain. Further, Distributed Ledger Technology (DLT) is used for implementing distributed databases that are controlled by the participating netizens [5]. Each transaction in the Blockchain is recorded with the hash (Cryptographic Signatures which are immutable). Each block consists of information about the transaction, timestamp, and hash (cryptographic) of proceeding block (Merkle tree representation). The timestamp proves the existence of transaction information at the time of block release.

Implementation and execution of distributed ledger requires that Blockchains be managed in peer – to – peer (P2P) networks as these networks implement and follow a particular protocol for communication and validation of new blocks. Blockchains by the way they function and work can be considered as secured on the basis of design. Further, it can be considered as a perfect example of distributed environments with high degree of Byzantine fault tolerance, inspite of the Blockchain records being modifiable because forks are conceivable [5].

On the basis of research carried out by S.Haber, W. S. Stornetta and D. Bayer, a netizen or a group of netizens online by the name Satoshi Nakamoto in 2008popularised the blockchain to act as the public transaction ledger of the cryptocurrency bitcoin. Till date, identity of Satoshi Nakamoto's stands as a mystery.

Integration of blockchain technology is possible in many fields. Blockchains are primarily used as a distributed ledger for cryptocurrencies, Smart Contracts, Financial Services (DEX, DAO, DeFi, etc.), Games, Supply Chain, Voting, Anti-counterfeiting, Healthcare, and a wide range of other applications.

2.2. Working

Each block in a blockchain is made up of a block header and a block body. Each block is identified by a hash that is produced on the block header using the SHA256 cryptographic hash method. Block Header contains the Metadata while the block body contains the transaction data. The block header also includes PrevBlockHash (previous block's hash value), Timestamp, Merkle Root (Tx root) and random number (Nonce) [6].

The block body of a Merkle Tree retains a large number of transactions from the block before it. The non-leaf node holds the hash value of every leaf node below it while the leaf node in the Merkle Tree retains the hash value of the transactional data. Following the transaction, each node engages in a consensus mechanism competition for accounting rights. All transactions that took place during a certain time period will be packaged by the winning node. All nodes will verify the block when it has been disseminated throughout the whole network. Once the vast majority of nodes have successfully authenticated, the block will be added to the chain.

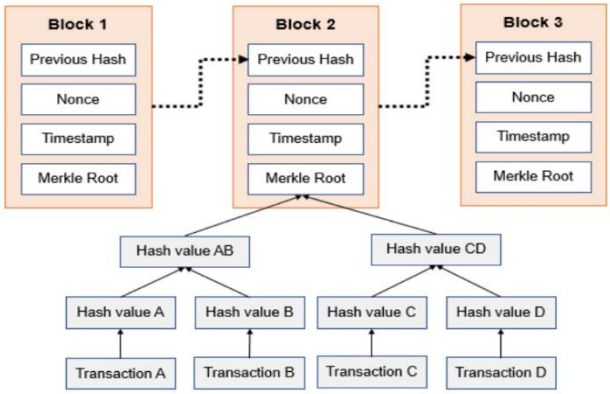


Fig. 1. Structure of a block in blockchain

2.3. Ethereum

Ethereum is a decentralized and open-source blockchain that implements smart contracts. A well-known blockchain called Ethereum encourages the creation of decentralised apps based on the solidity scripting language, which is Turing complete. In Ethereum, each user has access to a shared virtual machine, which is controlled by no one. It is always accessible, and nobody has the power to censor it or stop it from running. Ether is a cryptocurrency that is connected to Ethereum. Ether is a cryptocurrency that can be used to make transfers between accounts and to pay the miner nodes that keep the blockchain evolving. [4].

2.4. Smart Contracts

An essential part of the Ethereum system are smart contracts. They are blockchain-based computer programmes that are activated by particular transactions. They are not ruled by a single entity. Once they are placed on the blockchain, they are also traceable and immutable. Currency, data, and executable code can all be stored in contracts. Both new contracts and those already in existence can communicate with them. Smart contracts are created on the Ethereum network using the Solidity programming language. [4].

2.5. DAPPs

Digital apps or programmes known as "decentralised applications" (DAPPs) exist and operate on a P2P network rather than a standalone system. DAPPs fall outside of a single authority's jurisdiction and control. On the Ethereum platform, DAPPs are frequently created for a range of uses, including as gaming, finance, social networking, etc. [7].

Unlike conventional applications, DAPPs execute their backend code on decentralized networks (P2P mode) while conventional applications execute their backend code on centralised servers. Any language that can call its backend can be used for the frontend code and user interfaces of a DAPP. Blockchain platforms like Ethereum or Bitcoin are used to store and run decentralised applications [8]. DAPPs often have open-source code. Tokens are used as incentives to encourage DAPP validation when it complies with a particular protocol that has been adopted by the community.

3. Problem Identification

While going through the research papers of all the previous models that were made based on the idea of a decentralised crowdfunding application and the challenges people faced while using these applications, we came to a conclusion that they were all somewhere lacking a security mechanism that could prevent any fraud from happening under the name of crowdfunding. So we decided to go build such a dAPP that consisted of a consensus algorithm or consensus protocol in which the security of the crowdfunding application could be boosted and the chances of any fraud taking place could be reduced to minimal.

The major or the common problem that was seen across all the previous decentralised crowdfunding applications was that their security system somewhere lacked a mechanism or algorithm that was hard to breach. So we have tried to add a strong security mechanism in the application which verifies each and every transaction through multiple nodes and reduces the chances of any malicious activity taking place.

3.1. Consensus Protocol

A consensus protocol is a fault tolerant mechanism used in blockchain systems over networks which obtains the minimum required consensus from distributed processes or multi-agent systems for a single data value or a single state of a network.

In our DAPP, the funds will not be released until a consensus of more than 50% is reached, i.e. until more than 50% of contributors approve the transaction. This will help against fraud campaigns.

In decentralized consensus, all of the participants have right to give access. But in centralized consensus, the right to give access is held by only a single authority or person.

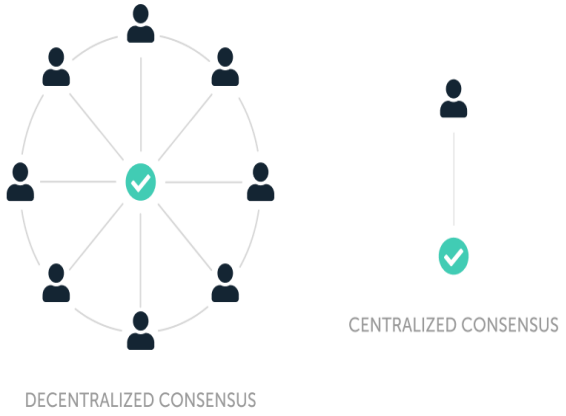


Fig. 2. Difference between Decentralized and Centralized Consensus

4. System Description

The goal of the crowdfunding DAPP is to establish an environment where anyone can easily launch or support a campaign intended to develop new goods or services. With the help of the crowdfunding DAPP platform, groups or people, including startup founders, business project managers, musicians, filmmakers, and others, will be able to raise money by accepting ethers from contributors or investors. [9].

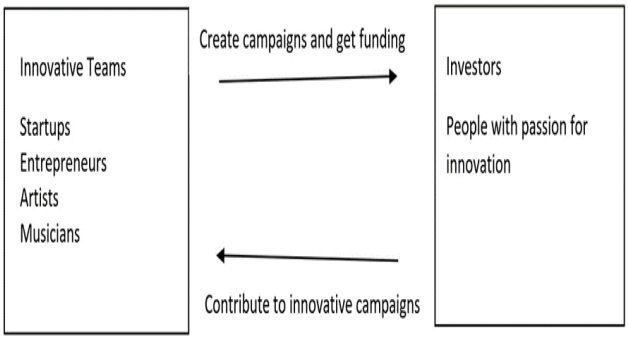


Fig. 3. Interaction in Crowdfunding Campaign

Ethereum-based smart contracts that have been installed control the campaign's finances. There is no blockchain storage for a campaign's metadata, such as the manager's address, the minimum contribution, the campaign balance, the number of contributors, and the number of requests. The two actors "manager" and "contributor," who utilise the platform for their needs, are used throughout this report. If we do not distinguish between the roles, we refer to both of them as "users." When a person or group uses the platform to establish a campaign and raise money, we refer to them as "managers." Examples of such groups include startup teams, artists, directors, and entrepreneurs. A manager or creator needs to have a clear idea of the campaign they want to build and how their product or service will benefit the contributors who use the platform.

All the metadata of a campaign is necessary when creating a campaign. In order to get the funds if his request is successful, he must also provide his Ethereum wallet address (i.e. address of manager). There is no certainty that the campaign will succeed; it all rests on the creator's study into how much the product/service is needed in the market and how he can get contributor interest for his campaign.

When a contributor visits the crowdfunding DAPP site, he or she can browse all of the campaigns and deposit ether to support their favourite campaign. For investing and paying for the transaction (gas) to be mined, the contributor must have enough money in his wallet and he must contribute minimum amount of fund (i.e. minimum contribution) so as to become a contributor.

The goal of UI is to make it as easy as possible for creators and contributors to use the platform and accomplish their objectives. The following fundamental UI features are essential for effectively using the platform: • Provide an interface for listing all campaigns.

- Offer a user interface that displays information about a certain campaign.
- Offer a platform for contributing to or investing in a campaign.
- Offer a campaign creation interface.
- Offer a request creation interface.
- Offer a platform for listing all campaign requests and approving / completing them.

The languages, tools and frameworks used to create this DAPP are:

• Solidity - high-level language (object-oriented) for constructing smart contracts, and JavaScript, frequently abbreviated as JS, are the languages used for the backend in the crowdfunding dapp. Both of these languages adhere to the ECMAScript specification.

• The languages used for front-end development include Next.js built on top of Node (open-source development framework) and ReactJS, an open-source front-end JavaScript toolkit for developing user interfaces and UI components. JavaScript enables server-side rendering, dynamic routing, and the creation of static websites for react-based web applications, and "Semantic-ui-react/css" is a set of prebuilt, ready-to-use styling components for react.

Other Frameworks / Tools utilised include web3.js, a group of frameworks that enables communication over HTTP, IPC, or WebSocket with a local or distant Ethereum node; asynchronous testing, test coverage reports, browser support, and usage of any assertion library are all features of the JavaScript test framework Mocha, which is designed for Node.js apps; The most recent iteration of TestRPC, a quick and adaptable blockchain emulator, is GanacheCLI. It enables communication with the blockchain without the costs associated with maintaining an actual Ethereum node; Using the Ethereum Virtual Machine (EVM), Truffle, a top-notch development environment, testing framework, and asset pipeline for blockchains, aims to simplify the lives of developers. Infura, a Web3 backend and Infrastructure-as-a-Service (IaaS) provider that offers a variety of services, tools, and infrastructure for blockchain developers, is also provided. It is used to sign transactions for addresses derived from 12 or 24 words mnemonic. It provides developers with simple, dependable access to IPFS, Ethereum, and MetaMask, a software cryptocurrency wallet used to connect with the Ethereum blockchain, enabling them to quickly move their blockchain application from testing to scaled deployment. Users can use a browser extension or mobile app to access their Ethereum wallet, which can then be used to interact with decentralised applications.

4.1. Steps

Install Metamask chrome extension and create an account on it. Add some Ethereum tokens (Rinkeby Test Network Faucet can also be used). Now you can interact with the web app.

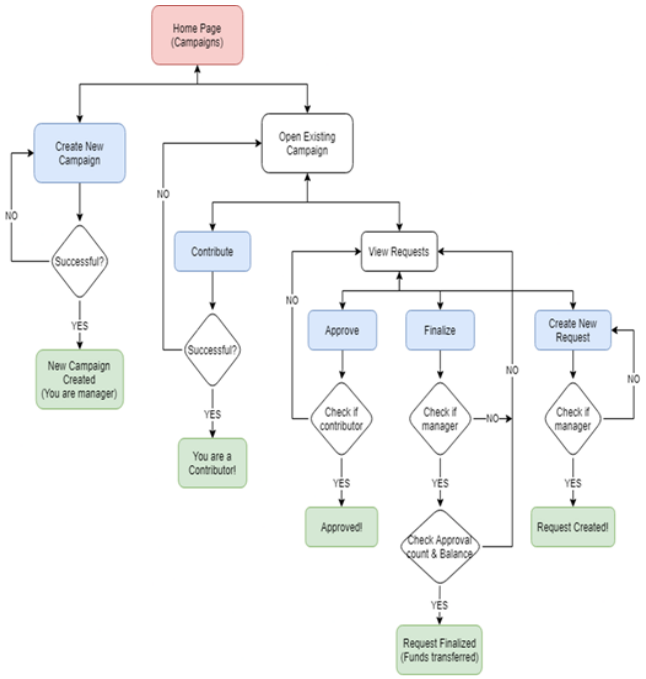


Fig. 4. Interaction with Web API

All interactions between a campaign manager (someone using the platform to raise money) and a campaign contributor are governed by the smart contracts created for the crowdfunding dAPP installed on the Ethereum blockchain platform. For instance, if a donor wants to contribute a certain amount of Ether to a cause that interests him, a transaction is made and sent to the Ethereum network along with extra Ether to pay for mining costs and the meta-data.

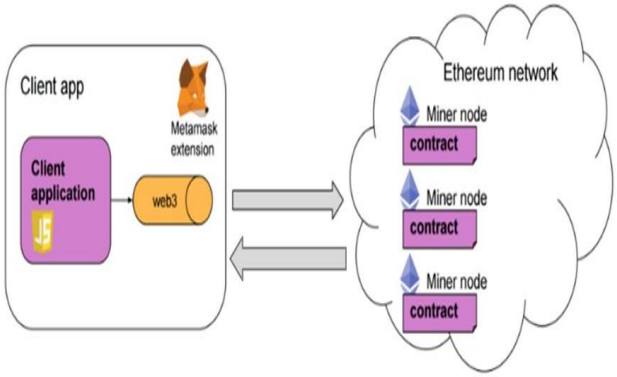


Fig. 5. Library Components using MetaMask to Communicate with Ethereum Nodes.

Fig. 5 illustrates how Metamask functions as a lightweight client that offers asynchronous capabilities to library components for calls to the Ethereum network using the web3 API. Additionally, Metamask monitors transaction processing and informs the library component on the progress of that transaction's mining. Before a transaction can be sent to the Ethereum blockchain, it must first be signed. This is handled by Metamask utilising the web3 library's available APIs. The transaction will be sent to the Ethereum network, where the smart contracts are deployed, via an RPC call made by Metamask after it has been signed. Using a callback function built into the library component, Metamask polls the Ethereum network to determine the status of the transaction and updates the library component.

5. Implementation and Discussions

In this decentralised crowdfunding application, through the use of consensus protocol only legitimate and trustworthy donations are allowed for the campaign after proper verification. The algorithm of consensus protocol consists of a mandatory requirement that the transactions which are verified by more than 50% of the nodes contributing in the network would be considered successful and hence validated for donation.

As a result, the transactions which will not be approved by 50% of the contributors would not be considered legitimate and hence rejected. The transaction will pop-up with an error message indicating there is a problem with the donation, due to which the option to finalize the transaction would not be visible to the manager. Thus, the consensus protocol helps in maintaining the integrity and security of the transactions taking place on the decentralised application which in return reduces the chances of monetary frauds and scams. The DAPP shows all the possible errors when triggered like insufficient funds in wallet, invalid input, unauthorized access (i.e. not a manager or contributor), etc. On every transaction, it will take about 15-30 seconds to confirm the transaction on blockchain. Each transaction on blockchain requires some amount of ether as gas fee, which is paid by the person doing the transaction.

5.1. Smart Contract Deployment

After deploying the smart contract on “Rinkeby Test Network”, it can be verified by finding the smart contract on the blockchain explorer (Fig. 6, https://rinkeby.etherscan.io/). The smart contract was deployed from wallet address “0x64a4a4f8575E48a941C73009BaE3f8F60053D912” and contract address generated is “0x40A5E44a24f7EAf8f38Fada53374E2788D4c50e8”.

5.2. Home Page

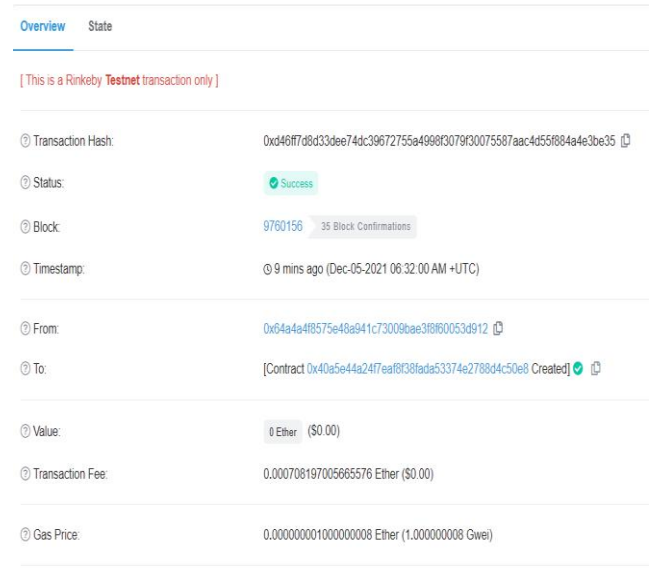
After deployment, the deployed contract is fetched by the frontend of the DAPP The home page displays the list of all the deployed campaigns along with the address of the smart contract on Ethereum Blockchain. Here we can either create a new campaign or view an existing one. (Fig.7)

5.3. Creating a New Campaign Page

To create and deploy a new Campaign on blockchain. It asks for a minimum contribution to be contributed by a person to become a “contributor” of the campaign. If at any transaction, the Metamask wallet show “Transaction Error. Exception thrown in contract code.”, then it indicates that there is an error and the transaction

will not be completed. (Fig. 8)

Fig. 6. Deployment of Smart Contract to Ethereum Blockchain.



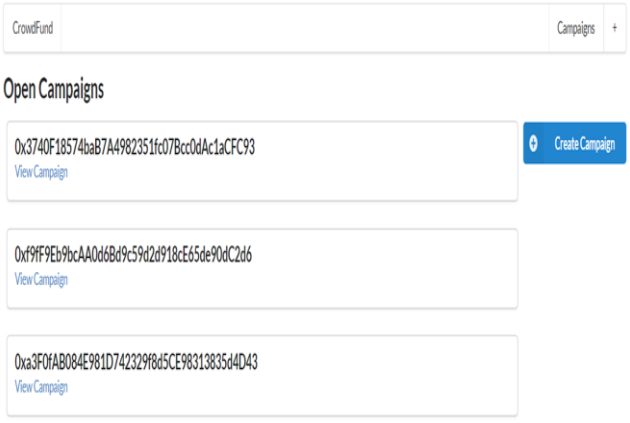


Fig. 7. Home Page.

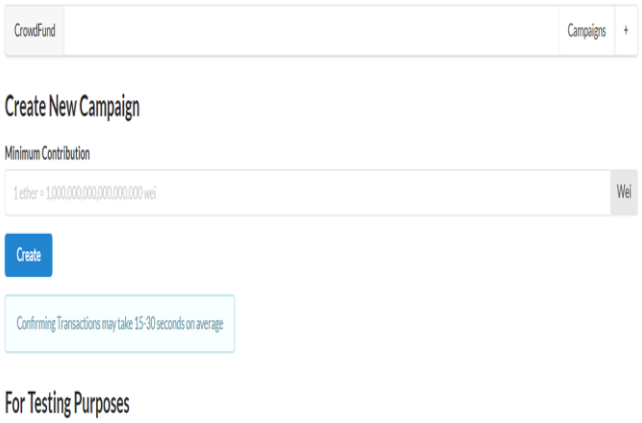


Fig. 8. New Campaign Page.

5.4. Existing Campaign Page

Display all the metadata of a campaign. It also gives the option to contribute to the campaign to become a contributor and a button to view all the requests of the campaign. A contributor can contribute any number of times. (Fig. 9)

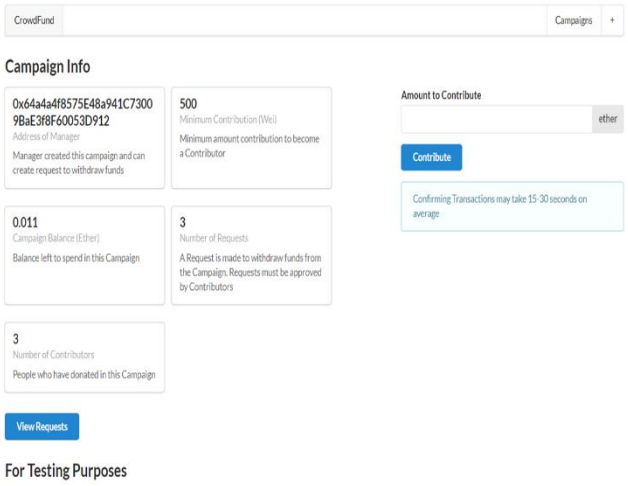


Fig. 9. Existing Campaign Page.

5.5. Requests Page

It shows all the requests of the campaign with two options of "Approve" and "Finalize". Only a contributor can approve a request if he thinks that the request is legit. After a consensus is reached (green background), the manager can finalize the request and the funds will be transferred from campaign to the Recipient by the smart contract after checking the balance of the campaign. After a request is finalized, it is marked as completed (grayed out). Here, there is a button to create a new request. (Fig. 10).

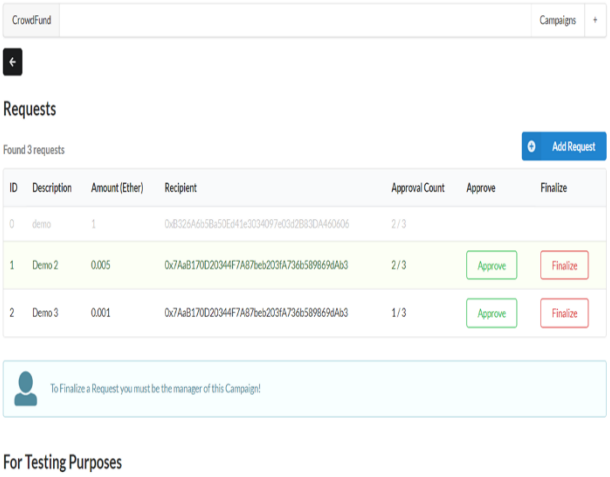


Fig. 10. Requests Page.

5.6. New Request Page

To create a new campaign, the manager must set the description, value and recipient's address. If all the inputs are correct and the request is being created by the manager of campaign then the transaction will be executed successfully, otherwise the wallet will show warning. (Fig. 11).

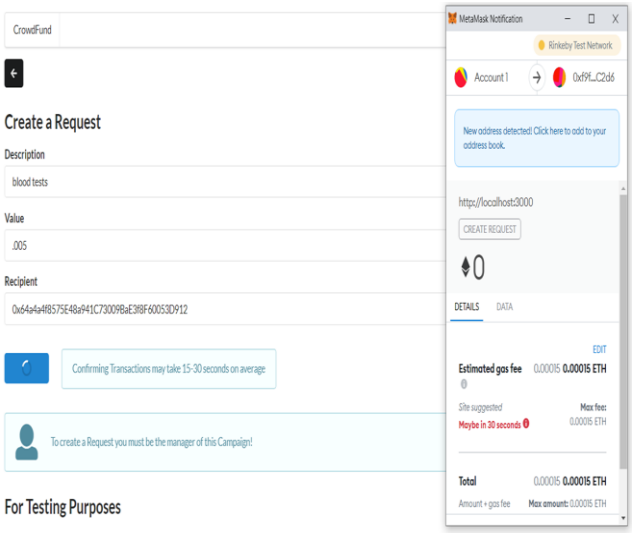


Fig. 11. New Request Page

6. Conclusion

It's crucial to test and construct new alternative architectures that show the concept behind offering fresh solutions as the world progresses toward Web 3.0 and decentralised systems to address common concerns. An alternative method based on a peer-to-peer network handling campaign transactions seems viable given that existing crowdfunding solutions are created and controlled by middlemen corporations that have a part in various campaign characteristics.

In a crowdfunding business use case, this research investigates solutions to eliminate intermediaries. This initiative also aids in the removal of any threat to the contributors' and campaign creator's sensitive data. The consensus protocol is a recently deployed technique that improves the security of this decentralised application while also assisting in the prevention of monetary fraud and other criminal conduct. This was implemented with the use of smart contracts, which were built for the crowdfunding DAPP application that was deployed on the Ethereum blockchain and direct the transaction's execution. Users can create and invest in campaigns that attract them, thanks to this interaction. Campaign creators and contributors can use the crowdfunding platform to carry out their targeted activities with little effort.

The only problem with the Ethereum blockchain is that, while it provides excellent security, the gas prices for each transaction are extremely costly. Despite the high gas prices, many other blockchains are emerging, such as Binance Smartchain (BSC), which is built on the Ethereum blockchain. Campaign creators who do not want to compromise data security and privacy continue to work on the Ethereum blockchain. Ethereum founder Vitalik Buterin has pushed out multiple improvements and updates for Ethereum, including EIP 1559 and Ethereum 2.0, which promise to reduce Ethereum's gas prices while simultaneously enhancing the blockchain's scalability.

References

[1] B. Hu and H. Li, “Research on Charity System Based on Blockchain”, SAMSE, IOP Conference Series: Material Science and Engineering, 2020.

[2] H. Baber, “Blockchain-Based Crowdfunding: A ‘Pay-it Forward’ Model of WHIRL”, International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-8 Issue-3, September 2019.

[3] M. Zichichi, M. Contu, S. Ferretti and G. D’Angelo, “LikeStarter: A Smart-contract based Social DAO for Crowdfunding”, arXiv:1905.05560v3 [cs.CY], 6th Nov 2019.

[4] V Buterin, “Ethereum: A next-generation smart contract and decentralized application platform”, White Paper, Vol:3, Issue: 37, 2014.

[5] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, www.bitcoin.org, 2009.

[6] A. M. Antonopoulos, “Mastering Bitcoin”, ISBN: 9781449374044, O'Reilly Media Inc., Dec 2014.

[7] J. Frankenfield, “Decentralized Applications (dApps): Definition, Uses, Pros & Cons”, www.inestopedia.com, Mar 2022.

[8] Weckerow, “Ethereum Documentation: Introduction to DAPPS”, www.ethereum.org, Sep 2022.

[9] S. S. Nagaraj, “Crowdsource Funding Solution Based On Blockchain Tokens”, California State University, Computer Science, Sacramento, 2018.