International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume X, Issue III, March - 2023

SMART CONTRACT CROWDFUNDING USING BLOCKCHAIN TECHNOLOGY

Muthu @Ramkumar S
Computer Science and Engineering,
Cyber Forensics Applied Lab,
Francis Xavier Engineering College,
Tirunelveli – Tamil Nadu - India
muthuramlap262003@gmail.com

Sudhan Raj Babu A
Computer Science and Engineering,
Cyber Forensics Applied Lab,
Francis Xavier Engineering College,
Tirunelveli – Tamil Nadu - India
sudhanraja.ug20.cs@francisxavier.ac.in

Muthu Kausalya
Electronics and Communication Engineering,
Cyber Forensics Applied Lab,
Francis Xavier Engineering College Tirunelveli– Tamil Nadu - India
muthukausalya.ug20.ec@francisxavier.ac.in

Dr. R. Ravi Professor /
Dept. of Computer Science and Engineering,
Cyber Forensics Applied Lab,
Francis Xavier Engineering College
Tirunelveli – Tamil Nadu – India
dr.r.ravi@francisxavier.ac.in

Abstract:

Blockchain-based smart contract crowdfunding platforms are transforming the fundraising sector by offering a decentralised, open, and safe way to raise money. These systems use distributed ledger technology from the blockchain to provide tamper-proof records of all transactions, guaranteeing the security and transparency of all financial processes. Automating fundraising efforts makes it possible to control the transfer of cash by using smart contracts, self-executing digital contracts that enforce the terms of the agreement. This lessens the need for intermediaries like banks and attorneys and takes away the chance of fraud. By encrypting transactions and storing them on a decentralised network, blockchain technology also offers a high level of security, making it nearly difficult to hack or change the data.Moreover, contributors may monitor how their contributions are being used because to the platform's openness, which guarantees that money are being used for the intended purpose. Overall, blockchain-based smart contract crowdfunding systems have several advantages over conventional fundraising techniques, including transparency, security, cost-effectiveness, and efficiency.

Keywords: Blockchain, smart contract, crowdfunding,

Introduction:

Smart contract crowdfunding platforms are among the main benefactors of this revolutionary technology, which has altered the way many sectors conduct transactions. Even while they are effective, traditional fundraising techniques can have a number of drawbacks, such as the need to employ middlemen like banks and attorneys, which can raise expenses, cause delays, and provide potential for fraud. Blockchain-based smart contract crowdfunding systems provide a decentralised, open, and safe solution that overcomes these issues. According to J. Sun, S. Huang, C. Zheng, T. Wang, C. Zong and Z. HuiThese, smart contracts can't be changed once it deployed [1]. platforms make use of blockchain's distributed ledger technology to provide tamper-proof records of every transaction, guaranteeing the security and openness of all financial operations. Smart contracts, often referred to as self-executing digital contracts, are used to do this since they automate fundraising efforts and only release cash when certain criteria are satisfied. By greatly reducing the need for middlemen like banks and attorneys, this strategy makes the fundraising process more economical and successful. Security has been greatly improved by the usage of blockchain technology in smart contract crowdfunding platforms. It makes data manipulation and hacking almost difficult by encrypting transactions and storing them on a decentralised network. According to M. Masthan ,and R. Ravi, the malware attacks outbreaks an

network easily in vulnerable system [2]. In addition to ensuring that money is spent for its intended purpose, this greatly lowers the chance of fraud. The transparency of blockchain-based crowdfunding platforms for smart contracts is one of its most important benefits. Donors may keep tabs on how their contributions are being put to use, ensuring that the money is going towards what it is supposed to. This degree of openness fosters confidence between donors and fundraisers, which motivates more individuals to support fundraising activities.

Problem With Centralized Application:

Centralized applications have problems like trust issues, monopoly and etc. According to K. Praghash , M. Masthan and R. Ravi firstly, they rely on central servers or databases, making them vulnerable to hacking and data breaches [3]. This can result in the theft of sensitive user data, such as personal information or financial data. Secondly, centralized applications are typically owned and operated by a single entity, giving them full control over the application and its data. This centralization of power can result in censorship, surveillance, and other forms of abuse of power. Finally, centralized applications can be expensive to maintain and operate, which can result in high fees for users. Overall, the centralized nature of these applications can result in a lack of trust, increased vulnerability, and high costs for users, making them less than ideal for many applications. These all problems can be solved with the help of blockchain technology.

Blockchain:

Blockchain is a distributed digital ledger technology that allows data to be stored in a secure and tamper-resistant manner. It was originally developed as the underlying technology for the cryptocurrency Bitcoin, but it has since been applied to a wide range of other applications. In a blockchain, transactions are recorded across a network of computers in a decentralised and transparent manner. Each block of data contains a cryptographic hash of the previous block, which creates a chain of blocks, hence the name "blockchain". This ensures that any attempts to alter the data in one block will be immediately detected and rejected by the rest of the network. One of the key benefits of blockchain technology is that it eliminates the need for intermediaries such as banks, allowing for direct peer-to-peer transactions. It also provides a high level of security, transparency, and immutability, making it ideal for applications such as supply chain management, identity verification, and voting systems. A chain of blocks containing digital data is referred to as a blockchain. In a blockchain, each block's contents are represented by a special code called a hash. The hash of each block is created using complex mathematical algorithms that are designed to be difficult to reverse engineer. Once a block is created, it is added to the blockchain in a linear, chronological order, forming a chain of blocks. The decentralization of a blockchain means that each block is validated and verified by a network of users or nodes, rather than a centralized authority. This validation process ensures that the information recorded in each block is accurate and tamper-proof. Moreover, each node in the network has a copy of the blockchain, which is synchronized with other nodes to ensure that all copies of the blockchain are the same. Once a block is added to the blockchain, it cannot be modified or deleted, and any attempt to alter the contents of a block will result in an invalid hash, which will be rejected by the network. This creates a secure and transparent system that is resistant to hacking, fraud, and other forms of tampering. Applications for blockchain technology include voting systems, supply chain management, cryptocurrency, and more.

Encryption System in Blockchain:

Encryption is a basic system in blockchain. According to A. Shakeela Joy and R.Ravi encryption plays a crucial role in the security of blockchain networks [4]. In blockchain, encryption is used to ensure that all data transmitted over the network is secure and tamper-proof. To achieve this, blockchain networks use public-key cryptography, which is a cryptographic system that uses two keys: a public key and a private key. The public key is used to encrypt data, while the private key is used to decrypt data. When a user sends data over the blockchain network, the data is encrypted using the recipient's public key. Only the recipient, who has the corresponding private key, can decrypt the data and read its contents. In addition to encryption, blockchain networks also use hashing algorithms to ensure the integrity of data. A. Monika, T. Samraj Lawrence, and R. Ravi proposed Hashing algorithms create a unique fixed-length output, or hash, based on the input data [5]. The hash is unique to the input data, and any small change in the input data will result in a completely different hash. This makes it impossible to alter data without changing the hash, which is easily detectable by the network.

Ethereum Network:

Ethereum is a decentralized blockchain network that enables developers to create and execute smart contracts and decentralized applications (DApps). It utilizes its cryptocurrency called Ether (ETH) as a means of payment for executing transactions on the network. One of the most significant features of the Ethereum network is the ability to create custom tokens and execute Initial Coin Offerings (ICOs) on the platform. With its Turing-complete programming language, Solidity, developers can build complex smart contracts and DApps on the Ethereum network.

Additionally, Ethereum has gained popularity in recent years due to its focus on decentralization, transparency, and security, making it an essential platform for the development of decentralized finance (DeFi) applications. Other than ethereum network bitcoin network is also widely used. But there are some differences in both networks. While Bitcoin was primarily designed as a digital currency, Ethereum was created to be a platform for building decentralized applications (DApps) and executing smart contracts. Bitcoin has a limited scripting language that allows for simple transactions, whereas Ethereum has a more complex scripting language, enabling developers to create complex DApps and smart contracts. Additionally, Ethereum has a faster block time and lower transaction fees compared to Bitcoin. However, Bitcoin is more widely accepted as a means of payment, and its limited supply gives it the potential to be a store of value. In summary, while both Ethereum and Bitcoin are valuable in their respective ways, Ethereum's focus on DApps and smart contracts makes it more versatile than Bitcoin.

Node Validation:

Node validation is an essential process in the Ethereum network that ensures the security and integrity of the blockchain. In Ethereum, node validation refers to the process by which nodes on the network verify the transactions and blocks that are added to the blockchain. A transaction is broadcast to all network nodes when it is submitted to the network. The transaction is then validated by each node by validating its digital signature, the sender's account balance, and that it satisfies all prerequisites.If the transaction is legitimate, it is added to the list of transactions that have not yet been validated by miners. A transaction is included in a block together with other verified transactions once it has been confirmed. Again, each node validates the block by checking its digital signature, verifying that the transactions in the block are valid, and ensuring that the block meets all the required conditions. If the block is valid, it is added to the blockchain, and the nodes update their copy of the blockchain accordingly. Node validation is critical to the security of the Ethereum network, as it ensures that all transactions and blocks added to the blockchain are legitimate and meet all the required conditions. This prevents the network from being compromised by malicious actors who might attempt to manipulate the blockchain for their own gain.

PoS vs PoW:

In blockchain networks, POS (Proof of Stake) and POW (Proof of Work) are two distinct consensus processes used to confirm transactions and add new blocks. In POW, miners compete to solve complex mathematical problems, and the first miner to solve the problem is rewarded with the right to create the next block. This process is computationally intensive and requires a lot of energy, which is why it's sometimes criticized for being environmentally unfriendly. On the other hand, in POS, validators (sometimes called "forgers") are selected based on the amount of cryptocurrency they hold, and are then responsible for creating new blocks and validating transactions. This means that the energy consumption of POS is significantly lower than POW. In addition to being more energy-efficient, POS also reduces the risk of centralization, as large mining operations in POW can sometimes lead to centralization of mining power. In POS, the risk of centralization is reduced, as validators are selected based on the amount of cryptocurrency they hold, rather than their computing power.Overall, while both POW and POS have their advantages and disadvantages, POS is generally considered to be a more energy-efficient and less centralized consensus mechanism than POW.

Why DeFi Application:

Decentralized finance (DeFi) apps offer several advantages over traditional financial applications. Firstly, they provide users with more control over their funds as they are built on decentralized blockchain networks, which eliminates the need for intermediaries like banks or financial institutions. This, in turn, reduces the risk of fraud or theft of funds. Secondly, DeFi apps offer more transparency, as all transactions are recorded on the blockchain and can be viewed by anyone. This increased transparency also reduces the risk of fraudulent activities. Finally, DeFi apps offer more accessibility, as they are accessible to anyone with an internet connection, regardless of their geographic location or financial status. And it also neglects the DDos attacks. According to M. Masthan ,and R. Ravi, the network in normal security is more vulnerable to DDoS attacks [6]. Overall, DeFi apps offer a more democratic, accessible, and transparent financial system that is open to anyone, making them an attractive alternative to traditional financial applications.

Smart Contract for Crowdfunding:

Crowdfunding has undergone a revolution thanks to smart contracts, which provide a decentralised, transparent, and safe way to raise money. These contracts enforce the terms of the agreement and enable automated fundraising efforts using blockchain technology, guaranteeing that funds are only distributed when certain requirements have been satisfied. As a result, there is no longer a need for intermediaries like banks and attorneys, which lowers expenses and boosts productivity.

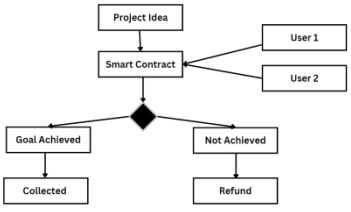
Methodology:

The deployment of a smart contract is a critical step in the development of a blockchain-based platform, as it ensures that the code is executed in a secure and decentralized manner. In the case of the smart contract crowdfunding platform, the deployment process was carried out with the help of Thirdweb, a blockchain development company that specializes in the deployment and integration of smart contracts. The platform was deployed on the Ethereum test network, specifically the Sepolia test network, which allowed for the testing and evaluation of the smart contract in a simulated blockchain environment.

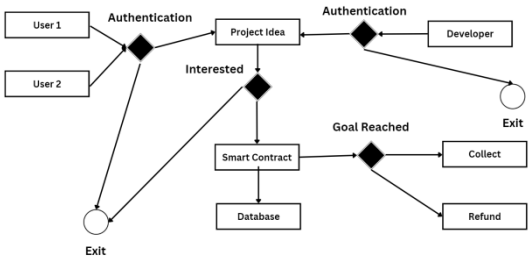
To deploy the smart contract, the Solidity code was compiled into bytecode, which was then uploaded to the test network using a tool called Remix. The bytecode is a low-level representation of the code that can be executed by the Ethereum Virtual Machine (EVM), which is a runtime environment for smart contracts on the Ethereum network. Once the bytecode was uploaded to the test network, it was stored in a block, which is a unit of data that contains a set of transactions, along with a unique cryptographic hash that links it to the previous block.

After the smart contract was deployed, it was integrated with the front-end user interface, which was developed using React JS. This integration involved linking the user interface with the smart contract address on the Ethereum network, which allowed the user interface to interact with the smart contract functions. The integration was carried out using a library called Web3.js, which is a collection of JavaScript APIs that allow for the interaction with the Ethereum network.

The deployment of the smart contract on the test network allowed for the evaluation of the platform's functionality, including the creation of campaigns, donation collection, and the retrieval of campaign and donor data. The Sepolia test network provided a simulated blockchain environment that allowed for the testing and evaluation of the smart contract in a secure and decentralized manner. Overall, the deployment of the smart contract on the test network was a critical step in the development of the crowdfunding platform and enabled the testing and evaluation of its functionality in a secure and simulated blockchain environment.

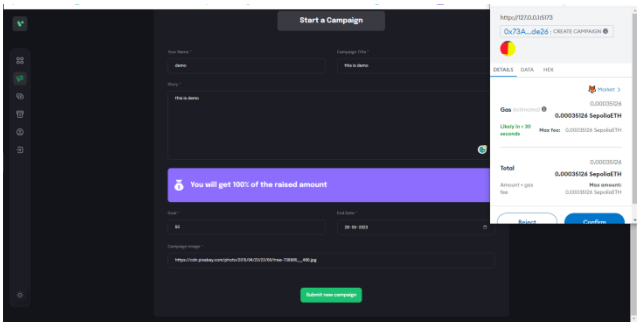


This figure describes the overall process of the platform.

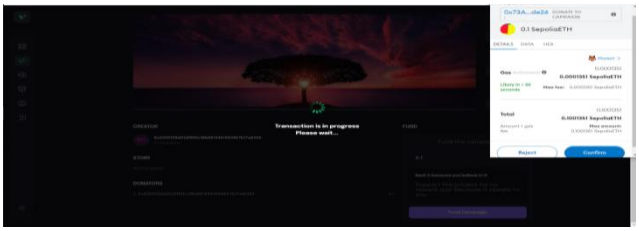


metmask is used for authentication. The person with the metamask account can only access this platform. The developer can create a camapaign. And the people whoever like the project can donate to the project. The project can only be funded with the ethereum.

Results:



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



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

Conclusion:

The crowdfunding platform is deployed successfully on the test network. The development of this smart contract crowdfunding platform has been an exciting and challenging journey. By leveraging the power of the Ethereum blockchain and using the Solidity language to write the smart contract, we have created a decentralized platform that allows users to create campaigns and receive donations in a secure and transparent way. With the integration of React.js, we have built a user-friendly front-end that enables users

to easily interact with the platform. The deployment of the smart contract on the Sepolia test network, with the help of ThirdWeb, has allowed us to test the platform and ensure its functionality. This project has provided valuable experience in blockchain development and has demonstrated the potential of blockchain technology to revolutionize traditional crowdfunding. Overall, this platform has the potential to empower individuals and organizations to raise funds in a fair and transparent manner, and we are excited to see its impact on the world of crowdfunding.

References:

1. J. Sun, S. Huang, C. Zheng, T. Wang, C. Zong and Z. Hui, "Mutation testing for integer overflow in ethereum smart contracts," in *Tsinghua Science and Technology*, vol. 27, no. 1, pp. 27-40, Feb. 2022, doi: 10.26599/TST.2020.9010036.
2. 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.
3. K. Praghash , M. Masthan and R. Ravi, "An investigation of security techniques for concealed DDOS exposure attacks", ICTACT Journal on communication technology, vol. 09, no. 01 pp.1681-1685, 2018.
4. A. Shakeela Joy and R.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 (2014) suggested that the three schemes that block real-time packet classification by fusing physical layer characteristics with cryptographic primitives. Finally, they looked at security measures and assessed their computational and communication costs [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.