A Review on Decentralized, Secured and Reliable Charity System Using Blockchain

Veena Kavathekar[1], Shraddha Yadav[2], Pawan Kale[3], Nutan .V.Patil[4]
[1,2,3]*Bachelor of Technology Student, Nanasaheb Mahadik college of Engineering, Peth, India*
[4]*Assistant professor Computer Engineering, Nanasaheb Mahadik college of Engineering, Peth, India*

***Abstract*— Individuals are progressing at the expense of cataclysmically damaging society and making people more distant and standoffish in our quick-paced modern environment. Others have no idea how to make even a penny, while some people are becoming too competitive to make any money. However, there are also those who want to give back to society for selfless reasons. However, the current centralized systems and brokers for charity are so dishonest that individuals stop believing in these unreliable mechanisms, rendering the charities useless. What if we could improve the efficiency and reliability of the charitable system by combining current technology with the ravenous ideology of money-minded people. Taking a decentralized approach, cryptocurrencies and finance with the additional benefit of include even these people in a beneficial way, the system of charity can be much improved for donations. We suggest a method, supported by cryptocurrency transactions, to increase the transparency and reliability of the charitable giving system, wherein charitable giving (in the form of work) is first performed by individuals or organizations, and then that work can subsequently be sold as a stock (here we call it a certificate). This will function similarly to how the cryptocurrency exchange market operates. People can raise money through it exactly like stocks, but since the certificates can only be produced by those who engage in charitable activities, the money would ultimately benefit charities. By utilizing Blockchain technology, smart contracts, and cryptocurrency, the entire system will be decentralized. This system would enable everyone to independently contribute to society using his skills and time in addition to money, which would ultimately result in an increase of hands working toward the improvement of society.**

***Index Terms*— Blockchain, SHA256 , Secured, Decentralized System, Donation, Reliable Charity System.**

I. INTRODUCTION

People are now becoming voracious to contribute to the society. People want to donate generously for the causes they believe in but usually end up doing nothing due to no trust in the system around them. We have a lot of charitable organizations and NGOs who are in needs of funds every now and then, which are really working for the betterment of the society. There are a lot of online portals to donate to these charities which usually seems to be trustless. They face a lot of problems to convey their genuineness and hence don't get enough donations. Hence, in spite of all the transparency that the charitable organizations are trying to incorporate, there still exists the distrust about the way in which this money is being put to practice. Also, if an individual by himself wants to go out and do a noble deed, nobody would fund him as people would only trust recognized charitable organizations. What is needed is an arrangement where individuals or organizations do noble deeds first and then get patronage for its contribution by showing the p8roof of work over some third-party platform.

It can be achieved by creating a certificate in favor of the contribution he made which can be put forward to the decentralized platform to trade using blockchain system and cryptocurrency. This helps resolve the trust issues, as people already know what they are paying for, and the system involves a decentralized way to solve the problem. The payment can be recorded by transacting cryptocurrency, which is known to be a very secure mode of payment. Going further, these certificates can have an exchange value just like stocks and can also be sold further like any other financial instrument, thus, involving some volatility in monetary value of that certificate. Hence the charity doer can further repeat its noble deed to earn more value against its contribution to the society. Hence, in this way apart from NGOs and Organizations, individuals can also contribute their talent and time to contribute for the wellness of the society and hence can make the world better place to live.

II. PROPOSED WORK

A. Review Stage

We have suggested a decentralized system for using cryptocurrencies for charitable endeavors to increase transparency. Many people have become more altruistic as a result of urbanization's increased care for others. However, there are also some who wish to ultimately profit from the process. Both of these needs will be met by this method. Additionally, it will offer a trustworthy method and increase transparency throughout the entire process. This will assist in removing middlemen between donations and those who perform acts of charity.

Thus, the adoption of blockchain technology has evolved to address problems associated with cross-regional and cross-domain charitable donations. The blockchain technology can be used to safeguard data security, establish access controls, guarantee donation transparency, and track donor behavior. No individual will have the power to make erroneous modifications to the database thanks to the blockchain deployment mechanism, which eliminates a flaw in the previous system. As a result, the system is more dependable and secure.

We also place a strong emphasis on the ability to manage and handle materials comprehensively, and we set up a system for charitable donation services that consistently advances in terms of structure, technology, and functionality. In the charity giving system, where data is shared, information is managed between contributors and recipients, contracts are managed between charitable organizations, and attention to blockchain technology is increasing daily.

III. SCHEMATIC DIAGRAM

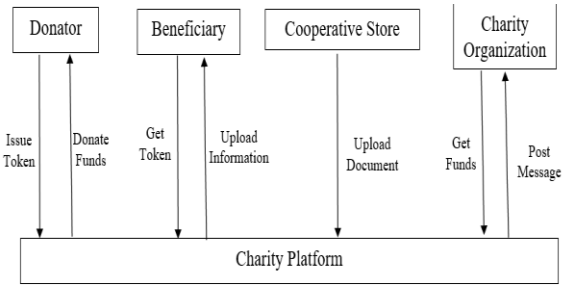

Fig. 1. Block Diagram of charity system

On charity platform there are three interfaces such as Donor interface where donor can donate funds, needy interface where needy can get the funds after enrolling, and admin interface where are transactions are validated.

I. CONCEPTUAL DESIGN

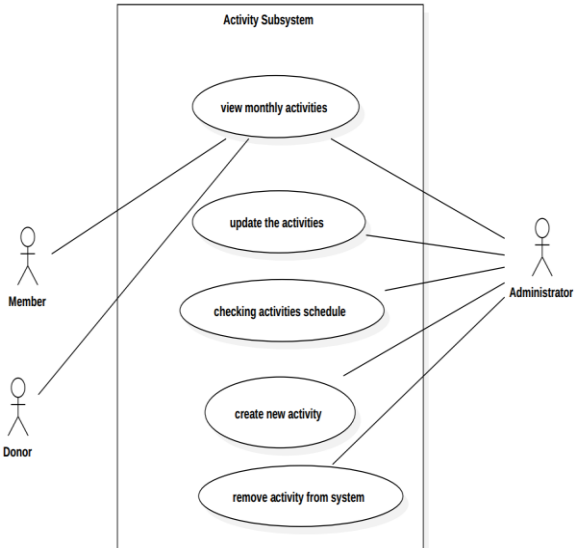

Fig. 2. Conceptual design of features

It emphasizes the comprehensive management and handling capability of material supply, and establish a charity donation service system with sustained innovation in framework, technology, and operation

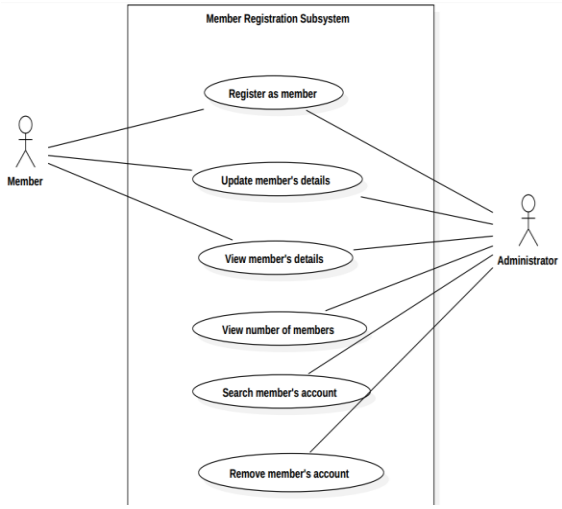

Fig 2.Block diagram of member interface

Multiple sections such as posts of the needy, charity lists are available which enhances convenience for the contributors to come across the challenges to decide and donate.

In this we introduce a platform to generate the charities systems. We present how the products are generated by the system. Here both Contributor as well as

needy(Charity) has to register first by undergoing the document verification in the sake of proof.

II.Experimental Work

Using HTML, CSS AND JavaScript user interface is developed. There are multiple pages such Needy Signup/Login, Needy Document verification, Needy Post, Donor Login/Signup, Donor Document verification, Admin Interface, Contact Us Page.

Backend which holds all the data of donor, needy insights, transaction history. This is implemented using Python and Mango DB. The Decentralized Deployment which is the major reason of the system is implemented using the Blockchain technology. Blockchain overview. Blockchain defined: Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding).

The goal of blockchain is to allow digital information to be recorded and distributed, but not edited. In this way, a blockchain is the foundation for immutable ledgers, or records of transactions that cannot be altered, deleted, or destroyed. As each transaction occurs, it is recorded as a "block" of data

Those transactions show the movement of an asset that can be tangible (a product) or intangible (intellectual). The data block can record the information of your choice: who, what, when, where, how much and even the condition — such as the temperature of a food shipment.

Each block is connected to the ones before and after it These blocks form a chain of data as an asset moves from place to place or ownership changes hands. The blocks confirm the exact time and sequence of transactions, and the blocks link securely together to prevent any block from being altered or a block being inserted between two existing blocks.

Transactions are blocked together in an irreversible chain

Each additional block strengthens the verification of the previous block and hence the entire blockchain. This renders the blockchain tamper-evident, delivering the key strength of immutability. This removes the possibility of tampering by a malicious actor — and builds a ledger of transactions you and other network members can trust.

For this purpose, the hashing is done. For the generation of Hashing the algorithm SHA-256 is used. The SHA-256 algorithm is one flavour of SHA-2 (Secure Hash Algorithm 2), which was created by the National Security Agency in 2001 as a successor to SHA-1. SHA-256 is a patented cryptographic hash function that outputs a value that is 256 bits long.

What is hashing? In encryption, data is transformed into a secure format that is unreadable unless the recipient has a key. In its encrypted form, the data may be of unlimited size, often just as long as when unencrypted. In hashing, by contrast, data of arbitrary size is mapped to data of fixed size. For example, a 512-bit string of data would be transformed into a 256-bit string through SHA-256 hashing.

In cryptographic hashing, the hashed data is modified in a way that makes it completely unreadable. It would be virtually impossible to convert the 256-bit hash mentioned above back to its original 512-bit form. So why would you want to create a scrambled message that can't be recovered? The most common reason is to verify the content of data that must be kept sec ret. For example, hashing is used to verify the integrity of secure messages and files. The hash code of a secure file can be posted publicly so users who download the file can confirm they have an authentic version without the contents of the file being revealed. Hashes are similarly used to verify digital signatures. Password verification is a particularly important application for cryptographic hashing. Storing users' passwords in a plain-text document is a recipe for disaster; any hacker that manages to access the document would discover a treasure trove of unprotected passwords. That's why it's more secure to store the hash values of passwords instead. When a user enters a password, the hash value is calculated and then compared with the table. If it matches one of the saved hashes, it's a valid password and the user can be permitted access.

III.CONCLUSION

To increase transparency through a decentralized system, we have suggested a way for employing cryptocurrencies for charitable endeavors. Many people's compassions for others have increased as a result of urbanization, which has also made many people more charitable. People who wish to ultimately profit from the process are present, but they are also

present. Both of these needs will be satisfied by this system. Additionally, it will offer a system that cannot be trusted, and the entire process will become more apparent. Getting rid of middlemen between donors and those who do acts of charity will help.

We have summarized all sections of the system. A full-fledged decentralized and secured charity system. Multiple interfaces such as Needy, Contributor and Admin are created and managed securely. Each action is validated which makes overall system more secure

REFERENCES

[1] H. Wu and X. Zhu, "Developing a Reliable Service System of Charity Donation during the Covid-19 Outbreak," IEEE Access, vol. 8, pp. 154848–154860, 2020, doi: 10.1109/ACCESS. 2020.3017654.

[2] H. Saleh, S. Avdoshin, and A. Dzhonov, "Platform for tracking donations of charitable foundations based on blockchain technology," in Proceedings - 2019 Actual Problems of Systems and Software Engineering, APSSE 2019, Nov. 2019, pp. 182–187. doi:10.1109/APSSE 47353. 2019.00031.

[3] R. Mauliadi, M. R. A. Setyautami, I. Afriyanti, and A. Azurat, "A Platform for Charities System Generation with SPL Approach." [Online]. Available: http://mesjidui.ui.ac.id

[4] Kyŏngbuk Taehakkyo. et al., Proceedings of the IEEE International Conference on Soft-Computing and Network Security: in association with "Kyungpook National University", South Korea: February 14th, 15th, 16th, 2018.

[5] Agnel Charities', Rodrigues Institute of Technology, and Institute of Electrical and Electronics Engineers. Bombay Section, 2019 International Conference on Nascent Technologies in Engineering (ICNTE-2019): proceedings: January 4-5, 2019, Fr. C. Rodrigues Institute of Technology, Agnel Technical Education Complex, Sector 9-A, Vashi, Navi Mumbai - 400703 India.

[6] Kyŏngbuk Taehakkyo. et al., Proceedings of the IEEE International Conference on Soft-Computing and Network Security: in association with "Kyungpook National University", South Korea: February 14th, 15th, 16th, 2018.

[7] Hongke Zhao, Voice of Charity: Prospecting the donations recurrence and donor retention in crowdfunding", International Conference on Nascent Technologies in Engineering 2019

[8] Wooyoung Lee, "A study on blockchain application in donation platform", 2021

[9] Li Xi, "Secure anonymous Donation Protocol", the IEEE International Conference on Soft-Computing 2009