Harnessing the Power of web3: A Blockchain Approach to Crowdfunding

Richa Vivek Savant, S Navin Sunder, Spoorthi M, Shinu M Rajagopal, Roshni M Balakrishnan*
Department of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
*Corresponding Author: m_roshni@blr.amrita.edu

***Abstract*—Conventional crowdfunding methods frequently involve intermediaries, lack transparency, encounter regulatory challenges, and are not highly secure. Instead, a blockchain-based agreement can be formed, carried out, and enforced between members without the assistance of a third party. To achieve this, creating smart contracts, with blockchain-compatible executable code, is crucial. Additionally, cryptocurrency can be used, for which crypto wallets can securely store private keys, giving users access, control, and ownership over their digital assets while also encouraging decentralization and interoperability. Crypto wallets protect users' assets against cyber threats and unauthorized access by utilizing technologies like encryption, two-factor authentication, and multi-signature support to provide strong authentication and protection. Using a web3 platform like Thirdweb eliminates the need for an administrator by providing automated tools and infrastructure that streamline the creation, management, and deployment of decentralized applications. This study proposes the use of web3 technology to create a multi-user cross-platform blockchain-based crowdfunding DApp which employs Ethereum, smart contracts via solidity and crypto wallets for decentralized fundraising.**

***Index Terms*—Crowdfunding, Blockchain, Smart Contracts, Cryptocurrency, Crypto Wallets, Private Keys, Digital Assets, Authentication, Thirdweb, web3 Technology, DApp, Ethereum, Solidity**

I. Introduction

Traditional crowdfunding uses fiat currency, leading to higher transaction fees, currency conversion fees, and longer processing times due to intermediaries like banks. These platforms rely on email and password logins, making them less secure and more prone to breaches, risking user data and funds. Instead, a blockchain-based crowdfunding application which leverages cryptocurrencies and crypto wallets, providing stronger authentication, enhanced security, and user privacy can be implemented. For instance, in a traditional scenario, a supporter sets up an account using an email and password, links a credit card or bank account, and the platform processes the pledge through a payment gateway, incurring fees and potential charges. After a successful campaign, the platform deducts its fee and transfers the remaining funds to the creator's bank account, potentially delayed by banking institutions. Sensitive user data stored on centralized servers is vulnerable to breaches, highlighting the benefit of a streamlined, secure method of blockchain-powered crowdfunding. Additionally, in order to maintain transparency and control financial activities, these apps also need administrators to continuously monitor operations, which creates a single point of failure and increases the risk of malicious activity or human error.

Blockchain-based crowdfunding makes use of transparent, decentralized ledgers, and is a secure and efficient method of raising capital. Data integrity is ensured by the immutability of the blockchain, which reduces the likelihood of fraudulent activity during crowdfunding. This tactic increases diversity and confidence in fundraising efforts by cutting out intermediaries. Ethereum is a decentralized blockchain platform that is well-known for its Ether (ETH) currency and smart contract functionality. It enables the construction of decentralized applications and enables transparent and traceable transactions, ensuring accountability and security in its decentralized ecosystem. Sepolia is an Ethereum testnet (that mimics the Ethereum mainnet), designed for testing and development, allowing developers to deploy and test smart contracts and dApps without financial risk. MetaMask is a popular cryptocurrency wallet that facilitates communication between users and Ethereum blockchain decentralized programs (DApps). It enables the storage, transmission and reception of Ether (ETH) as well as other Ethereum-based ERC tokens. Because of its user-friendly interface, MetaMask is a vital tool for engaging with the decentralized ecosystem and bridging the gap between traditional internet users and blockchain technology.

Smart contracts are pre-written computer programs that function on Ethereum and other blockchain platforms. Once certain requirements are satisfied, these contracts automatically enforce and respect their terms. This automation of the fundraising process ensures that contributions and disbursements strictly adhere to predefined rules. Smart contracts improve productivity, security, and transparency across a range of industries since they don't need intermediaries to operate. They can be utilized for a variety of tasks including supply chain management, financial transactions, and contract negotiations, and provide a dependable and secure foundation for automated procedures. ThirdWeb is a trailblazing decentralized technology platform that is the first to incorporate Solidity smart contracts into its architecture. Solidity is a programming language designed specifically for Ethereum's blockchain to implement smart contracts, which enable safe and automated interactions between users, devices, and apps. ThirdWeb, renowned for its intuitive and user-friendly interface, simplifies the complexities of blockchain development. By leveraging web3 technology, it creates a decentralized and secure environment where applications are controlled by a network of nodes rather than a single entity.

Based on the aforementioned observations, the creation of a multi-user Ethereum-based crowdsourcing DApp is proposed, with the following implementations:

- Employing MetaMask as a cryptocurrency wallet and for user authentication to introduce added security.
- Utilizing Thirdweb's web3 technology along with smart contracts to automate transactions and ensure transparent and secure contributions, hence eradicating the need of an administrator.

II. Literature Survey

Naveen Kumaran et al., in his paper "Blockchain Based Crowd Funding" discusses how crowdfunding platform uses interactive forms to make it simple for users to participate in campaigns, and it records transactions on the blockchain to ensure transparency. Smart contracts and blockchain accelerate fundraising and promote trust, which improves crowdfunding. Their easy-to-use, affordable app seeks to increase accessibility to crowdfunding and has a promising future in the dynamic blockchain and initial coin offering (ICO) space, with growing usage predicted as public awareness of blockchain technology increases[1].

Viren Patil et al., in his paper, "Blockchain-Based Crowdfunding Application", discusses how blockchain transforms data management by guaranteeing transparency through irreversible logs and time-stamped transactions. Processes are automated using smart contracts, improving security. With real-time project updates and fund tracking, the multi-user software benefits Admin, Backers, and Start-ups. The software guarantees refunds in the event that a project is abandoned and provides transparency for backers to monitor startup development. Reliability is maintained by only adding money to the smart contract when the initial conditions are satisfied.[2].

Harsh Khatter et al. in his paper, "Secure and transparent crowdfunding using blockchain", discusses how global fundraising is enabled by crowdfunding, which is assisted by platforms such as Kickstarter. However, problems with high costs, transparency, and trust still exist in the current systems. The approach proposed replaces traditional crowd sourcing with a transparent, affordable option by utilizing blockchain technology and smart contracts. However, Ethereum-based Dapps will take some time to become well-known as the world becomes used to blockchain technology and cryptocurrencies.[3]

Wenjie Teng et al. in his paper, "A Smart Contract-based Service Platform for Trustworthy Crowd Funding and Crowd Innovation" discusses the economic benefits of crowdsourcing and crowd innovation go to creators, but safeguarding stakeholders' rights is still a problem. To ensure equitable rewards and process trust, their approach provides blockchain-based smart contracts with tokens and governance. The establishment of a dependable platform results from the abstraction of these contracts in order to maintain business processes. Case studies with illustrations show how well the technology works for crowdsourcing and crowd creativity.[4]

Dr. Sumathi VP et al., in the paper, "Crowd-Funding Using Block Chain", discusses how the traditional method of building a crowdfunding platform has problems with user confidence, transparency, and expensive prices. In order to solve these issues with crowdfunding, the project leverages blockchain technology for maximum security and transparency. The platform's future ambitions include moving to EOS if it makes sense. A few possible improvements are augmented reality, machine learning to avoid fraud, badges for regular investors, stake modifications, and API connectivity.[5]

Adarsh Kumar Dubey et al., in his paper, "Crowdfunding using Blockchain for Startups and Investors" discusses on crowdfunding websites and social media sites that collect small payments from a large number of people to fund startups but they do not have investor control and safeguards. This is why there need to be a decentralized, private, and secure blockchain-based crowdfunding platform. It increases security while promoting transparency in order to stop fraud and infuse confidence in the public system thereby enabling giving safely to deserving institutions.[6]

Harsh Shankar Rao et al., in his paper, "Blockchain Based Crowdfunding Platforms - Exploratory Literature Survey",talks about Blockchain-based crowdfunding can be used by content creators to obtain safer and more transparent funding. Crowdfunding, which is a traditional way of seeking funds for a startup business or project, has been revolutionized by blockchain technology; this includes smart contracts, money management improvement, reduction in fraud cases and dealing with high costs and transparency issues. The creative community requires a blockchain platform that will enable crowdfunding safely for projects that are sponsored themselves. For the blockchain-based crowdfunding to expand in its adoption and reach a wider audience, it must have a market place and sharing revenue mechanism.[7]

Rani et al., in the paper, "Trustworthy Blockchain Based Certificate Distribution for the Education System" addresses on the blockchain-based decentralized certificate management system combats diploma fraud and protects student privacy. The system ensures the publication, retention, and authentication of academic documents through encrypted storage, digital signatures, proof of work, SHA-256, and ECDSA. Improvements include better security, a simple verification interface, and more learning records. This creates an efficient and secure model for the decentralized management of educational foundations.[8]

Khwaja et al., in the paper, "A survey on blockchain technology: evolution, architecture and security" focuses on blockchain challenges in scalability, security risks, and the need for faster verification. It examines technological changes, architectural designs, and consensus algorithms, and highlights future areas of research. The approach assesses the current state and security risks to identify necessary changes. Approaches include new consensus algorithms such as PoS, improved network performance, and advanced cryptographic protections to address key blockchain issues beyond business operations.[9]

Varun et al., in the paper titled, "Decentralised crowdfunding platform using blockchain technology",discusses on the traditional crowdfunding faces inefficiencies and transparency issues, leading to fraud and trust issues. Decentralized blockchain platforms can improve security, transparency, and efficiency by using smart contracts to automate processes, eliminate middlemen, and ensure proper allocation of funds. Future advancements include anonymous investing, AI integration, and government identity verification for greater reliability. These improvements are designed to simplify crowdfunding and increase contributor confidence. [10]

Khan et al., in the paper, "Blockchain smart contracts: Applications, challenges, and future trends" conducts survey on blockchain-enabled smart contracts, focusing on technical and usage aspects. It starts by classifying existing smart contract solutions and categorizing research papers before discussing what has been researched about this topic through a smart contract basis. The paper emphasizes possible future research by highlighting some of the challenges and open issues involved with smart contracts. With a particular emphasis on the potential impact of smart contracts on various industries, this study attempts to offer useful information to the stakeholder in smart contract research field.[11]

Wang et al., in the paper"Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends" provides thorough review of smart contract research is given. Highlighted are the various mechanisms and frameworks applied in the process. The applications, progressions, and problems associated with these technologies are discussed in this paper, which presents a snapshot of the current state of play and possible future developments. Smart contracts are introduced along with blockchain technology, Ethereum and Hyperledger Fabric platforms. This paper discusses challenges to be overcome by recent researches, application scenarios as well as what can be expected in years to come so as it will serve as guide for any further study in it.[12]

The literature review revealed several shortcomings in traditional crowdfunding applications. The reliance on email and password logins for user authentication, is inherently less secure and more susceptible to breaches. This traditional approach does not leverage advanced security measures such as multi-factor authentication (MFA). Additionally, the reliance on managers to oversee operations, ensure transparency, and manage monetary transactions results in a single point of failure and the potential for human error or malicious activity.

III. Methodology

The implementation culminates in the development of a sophisticated crowdfunding platform that brings crowdsourced projects to life with a highly responsive user interface built on React.js and Tailwind CSS. The platform is seamlessly integrated with blockchain technology to enable secure and transparent transactions. Users can connect their crypto wallets through MetaMask to authenticate themselves and easily pair and interact with smart contracts on the Ethereum network implemented through Solidity. Using the Web3 development framework Thirdweb, the creation, publishing and deployment of the smart contracts is optimized. This integration enables functionality such as creating, deleting and donating to cryptocurrency campaigns, thereby facilitating direct transactions on the blockchain.

A. Initializing the Web3 Environment

The application consists of two different components: the client side and the web3 side. The client contains the React.js code and the web3 side covers blockchain interaction, including providing smart contracts and integrating Ethereum wallets to ensure secure and transparent transactions. To enhance the security of the application, environment variables are utilized. To initialise the blockchain environment, necessary dependencies are installed and the environment is set up for creating a smart contract using Thirdweb.

1) Smart Contract using Solidity for Sepolia Blockchain Network: The Solidity contract enables the creation, updating, donation to, and deletion of crowdfunding campaigns. It manages campaign details, handles donations, and facilitates the transfer of collected funds to campaign owners. Additionally, the contract implements security checks and restrictions to ensure safe and transparent operations. The major components and functionalities of the contract are as follows:

- Libraries and Inheritance:
  - The contract imports Ownable from OpenZeppelin, which provides ownership functionality and restricts certain functions to the owner of the contract.
- Campaign Struct (Data Structure):
  - owner: The address of the campaign creator.
  - title: Title of the campaign.
  - description: Description of the campaign.
  - target: Target amount to be raised (in wei)
  - deadline: Deadline for the campaign. (As a Unix timestamp)
  - amountCollected: Amount collected so far.
  - image: URL or IPFS hash of the campaign image.
  - donators: List of addresses that have donated.
  - donations: List of amounts corresponding to each donator.
- Mappings and State Variables:
  - campaigns: A mapping that stores all campaigns by their unique ID.
  - numberOfCampaigns: A 24-bit unsigned integer that tracks the number of campaigns.
- Functions:
  - createCampaign
  - updateCampaign
  - donateToCampaign (utilizes payToCampaigner)
  - deleteCampaign (utilizes refundTheDonators)
  - getDonatorsAddresses
  - getCampaigns

The createCampaign function allows the user to create a new fundraising campaign and returns a unique ID (uint256) assigned to the newly created campaign. The campaign struct is created by specifying details such as the name, description, target number, deadline and image URL of the campaign. The function checks if the entered deadline is in the future, increments the 'numberOfCampaigns' counter and returns the ID of the newly created campaign.

The updateCampaign function intakes details such as the ID of the campaign to be updated, the new title, description, target, deadline and/or image, and returns a Boolean indicating the success of the update operation.

The payToCampaigner function takes in the recipient's address and the amount to be transferred as inputs and returns a Boolean indicating the success of the payment.

The donateToCampaign function takes in the Campaign ID, checks if the donation amount is greater than zero, validates that the donation is within the campaign's deadline and then adds the donation amount to the campaign's collected amount. It also records the donator's address and donation amount.

The refundTheDonators function takes the campaign ID as a parameter, iterates through the list of donators for the specified campaign and refunds their donations.

The deleteCampaign function takes in the ID of the campaign to be deleted, and returns a Boolean indicating the success of the delete operation. The function first checks if the campaign exists, then refunds the donators if the campaign has collected any amount before deleting the campaign from the campaigns mapping and decrementing the 'numberOfCampaigns' counter.

The getDonatorsAddresses function takes in the Campaign ID and returns an array of donators' addresses and their corresponding donation amounts for that specific campaign.

The getCampaigns function creates a 'Campaign' map, copying the data of each campaign into a temporary array, before returning it.

2) MetaMask Crypto Wallet: The next step is to create a MetaMask wallet, for secure cryptocurrency transactions. During the creation process, the owner of the wallet is provided with a 12-word recovery phrase for restoration which ensures the security of the wallet by allowing the individual to regain access in case of failure or loss. This mechanism preserves the integrity and dependability of the protection features inherent in the wallet, providing users with confidence in the security of their digital assets.

MetaMask allows users to switch between different Ethereum networks. The Sepolia test network is one such network which allows users to interact with a simulated blockchain environment that mirrors the main Ethereum network but uses test ETH, which has no real-world value. This feature is particularly useful for developers who wish to test their applications or smart contracts without the risk of losing real funds. Compared to other testnets, Sepolia boasts a faster block time, resulting in faster transaction confirmations and feedback for developers. Also, unlike some testnets with capped testnet tokens, Sepolia has an unlimited supply.

In the MetaMask settings, the network is switched to "Sepolia Testnet." This exposes the RPC endpoint of the Sepolia network, the critical address applications use to interact with the blockchain. This allows Hardhat to interact with testnet to deploy and test smart contracts. Test ETH funds, which are required to finance operations and gas payments for smart contract engagement in the development process can be obtained from a sepolia testnet faucet online. Fig. 1 shows the process of acquisition of test ETH via the wallet address.

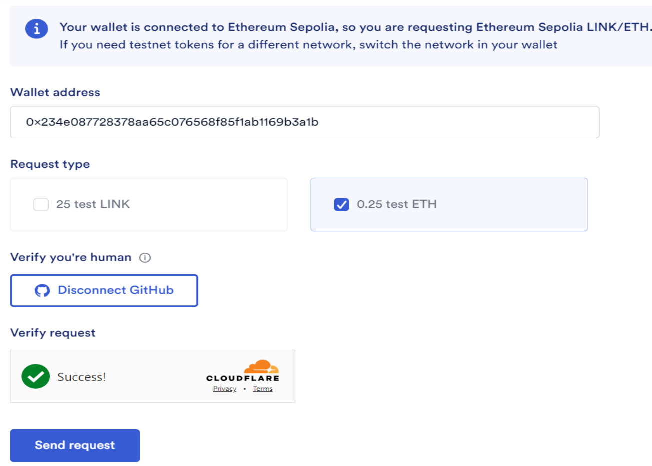

Fig. 1. Acquiring Test ETH

Every MetaMask wallet contains a necessary private key for authorizing transactions on the blockchain. Furthermore, through this mechanism, users maintain full control over their digital assets and funds hence increasing security while reducing dependency on third-party custodians. This private key is stored as an environment variable in the code. MetaMask also has built-in tools that help manage multiple Ethereum accounts, set up transaction costs, and monitor transaction statuses. Moreover, its compatibility with the web3 API enables dApp developers to create services that are easily interoperable with end-users' MetaMask wallets, fostering an ecosystem of decentralized services. Fig. 2, shows a MetaMask wallet on the Sepolia test network.

3) Hardhat Framework Configuration: This study utilises the Hardhat framework. Hardhat allows programmers to establish a local blockchain environment using Ethereum nodes, saving time and money by avoiding the need for deploying smart contracts on public networks during development. It is equipped with powerful tools for unit testing, enabling developers to isolate individual functions in their contracts to ensure they behave as expected under different conditions before deployment on the mainnet—this is critical for security and functionality of smart contracts realized via paid programs. Other than this, it also helps in configuring network connection details, including the sepolia RPC endpoint—the URL required to connect the development environment to the Sepolia testnet blockchain node. External providers offer RPC endpoints to interact with the Ethereum blockchain, ensuring that the Ethereum client software stays up-to-date

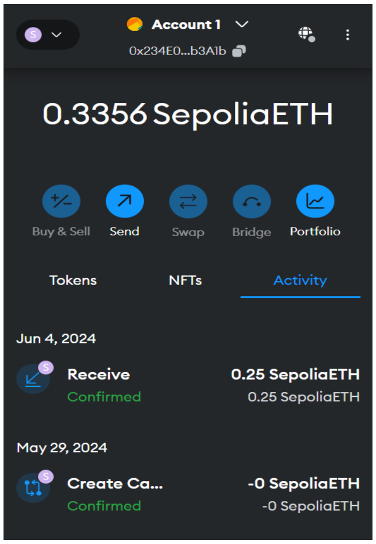

Fig. 2. MetaMask Wallet - Sepolia Blockchain Network

with the latest network upgrades, security fixes, and performance improvements. The Hardhat configuration object (HardhatUserConfig) consists of several key properties:

- solidity: Specifies the Solidity compiler version to be used.
- networks: Defines the networks to which the user can connect to deploy contracts. Three networks are defined:
  - localhost: Points to a local Ethereum node running.
  - sepolia: Connects to the Sepolia test network. It uses the RPC URL for the Sepolia network RPC HTTPS endpoint as shown in Fig. 3 and the private key obtained from the connected MetaMask wallet, both of which are stored as environment variables for deployment and transactions.
  - hardhat: This is the built-in Hardhat network used for testing and development. It doesn't require any URL or account configuration.
- etherscan: This configuration is used to retrieve blockchain data, verify smart contracts, check transaction statuses, and more. It uses an API key to authenticate requests made to the Etherscan API.

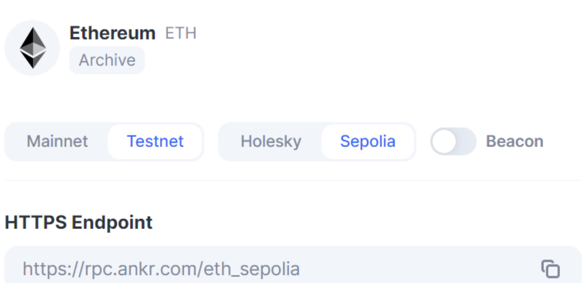

Fig. 3. RPC HTTPS Endpoint for Sepolia Testnet

4) Smart Contract Deployment via Thirdweb: Through the use of Thirdweb's web3 technologies, automated and decentralized procedures can enable the crowdfunding application to function without constant human interaction. Thirdweb does away with the necessity for a central administrator, who would typically be in charge of keeping an eye on and overseeing transactions, by leveraging blockchain technology and the use of smart contracts.

Since the blockchain is decentralized, there is less chance of fraud or manipulation because no one party can control the entire system. Additionally, when the necessary predetermined criteria are met, the smart contracts automatically enforce rules and carry out transactions, reducing the mistakes and processing delays that come with manual processing.

The Solidity smart contract created can be deployed using a single command through Thirdweb. The user is securely authenticated by connecting their MetaMask wallet to Thirdweb, after which the user will be able to deploy and navigate through smart contracts on Thirdweb's intuitive interface. The address of the deployed Smart Contract is utilized in the React.js application code to connect the contract to the crowdfunding application.

Thirdweb allows users to view real-time analytics and insights of deployed contracts, and to quickly navigate to different projects and manage them efficiently. Each contract has a dedicated section where users can view and manage specific details such as deployment status, user interactions and transaction history. This allows users to monitor the status of their deployments, track transaction progress, and receive alerts for any issues that require attention.

B. Creating the Crowdfunding Application using React.js

1) Application Initialization: The React application is initialized via a Thirdweb command, after which the necessary packages are installed. The Vite framework is chosen in this study. The main.jsx code sets the blockchain network and activates web3 features by importing necessary modules from the Thirdweb library. More specifically, it chooses the Sepolia network for blockchain interactions and incorporates the Thirdweb provider. To manage global state across the application, the code makes use of React's context API to provide consistent state management across various components.

The app.jsx code sets up the layout of the web application with the custom-created components (including the Navbar and Sidebar) and main content area. The Navbar component serves as a navigation bar for the web application, incorporating both desktop and mobile responsive designs hence facilitating a multi-platform design.

2) Creation of Navigable Pages: The 'Home' page, 'Create Campaign' page, 'Update Campaign' page, 'Profile' page, and 'Campaign Details' page of the crowdfunding platform may be easily navigated through using an intuitive user experience. Every page is made to offer the necessary features for efficiently administering, perusing, and assisting with crowdfunding initiatives.

The 'Home' page displays all the campaigns that have been published on the crowdfunding platform. Users can browse through the various campaigns listed here. The 'Create Campaign' page features a form designed to collect all necessary campaign details as input from the user. This form allows users to initiate new crowdfunding campaigns. The 'Update Campaign' page allows campaign creators to change any details originally inputted on the 'Create Campaign' page. This entails revising the campaign's description, duration and other relevant information. This page makes sure that campaign data is correct and up to date, giving prospective backers the most recent information available. The 'Profile' page presents the active campaigns associated with the user currently logged in through their MetaMask wallet. Users can view and manage their active campaigns here.

The 'Campaign Details' page provides additional information about a specific campaign. This page is accessible by clicking on a campaign from either the Home Page or the Profile Page. It includes the following details:

- The number of days remaining until the campaign ends. (to help provide an incentive to donators).
- The amount of funds currently raised.
- The MetaMask address of the campaign creator.
- A list of donators' addresses and their respective donation amounts.
- A fund field for contributors to donate ETH via their MetaMask wallet.

For the creator of a particular campaign, the 'Campaign Details' page includes two additional functionalities, namely, updating the campaign details and deleting the campaign (which will result in all donators being refunded).

react-router-dom is used for routing and navigation between the different created pages allowing for a single-page application experience. Fig. 4 shows the detailed workflow of the proposed architecture which will be further elaborated in the upcoming sections.

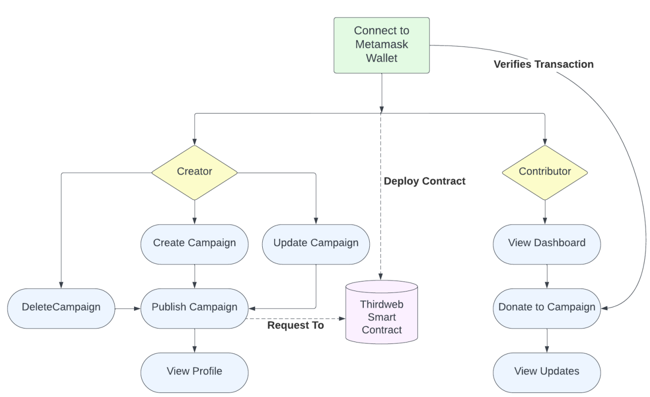

Fig. 4. Workflow of the Decentralized Application

3) Creation of React Context API: The contract address (obtained from the Thirdweb dashboard) uniquely identifies the deployed smart contract on the blockchain, the smart wallet address (retrieved using the useAddress hook from the Thirdweb library) uniquely identifies the user interacting with the application, and the connect function (via the useConnect hook from the Thirdweb library) connects the MetaMask wallet to the crowdfunding applications.

Establishing a global state management system that enables consistent access to and updating of shared data by many components of the application is necessary to create a React context API as a centralized source of truth. This is especially helpful when integrating Thirdweb logic for blockchain interactions or in large applications where several components need to communicate with the same data. One can effectively manage the data flow between the front end and back end by using the Context API.

Throughout the application, this configuration offers a centralized method of managing states and communicating with the smart contract. Ethereum utilities and Thirdweb hooks facilitate blockchain interactions, while toast alerts provide feedback to users. Data that has been retrieved from the back end may be stored in the global state, where front-end elements can access and modify it. In a similar vein, information gathered from front-end user interactions can be routed to the back end for updating, processing, or storing.

Hence, the Decentralized model of the crowdfunding application is derived from an architecture that combines front-end web interfaces with back-end smart contracts deployed on the Ethereum blockchain. The MetaMask Crypto wallet acts as an intermediary between the Ethereum network and the users via their browsers while ensuring secure communication. By utilizing blockchain technology and smart contracts, Thirdweb eliminates the need for a central administrator, who would normally be in charge of monitoring and supervising transactions. It enables effective project management as well as the viewing of deployed contract data and insights in real time.

IV. Results and Analysis

On the 'Home' page of the crowdfunding application, all currently active campaigns are displayed. Users authenticate themselves by linking their MetaMask wallet to the decentralized application (DApp). Upon a successful wallet connection, users now have the option to create a new campaign or contribute to an existing one.

When a user decides to start a campaign, they must fill out the form on the 'Create Campaign' page with the following information: the name of the campaigner, the campaign's title, its description, its funding target, its expiration date, and the URL of a representative campaign image. For the campaign to be published on the application, the user has to pay a gas fee. The campaign will appear on the application dashboard and the user's 'Profile' page after it is published. Two further features are available to the campaign creator: updating the campaign's information and deleting the campaign. Deleting an existing campaign also requires a gas fee to be paid.

"Gas" is a unit of measurement used in blockchain networks, specifically Ethereum, to indicate the computing effort needed to carry out various functions linked to the blockchain, including transactions and smart contract interactions. When a transaction is made on the blockchain, a fee known as the ”Gas Fee” is needed. This money is given to miners or validators who handle and verify the transactions. The cost is frequently expressed in the blockchain’s native cryptocurrency, such as Ether for Ethereum.

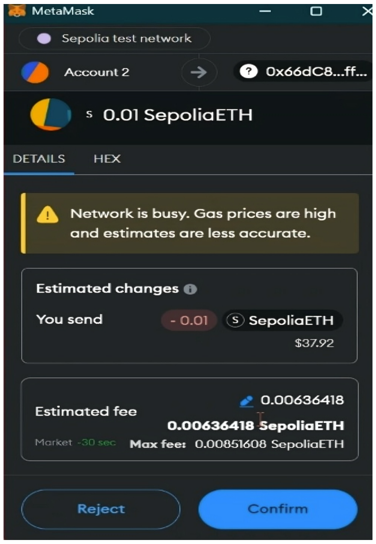

Fig. 5. Donating to a Campaign

A user has the option to contribute to any campaign of their choice. A campaign’s complete details, such as the number of days left till the deadline, the total money raised, and a list of donors and their corresponding donation amounts, are all provided on the ’Campaign Details’ page. Apart from the funded amount, donators must also pay a gas fee as shown in Fig. 5.

Towards the backend, the Thirdweb platform is logged into via MetaMask. The ’Overview’ page on Thirdweb offers a synopsis of the contract along with important metrics and current activity. This tab acts as a focal point for comprehending the objectives, results, and advancement of the project. The user can see an overview of their smart contract, as well as important analytics like the unique wallets and total transactions on the contract as seen in Fig. 6.

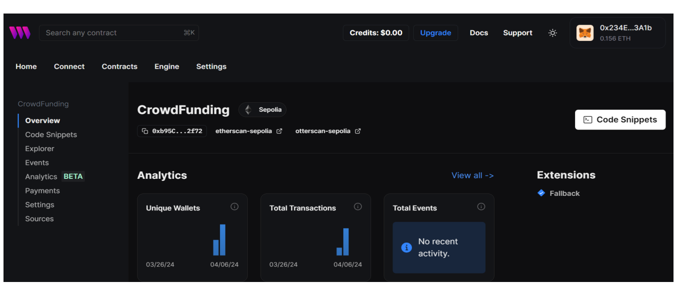

Fig. 6. Overview dashboard of Thirdweb

On navigating to the ’Explorer’ tab on Thirdweb, the user can see the read and write functions of the smart contract called by the decentralized crowdfunding application. The user

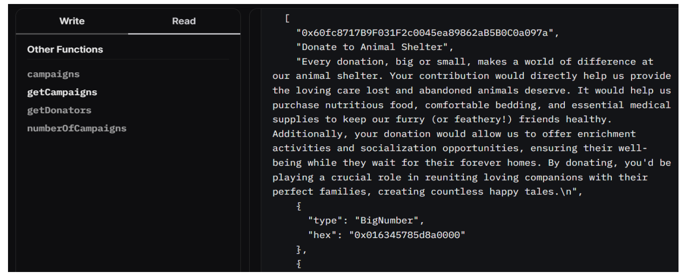

Fig. 7. getCampaigns function on the Thirdweb Dashboard

can also call these functions directly from this tab. For all implemented smart contracts, the transaction histories and real-time data are shown on Thirdweb’s Explorer tab. On-chain activity can be filtered, searched, and analyzed. Fig. 7 shows the getCampaigns read function on Thirdweb.

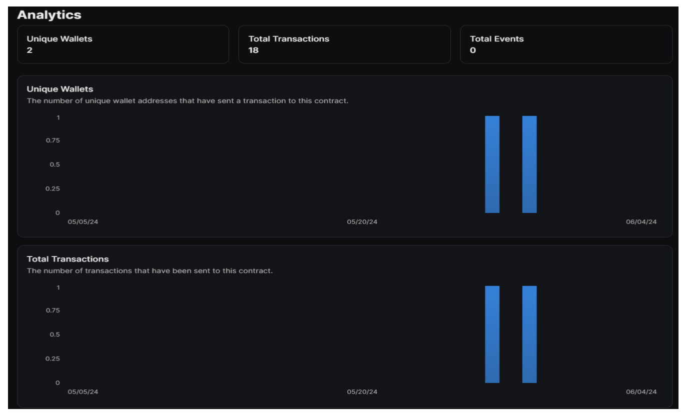

Fig. 8. Analytics dashboard of Thirdweb

The ’Analytics’ tab on the Thirdweb platform provides comprehensive insights into project performance, including measures like transaction volume, unique user activity, and events as seen in Fig. 8. It also shows the breakdown of calls to each write function from transactions and the breakdown of events emitted by the contract. By using graphs and charts to show data, it makes trends and KPIs easier to follow. Users are able to examine usage and interaction trends. For well-informed decision-making and contract assessment, this tab is essential.

V. Conclusion and Future work

This research suggests a blockchain-based crowdfunding DApp utilizing the Thirdweb platform for smart contract deployment without the need of an administrator. MetaMask serves as the crypto wallet for safe user verification and asset administration. By using MetaMask, users benefit from advanced security features like encryption, multi-factor authentication, and multi-signature support, as well as complete control and ownership over their digital assets. MetaMask also guarantees the safe storage of private keys. Smart contracts streamline transactions by automating the execution of pre-defined terms without the need for intermediaries, reducing costs, enhancing security, and increasing efficiency. Using a blockchain-based agreement removes the need for middlemen, which improves security, lowers regulatory hurdles, and increases transparency.

ThirdWeb guarantees efficiency, security and transparency in crowdfunding applications using its decentralized platform. Using smart contracts and blockchain technology, ThirdWeb transforms crowdfunding by doing away with the need for an administrator. Smart contracts' self-governing system guards against fraud and guarantees accurate transactions. Furthermore, blockchain technology gives stakeholders complete visibility and auditability by recording every transaction on an immutable ledger. Additionally, ThirdWeb makes contract management easier with its user-friendly interface. Through an intuitive interface, users can easily establish, monitor, and administer smart contracts, which reduces the complexity typically involved with crowdfunding administration.

Future enhancements can further improve trust, transparency, and accessibility in the decentralized fundraising industry. User-controlled secure identity verification can be made possible with the integration of decentralized identification solutions. Incorporating oracles can enable automated smart contract execution based on real-world events. NFTs can be used to represent ownership or rewards in crowdfunding campaigns, adding uniqueness and exclusivity to contributions. Crowdfunding activities can also become more efficient and economical with Layer 2 scaling solutions. Additionally, regular milestone-based updates can further increase the trust factor and further incentivize contributors.

References

[1] R. NaveenKumaran, S. K. Geetha, K. Selvaraju, C. Kishore and A. Nagha Rathish, "Blockchain Based Crowd Funding," 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023, pp. 1-8, doi: 10.1109/ICCCI56745.2023.10128334.Available: https://doi.org/10.1109/ICCCI56745.2023.10128334.

[2] V. Patil, V. Gupta, and R. Sarode. (2021, November). "Blockchain-based crowdfunding application." In 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) [Conference paper], pp. 1546-1553.

[3] H. Khatter, H. Chauhan, I. Trivedi, and J. Agarwal.Available: IEEE Xplore (2021, August). "Secure and transparent crowdfunding using blockchain." In 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT) [Conference paper], pp. 76-80. Available: IEEE Xplore

[4] W. Teng, H. Xu, Z. Huang, Y. Bai, and Z. Wang. (2022, May). "A Smart Contract-based Service Platform for Trustworthy Crowd Funding and Crowd Innovation." In 2022 International Conference on Service Science (ICSS) [Conference paper], pp. 263-270. Available: IEEE Xplore

[5] S. Vp, L. Jain, and H. Ahmed. (2023, June). "Crowd-Funding Using Blockchain." In 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) [Conference paper], pp. 1-5. Available: IEEE Xplore

[6] A. K. Dubey, S. C. Shingte, M. S. Siddiqui, and S. Patil. (2023, May). "Crowdfunding using Blockchain for Startups and Investors." In 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS) [Conference paper], pp. 1400-1405. Available: IEEE Xplore

[7] H. S. Rao, P. Sinha, S. S. BC, V. P. Aniketh, and M. Namratha. (2023, January). "Blockchain Based Crowdfunding Platforms-Exploratory Literature Survey." In 2023 5th Biennial International Conference on Nascent Technologies in Engineering (ICNTE) [Conference paper], pp. 1-4. Available: IEEE Xplore

[8] P. S. Rani and S. B. Priya. (2022, December). "Trustworthy Blockchain Based Certificate Distribution for the Education System." In 2022 International Conference on Computer, Power and Communications (ICCPC) [Conference paper], pp. 393-397. Available: IEEE Xplore

[9] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao. (2021). "A survey on blockchain technology: Evolution, architecture and security." IEEE Access [Journal], 9, pp. 61048-61073. Available: IEEE Xplore

[10] M. Varun, S. Devi, U. Jaiswal, V. Pratap, and M. P. Choudhary. (n.d.). "Decentralized crowdfunding platform using blockchain technology." Unpublished manuscript.

[11] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani. (2021). "Blockchain smart contracts: Applications, challenges, and future trends." Peer-to-Peer Networking and Applications [Journal], 14, pp. 2901-2925. Available: Springer

[12] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Y. Wang. (2019). "Blockchain-enabled smart contracts: Architecture, applications, and future trends." IEEE Transactions on Systems, Man, and Cybernetics: Systems [Journal], 49(11), pp. 2266-2277. Available: IEEE Xplore

[13] A. N. Mahesh, N. S. Shibu, and S. Balamurugan. (2019, November). "Conceptualizing blockchain based energy market for self sustainable community." In Proceedings of the 2nd Workshop on Blockchain-enabled Networked Sensor [Conference paper], pp. 1-7. Available: ACM Digital Library

[14] P. Kumar, G. A. Dhanush, D. Srivatsa, A. Nithin, and S. Sahisnu. (2019). "A buyer and seller's protocol via utilization of smart contracts using blockchain technology." In Advanced Informatics for Computing Research: Third International Conference, ICAICR 2019, Shimla, India, June 15–16, 2019, Revised Selected Papers, Part I 3 [Conference paper], pp. 464-474. Available: Springer

[15] K. D. Kumar, M. Sudhakara, and R. K. Poluru. (2023). "Towards the integration of blockchain and IoT for security challenges in IoT: A review." Research Anthology on Convergence of Blockchain, Internet of Things, and Security [Book chapter], pp. 193-209. Available: IGI Global

[16] A. Gayathri, S. Saravanan, P. Pandiyan, and V. Rukkumani. (2023). "Blockchain technologies for smart power systems." Artificial Intelligence-Based Smart Power Systems [Book chapter], pp. 327-347. Available: Wiley

[17] M. Kripa, A. Nidhin Mahesh, R. Ramaguru, and P. P. Amritha. (2021). "Blockchain framework for social media DRM based on secret sharing." In Information and Communication Technology for Intelligent Systems: Proceedings of ICTIS 2020, Volume 1 [Conference paper], pp. 451-458. Available: Springer

[18] P. K. Preetha and M. G. Nair. (2022, November). "Smart contract based energy trading-an overview." In 2022 IEEE 19th India Council International Conference (INDICON) [Conference paper], pp. 1-7. Available: IEEE Xplore