IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

DECENTRALIZED BLOCKCHAIN BASED CROWDFUNDING PLATFORM

[1] Mathan R, [2] James Sadhu Sundar M, [3] Fayaz Ahmad S A, [4] Mrs. Doulas J

[1]Student, [2] Student, [3] Student, [4] Assistant Professor
[1] Computer Science and Engineering,
[1] Francis Xavier Engineering College, Tirunelveli – Tamil Nadu – India

Abstract:
Blockchain-based smart contract crowdfunding platforms are revolutionizing the fundraising industry by providing a decentralized, transparent, and secure way to raise funds. These platforms utilize blockchain's distributed ledger technology to create tamper-proof records of all transactions, ensuring the security and transparency of financial processes. By automating fundraising efforts, smart contracts—self-executing digital agreements—govern the transfer of funds according to the pre-defined terms. This reduces the reliance on intermediaries such as banks and legal professionals, thereby lowering costs and minimizing the risk of fraud. Blockchain technology also enhances security by encrypting transactions and storing them on a decentralized network, making it nearly impossible to hack or alter the data. Furthermore, the platform's transparency allows contributors to track how their donations are utilized, ensuring that the funds are directed toward their intended purpose. Overall, blockchain-based smart contract crowdfunding platforms offer several benefits over traditional fundraising methods, including increased transparency, enhanced security, cost efficiency, and improved effectiveness. Keywords: Blockchain, smart contract, crowdfunding, decentralization, security, transparency.

Introduction:
Smart contract crowdfunding platforms are among the key beneficiaries of blockchain technology, which has reshaped how various industries manage transactions. Although traditional fundraising methods can be effective, they often have drawbacks, such as dependence on intermediaries like banks and legal professionals, which increases costs, causes delays, and introduces potential fraud risks. In contrast, blockchain-based smart contract crowdfunding platforms provide a decentralized, transparent, and secure alternative that addresses these challenges. According to J. Sun, S. Huang, C. Zheng, T. Wang, C. Zong, and Z. Hui, once smart contracts are deployed, they cannot be modified [1]. These platforms leverage blockchain's distributed ledger technology to generate tamper-proof records of all transactions, ensuring both the security and transparency of financial operations. Smart contracts, which are self-executing digital agreements, automate the fundraising process by disbursing funds only when predefined conditions are satisfied. This significantly reduces the need

for third-party involvement, making the fundraising process more cost-effective and efficient. The use of blockchain technology in smart contract crowdfunding platforms has also significantly strengthened security. By encrypting transactions and storing them on a decentralized network, the system makes data manipulation and hacking nearly impossible. However, as M. Masthan and R. Ravi highlight, malware attacks can still exploit vulnerabilities in certain systems [2]. One of the major benefits of blockchain-based crowdfunding platforms is their transparency. Donors can track how their contributions are being utilized, ensuring that funds are directed toward their intended purpose. This level of visibility fosters trust between donors and fundraisers, encouraging more people to support fundraising campaigns.

Challenges of Centralized Applications:
Monopolies and trust issues are two of the issues that monopolized applications face. M, according to Masthan,
R. Ravi, and K. Praghash, one major problem is their reliance on central servers or databases, which makes them vulnerable to data breaches and hacking attempts [3]. This can lead to the theft of sensitive user information, such as financial or personal data. Additionally, centralized applications are typically owned and operated by a single entity, giving them full control over the platform and its data. Censorship, surveillance, and the misuse of authority are all possible outcomes of this concentration of authority. Finally, the high costs associated with maintaining and operating centralized systems often translate into expensive services for users. These applications are less suited to many use cases because of their centralized nature, which can lead to a lack of trust, increased risks, and higher costs. Blockchain technology offers a promising solution to these issues by providing a decentralized, secure, and transparent alternative.

Introduction to Blockchain:

Blockchain is a distributed digital ledger technology designed to store data securely and prevent tampering. It was initially created as the basis for the cryptocurrency Bitcoin, but it has since been used in a variety of other areas. In a blockchain, transactions are recorded across a network of computers in a decentralized and transparent way. Each block of data contains a cryptographic hash of the previous block, linking them together to form a continuous chain—hence the term "blockchain." This structure ensures that any attempt to modify the data in one block is immediately detected and rejected by the entire network. Direct peer-to-peer transactions are made possible by blockchain technology, which eliminates the need for intermediaries like banks. This is one of the main benefits of blockchain technology. It also offers a high level of security, transparency, and immutability, making it ideal for applications like supply chain management, identity verification, and voting systems. In a blockchain, each block's contents are represented by a unique code called a hash. These hashes are generated using complex mathematical algorithms that are difficult to reverse engineer. Once a block is created, it is added to the blockchain in a linear, chronological order, forming an unbroken chain. Blockchain's decentralized nature ensures that each block is validated and verified by a network of users or nodes, rather than a single central authority. This validation process guarantees the accuracy and integrity of the data. Additionally, every node on the network maintains a copy of the blockchain, which is synchronized with all other nodes to ensure consistency. Once added, a block cannot be modified or deleted. Any attempt to alter its contents will result in an invalid hash, which the network will reject. This makes blockchain a secure and transparent system that is highly resistant to hacking, fraud, and other forms of data manipulation. Blockchain technology has a wide range of applications, including voting systems, supply chain management, cryptocurrency, and more.

Encryption System in Blockchain:

A fundamental component of blockchain technology is encryption. According to A. R and Shakeela Joy Ravi, encryption is very important for protecting blockchain networks [4]. Encryption in a blockchain makes sure that all data sent across the network stays safe and can't be changed. This is achieved through public-key cryptography, a system that uses two keys: a public key and a private key. The public key is used for encrypting data, while the private key is used for decryption. When a user sends data over the blockchain network, it is encrypted using the recipient's public key. Only the recipient, with their corresponding private key, can decrypt the data and access its contents. In addition to encryption, blockchain networks also rely on hashing algorithms to maintain data integrity. A. Monika, T. Samraj Lawrence, and R. Ravi explain that hashing algorithms generate a unique, fixed-length hash based on the input data [5]. Each hash is distinct to the specific data, and even the slightest modification in the input will produce a completely different hash. This makes it nearly impossible to alter data without changing the hash, which the network can easily detect, ensuring the authenticity of the stored information.

Ethereum Network:

Ethereum is a decentralized blockchain network that allows developers to create and run smart contracts and decentralized applications (DApps). It uses its native cryptocurrency, Ether (ETH), as a payment method for executing transactions on the network. The platform's capacity to facilitate Initial Coin Offerings (ICOs) and the creation of custom tokens is one of Ethereum's most distinctive features. With its Turing-complete programming language, Solidity, developers can build and deploy complex smart contracts and DApps. In recent years, Ethereum has gained significant traction due to its emphasis on decentralization, transparency, and security, making it a key platform for the development of decentralized finance (DeFi) applications. Alongside Ethereum, the Bitcoin network is also widely used. However, there are key differences between the two. While Bitcoin was primarily designed as a digital currency, Ethereum was developed as a platform for building DApps and running smart contracts. Bitcoin has a limited scripting language, which supports only basic transactions, whereas Ethereum offers a more advanced scripting language, enabling the creation of complex DApps and smart contracts. Additionally, Ethereum has a faster block time and generally lower transaction fees compared to Bitcoin. However, Bitcoin is more widely accepted as a payment method, and its capped supply gives it the potential to act as a store of value. In summary, while both Ethereum and Bitcoin hold significant value, Ethereum's focus on DApps and smart contracts makes it more versatile, whereas Bitcoin's primary strength lies in its use as a digital currency and store of value.

Understanding Node Validation:

Node validation is a crucial process in the Ethereum network that maintains the security and reliability of the blockchain. In Ethereum, node validation involves verifying transactions and blocks before they are added to the blockchain. When a transaction is submitted to the network, it is broadcast to all participating nodes. The transaction is then validated by each node by examining its digital signature, verifying the sender's account balance, and ensuring that it satisfies all requirements. If the transaction is valid, it is added to a pool of unvalidated transactions waiting to be confirmed by miners. Once a transaction is verified, it is grouped with other valid transactions and included in a block. Each node checks the block's digital signature, verifies the legitimacy of all transactions, and ensures that the block complies with the rules of the network after it has been created. If the block passes validation, it is added to the blockchain, and every node updates its copy accordingly. The Ethereum network's security relies heavily on node validation. It ensures that only valid and trustworthy transactions and blocks are added to the blockchain, protecting the network from potential attacks or fraudulent activities that could compromise its integrity.

PoS vs PoW: Key Differences and Comparison:

In blockchain networks, Proof of Work (POW) and Proof of Stake (POS) are two different consensus mechanisms used to validate transactions and add new blocks. In POW, miners compete to solve complex mathematical problems, and the first miner to solve the problem earns the right to create the next block. This process is bad for the environment because it uses a lot of computational power and energy. In contrast, POS uses validators (also known as "forgers") who are selected based on the amount of cryptocurrency they hold. These validators are responsible for creating new blocks and verifying transactions. As a result, POS is significantly more energy-efficient than POW. Besides being less energy-intensive, POS also reduces the risk of centralization. In

POW, large mining operations with extensive resources can dominate the network, leading to centralization of mining power. However, in POS, the risk of centralization is lower, as validators are chosen based on their cryptocurrency holdings rather than their computing power. Overall, while both POW and POS have their own strengths and weaknesses, POS is generally seen as more energy-efficient and less centralized consensus method compared to POW.

Benefits of DeFi Applications:

Applications for decentralized finance (DeFi) have a number of advantages over conventional financial systems. Firstly, they give users greater control over their funds by operating on decentralized blockchain networks, removing the need for intermediaries such as banks or financial institutions. This reduces the risk of fraud or theft. Secondly, DeFi apps promote

transparency, as all transactions are recorded on the blockchain and are publicly accessible. It is harder for fraudulent activities to go unnoticed when there is this level of transparency. Thirdly, DeFi applications are highly accessible, as they can be used by anyone with an internet connection, regardless of their location or financial status. Moreover, DeFi systems are less prone to Distributed Denial-of-Service (DDoS) attacks. M, according to Masthan and R. Ravi, networks with standard security measures are more vulnerable to DDoS attacks [6]. Overall, DeFi apps offer a more open, accessible, and transparent financial system, making them an appealing alternative to traditional financial platforms.

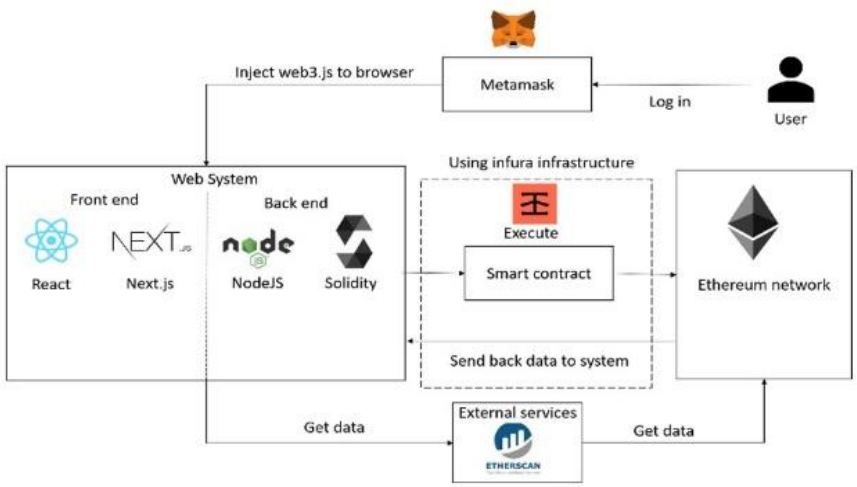
Using Smart Contracts for Crowdfunding:

Smart contracts have transformed crowdfunding by offering a decentralized, transparent, and secure method for raising funds. These contracts automatically enforce the terms of the agreement and facilitate fundraising through blockchain technology, ensuring that funds are only released when specific conditions are met. This automation eliminates the need for intermediaries such as banks and lawyers, reducing costs and increasing efficiency.

Development Methodology:

Deploying a smart contract is a crucial step in building a blockchain-based platform, as it ensures the code is executed securely and in a decentralized manner. For the smart contract crowdfunding platform, the deployment was done using Thirdweb, a blockchain development company specializing in smart contract deployment and integration. The platform was deployed on the Ethereum test network, specifically the Sepolia test network, allowing the contract to be tested and evaluated in a simulated blockchain environment. The deployment process began with compiling the Solidity code into bytecode, which was then uploaded to the test network using Remix, a popular development tool. Bytecode is a low-level representation of the contract that the Ethereum Virtual Machine (EVM) can execute. After the bytecode was uploaded, it was stored in a block, which contains a set of transactions and a unique cryptographic hash linking it to the previous block. Once the smart contract was deployed, it was integrated with the front-end user interface, developed using Next JS. This integration involved connecting the interface with the smart contract address on the Ethereum network, enabling the interface to interact with the contract's functions. The integration was achieved using Web3.js, a JavaScript library that provides APIs for interacting with the Ethereum network.

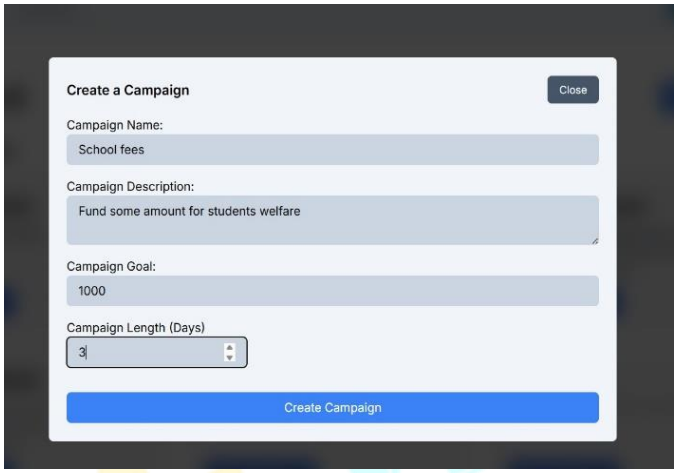
Deploying the smart contract on the test network allowed for the assessment of the platform's functionality, including creating campaigns, collecting donations, and retrieving campaign and donor data. The Sepolia test network provided a simulated blockchain environment, enabling the smart contract to be tested and evaluated securely and in a decentralized manner. Overall, the deployment on the test network was a key step in the development of the crowdfunding platform, allowing for thorough testing and validation of its features in a safe and controlled blockchain environment.



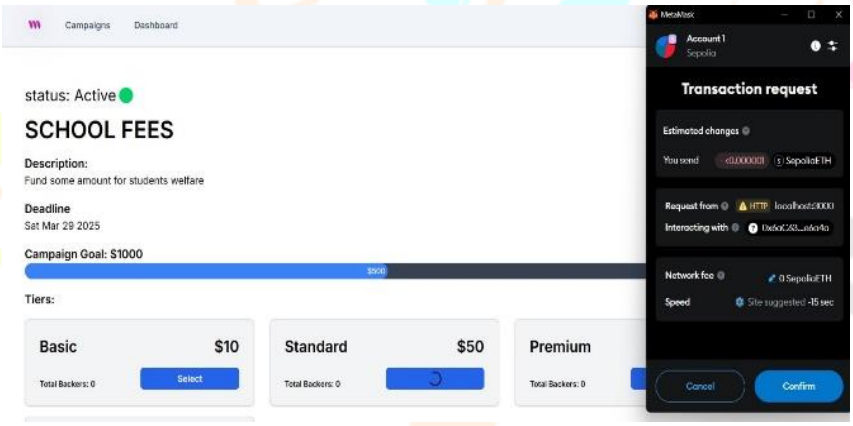
This figure describes the overall process of the platform.

metmask is used for authentication. The person with the metamask account can only access this platform. The developer can create a camapaign. And the people whoever like the project can donate to the project. The project can only be funded with the ethereum.

Results:



The createCampaign function works well and the transactions are done with the gas fees.



The donate campaign also works well and transaction done with the gas fee.

Conclusion:

The crowdfunding platform has been successfully deployed on the test network. Building this smart contract-based crowdfunding platform has been an exciting and rewarding journey. By utilizing the power of the Ethereum blockchain and writing the smart contract in Solidity, we have developed a decentralized platform that allows users to create campaigns and receive donations securely and transparently. With React.js, we created a user-friendly front-end, making it easy for users to interact with the platform. We were able to thoroughly test the platform and verify its functionality with the assistance of ThirdWeb by deploying the smart contract on the Sepolia test network. This project has provided valuable hands-on experience in blockchain development and showcased the potential of blockchain technology to transform traditional crowdfunding. We are excited about the platform's potential to change the crowdfunding landscape and give individuals and organizations the ability to raise funds in a fair and transparent manner.

References:

1. J. Sun, S. Huang, C. Zheng, T. Wang, C. Zong, and Z. Hui, "Mutation testing for integer overflow in Ethereum smart contracts," Tsinghua Science and Technology, vol. 27, no. 1, pp. 27-40, February 2022, doi: 10.26599/TST.2020.9010036.

2. M. Masthan and R. International Journal on Recent Researches in Science, Engineering, and Technology, vol. 4, no. 6, pages Ravi, "Preventing Zero Day Malware Attack Outbreaks in a Network Using Cyber Resilience Recovery Model." 1-20, 2016.

3. K. Praghash, M. R, Masthan, and Ravi, "An investigation of security techniques for concealed DDoS exposure attacks," ICTACT Journal on Communication Technology, vol. 9, no. 1, pp. 1681-1685, 2018.

4. A. R and Shakeela Joy Ravi, "Enhanced Endorsement Scheme for Smart Card Using Elliptic Curve Cryptography," International Journal of Advanced Research in Basic Engineering Sciences and Technology, vol. 3, no. 9, pp. 17-22, 2017.

5. A. Monika, T. Samraj Lawrence, and R. Ravi, "Three schemes to block real-time packet classification by combining physical layer characteristics with cryptographic primitives. They also looked at security measures and the costs of computing and communicating with them," 2014, page 108.

6. M. Masthan and R. Ravi, "Preventing Zero Day Malware Attack Outbreaks in a Network Using Cyber Resilience Recovery Model," International Journal on Recent Researches in Science, Engineering and Technology, vol. 4, no. 6, pp. 1-20, 2016.

7. L. Brent, A. Jurisevic, M. Kong, E. Liu, and B. Scholz, "Vandal: A static analysis framework for smart contracts," Proceedings of the ACM Conference on Systems and Programming Languages, 2018, pp. 1-10.

8. N. Atzei, M. Bartoletti, and T. Cimoli, "A Survey of Attacks on Ethereum Smart Contracts (SoK)," Proceedings of the 6th International Conference on Principles of Security and Trust, Springer, 2017, pp. 164–186.

9. D. Perez and B. Livshits, "Smart Contract Vulnerabilities: Vulnerable Does Not Imply Exploited," USENIX Security Symposium, 2021.

10. S. Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Tikhomirov, and Y. Alexeev, "SmartCheck: Static Analysis of Ethereum Smart Contracts," Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, ACM, 2018, pp. 9–16.