

Secure and Genuine Charity Application for Orphanages and Old Age Homes

Prof. P. R. Kene^{#1}, Jabin Patel^{*2}, Sneha Khandale^{*3}, Vishal Sangale^{*4}, Vaishnav Raut^{*5}
^{2,3,4,5}Students & ¹Assit. Prof. of Department of Computer Engineering,
JSPM's Jayawantrao Sawant College of Engineering
Hadapsar, Pune-28
Savitribai Phule Pune University, Pune

Abstract— The cause association worldwide need straight forwardness and the management to them is hard to accomplish, which adversely affects the ability of the individuals to give. Orphans are increasing in large scale day by day. There are 163 million orphans worldwide. Additionally, the number of old age homes is in same race. Therefore, whoever is willing to do charity they can make use of this application. Blockchain as a fundamental innovation of Bitcoin framework gives a new answer for the cause framework as far as innovation. This paper proposed a good cause framework dependent on blockchain innovation and elucidates the plan design, design and functional course of the stage. We trust to expand the straight forwardness of this noble cause to improve the society's confidence in foundations and advance the improvement of generosity by blockchain based foundation framework.

Keywords— Data Security, Smart Contract, Charity Application, Algorithm AES, Blockchain technology.

I. INTRODUCTION

Blockchain technology which is derived from Bitcoin is considered a subversive innovation of the computing model after mainframes, the Internet, and personal computers. A blockchain is defined as a counterfeit-proof, irrevocable, non-centralized cryptographic common ledger that chronologically combines data blocks into certain data structures. Therefore, pervasive blockchain technology is a new decentralized infrastructure and a distributed computing paradigm that uses encrypted chain block structures to review and store data and uses smart contracts to manipulate data on the blockchain. Blockchain technology's broad application perspectives have many areas of transparency, openness, traceability, and irrevocability, as well as the areas of the Similar good and logistics traceability.

II. LITERATURE SURVEY

Charity Donation System Based on Blockchain Technology

In this paper ^[1], the authors look at the requirements of blockchain-based charity networks around the world. They show how distributed registry systems can be utilized to build a forum for charitable donation making and tracking. This article is to illustrate how a blockchain-based framework for tracking donations can be implemented ^[1].

Transparent charity application using blockchain

In this paper ^[2], authors using blockchain for a charity donation to make it more transparent. This Application provides trust between the users and donors. This helps resolve the trust issues, as people already know what they are paying for and the system will help to solve the problem ^[2].

Blockchain based Transparent and Genuine Charity Application

In this paper ^[3], author discusses a blockchain-based charity foundation platform that the trustful network's formation and is accountable for collecting donation funds. All organizations' operations within the platform will become fully transparent facilitates and visual, leveraging properties of immutability, provenance, and nonrepudiation ^[3].

Feasibility Analysis of Blockchain for Donation-based Crowdfunding of Ethical Projects

This paper ^[4] is highlighted on A novel model in the form of a decentralized app was designed in the Ethereum blockchain to solve the challenges present and optimize the process of Zakah donation. Load and stress tests on the prototype of the smart contract in the public test-net of Ethereum were analysed to gauge the feasibility of mass usage. Similar tests were done in Hyperledger to conclude on the optimum blockchain platform for Zakah ^[4].

III. METHODOLOGY

▪ AES Algorithm: -

AES is an iterative cipher not a Feistel cipher. It is based on substitution permutation network. It's made of a series of linked operations, some of which are replacing inputs by specific outputs (substitutions) and shuffling bits around (permutations). Interestingly performs all its computations on bytes rather than bits. All these 16 bytes are arranged in four rows and four columns to process as a matrix. The number of rounds in AES is variable and depends on the length of the key which is different than the DES. All individual rounds use a different 128-bit round key, which is calculated from the original AES key. In modern day cryptography, AES is widely supported and adopted in both hardware and software. Till now, no practical crypto-analytic attacks against AES have been seen. AES also has built-in flexibility of key length, which gives a degree of future proofing against progress in the ability to perform exhaustive key finding. However, the AES security is assured only if it is correctly implemented, and good key management is employed, just like the DES. The encryption process uses round keys, a set of specially derived keys. Which are applied, along with other operations, on an array of data that holds exactly one block of data i.e., the data to be encrypted. This array is called the state array. Every round of the encryption process needs a series of steps to alter the state array. These steps involve Three types of operations called:

1. Sub-Bytes
2. Shift-Rows
3. Mix-Columns

IV. PROPOSE SYSTEM

We will develop a system for Orphanages and Old Age Homes using smart contracts. Users as well as Orphanages and Old Age Homes can register with our system. Orphanages and Old Age Homes can post donation requests on the system. Users will check the donation and process for the money transaction. We will encrypt all the data of transactions to provide high security from hackers. Each time the System will check all blocks for security during all the transaction.

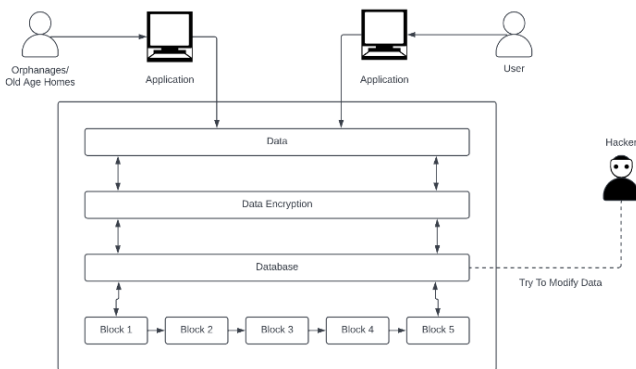
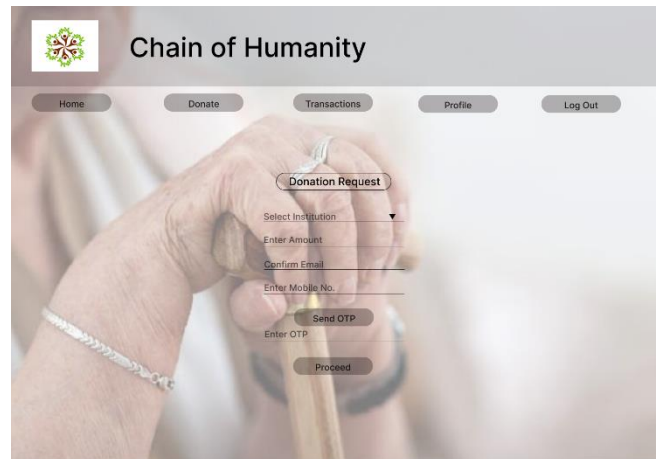
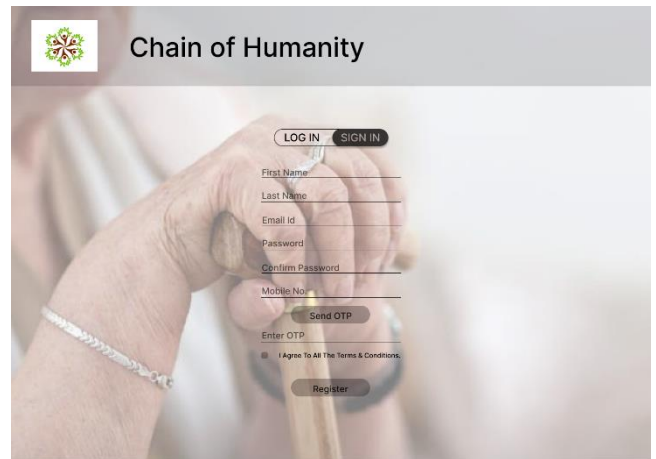
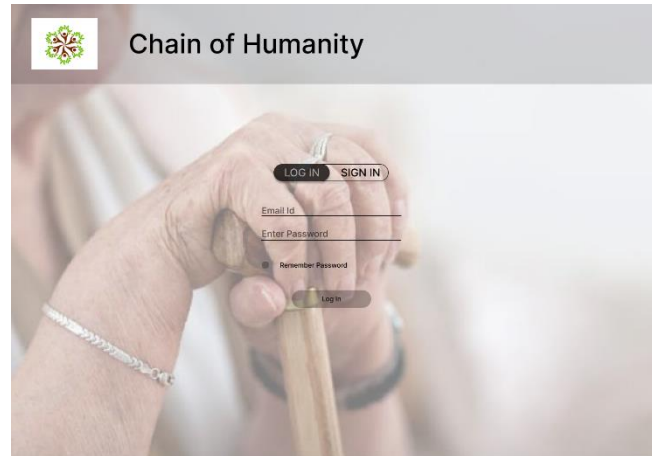


Fig.1: System Architecture

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are satisfied. They are generally used to automate the execution of an agreement so that all participants can be immediately certain of the output, without any middle authority's involvement or time loss. They can also automate a workflow, triggering the next process when conditions are satisfied. Smart contracts work by following simple “if/when. . . then. . .” statements that are written into a code on a particular blockchain. A network of computers executes the process when predetermined conditions have been satisfied and verified. These actions could include releasing funds to the proper parties, registering a vehicle, sending notifications, or issuing a ticket. The blockchain is then updated when the whole transaction is completed. That means the transaction cannot be altered, and only parties who have been granted access can see the results.

V. EXPECTED OUTPUT

This are some screenshots of our expected output of our project.





VI. CONCLUSIONS

We have put forth a framework utilizing Blockchain alongside digital currency for a noble cause to make it more straightforward through a non-centralised framework. Urbanization has made many individuals more worried about others and this has also made many individuals charitable. And yet there are many peoples who need to at last bring in unlawful cash all the time. This framework will provide both the necessities which are better credibility and security. Likewise, it will furnish with a believed framework and will make the whole process more straightforward. This will help dispose of centre men between contributors and noble cause practitioners.

ACKNOWLEDGMENT

We would like to give thanks to the researchers likewise publishers for creating their resources available for use. We are conjointly grateful to our guide, reviewer for their valuable suggestions and thank the college authorities for providing the required infrastructure and support.

REFERENCES

- [1] Prof. Dhanashri Patil, Abhishek Kadam, Gargi Shetye, Tanmay Budage, Ashutosh Sonar, "Charity Donation System Based on Blockchain Technology", Computer Engineering, PCET's Nutan Maharashtra Institute of Engineering and Technology, May 2022.
- [2] Prof. Sunil Sonawane Sir, Miss. Amisha Bharat Borana, Miss. Riya Chandrakant Chawate, Mr. Mandar Pravin Patil, Mr. Omkar Sunil Naiknavare, "Blockchain based Transparent and Genuine Charity Application", Department of Information Technology, AISSMS's Polytechnic, May 2022.
- [3] Prof. H.B. Sale, Pooja Molavade, Apeksha Sable, Shweta Sanas, "Transparent Charity Application Using Blockchain", Information Technology Engineering, Bharati Vidyapeeth College of Engineering, April 2021.
- [4] Nida Khan, Rachid Ouach, "Feasibility Analysis of Blockchain for Donation-based Crowdfunding of Ethical Projects", University of Luxembary 2019.
- [5] Iqra Khalil, Omer Aziz, Numan Asif, "Blockchain and Its Implementation for Charitable Organizations" Department of Computer Science, School of Systems & Technology, University of Management & Technology, Lahore, Pakistan, November 2021.