Ramakrishna Mission Crowdfunding System using Blockchain

Securing donation records

.

Table of Contents

[Executive Summary 2](#_Toc534293452)

[1.1 Background 2](#_Toc534293453)

[1.2 What is blockchain? 2](#_Toc534293454)

[1.3 Blockchain solution for Ramakrishna Mission(RKM) crowdfunding: 3](#_Toc534293455)

[1.4 Advantages: 4](#_Toc534293456)

[1.5 Application Architecture: 4](#_Toc534293457)

[Server Details:- 6](#_Toc534293458)

[2.1 Server Details 6](#_Toc534293459)

[2.2 Application snapshots 6](#_Toc534293460)

[Hardware Requirements 9](#_Toc534293461)

[Conclusion 10](#_Toc534293462)

# Executive Summary

## Background

West Bengal Electronics Industry Development Corporation Limited (WEBEL) created an absolutely transparent, traceable, impermeable and full proof solution based on crowdfunding, meant to facilitate donation of funds for socially relevant projects pertaining to a highly revered social welfare organization. The system uses an Ethereum blockchain framework wherein after any user makes a successful payment it triggers a transaction to be fired from the client account to the donor’s account in the Ethereum node. Thereafter the transaction is mined, and a new block is added to the existing blockchain. Consequently, an amount of token is transferred on the blockchain platform which is equal to the donation made. This record is thereafter immutably stored on the blockchain system.

Ramakrishna Mission (RKM)) crowdfunding as a means of financing projects is inspired from the models of microfinance and crowdsourcing, and has been facilitated considerably off late by the influx of the Internet. One of the factors that largely differentiates crowdfunding from other modes of financing is the geographically distributed and largely unorganized source of funds. Given, the unique nature of sourcing funds, crowdfunding as a business has its own unique set of challenges and critical success factors. One of the factors that is known to determine the volume of crowdfunding in any country is the control of corruption. Automation, conventionally has been regarded as a means of reducing corruption, albeit with its own set of inadequacies. One of these adequacies is the centralized nature of data storage. In a conventional database with a client server architecture, an authority gives permission to a client post the authentication of their identity, to modify the data stored on the central server. This way if the security of the authorization is compromised then the data becomes vulnerable to unauthorized modifications.

In the context of a crowdfunding system this poses the risk in traceability of funds and the data related to crowdfunding transactions. Given the fact that the volume of transactions is directly impacted by the confidence of donors in the utilization of funds, the vulnerability of a conventional system makes it insufficient to trigger the success of a crowdfunding system.

The need for a robust system that is full proof and resistant to attacks and modifications by unauthorized entities, triggered the need for a blockchain based crowdfunding solution. In this pursuit we created a blockchain based crowdfunding solution for a social welfare organization which was implemented in September’ 2018 and has been successful at achieving the intended state of track and trace of transactions.

## What is blockchain?

Blockchain is a digital, decentralized (distributed) ledger (database) that keeps a record of all transactions that take place across a peer-to-peer network. It is an interlinked and continuously expanding list of records stored securely across a number of interconnected systems. This makes blockchain technology resilient since the network has no single point of vulnerability. Additionally, each ‘block’ is uniquely connected to the previous blocks via a digital signature which means that making a change to a record without disturbing the previous records in the chain is not possible, thus rendering the information tamper-proof. The key innovation in blockchain technology is that it allows its participant to transfer assets using internet protocol and without any centralized third party (intermediary).

A node is simply a computer server that is connected to a network. When a node connects to a network for the first time, it downloads the copy of the ledger.

Node 1

Node 2

Node 6

Node 4

Node 5

Node 3

Ledger is basically a chain of blocks where each block points to it previous block with a hash pointer, thus blockchain. Each block contains valid transaction data.

A blockchain network can either be public or private based on who is authorized to participate. The essential difference between a public and private blockchain is that one operates in a decentralized open environment where there are no restrictions on the number of people joining the network, while the other operates within the confines defined by a controlling entity. A simple analogy is the difference between the Internet and the intranet. While the inherent technology for networked computers remains the same, there is a big difference between the dynamics and utility associated with a closed network (such as a home network) and an open network (such as the Internet).

In reality, this difference plays out based on how ‘nodes’ are incentivized to remain active within a network. The key idea here is that in a public blockchain, the consensus mechanism is based around rewarding each individual participant to remain active within the network. In a private blockchain, the need for creating this incentive does not exist.

The democratized nature of a true transparent public ledger might not be of utility to an organization or an enterprise network as the parties are known, and a level of understanding exists about which members can participate in the network and on what type of transactions. The general consensus is that while public blockchain work well for certain applications such as cryptocurrency-based transactions (bitcoin), the larger application of blockchain technology as an enterprise solution would only be possible with the increased regulatory control associated with a private blockchain ecosystem.

## 1.3 Blockchain solution for Ramakrishna Mission (RKM) Crowd funding:

Ramakrishna Mission (RKM) Donation Management is an Ethereum based crowdfunding platform designed to enable immutability and transparency.

Donor Registration: Donors making donation for the first time will have to first register themselves on the website. Registration on the said website is very simple process where user will have to give their email ID and select a password for authentication. Once registration form is submitted, a public key is generated on the Ethereum node which is basically a pseudonym of user. A confirmation mail will be sent to the user provided email

Ramakrishna Mission(RKM)Portal

Ramakrishna Mission(RKM) Blockchain

Potential Donor

Enters Detail

Is this person already registered?

You are already registered

Gives the unique address

You are now registered

Making Donation: To make donation, donor will have to login using the registered user name. Once donor has logged into the system, there is a link “Donate” which will navigate the donor the donation page. After providing the donation detail such as amount, donor address etc. user can finally make payment using Net Banking/Debit Card/Credit Card. After successful completion of payment, a transaction is fired from Ramakrishna Mission(RKM) account to donor account in Ethereum node. This transaction is mined and a new block is added to the existing Blockchain. The amount of token transferred on Blockchain platform is equal to the INR which was donated. An SMS and email is also sent to user after successful payment.

Ramakrishna Mission(RKM) Portal

Ramakrishna Mission(RKM) Blockchain Node

Here are my details

Donor Donates ‘X’

Transaction from Admin account to Donor Account

Credit the account of the donor with token

Confirmation

Confirmation

*Donation Flow Diagram*

In case a donation was made by the donor will be shown

If donor wants to donate

Give Amount

Viewing Donation Record: User can see the details of all the donations which he/she has made previously. User can also download a donation certificate for Exemption of Income tax under section 80G of Income Tax Act, 1961.

## 1.4 Advantages:

Blockchain allows different parties that do not trust each other to share information and do business. Transactions are processed by a network of users acting as a consensus mechanism so that everyone is creating the same shared system of record simultaneously. Therefore, no manual reconciliation is required.

The value of decentralized control is that it eliminates the risks of centralized control. With a conventional enterprise application, anybody with sufficient access to that system can destroy or corrupt the data within. This makes users dependent on the administrators.

Blockchain can speed up process execution in multi-party scenarios – and allow for faster transactions that aren’t limited by office hours. Distributed ledgers will provide quick ROI by helping businesses create leaner, more efficient, and more profitable processes.

## Application Architecture:

Web App

Ethereum

API

SQL

SQL Database

Data Storage

1

4

N3

N2

Ethereum Fabric Blockchain Network

Cloud Infrastructure

Load Balancer

The following are the properties of the technical architecture:

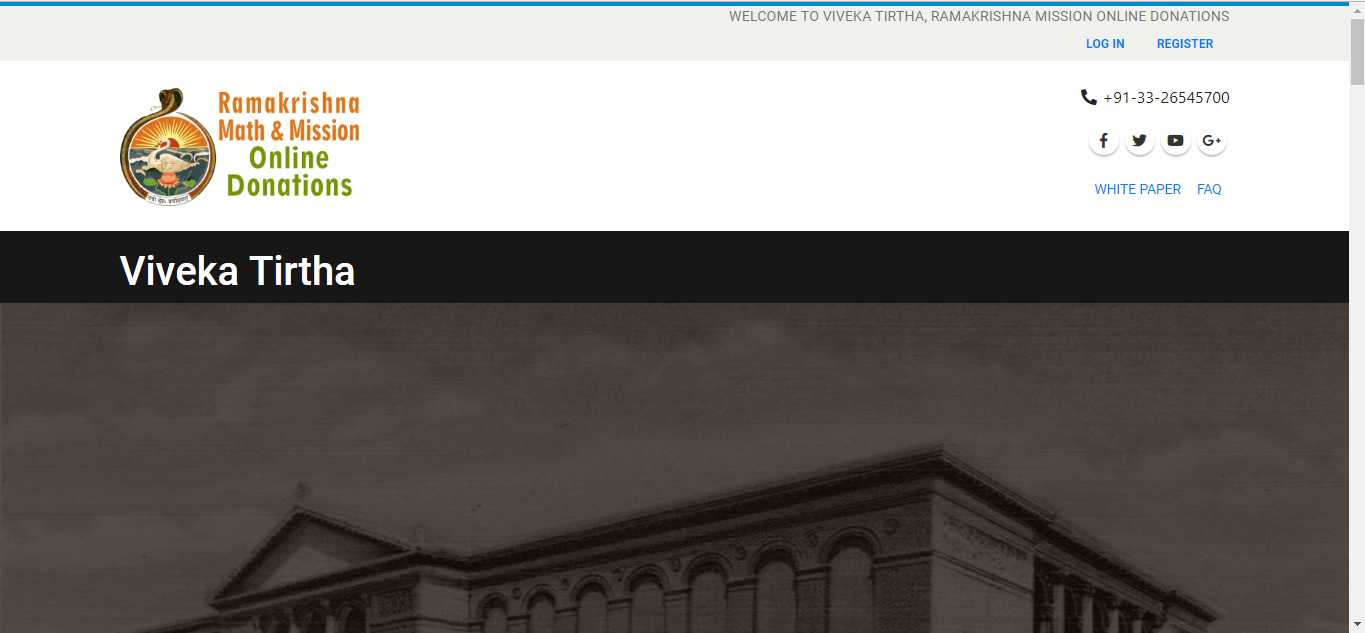
* Ethereum Nodes are running on port 8545
* Two of the nodes acts as transaction nodes and will have load balancer.
* Rest of the two nodes are miner nodes.
* There is a custom mining script which is preloaded when starting a node.
* Only Ethereum API has access to running Ethereum nodes i.e. RPC access to node should be restricted for an IP i.e. the IP of the machine where Ethereum API is hosted.
* Ethereum API is hosted on port 4000
* Ethereum back end, Ethereum, Web Application and SQL server talks to each other through internet.
* User accesses the Web application through internet.

## Server Details:

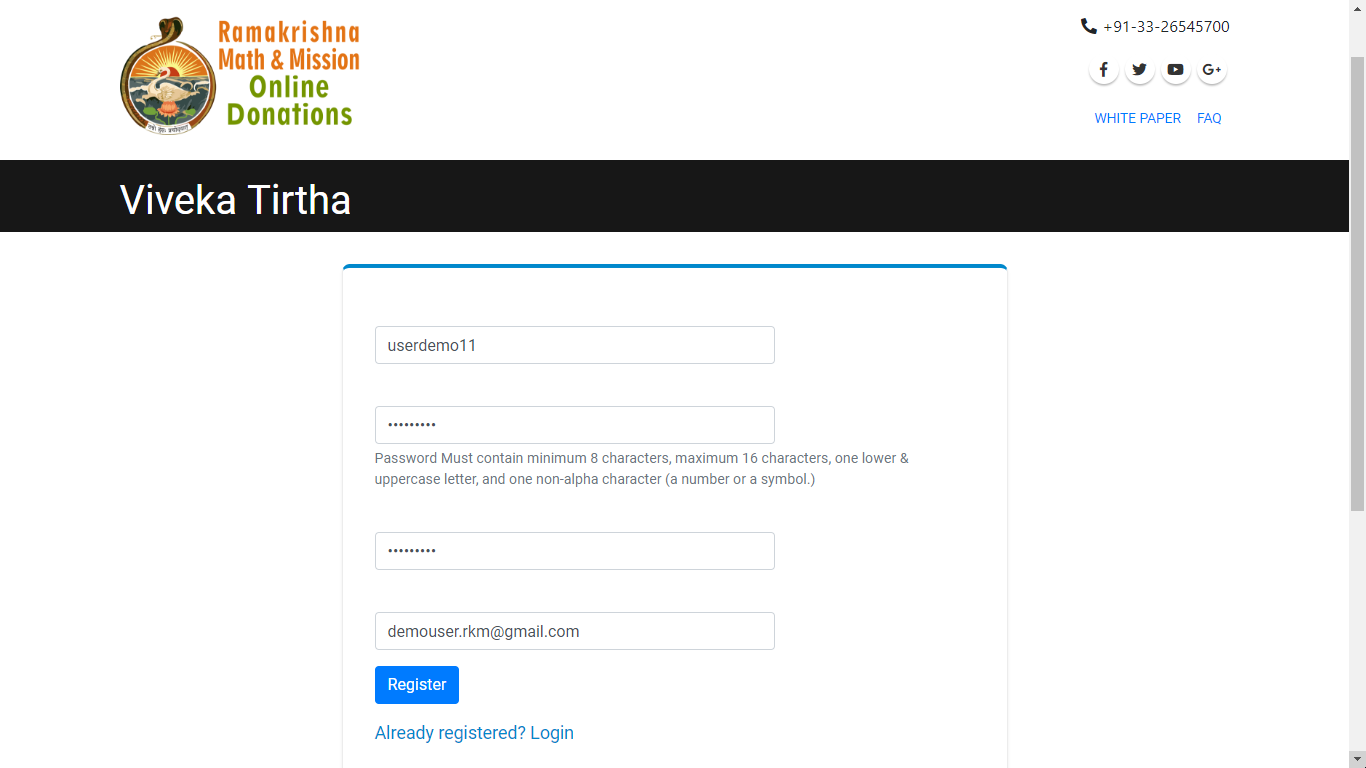
|  |  |  |  |
| --- | --- | --- | --- |
| **Instance Name** | **Server type** | **IP ADDRESS** | **Port** |
| ITE-RAMAKRISHNA MISSION(RKM)-WEB-01 | Web server | 172.20.140.105 | 80 & 443 |
| ITE-RAMAKRISHNA MISSION(RKM)-APP-01 | App server | 172.20.140.115 | 4000 |
| ITE-RAMAKRISHNA MISSION(RKM)-BLKC-NODE-01 | Ethereum Node | 172.20.60.78 | 30307 |
| ITE-RAMAKRISHNA MISSION(RKM)-BLKC-NODE-02 | Ethereum Node | 172.20.60.13 | 30306 |
| ITE-RAMAKRISHNA MISSION(RKM)-BLKC-MINER-01 | Ethereum Node (miner) | 172.20.60.48 | 30308 & 8545 |
| ITE-RAMAKRISHNA MISSION(RKM)-SQL-DB-01 | Database server | 172.20.60.73 | 1433 & 1434 |

## Web Application

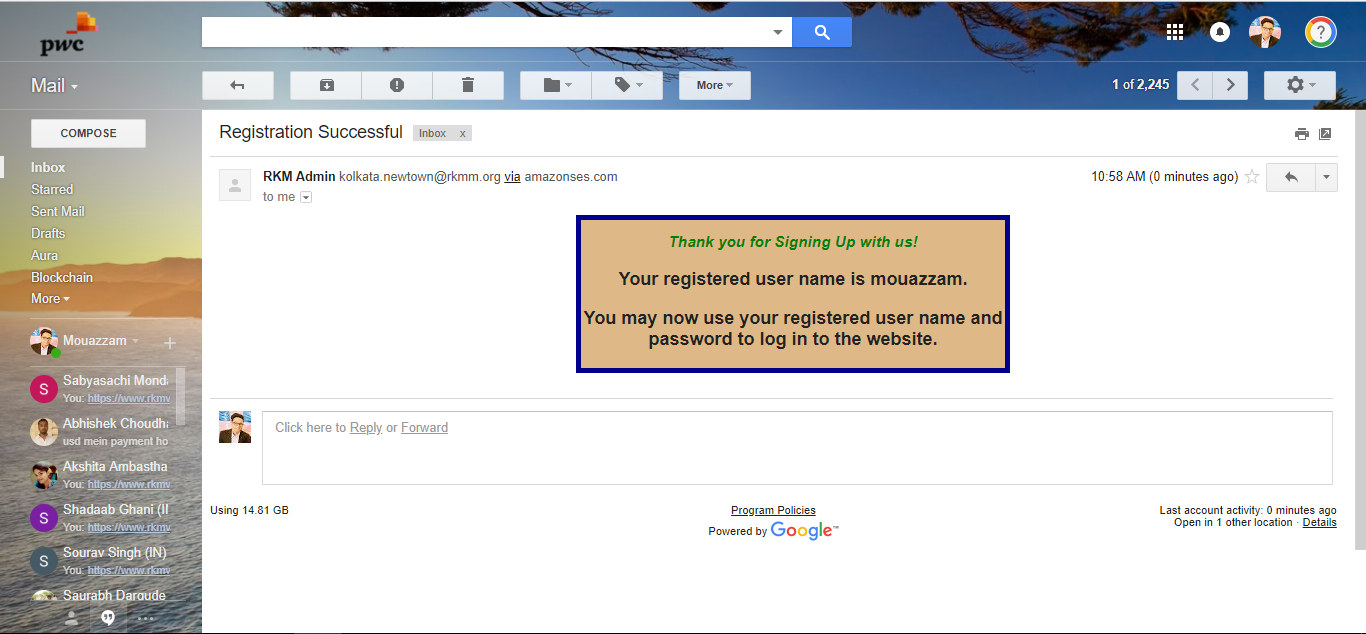
**User login** – Landing Page (URL to website: https://www.rkmvivektirtha.org/home)



**User Registration:**

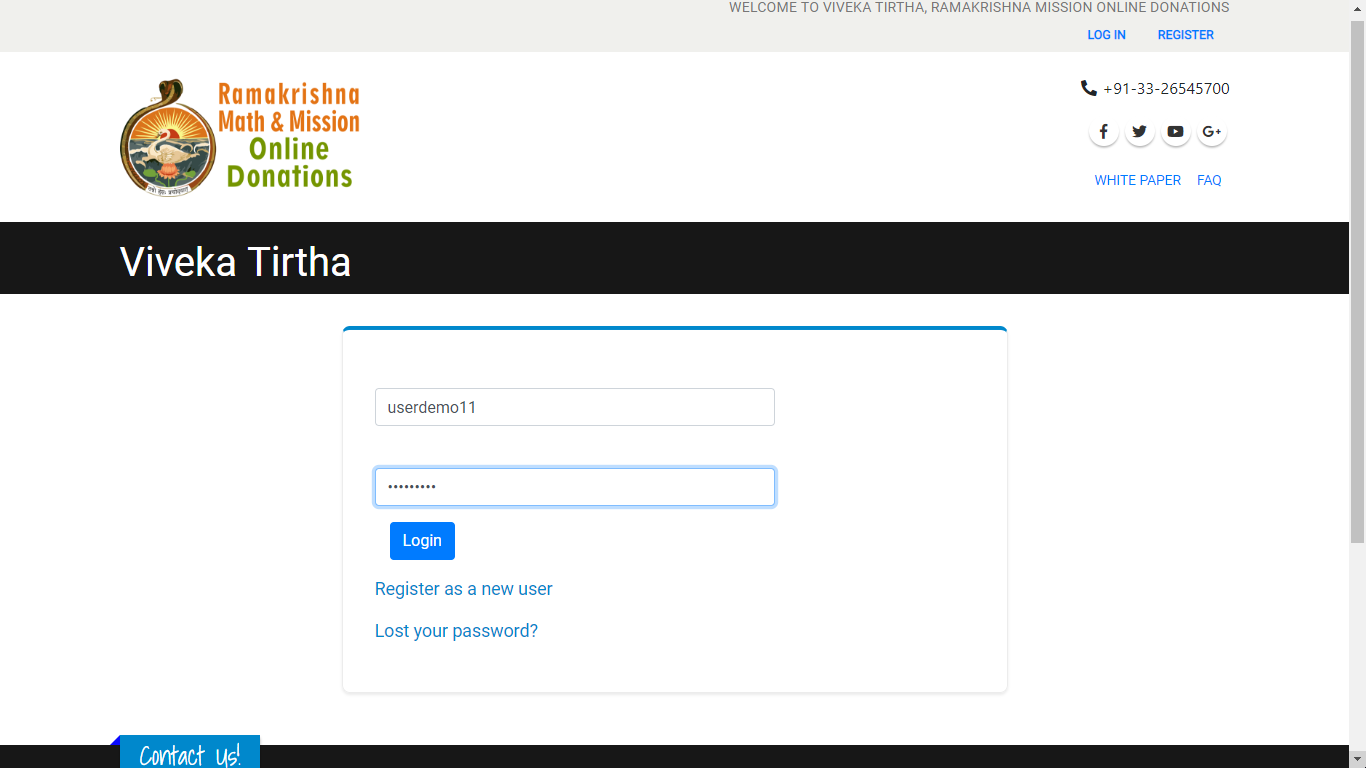


**Registration Email:**

g

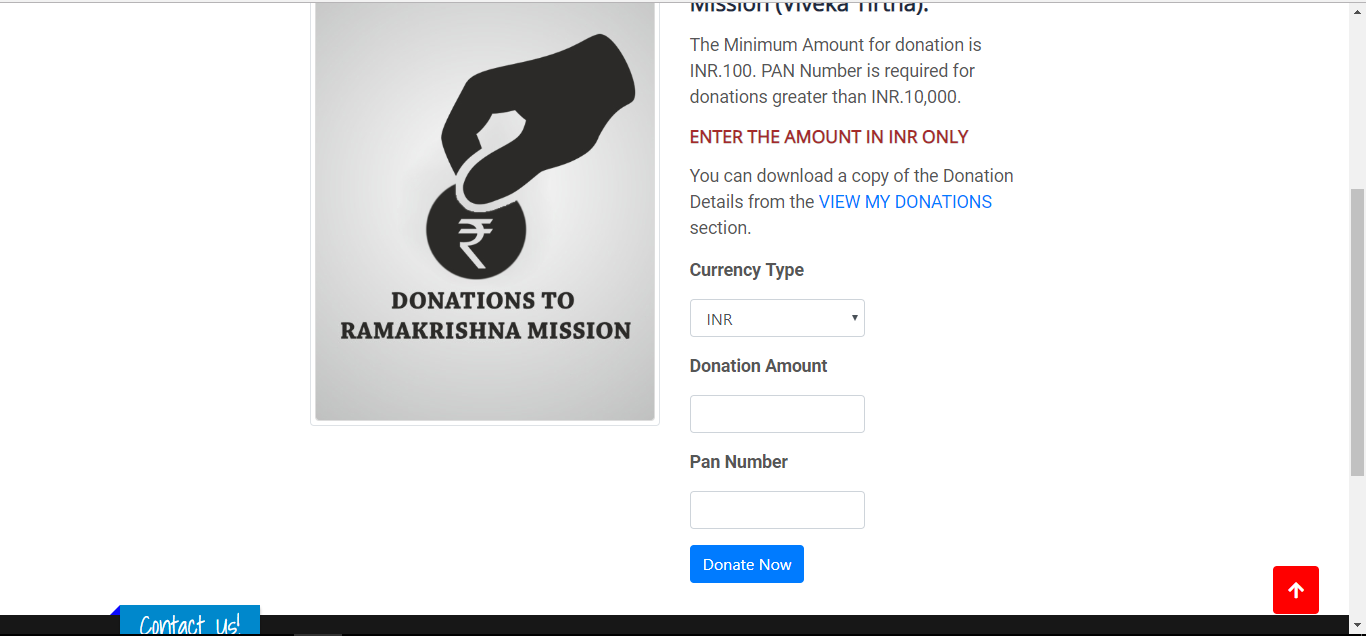
As soon as user completes the user registration step a welcome mail will be sent to the email id.

**User Login:**

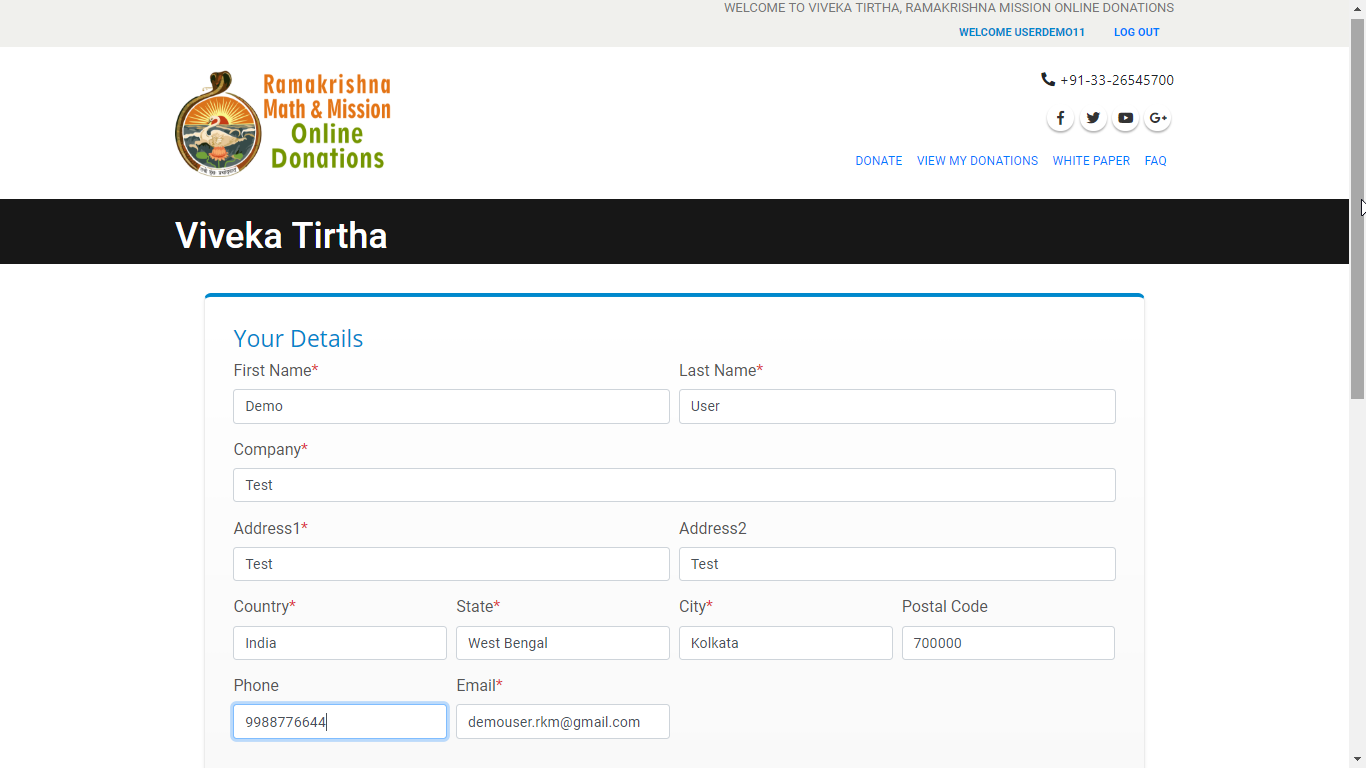
****

**Landing Page & Navigation to Donation view:**

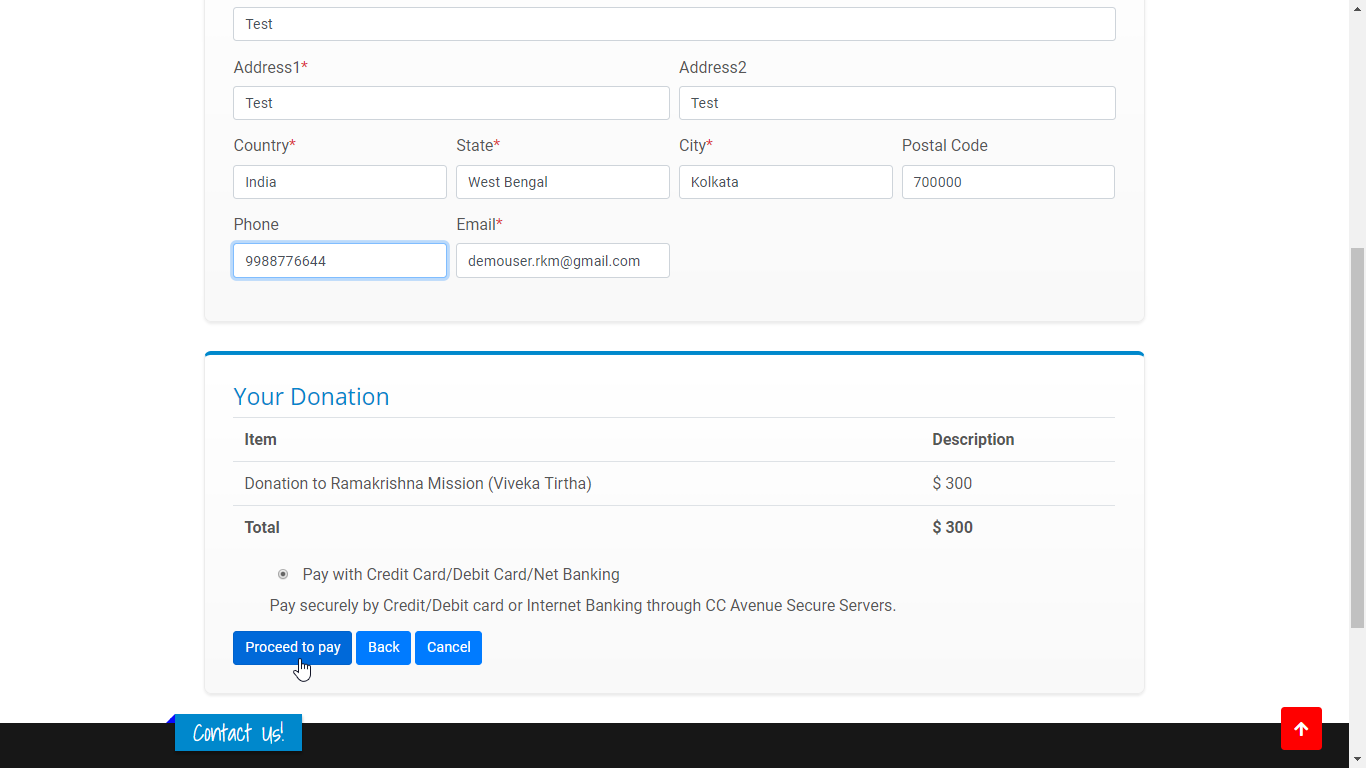
**Make Donation:**

****

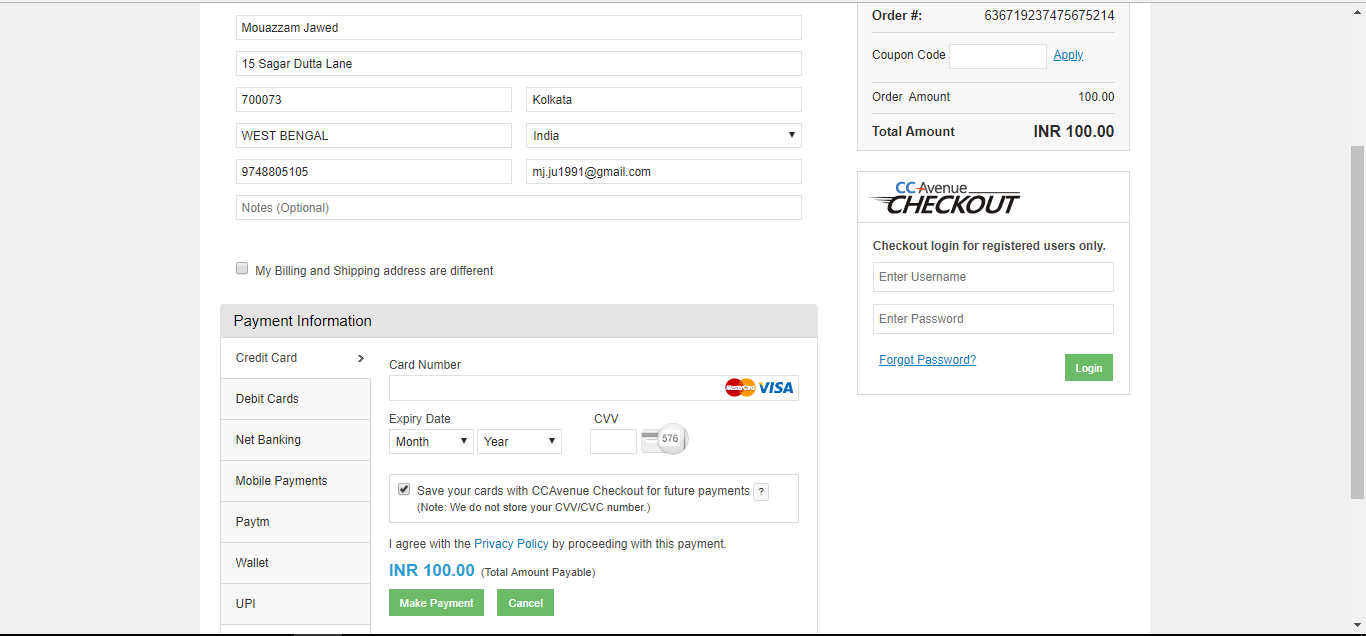
**Donation Details:**

****

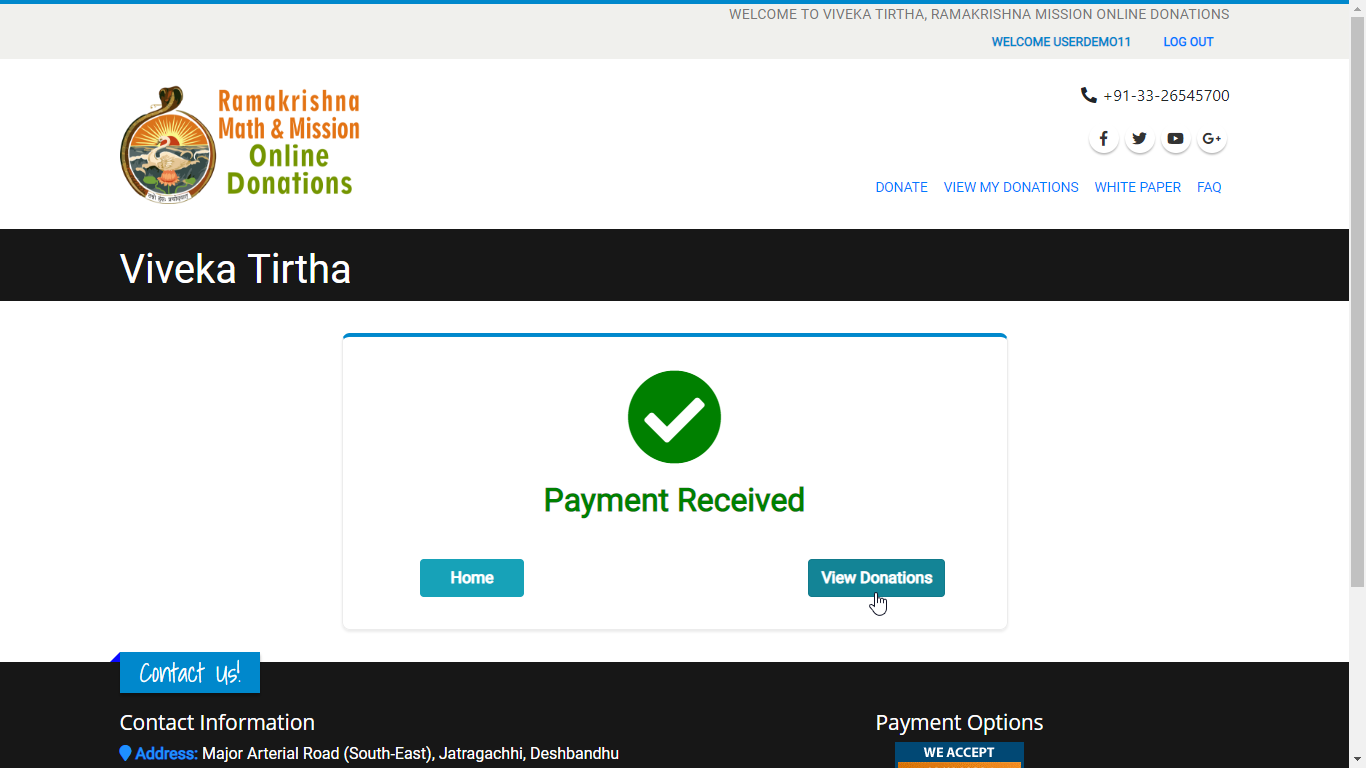
**Payment sub view:**

****

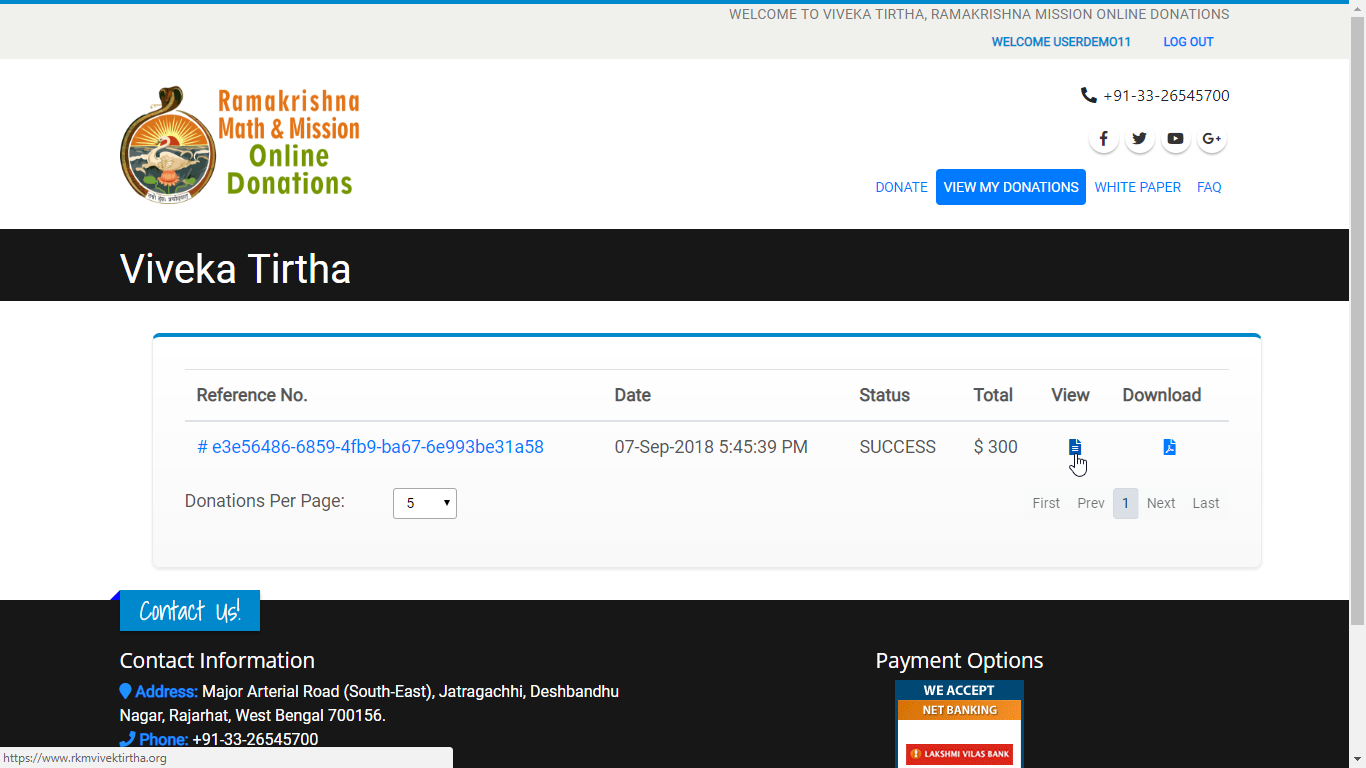
**Payment Gateway:**

****

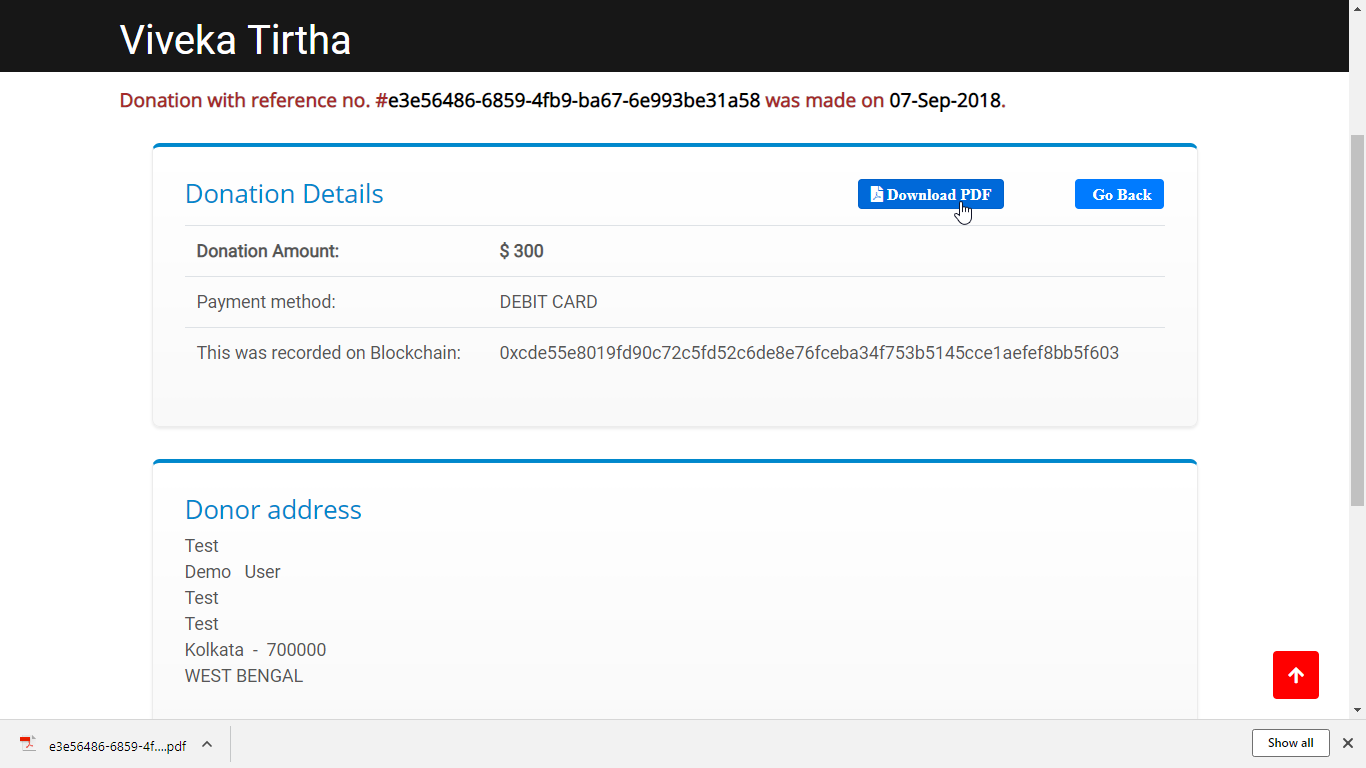
**Payment Successful:**

****

**My Donations View:**

****

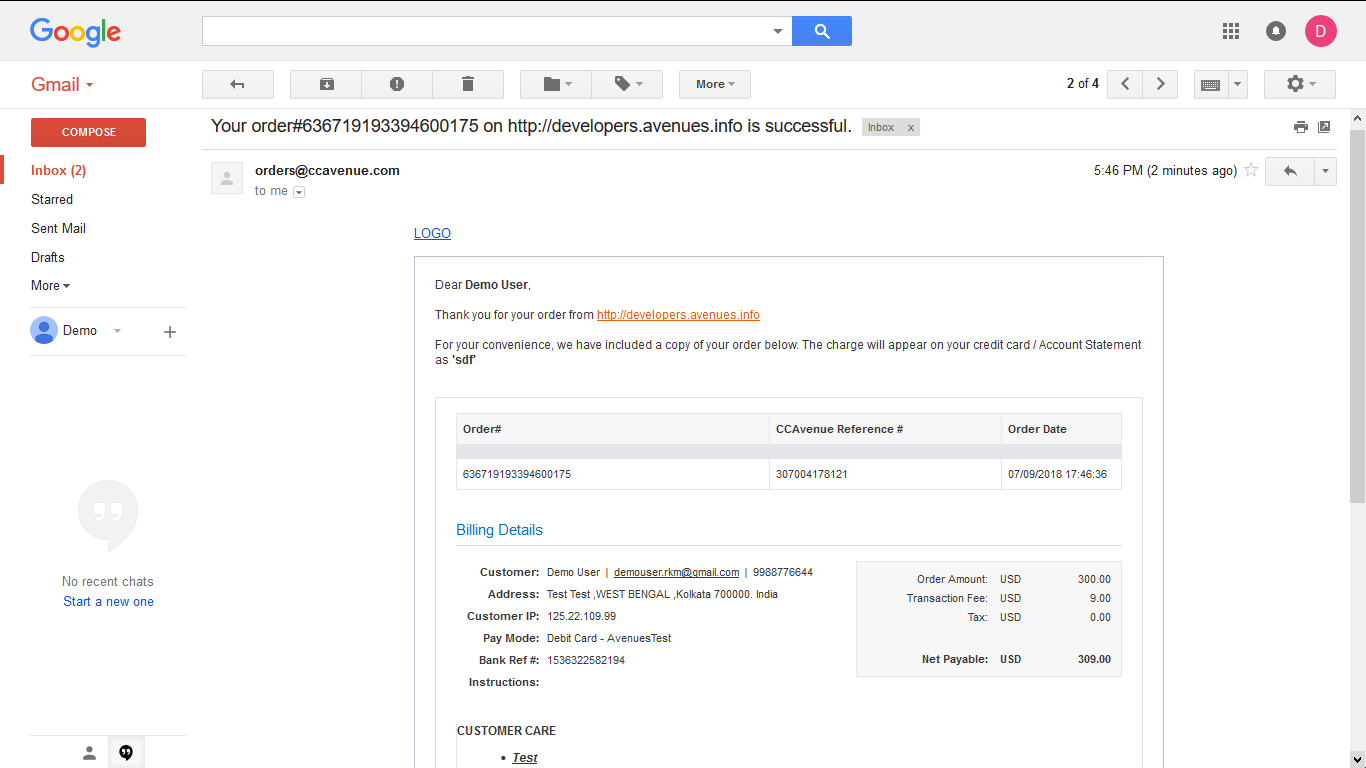
**Donation Detail and donation receipt**

****

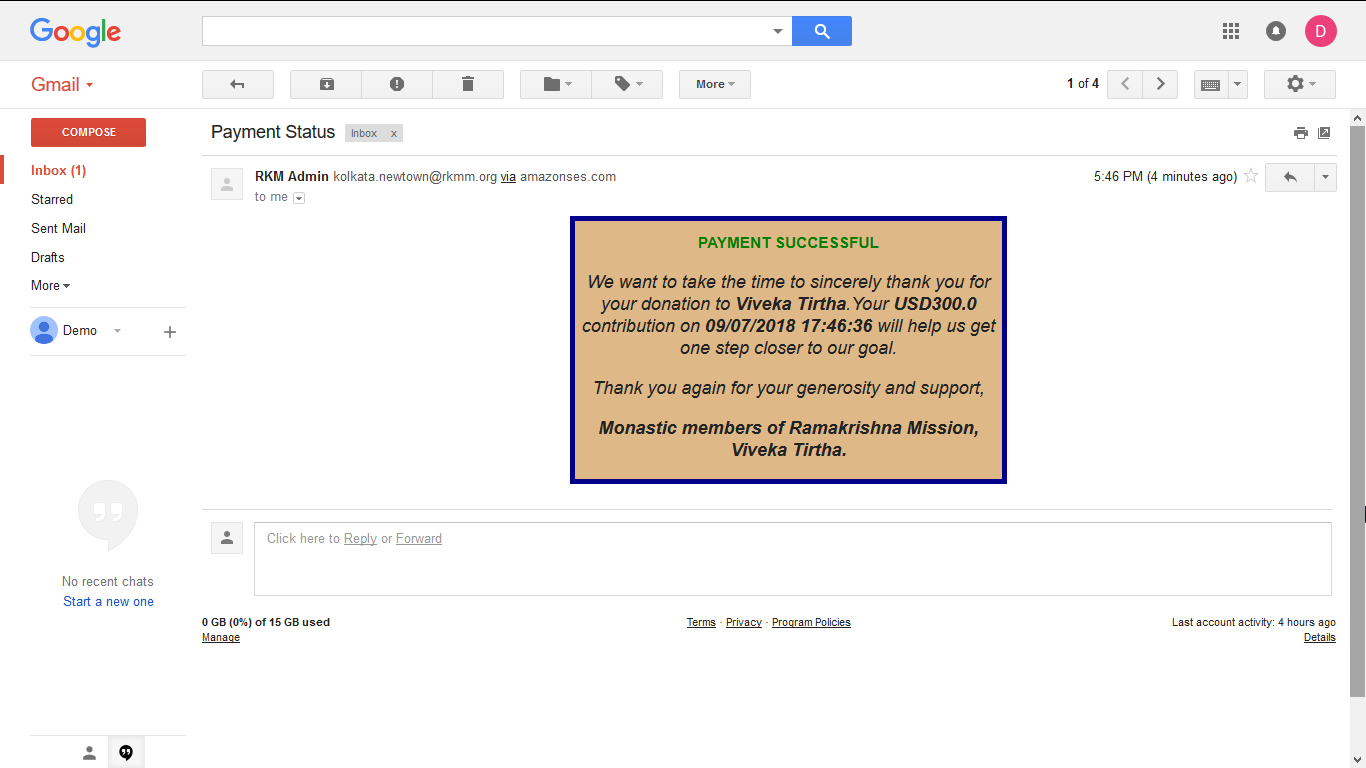
**Donation Receipt**

****

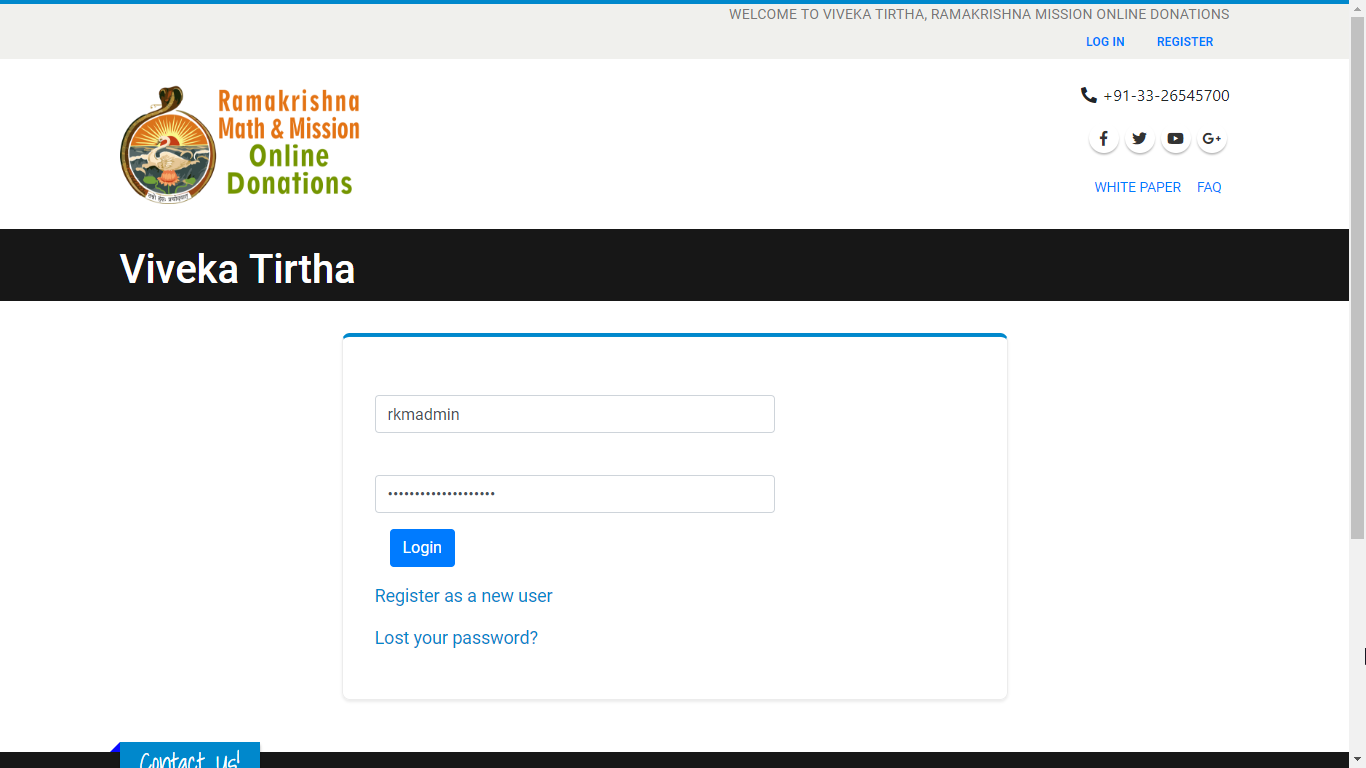
**Payment Email from CC avenue**

****

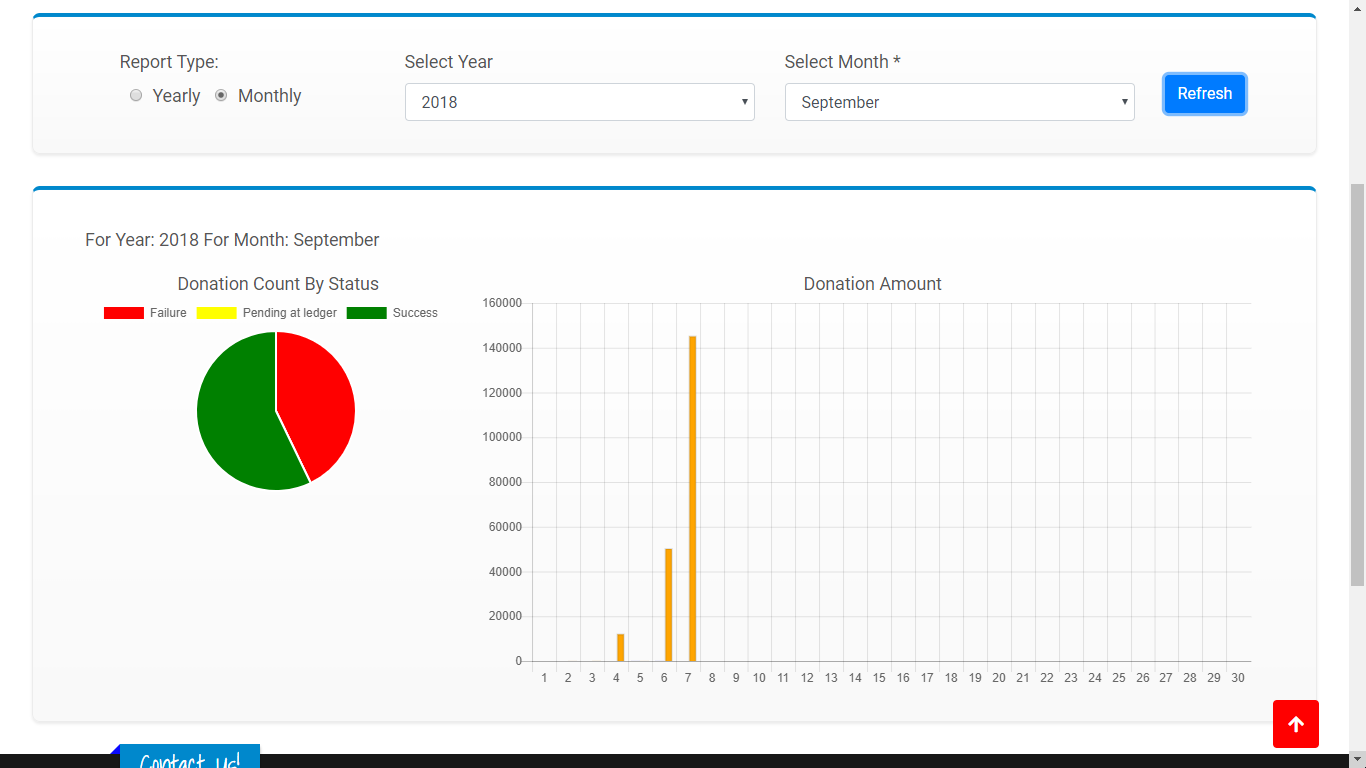
**Payment acknowledgement email from Viveka Tirtha**

****

**Admin Login:**

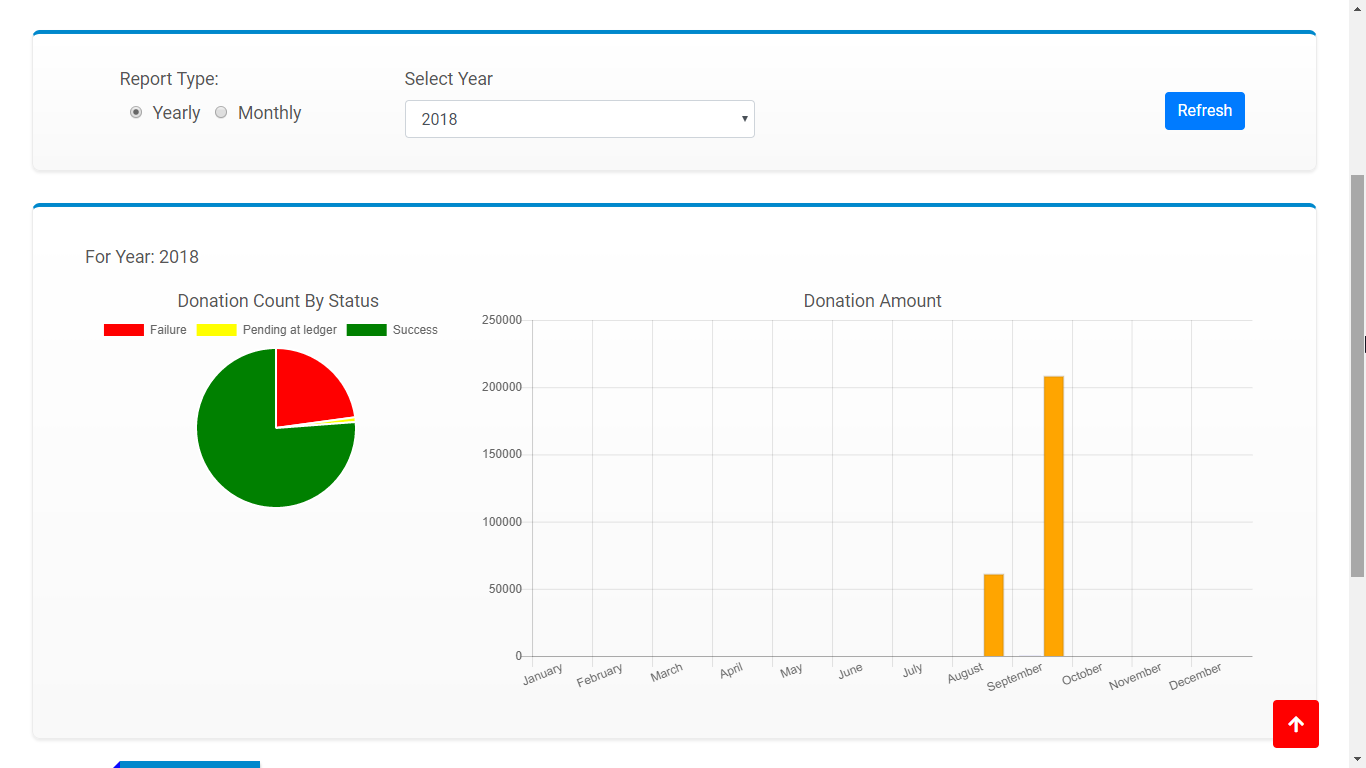
****

**Admin Dashboard monthly view**

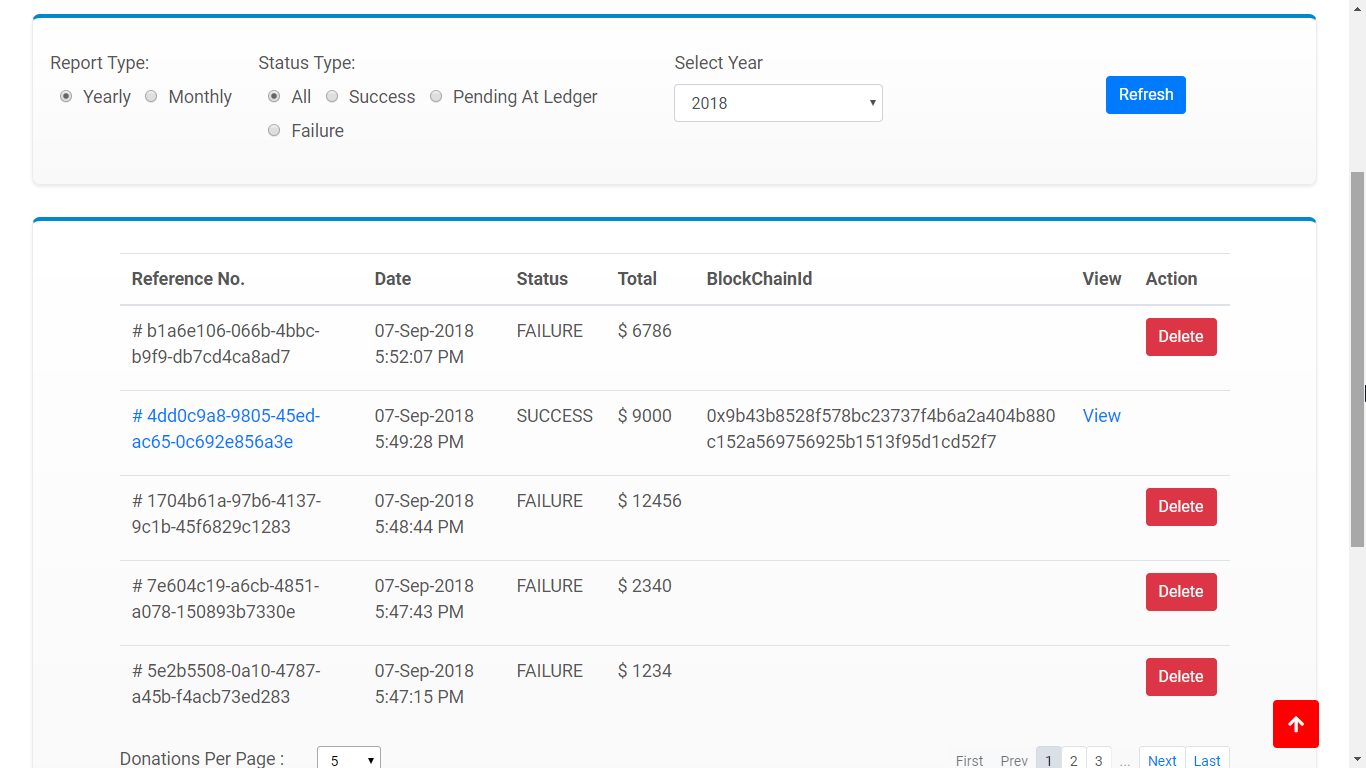
****

* Success: Success means the donation was successful at payment gateway and blockchain ledger.
* Failure: Failure means payment failed at payment gateway, consequently it was not recorded in the blockchain ledger.
* Pending at Ledger: Pending at Ledger means the payment was successful at payment gateway but could not be processed in blockchain. Blockchain transaction can be generated at later stages by admin by clicking a simple button.

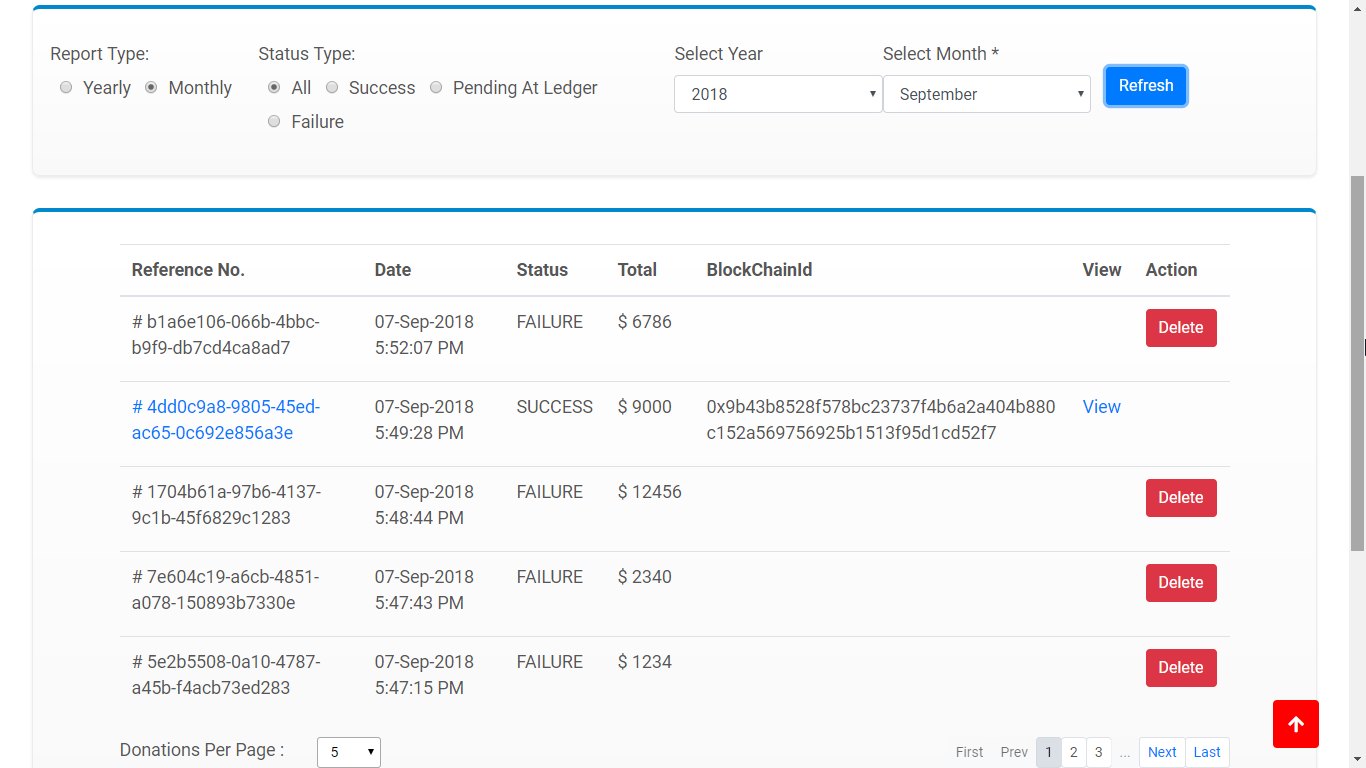
**Admin Dashboard Yearly view**

****

**Reconciliation Yearly view**

****

**Reconciliation monthly view**

****

# Hardware Requirements

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Component | Unit | Core (Per Unit | Core (Total) | RAM (GB)(Per Unit) | Hard Disk (GB) (Per Unit) | Total Disk (GB) | OS/Software Required |
| App Server | 2 | 4 | 8 | 8 | 60 | 120 | (Ubuntu 16.04 LTS) & node.js (v8.11.2) |
| Web Server | 2 | 4 | 8 | 16 | 125 | 250 | (Windows (OS - MS Windows 2016 Std ) .Net  Framework 4.7.1 & IIS) & node.js (v8.11.2) |
| Blockchain Node | 6 | 2 | 12 | 8 | 120 | 720 | Ubuntu 16.04 LTS |
| SQL | 1 | 8 | 8 | 16 | 250 | 250 | SQL Server 2014 express edition (OS - MS Windows 2016 Std) |
| Total | |  |  |  |  | 1840 |  |

|  |  |  |
| --- | --- | --- |
| Blockchain Framework | Version | No of Ubuntu Node to be installed in |
| Ethereum | Geth/1.8.1-stable-1e67410e/ | 4 |

|  |  |  |
| --- | --- | --- |
| Sl No | Software/Service Requirement | Qty |
| **1** | **License: Ubuntu 16.04 LTS** | **As Required** |
| **2** | **Load Balancer** | **1) One for App Servers 2) One for Blockchain Nodes** |
| **3** | **SSL** |  |

# Conclusion

Crowdfunding as a source of triggering various social welfare projects can herein gain widespread acceptance with the introduction of blockchain in the application. Specially, the advantages accorded to the Donation process by Blockchain are:

* Immutability: The transactions of the donations for Viveka Tirtha is immutably recorded in the number of Nodes in the Private Blockchain network based on Ethereum platform.
* Trusted & Secure: Secure Blockchain is an append-only ledger protected by strong cryptography. Once data is added to Blockchain it cannot be changed or deleted.
* Single Source of Truth: All the Audit trials with time stamp of the Donations made to Viveka Tirtha can be tracked on distributed Database.
* Transparency: This system ensures transparency and builds trust.
* Distributed Ledger: Distributed ledger creating a single shared view of transactions - every participant in the network has simultaneous access to a shared view of information