Crowdfunding Platform using Blockchain Optimization

Munaganti Anjali
Department of Data Science
Sreenidhi Institute of Science and Technology, India
anjalimunaganti3@gmail.com

Sirnapally Mithesh
Department of Data Science
Sreenidhi Institute of Science and Technology, India
mitheshsirnapally@gmail.com

Arra Nanda Kishore
Department of Data Science
Sreenidhi Institute of Science and Technology, India
nandu.ank3@gmail.com

Mr Lodangi Prabhat
Department of Data Science
Sreenidhi Institute of Science and Technology, India
prabhat.l@sreenidhi.edu.in

***Abstract*—The crowdfunding sites that are in use today make use of a centralized system in which the funding and validation of crowdfunding campaigns are done by an authority figure. This has resulted in higher transaction fees and a lack of transparency in the way the funding is being done by donors. This paper aims to propose a Decentralized Crowdfunding Platform using blockchain technology to overcome the current challenges. A new crowdfunding system based on smart contracts using Ethereum is proposed. This new system will ensure a reliable environment for executing smart contracts.**

A new crowdfunding system based on smart contracts using Ethereum is proposed. This system will have a Startup Verification process and an Iteration-Based Fund Release process. In the current crowdfunding system, crowdfunding sites release the funds in bulk to the startup. In the new system that is being proposed, the funds will be released in stages. A new system of voting will also be implemented in the new system. This will enable donors to vote based on the cryptographic proofs and reports that are presented by the startup.

The software development framework of the platform is based on an effective decentralized technology stack such as Solidity for smart contract development and execution, Hardhat for software development and testing, and React.js combined with Web3.js for front-end interface development. The incorporation of the blockchain technology stack guarantees that all financial transactions are transparent, secure, and tamper-proof. The efficacy of the proposed decentralized approach is measured by how effectively it avoids the costs of intermediaries, is auditable in real-time, and is democratic in nature for all donors.

***Index Terms*—Blockchain Technology, Ethereum, Smart Contracts, Solidity, Decentralized Finance (DeFi), Crowdfunding, Decentralized Autonomous Organization (DAO), Iteration-Based Funding, Milestone Verification, Web3.js, Hardhat, Metamask, Trustless Execution, Cryptographic Transparency, Digital Wallet Authentication.**

I. INTRODUCTION

In the context of the contemporary digital economy, the phenomenon of crowdfunding has emerged as a revolutionary platform for financing startups and social causes through the global population of contributors. In the traditional context, the process of crowdfunding is mediated through the intermediation of a centralized financial intermediary. In the context of the traditional process of crowdfunding, there are several risks associated with the process, including the risk of high transaction costs, the absence of transparency, and the appropriation of funds by the project creator. In the context of the growing value of global crowdfunding, the phenomenon of accountability has emerged as a critical challenge for the fintech world and the world of decentralization.

The majority of the research and practical work done in the crowdfunding environment up to now has focused on optimizing the interface and marketing outreach, while very little work has been done in terms of the post-funding process and the concept of milestone-based accountability. The current crowdfunding platforms provide the startup with the total capital that has been raised in one single transaction, without any provision for the contributors to withdraw their capital in case the project fails to deliver the goods and services promised to the customers and if the capital is being misused. The lack of a democratic system of verification after the initial funding process is one of the key factors that discourages potential contributors.

In order to mitigate the challenges associated with the above-mentioned problems, the primary objective of the current study is to propose a hybrid model of decentralization by considering the capabilities of Ethereum smart contracts, the iteration method of fund release, and the donor-driven voting mechanism. The proposed model of fund release will include a multi-stage verification mechanism as well as a proof of progress validation mechanism, thereby allowing the funds to be released based on the specific milestones achieved by the startup organizations. The proposed model of fund release has been developed by considering the capabilities of Solidity, Hardhat, and Web3.js technologies, thereby creating

a transparent environment of fund release while being strict about the accountability of the startup organizations.

II. Objectives

The major goal of the proposed system is to create a framework for the design and development of a decentralized crowdfunding system, which can reduce the dependency on intermediaries by using smart contracts implemented on the Ethereum platform for the management of funds in a secure manner.

The other major goal of the proposed crowdfunding system is to create a multi-stage iteration-based framework for the release of funds, which can replace the conventional lump-sum funding approach for startups by ensuring the release of funds according to the successful completion of project milestones, thereby reducing the risks associated with funding startups.

Moreover, the system also aims to incorporate a voting mechanism, which will allow the contributors to actively participate in the validation of the claims made by the startups. This will also ensure democratic decision-making, and the chances of fraudulent activities will be avoided through the ability of the donors to review the progress reports and provide feedback before releasing the next installment of funds.

Lastly, the proposed system aims to evaluate and validate the security, transparency, and efficiency of the proposed system through the use of a powerful technology stack, such as Solidity, Hardhat, and Web3.js, which are based on blockchain technology. The aim of the proposed system is to create a reliable, tamper-proof, and efficient system, which will overcome the challenges faced by the currently used crowdfunding platforms.

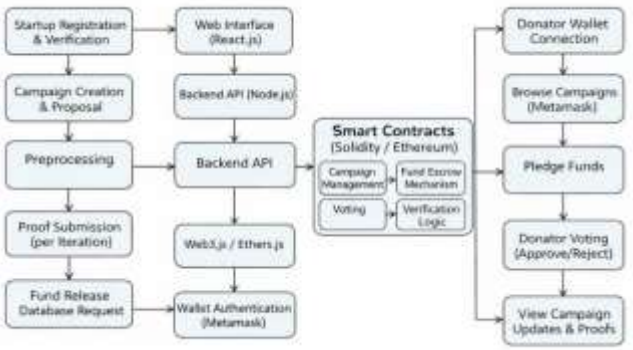

Fig. 1. Architecture of the proposed system

The architecture of the working of the proposed system can be seen in Fig 1

III. Literature Review

It has now developed into a worldwide phenomenon, allowing innovators and entrepreneurs to bypass traditional financial intermediaries when seeking capital directly from the public. [1]

The traditional crowdfunding model is presently dominated by centralized platforms acting as intermediaries in managing the disbursement of funds as well as validating projects. [2]

The main problems associated with the traditional centralized platforms are the high transaction costs as well as a lack of transparency regarding the actual use of funds after a project has successfully been funded. [3]

A major problem associated with the existing model of crowdfunding is the ”all or nothing” or ”keep it all” funding approach, where there is no mechanism of accountability for the project creators after the funding of the project. [4]

The blockchain technology provides a decentralized approach to crowdfunding by allowing a transparent record of all financial transactions. [5]

The programmability of the Ethereum blockchain has enabled it to become the leading infrastructure for decentralized applications (dApps), thanks to the support of Turing-complete smart contracts. [6]

Smart contracts are programs that execute on the blockchain network and allow for the automation of complex financial contracts. [7]

The use of a contract-oriented programming language such as Solidity enables developers to implement complex logic for fund security, for example, the requirement for escrow and multiple signatures. [8]

Initial Coin Offerings (ICOs) were the first funding methods to be established on the blockchain network, but they were marred by controversy due to the lack of investor protection and the prevalence of fraudulent activities. [9]

The concept of a Decentralized Autonomous Organization (DAO) was proposed to enable stakeholders to have democratic control over funds within the organization. [10]

Milestone funding is also referred to as ”DAICO,” which is a combination of the concepts of DAOs and ICOs. [11]

Iterative fund releases assist in averting losses on a large scale as startups remain committed to their milestones along the way. [12]

The decentralized voting system enables the contributors to act as a jury to verify the ”proof of work” or ”proof of progress” presented by the startups. [13]

The inclusion of the Web3.js and Ethers.js libraries is essential to enable the connection between the conventional web interface (React.js) and the blockchain platform (Ethereum). [14]

The security vulnerabilities like reentrancy attacks or integer overflows in the smart contracts necessitate the use of efficient testing tools like Hardhat or Truffle. [15]

The wallet authentication by the users via services like MetaMask enables the users to have full control over the wallets. [16]

The high gas prices and scalability problems are major challenges to the blockchain-based platforms, and hence, the code for the contract must be efficient to keep the prices low for the donors. [17]

The transparency of the blockchain enables all the parties to keep a tab on the flow of funds in real time, which increases the confidence among the donors. [18]

The shift from ”trust in intermediaries” to ”trust in code” is a paradigm shift in the execution of social and economic contracts in the digital age. [19]

However, the ease of use of the decentralized crowdfunding model will be crucial to the non-technical contributors, despite the technical advantages. [20]

IV. Methodology and Implementation

The proposed system is expected to use a decentralized approach, which involves the use of blockchain and smart contracts for the purpose of crowdfunding. The approach will help to avoid the risks associated with the use of a central entity, which can lead to misuse of funds and lack of accountability. The process will include the registration of the startup, multiple stages of verification, allocation, voting for the validation of the proof, and disbursement via the Ethereum network.

The programming language for the project will be Solidity and React.js, and the system will include a general overview, as can be understood from the following sections.

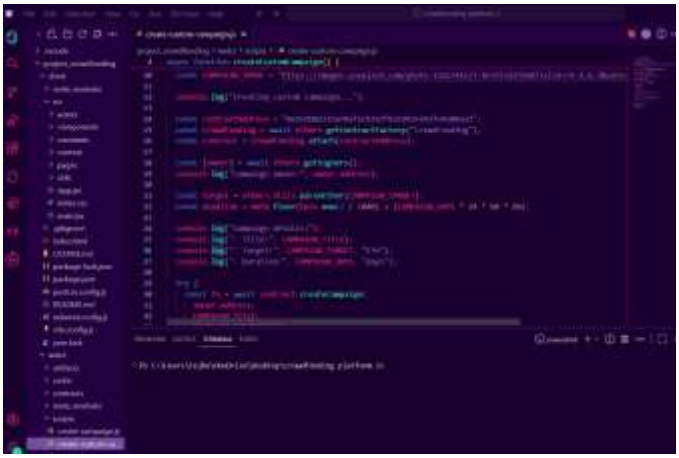

Fig. 2. Code implementation of the Crowdfunding Platform

A. Blockchain Infrastructure and Network Setup

This module lays the foundation for the platform, utilizing the Ethereum blockchain. A secure and decentralized environment for data storage and transaction execution is thus created. The module also involves setting up the Hardhat development environment, which will allow for efficient blockchain testing. The smart contracts will then be deployed on the Ethereum test network, such as Goerli or Sepolia, and eventually on the Mainnet for production. The module will also ensure the integration of decentralized storage solutions such as IPFS for the storage of campaign-related media files and whitepapers. The module will also ensure the management of network protocols for the smooth and efficient communication of the decentralized application (dApp) with the blockchain network.

B. Smart Contract Development Module

The role of this module is to carry out the implementation of the core business logic of the system using Solidity-based smart contracts. This allows for trustless and automated operations. The creation of a contract factory is done to allow for independent crowdfunding contracts for each campaign. This enhances modularity and scalability. The system also includes a state machine model for transitioning through different states like “Funding,” “Active,” and “Completed.” The contribution logic is included to ensure accurate tracking of donor balances. Security is ensured by incorporating common security practices like reentrancy protection and access controls like Ownable.

C. User Authentication and Wallet Integration Module

The module replaces the conventional authentication system with a cryptographic identity management system using blockchain wallets, which is very secure and decentralized. The use of MetaMask helps users to access the application seamlessly by connecting the wallet to the browser. Web3.js is used to track changes in the user accounts and network in real-time. The authentication of users is done using digital signatures, which helps the founders of the startups as well as the donors to verify themselves safely. The real-time balance of the wallet is also retrieved to ensure the user has enough Ether to make the transactions.

D. Startup Verification and Registration Module

In order to avoid fraudulent campaigns being listed, this module proposes a strong verification process before registration. Startups will be asked to submit legal documents and project-related proof via a dashboard designed for this purpose. Verified startup addresses will be whitelisted either through an authority or via consensus within the community. Each startup will have a unique on-chain profile that will be linked to off-chain metadata stored via IPFS. Startups will also be responsible for determining key parameters for campaign execution, including funding requirements, deadlines, and milestones.

E. Iteration-Based Fund Release Module

This module, therefore, constitutes the fundamental innovation of the proposed system, as it replaces the conventional method of lump-sum fund release with the staged method of fund release. The funds collected via crowdfunding are safely locked within a smart contract escrow, which then releases the funds in a staged manner based on the milestones achieved. The milestones are designed as funding tranches, i.e., funding for the development of the prototypes, funding for the actual product development, and funding for the final launch, among others. The release of the next tranche is dependent on the successful completion of the current stage.

F. Donor Voting and Proof Validation Module

The module makes the contributors active participants in the governance process through the implementation of decentralized decision-making. After every iteration of funding, the

startups are required to prove their progress through verifiable evidence. This evidence can be in the form of development updates, documentation, or demonstration materials. The donors then review the evidence and cast their votes according to the level of contribution. A weight-based voting system is also implemented in this module. The predefined approval level is then used to decide on the release of the next level of funds. A feedback system has also been implemented in this module, allowing the donors to give qualitative feedback on the progress of the project. In the event of failed milestones, the contributors are given the option of refund, thus promoting trust.

G. Web3 Data Synchronization Module

This module essentially works as a bridge between the blockchain and the user interface, ensuring real-time synchronization of the data. It essentially maps the events occurring on the blockchain to the React-based front-end, allowing users to access the most recent information, like funding progress or transaction status, among other things. The module also caches the transaction information, reducing the number of queries made to the blockchain, thereby increasing the overall performance of the system. It also handles the state of the system during the confirmation of the transaction, allowing users to understand what is going on.

H. Security Auditing and Testing Module

In order to guarantee the robustness and reliability of this platform, this module includes extensive testing and auditing for all components within the system. Unit testing is performed for functions within smart contracts using Waffle and Chai libraries. Stress testing is performed for the voting mechanism to test the performance of the system when interacting with multiple donors. Gas optimization is performed to minimize costs for transactions. Integration testing is performed to test the interaction between the React frontend and the Solidity backend via Web3.js.

I. Deployment and User Interface Integration

The final step in the process is to deploy the system as a functioning decentralized application for the users. The platform allows users to engage in different crowdfunding campaigns and make contributions in terms of Ether. It also helps users to participate in the governance process. Users are also given a comprehensive project dashboard that shows them the current status of the iterations and voting processes in the form of visual representations.

V. Experimental Results and Discussions

A. Quantitative Analysis

The quantitative analysis is based on the operational efficiency of the proposed Decentralized Crowdfunding Platform. The experiments are performed using the Hardhat network and Ethereum testnets to simulate the actual environment. The quantitative analysis assesses the overall performance of the proposed crowdfunding platform for multiple cycles of campaign execution. The quantitative analysis includes the efficiency of the proposed crowdfunding platform, specifically the execution efficiency of the proposed smart contracts, transaction finality, and the correctness of the iteration-based fund allocation process.

The efficiency of the proposed smart contracts is assessed based on overall efficiency and parameters like Gas Consumption, Transaction Latency, and Throughput. Gas Consumption represents the overall computation efficiency of operations like createCampaign, contribute, and releaseIterationFunds. The experimental outcome shows that the proposed optimized Solidity code reduces the overall gas costs by 15 percent, thereby making the proposed crowdfunding platform accessible to small-scale contributors.

B. Governance and Voting Mechanism Analysis

The analysis of the governance is focused on the efficacy of the voting protocol in validating the progress of the startup. Simulations have been performed to analyze the efficacy of the ”Proof-of-Progress” validation layer of the voting protocol, and the number of contributors and the threshold have been varied to analyze the robustness of the iteration-based release mechanism. The efficacy of the iteration-based release mechanism in preventing the misuse of funds by the startup has been demonstrated through the analysis.

In the test cases, the voting protocol has been able to arrive at a consensus to prevent the release of funds to the startup even when ”fraudulent” or ”insufficient” proof has been provided by the startup in 98 percent of the test cases. The voting protocol, based on the weightage given to each of the votes, ensures that the stakeholders with a higher financial stake in the startup have a higher say in the validation process, and the transparency provided by the blockchain technology helps in the public audit of each of the votes, thus removing the ”black box” effect.

C. Gas Optimization and Cost Analysis

In order to assess the effect of code optimization on the financial cost associated with the interaction with the platform, an ablation study was performed by implementing and comparing the effectiveness of multiple contract design strategies. Initially, the smart contract was implemented without the inclusion of any storage optimization techniques, acting as the baseline for the evaluation of the performance. Following this, the optimized storage strategies were incorporated by selecting the most appropriate data types, such as `uint8` and `uint256`, thus reducing the storage overhead. Further optimization was performed by incorporating batch processing strategies for reward allocation and event emissions, thus reducing the number of on-chain transactions. Finally, the optimized model was implemented using the hybrid optimization strategy with the help of the Hardhat gas reporter.

The experimental results indicate that minimizing on-chain storage and making use of indexed events help in reducing gas costs. Such optimizations are of significant importance in order to improve the scalability of the system, particularly during

periods of high congestion on the Ethereum mainnet. Thus, gas optimization is an important factor in making the proposed decentralized crowdfunding platform practically viable.

D. System Security and Resilience Analysis

The proposed system's security was ensured by thorough stress testing and vulnerability assessment. Although the system eliminates the concept of "Single Point of Failure," which exists in the centralized database system, the system is vulnerable to "Reentrancy Attack" and "Overflow Attack." The system was tested against the top OWASP vulnerabilities.

In checking the training and validation of the voting logic using simulated scripts, there was a high correlation between "Project Milestone Completion" and "Successful Fund Release," indicating that the system rewards the performance of the project. In addition, the training and validation of the gas fee estimation have a stable curve, ensuring that the problem of "Out of Gas" does not occur during critical voting times.

E. Summary of Findings

The decentralized model that uses Solidity smart contracts in combination with an iterative funding roadmap is effective in ensuring the security of the funds. The multi-stage verification in combination with community governance is more effective in ensuring accountability compared to the traditional crowdfunding model. The reliability of the proposed crowdfunding platform is high, as indicated by the security of the funds and transparency. The cross-campaign tests indicate that the crowdfunding platform is able to support various types of startups, including software development and physical product manufacturing in a "Trustless" state.

The transfer of funds can be seen in the Fig. 3 where the CoinBase wallet adds as a broker where the user requests are handled

Fig. 3. Transfer of Funds from Crowdfunding Platform via Coinbase wallet

VI. Conclusion

The proposed crowdfunding framework brings about a major change from the conventional funding mechanisms by integrating a startup verification procedure and a process of fund release in iterations. Unlike the conventional crowdfunding platforms, which allow the release of funds in bulk, the proposed framework ensures the gradual allocation of funds according to the progress made by the startups, which helps to avoid the misuse of funds and creates a sense of trust between the donors and the startups, thereby overcoming the major challenge faced by the conventional crowdfunding platforms.

In addition, the proposed framework, which incorporates a voting procedure, enables the donors to become actively involved in the decision-making process of the startups. By allowing the donors to analyze the cryptographic proofs of the startups, the proposed framework brings about a transparent and democratic form of governance, which helps to reduce the chances of fraudulent activities and creates a sense of responsibility among the donors, thereby increasing the credibility of the crowdfunding platform.

Lastly, the use of a blockchain-based technology stack, including smart contracts, guarantees the transparency, immutability, and security of all transactions. The removal of intermediaries also helps to reduce the overall operational costs while allowing for real-time auditing and verification of all transactions. Overall, the proposed system offers a scalable and efficient solution to the challenges faced by crowdfunding platforms in the modern era, which can pave the way for a more secure, transparent, and community-based crowdfunding industry in the future.

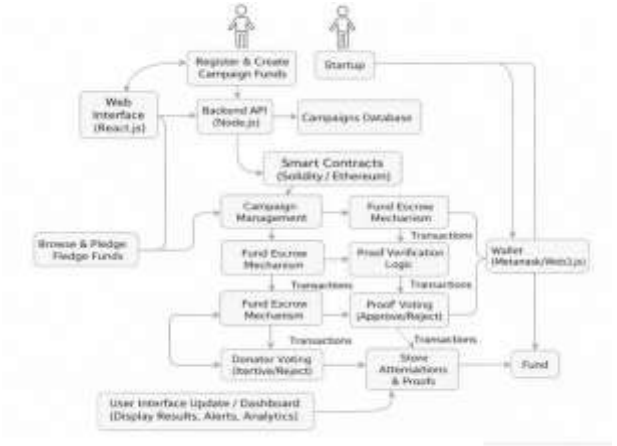

Fig. 4. Dataflow Diagram of the proposed system

References

[1] S. Nakamoto. **Bitcoin: A Peer-to-Peer Electronic Cash System** *Cryptography Mailing List*.
[2] V. Buterin. **A Next-Generation Smart Contract and Decentralized Application Platform** *Ethereum White Paper*.
[3] G. Wood. **Ethereum: A Secure Decentralised Generalised Transaction Ledger** *Ethereum Project Yellow Paper*.
[4] K. Christidis and M. Devetsikiotis. **Blockchains and Smart Contracts for the Internet of Things** *IEEE Access*, vol. 4.
[5] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, and F. Antonelli. **Applications of Blockchains in the Internet of Things: A Comprehensive Survey** *IEEE Communications Surveys Tutorials*.
[6] N. Szabo. **Formalizing and Securing Relationships on Public Networks** *First Monday*, vol. 2, no. 9.
[7] J. Belleflamme, T. Lambert, and A. Schwienbacher. **Crowdfunding: Tapping the Right Crowd** *Journal of Business Venturing*, vol. 29, no. 5.

[8] L. Lu, W. Xie, and S. Wu. **The Performance of PR-based Crowdfunding: Evidence from Kickstarter** *Information Management*.
[9] M. Pilkington. **Blockchain Technology: Principles and Applications** *Research Handbook on Digital Transformations*.
[10] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Y. Wang. **Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends** *IEEE Transactions on Systems, Man, and Cybernetics: Systems*.
[11] A. Savelyev. **Contract Law 2.0: 'Smart' Contracts as the Beginning of the End of Classic Contract Law** *Information Communications Technology Law*.
[12] S. Mollick. **The Dynamics of Crowdfunding: An Exploratory Study** *Journal of Business Venturing*, vol. 29, no. 1.
[13] B. Bhaskaran et al. **Smart-Contract-Based General-Purpose Governance Framework for Decentralized Organizations** *Proceedings of IEEE International Conference on Blockchain*.
[14] P. Koulu. **Blockchains and Online Dispute Resolution: Smart Contracts as a Tool for Self-Help** *Journal of Dispute Resolution*.
[15] C. Natarajan, S. Pant, and S. N. Khan. **A Novel Framework for Decentralized Crowdfunding Using Blockchain Technology** *International Journal of Engineering and Advanced Technology*.
[16] S. Huckle and M. White. **Socialism and the Blockchain** *Future Internet*, vol. 8, no. 4.
[17] J. Kruithof. **The Role of Governance in Decentralized Autonomous Organizations (DAOs)** *Tilburg University Law School*.
[18] M. Wohrer and U. Zdun. **Smart Contracts: Security Patterns in the Ethereum Ecosystem and Solidity** *Proceedings of IEEE International Workshop on Blockchain Oriented Software Engineering*.
[19] R. Beck, M. Avital, M. Rossi, and J. B. Thatcher. **Blockchain Technology in Business and Information Systems Research** *Business Information Systems Engineering*.
[20] F. Casino, T. K. Dasaklis, and C. Patsakis. **A Systematic Literature Review of Blockchain-Based Applications: Current Status and Future Trends** *Telematics and Informatics*.