WEB APPLICATION FOR CAMPAIGN FUNDING WITH FORGERY PREVENTION USING SHA-256 IN BLOCKCHAIN

J. Sathya Priya[1], G.Ignancya Michelle[2], S.Jayadharrshani[3], S.Sangavi [4]

[1] *Associate Professor, Information Technology, Velammal Engineering College, Tamilnadu, India*
[2] *Student, Information Technology, Velammal Engineering College, Tamilnadu, India*
[3] *Student, Information Technology, Velammal Engineering College, Tamilnadu, India*
[4] *Student, Information Technology, Velammal Engineering College, Tamilnadu, India*

ABSTRACT

People who are in need of funds to develop a project can collect money through various online platforms. The donated money collected reaches the project manager, which is used to complete the project or to make a product online. The traditional method of online campaign funding has a major drawback. It does not allow contributors to have control over the money they have contributed and the admin or the higher authority has control over the money that is funded which leads to many malicious activities and discomfort. Here we address this problem faced by the existing online campaign funding platforms by using the Ethereum network and smart contract using blockchain. The decentralized blockchain platform called Ethereum establishes a peer-to-peer network relation that securely executes and verifies various application codes called smart contracts. The development of Blockchain technology is allowing businesses to build decentralized models. Data is validated with the help of the POW technique, this makes the new block gets added to the chain. Blockchain technology has developed in such a way that it allows the business to build decentralized models which help in deriving new methodologies to conduct transactions and make agreements. One of the technologies that propose another solution to the traditional model is the smart contract. A smart contract is the same as that of a contract in the physical world, but it is digital and represented by a tiny computer program stored in a blockchain. SHA-256 encryption algorithm has been used to improve the security of this project by providing the Hash value to every single block which becomes very tough for the scammers to access the data stored in the blocks.

Keywords: - *Blockchain, SHA-256, Decentralized, Ethereum*

1. INTRODUCTION

Campaign funding is a way of collecting funds for projects which were done through the internet with many investors for small businesses and some sort of beneficiary to an emergency kind of projects. Entrepreneurs are motivated to employ campaign funding by the need to raise money, with the aim of raising awareness for their gaining validation. One big problem with campaign funders is being hacked and misleading the private information as well as the payment information of the investors to another source by fraud. Campaign funding forgery occurs when a campaign requests and accepts money from funders or investors using deliberately misleading about the nature of the project or the expected outcomes. Nowadays fraud in campaign funding has increased throughout all projects so we have to prevent those suspicious things to protect the investor's funds and information. Due to this issue, many investors fear donating funds to this platform. In this study, we aim to provide such kind of fraud prevention in our project by using the SHA-256 algorithm on the blockchain-based website to prevent fraud. We have used SHA-256 is one of the strongest secure hashing algorithms. It is hashing algorithm. Created and calculated by hash values. We have used a simple interface of Html and CSS for the user to raise a project and invest in a project which is based on

the blockchain-based website. Blockchain network website is highly secure in data and helps to prevent forgery activities.

Blockchain comes in the form of open and decentralized databases with high security. Because blockchain has robustness and trustworthiness. Blockchain has interconnected blocks of transactions with current and previous hash values. Blockchain network is not immune to fraud. We use blockchain to create blocks of information for the investors with high security of information to prevent fraud. The blocks will have current and previous hash values to prevent irregular data. We use network-based blockchain to overcome the problem of less security by creating multiple blocks of information. So we can prevent forgery by running the blocks and the block ends when it detects the fraud. The blockchain makes the platform better without a centralized authority. Because the blockchain removes the risk of the data being centralized.

2. RELATED WORK

In the literature, the authors have implemented the idea to bring up the percentage of successful fund collection from 30-35% which is really low considering the fact that more than 60% of the projects fund are only partially collected or not collected at all [1]. This is due to the high-level possibility of scams. Hence, to overcome this challenge the transparency of the fund transfer has been made visible to users and admin [2]. However, this appears to be a major drawback considering the possibility of misusing such an opportunity. Another major requirement in a campaign funding platform is to accept only the projects which abide by the guidelines of the government and be checked. This also means high cost[8]. Bitfund was a new global crowdfunding platform to develop a smart nation and the inherent features of blockchain technology.[3] There are a few ways in which donors' trust can be gained like showing them how the money collected is used and this idea was brought by this author. The other idea shared was that the project's proposal can be viewed as a PDF using peer to peer file sharing system. Only when the majority of contributors agree on the proposal of the project it would be sent to the vendors to be put up for fundraising [5]. Preventing fraud using the fraud triangle is yet another option. Here, three characteristics are considered namely decentralization to largely increase fraud cost, append-only linear form of transactional data rather than a relational database to make the data more difficult to modify, and the third characteristic [13]is with smart contracts serving as automatic controls which means the human factor is removed and enhances the control environment.

This can act as a major disadvantage in the time reviewing every project can take time. Increasing the ambiguity of the smart contract was considered and implemented to reduce fraud percentage but this may also lead to difficulty for the user to use[12]. Reviewing and accepting the project by many contributors result in a delay of time and wastage of resources. A few ideas have been proposed by only allowing the authenticated recipient and donor to request and donate money. [6] The proposed idea uses a clustering algorithm that filters data from a large set of datasets and uses the k-nearest neighbor algorithm to combine similar data in a group of large datasets. Income tax frauds must also be avoided which can end up with people escaping from tax pay by false statements. It also helps considering the behavioral events such as donor retention and donation recurrence [5]. Bringing in transparency in transactions would discourage potential donors from participating which may be one major disadvantage and can decrease possible donors and fundraisers. However, analyzing the data on fraudulent behavior can help in understanding better the area to be focussed on [6].

There are a few more challenges faced by the industries to execute a platform with improved transparency, efficiency, and security of the system. Decentralized crowdfunding is introduced to include transparency, global availability, and lower fees. [12] Scaling mechanisms are introduced to projects to increase the scalability of platforms that lack that quality. Multiple iterations of bidding until an optimal solution is reached are done by developers. This can be turned around by considering the fact that small projects or even the projects which are being oblivious are left out. Information asymmetry is where one group of people receives more information than the other. This is another major drawback of a platform. [10] And this asymmetric information along with forgery information must be avoided in a campaign funding platform. [11]Not only the implementation part of a platform but also the efficiency of a platform must be on point for it to run without any faults. Hence, an author has created a tamper-proof environment which is also put to testing like positive and negative unit testing to beat the efficiency of the existing solution. But a complete tamper-proof environment is not possible. With the multi-level of testing the expense may increase.[7] There are no intermediaries involved, a clear money trail is followed here. A centralized crowdfunding concept can bring in more potential investors, which means more people may reject the proposal, resulting in a lower fund being raised. In the Bitfund platform, the investors can select and request a specific project of their interest and put in an initial bid value in terms of time, cost, and the maintenance required which is a good initiative considering a

project is valued for its capability and worth[9]. This is a significant requirement as many projects that are in serious need of funds lose their opportunities due to scammers who misuse the platform.

Famous crowdfunding platforms like Kickstarter and Indiegogo stand away from other crowdfunding platforms for their features like revolutionizing flexibility and efficiency in raising funds and getting access to top investors for small business people with great ideas [4]. In the end, it is about the act of helping the people in need and making sure the right amount reaches the right people at the right time. [3]Pay-it-forward was one such model to ensure that anyone who has launched the campaign must have already paid their dues.

3. PROPOSED WORK

3.1. OVERVIEW

Both crowdfunding and cryptography are the trends on the internet nowadays and they match each other very perfectly. Blockchain is one of the famous and major technologies that is used to reduce malicious activities in crowdfunding. The project is designed in such a way that the people who are in need of money to develop their project raise a request for the funds needed. Seeing those requests the donors who are interested in the project development donate the money. Once the donated money reaches the requested amount it will be transferred to the recipient The decentralized global software platform powered by blockchain technology is Ethereum. Ethereum is used by people to create a secure digital technology they think to do. It has a token designed for use in the blockchain network, but it can also be used by participants as a method to pay for work done on the blockchain.

3.2 BLOCKCHAIN

A blockchain is a list of growing records which are called blocks, that are securely linked together using cryptography. This block contains a cryptographic hash value of the previous block, a timestamp, and transaction data. The timestamp tells about the transaction data in the block. These blocks contain information about the block previous to it so they form a chain, with each additional block following the ones before it. Therefore, blockchains have restricted the modification of data because once the data is added they get recorded in the blocks, and when we need to alter the data of a particular block we have to first alter the previous block of the referred block.

3.3 SHA-256

Hashing is the process of converting the raw information to an extent that it cannot reproduce its original form. It takes a key from the whole information and passes it to a function that performs mathematical operations on the key which is a plain text and converts it into ciphertext. This function that is used is called the hash function. Although there are many new algorithms and methodologies in network security, encryption and hashing have been the most important and core importance of security modules. The secure hash algorithm of value size 256, or the SHA 256 algorithm, is the widely used and important hash algorithm in real-world applications. We can divide the complete process of the SHA-256 algorithm into five different segments, which are

- **Padding bit:** At first, it checks the bit size of the message if the size is less than the required size it adds extra bits to the message, such that the length of the message is exactly 64 bits short which is the multiple of 512. During the addition of the bit process, the first bit which is filled will be one, and the rest of the bills that are filled will be with zeroes.
- **Padding length:** We can add up to 64 bits of data to make the final plaintext a multiple of 512. We have to calculate these 64 bits of characters by applying the modulus to the original plaintext without the padding. Initializing the buffer: We have to initialize the default values for the eight buffers to be used in the rounds and we also need to store 64 different keys in an array, ranging from K[0] to K[63].
- **Compression function:** The entire message gets broken down into multiple blocks of 512 bits each. Each message undergoes 64 rounds of operation, with the output of the first block serving as the input for the following block.
- **Result production:** After completing all the iterations, the final output of the block acts as the input for the next block. This entire cycle keeps repeating until it reaches the last 512-bit block, and that is considered the final hash value. This value will be of the length 256-bit.

4. MODULES

4.1 FUNDRAISING MODULE

A new request is created by making an instance on the website. The user will access the website with the help of the user interface to create a new request for fundraising. For every new request, a new fundraising column gets created with the data of the fundraiser and the cause of raising the fund will be associated with the database. After the request is created it will be displayed on the Home page from where the user and the donor interact. Once the request is created a new block is created which is called the genesis block and for each successful transaction, a new block gets created and gets added to the genesis block thus forming a blockchain.

4.2 REQUEST CREATION MODULE

After creating a new request for the fund the donor will donate and contribute to the request. The fund received from the user cannot be directly used by the fundraiser without providing a request for using it. For example, if there is a need for the user to buy something for the project first he has to raise a request for buying with detail and the vendor address. The cases where the fundraiser directly uses the fund without acknowledgment may lead to scams.

4.3 AUTHENTICATION MODULE

In this module, we are going to check whether the block should be valid or not. Here we have three criteria: first, it checks the block number, then it checks the previous hash value. Finally, it checks the Block's current hash which is matched with the SHA-256 hash for the particular block.

5. CONCLUSION AND FUTURE WORK

The possible application of Blockchain technology in different fields is still under study and this is an indication of the possibility of blockchain technology resolving most of the problems related to humans in terms of the trust. The call for investor protection and security in Campaign funding contracts could be answered by the introduction of blockchain technology which functions on a trust-free system where individuals have little to do to make it work. There are challenges with Campaign funding in relation to abuse, trust, and confidentiality and the adoption of blockchain technology in Campaign funding contracts could provide a much-needed solution. Blockchain technology provides a cheaper, easy, secure, and convenient means for the exchange of information and transfer of funds. The technology is programmable and can be extended to cater to any other requirement in the Campaign funding contract where necessary. In the future, the limitations of the previous idea with regard to the high power usage and computing resources by the distributed system by blockchain must be overcome. A cheaper alternative must be found to overcome these limitations.

6. REFERENCES

[1] Michael Siering, Jascha-Alexander Koch, Amit V. Deokar (2018) "Detecting Fraudulent Behavior On Crowdfunding Platforms: The Role Of Linguistic And Content-Based Cues In Static And Dynamic Contexts' - Journal of Management Information Systems.

[2] Benila S, V. Ajay, R. Karthick, K. Hrishikesh (2020) "Campaign Factory Using Blockchain" - Facial emotion recognition using deep learning: review and insights.- IEEE Trans. Syst.Man Cybern.Syst

[3] Hasnan Baber (2019) "Blockchain-based crowdfunding - A 'Pay-It-Forward' Model of Whirl" - International Journal of Recent Technology and Engineering

[4] Shivansh Pandey, Shivam Goel, Dhiraj Pandey, Subodh Bansal (2019) "Campaign Contract Using Blockchain" - Sixth International Conference on Computing For Sustainable Global Development

[5] MD Nazmus Saadat, Syed Abdul Halim, Husna Osman, Rasheed Mohammed Nassr, Megat F. Zuhairi (2019) "Blockchain-Based Crowdfunding Systems"

[6] G Rajasekaran, E Nirosha, V Sivaranjani (2020) 'Online Detection Based Crowdfunding Using Clustering and K-Nearest Neighbor Algorithm' -International Research Journal Of Engineering And Technology(Volume 7 Issue 2).

[7] Beatrice Perez, Sara R Machado, Jerone T A Andrews, Nicolas Kourtellis (2020) - I Call BS: 'Fraud Detection In Crowdfunding Campaigns'- http://www.researchgate.net/publications/342587156

[8] Siddhesh Jady, Swarup Chattopadhyay, Yash Khodankar, Dr. Nita Patil (2021) - 'Decentralized Crowdfunding Platform Using Ethereum Blockchain Technology' - International Research Journal Of Engineering And Technology (Volume 8 Issue 04)

[9] Vikas Hassija, Vinay Chamola, Sherali Zeadally (2021) - 'Bitfund: A Blockchain-Based Crowdfunding Platform For Future Smart And Connected Nation'- https://www.researchgate.net/publications/341450390

[10] Nik Azlina Nik Ahmad, Syed Abdul Halim, Syed Abdul Rahman (2021) - 'Applying Ethereum Smart Contracts To Blockchain-Based Crowdfunding System To Increase Trust And Information Symmetry' - ICCTA 2021: 2021 7th International Conference On Computer Technology Application.

[11] Shubhangi Priya, Garima Srivastava, Sachin Kumar(2021)- 'Blockchain Integrated Crowdfunding Platform For Enhanced Secure Transactions' -IEEE 4th International Conference On Recent Developments.

[12] E.M.S.W Balagolla, W.P.C Fernando, M.J.M.R.P Wijesekera, S Rathnayake (2021)- 'Credit Card Fraud Prevention Using Blockchain' - IEEE 2021 6th Internal Conference.

[13] Tianhao Chen (2022)- 'Blockchain And Accounting Fraud Prevention'- 7th International Conference on Social Science and Economic Development (2022) (ICSSED).