PROJECT ID:

SYNOPSIS

On

Stiften Donation App

Submitted In Partial Fulfillment of the Requirements for the Degree of

Bachelor of Technology

In

Computer Engineering

By-
Aman Sharma

Roll No.-
1803211007

Under the Supervision of
Mr. Ashwin Pirti
Under the Co-supervision of
Mr. Rahul Sharma

ABES ENGINEERING COLLEGE
GHAZIABAD, UTTAR PRADESH
**AFFILIATED TO DR. A.P.J. ABDUL KALAM TECHNICAL UNIVERSITY **
LUCKNOW, UTTAR PRADESH

(SESSION: 2020-2021

Stiften Donation Dapp

Aman Sharma & Aanchal Giri

[#]*Department of Computer Science & Information Technology*
ABES Engineering College, NH-24 highway, Ghaziabad, U.P., India
aman.18bci1024@abes.ac.in
aanchal.18bci1007@abes.ac.in

***Abstract*— This paper discusses the project implementation of a donation dapp (decentralised) that can accept payment done through both medium that is crypto currency and normal indian currency. It is made to be ease the work for the good donors, they won't be needed to find the organisation from different corners of the world. Instead they will have the list of organisation from all the places. It will help in gaining trust of customers (donors). It will be supporting donations in both Indian currency via Razorpay payment gateway and in crypto currency both.**

***Keywords*— donations, donor's trust, block chain, organisations, rating system for organisations**

I. INTRODUCTION

A blockchain is a public ledger of information collected through a network that sits on top of the internet. It is how this information is recorded that gives blockchain its ground-breaking potential.

Blockchain [1], as its name suggests, consists of multiple blocks strung together. The words "block" (digital pieces of information) and "chain" (stored in a public database). Each block in the network containing the data is secured and connected to each other with the help of cryptography principles Data cannot be changed or altered once recorded in a block, making it impossible to do so without it being seen by the other participants on the network

Moreover, blockchain should be considered as an overarching idea that includes various technologies and applications. The concept of blockchain can be compared to the Internet, which has many technologies and applications. It is argued that blockchain is likely to transform business in as great a manner as the Internet. Blockchain can disrupt in a positive manner central banking platforms and many business models and use cases, including trades, financial services, supply chains, business process improvement, health information sharing, and logistics management (Woodside et al., 2017).

A node can be any electronic device, including a computer, phone, a printer or even a fridge, as long as it is connected to the internet. All nodes are equal in importance on a blockchain, but a node can have different roles in making a blockchain work. In comparison to the normal network, the blockchain network is completely different having no central point that stores and controls information. Instead, the responsibility to look after the network and store information is shared by different devices, known as peers, on that network. This is why a blockchain network is known as a peer-to-peer network. Instead, information is being constantly recorded and interchanged between all of the participants on the network.

With the development of Internet technology, there are more and more information access channels for people, philanthropy has become more open and transparent. Many problems in the process of philanthropy has been exposed."Guo Meimei Incident" and "Hu Manli Incident" were spread widely on the Internet. According to media reports, some people sold relief supplies and tents for money in the " 5.12 Wenchuan Earthquake", which showed the confusing daily management of charitable funds and materials. These caused a decline in willingness to donate and a reduction in donations between 2009 and 2012 [2]. At the same time, online crowdfunding has become a new way for the public to participate in public welfare undertakings. The crowdfunding platform has established a database for the project, a proper monitoring of the project is also an important part of the risk automatic control mechanism of the public welfare crowdfunding platform [3]. Improving the transparency of philanthropic information is an important way to improve credibility for traditional donation and internet crowdfunding. Using Internet technology, a traceability system can be established to increase the transparency of charities technically [4]. For this purpose, this paper proposed a new model of charity system based on blockchain technology

So we are making a donation Dapp based on react and solidity. It will help in gaining trust of customers (donors). It will be supporting donations in both Indian currency via Razorpay payment gateway and in crypto currency both.

In today's world nothing can be trusted blindly and the good donors don't have enough time to do the background check for all the organisations so what we do all the work for them already. We will have a personal curated list for those good donors so that they don't have to waste their time checking the background for the organisation that wether it is fake or real. In any case they know how is the organisation, they can rate and comment about that organisation. The list will be shown to him according to their location.

The organisations details will be provided along with list. The details will have the organisation name, address and the nearest site where they provide the services so that if you want then you can go there and watch things for yourself. It will also be containing a slideshow of the images.

Once a customer get him verified on the app. He will be allowed to become the active volunteer for the organisation. He will be provided with the contact within the app so that he can talk to them and ask them where the nearest site for him to help is.

If there is no site near to his place or not in his city, and there is a place where help is needed he can apply for the new site for that city and he will be needed to wait to get verified. Verification will be done on the basis of number the applications for that particular site.

II. LITERATURE REVIEW

In the white paper Bitcoin: [5] introduced two technological and innovative ideas. The first idea was that bitcoin, a digital currency that can be traded without a central financial authority. The second idea was the concept of blockchain. As its name explains, blockchain is a chain of blocks interconnected with complex computational crypto algorithms. The underlying notion of this technology is storing digital assets of any kind in blocks; blocks are linked by a

digital fingerprint called hash and stored in limitless places on a distributed database [6]. Blockchain is a "distributed ledger technology for a new generation of transactional applications that establishes transparency and trust" [7] emphasized that blockchain is both a peer-to-peer network and a public database, operating without a central server.

The essential concept of blockchain is little more than the idea of a secured register or list for data records and storage of past transactions, which are validated and confirmed by blockchain parties. The core value of blockchain is the true representation of reality at any given time, thus creating trust in businesses between participants. Blockchain can be thought of as a state machine; it stores the status of things that have happened, then updates that status while a permanent record of past states remains. These past states are almost impossible to be changed [8]. One of the key strengths of blockchain is "hashing." Each block has information to be stored, and every new block added in the chain is encoded with a "hash," a code arithmetically produced and generated from the block's date. "Hashing" is not a new method; it is often used to secure passwords. Moreover, each newly added block includes the hash of the preceding block in the same block hash. In this way, falsifying new or old blocks becomes very difficult. Hashes of previous blocks determine the hashes of subsequent blocks; therefore, altering a single block would require rewriting the entire blockchain. This mechanism of linking the blocks into a chain makes tampering extremely difficult [9].

It will have two sides

A. Customers side
B. Admin side
C. Organisation Side

Dapp will be created on the express.js and next.js on the top of solidity. Frontend will be done on the flat Next.js framework and backend will be done on the Solidity and Express.js framework. For this app to be connected to the database we will use MongoDB and solidity. MongoDB will be used for the authentication purposes mostly on the other side solidity will be used to do all the transactions of crypto currency and list of organisations will be saved in block chain server. At the end this application will be converted into PWA from js html and css for the use in mobile phones

III. SYSTEM DESIGN

The core features of a blockchain-based design are critical to the superiority and uniqueness of this technology. [10] emphasized that these design features are highly appreciated, especially in environments where transaction verification, reconciliation and settlement, and dispute resolution take up an unreasonable amount of energy and resources

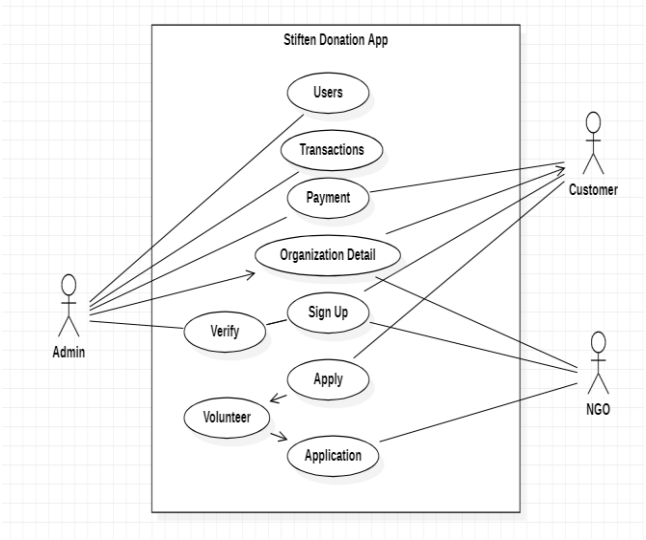

Figure 1: Use Case Diagram

A. *METHODOLOGY*

Every time a new user starts with our application, he/she has to register in the application with the account details. Then he/she has to verify his account by the clicking on the link that has been sent to his email id. Once he verifies his account he will be given the post of subscriber in the database. User's access will be restricted for the organisation and admin rights. His rights can only be changed by the admin.

After successful registration, the user can login into the application using the username and password, where each user is uniquely identified by his/her username. Post successful login the user can initiate the transaction, where he/she can donate the money to the organisations within the application. Once user initiates the transaction, it is been shared with all the miners. User will have two options while making the transaction he can donate the money anonymously and initially, a hash value is generated for the transaction using the sender's username, receiver's username, the amount and timestamp. Timestamp parameter makes sure that each block is unique which in turn generates a unique hash value.

Now in the MongoDB we have 4 collections. One is the user collection having all the user account details. Then we have transaction collection which contains the validated transactions. Here, the UserID is considered as the key, and the value is transaction ID and its relevant details. And the third table is the validation table, where after a transaction is initiated it is been added to the table. UserID again remains key and value for this key is again the transaction ID and the hash value generated after transaction initialization. Fourth we have the collection of all the orrganisation that have been approved and updated by the administrator.

In admin side there will be access to change the ownership of users and to add and give access to organisations. Admins main focus will be on the transactions and the customer (donors) satisfaction.

In client side there will be organization page where customer can choose which organization to pay and there will be page to see the details of that organization that where are recent transaction were

made by that organization. There will be payment page where there will be two options given to customer that which type of payment customer wants in crypto or in Indian currency then it will be forwarded to payment gateway.

Organisations only access will be the access to update their information. Their main areas of information are divided in two areas mainly. Firstly, updating the information about them that is their details and secondly, the information about their camp sites.

Going deeper, proof of work is a requirement to define an expensive computer calculation, also called mining, that needs to be performed in order to create a new group of trustless transactions (the so-called block) on a distributed ledger called blockchain. Mining serves as two purposes:

1. To verify the legitimacy of a transaction, or avoiding the so-called double-spending;
2. To create new digital currencies by rewarding miners for performing the previous task. So in our application the difficulty level is set to 4.

So the hash value must have four zeros in the start and then the algorithm tries to find the nonce value. For example if this is our hash is 4dd3426129639082239efd583b5273b1bd75e8d78ff2e8d then the miner tries to find the nonce value where after appending random value if the resultant hash has four zeros in the start then that value is considered as the nonce value. Once nonce value is determined, the value is shared between the miners. We again have a database, where for each transaction we have the miner and their nonce value. If the maximum number of miners have the same nonce value then the transaction is validated or it is rejected. The difficulty level is set to 4 precisely because if it is kept more than 4, the time consumption would be more and if set less than 4 probability of finding the nonce value becomes easy.

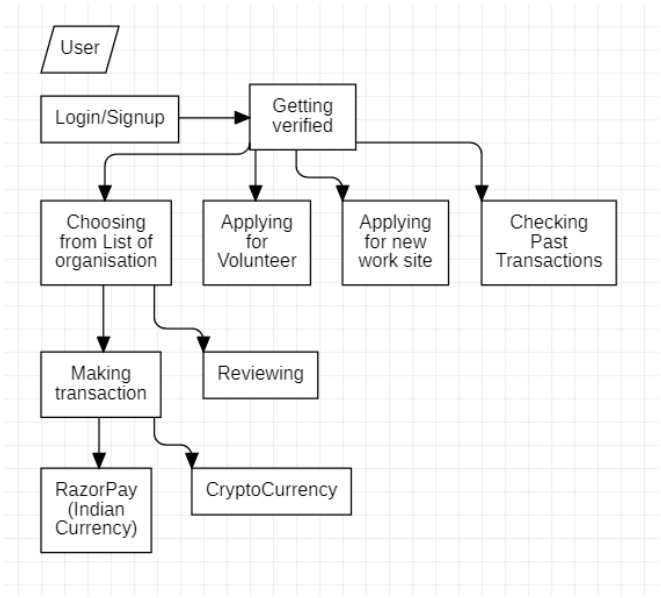

Figure 2: Flow Diagram for the Client Side of Application

IV. CONCLUSION

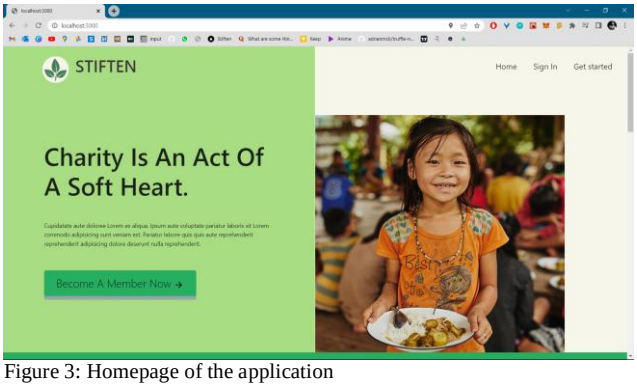

Figure 3: Homepage of the application

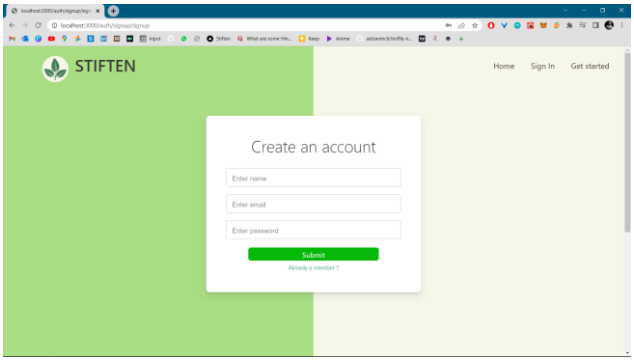

Figure 4: SignUp page of the application

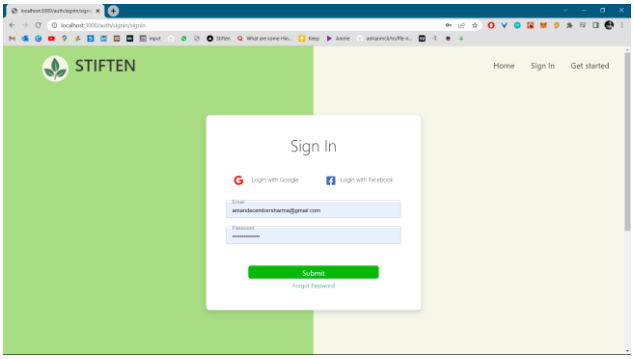

Figure 5: SignIn page of the application

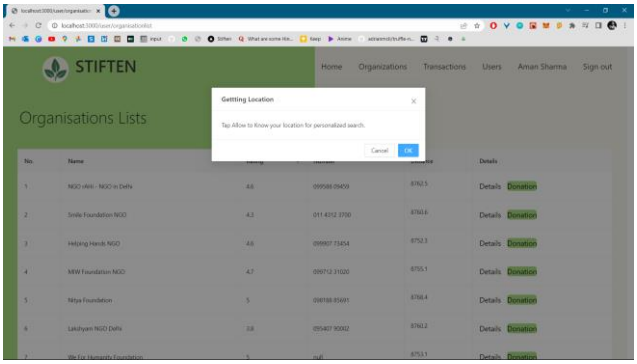

Figure 6: Organisation List page, where it needs access for location.

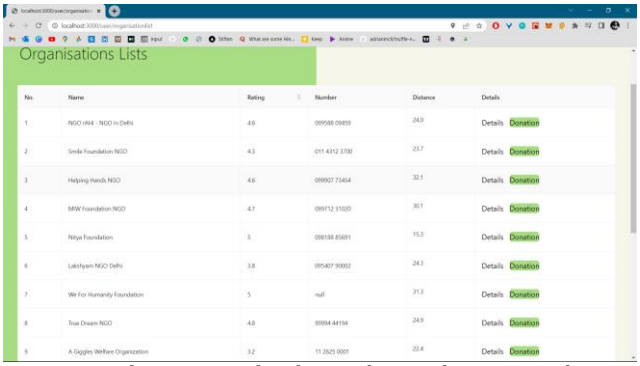

Figure 7: Total organisation list that can be sorted, it contains the rating that has been given to the organisation by the google, distance from your location

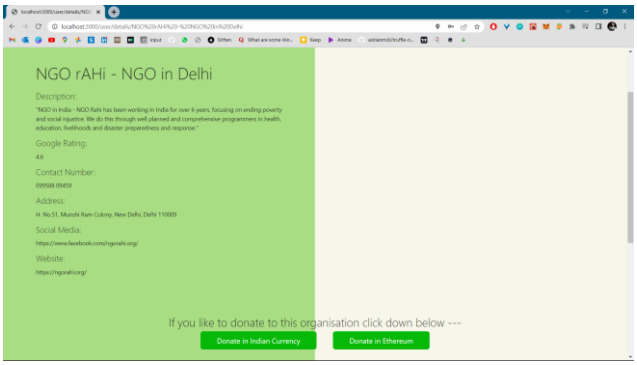

Figure 8: This page contains the details of the organisation, and it gives two options of payment.

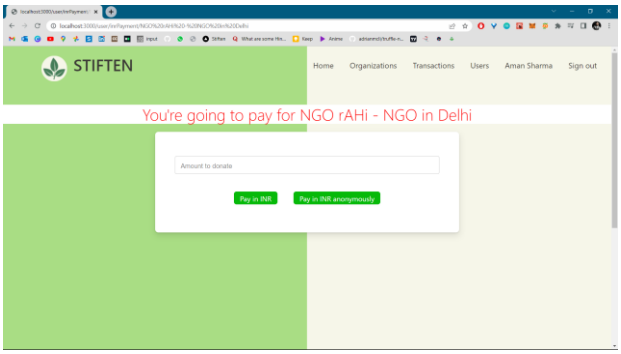

Figure 9: Here it asks for how much donation is needed in Indian rupees

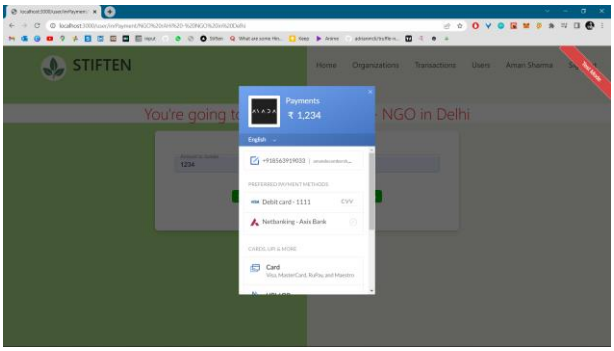

Figure 10: It is the razorpay gateway.

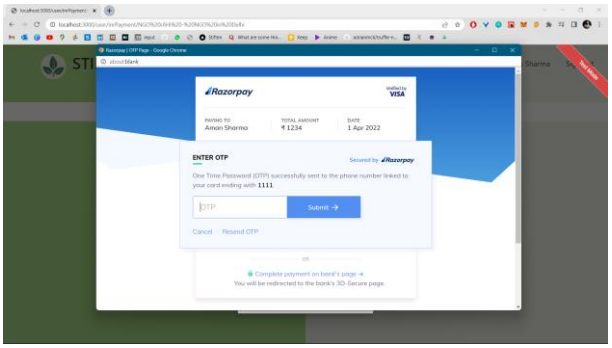

Figure 11: Transaction needs otp to be completed

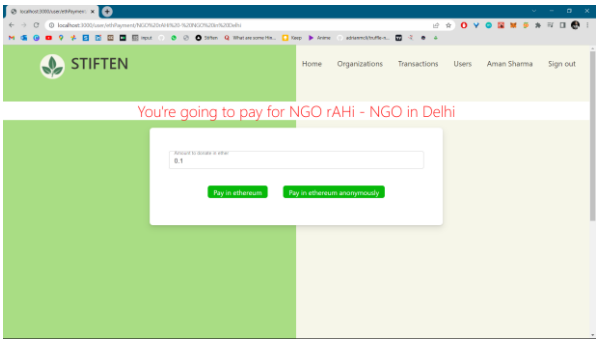

Figure 12: Here it asks for how much donation is needed in Ethereum.

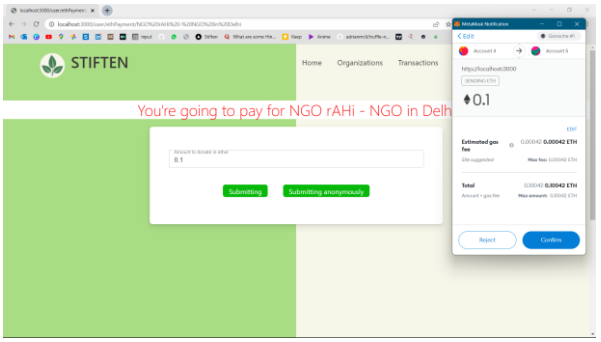

Figure 13: It is the metamask gateway for the transaction in terms of cryptocurrency.

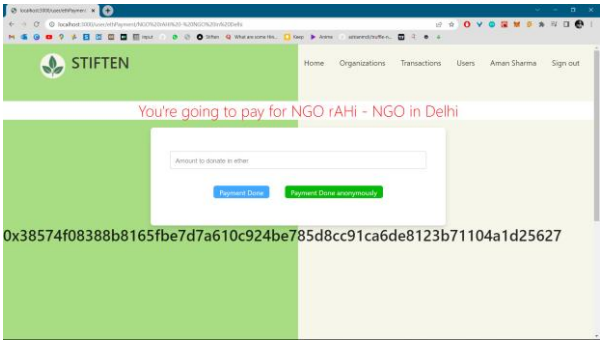

Figure 14: When the transaction is completed successfully transaction hash is shared which can be checked anytime.

V. REFERENCES

[1]. What is Blockchain Technology? A Step-by-Step Guide For Beginners. Available Online: https://blockgeeks.com/guides/ is-blockchaintechnology/

[2]. Sun Xiaoshu, A Brief Analysis of 2012 China Charity Donation Data, China Development Brief, 2013(4).

[3]. Ke Xiang, Analysis on the Operation of Internet Public Welfare Crowdfunding Platform and Its Risk Control Mechanism, Hainan Finance, 2016(11)64-68+83.

[4]. Zhang Peng, Li Ping, Zhao Wenbo, Resolving the Dilemma of Charity and Credibility: The Theory and Evidence of the Application of Traceability System Principles, Social Sciences Research, 2016(03)40-46.

[5]. A Peer-to-Peer Electronic Cash System, Nakamoto (2008)

[6]. Cirstea et al., 2018; Woodside et al., 2017

[7]. (Linn & Koo, n.d., p. 2). Koshechkin et al. (2018)

[8]. Adams et al., 2017

[9]. Hughes & Morrow, 2019; White, 2017

[10]. Perkinson and Miller (2016)