Mini Project Proposal (III Semester MCA)

Approval of the mini project proposal is mandatory to continue and submit the project work.

The mini project proposal should clearly state the project objectives and the environment of the proposed project to be undertaken.

The following documents are to be submitted for approval

1. Pro forma for approval of the mini project (Present in this document)
2. Synopsis/Abstract with following contents

i. Title of the Mini Project.
ii. Introduction and Objectives of the Project.
iii. Tools / Platform, Hardware and Software Requirement
iv. Problem Definition and Initial Requirements
v. Basic functionalities of the project

The abstract should be submitted in the format given in the 3rd page of this document.

The Abstract in the given format shall be uploaded on or before **01.12.21**

MES COLLEGE OF ENGINEERING, KUTTIPPURAM
DEPARTMENT OF COMPUTER APPLICATIONS
20MCA245 – MINI PROJECT

PRO FORMA FOR THE APPROVAL OF THE THIRD SEMESTER MINI PROJECT

(Note: All entries of the pro forma for approval should be filled up with appropriate and complete information. Incomplete
Pro forma of approval in any respect will be rejected.)

Mini Project Proposal No : ___1_____ *(Filled by the Department)*	Academic Year : 2021-2022 Year of Admission : 2020

1. Title of the Project : CROWD-FUNDING USING BLOCKCHAIN
2. Name of the Guide : PRIYA JD
3. Number of the Student: MES20MCA-2039
4. Student Details (in BLOCK LETTERS)

Name RINSHA AP Roll Number 40 Signature

1.

Date: 1/11/2021

Approval Status : Approved / Not Approved

Signature of Committee Members

Comments of The Mini Project Guide Dated Signature

Initial Submission :

First Review :

Second Review :

Comments of The Project Coordinator Dated Signature

Initial Submission:

First Review

Second Review

Final Comments :

Dated Signature of HOD

CROWD-FUNDING USING BLOCKCHAIN

RINSHA AP

Introduction:

Crowd funding is the practice of funding a project or venture by raising small amounts of money from a large number of people, typically via the internet. Before crowd funding were started people would really struggle to get funding for start ups. It was difficult for people to convince investors to invest in their ideas. But now there is no need of such struggle as many crowd funding platforms have evolved like Kick starter, Indiegogo etc. which are helping people for getting the required funding and thereby making their dreams come true. In the existing system of crowd funding platform like Kick starter in order to list any campaign, the campaign creator should give details like the idea of their project, funding goal, government issued ID proof, credit/debit card details etc.

The investors who are interested will invest in these ideas and if the amount reaches the desired goal within the deadline, the entire amount excluding some middlemen fee will be given to campaign creator. The main problem faced in this system is that there no ensured security, the whole funding amount is giving to the person who created the campaign. There are chances that this may lead to miscellaneous activities. People with intention to make money easily will use this platform in a wrong way by coming up with fake ideas and the investors will end up losing all the money invested. Even though there are digital contracts available, they are not ensuring the investor's interest or security. So investing in these kind of platforms are highly risky and depends on luck. So our project focuses on increasing the security with the help of block chain technology and smart contracts, which makes the transactions transparent for the investors and it ensures the funding amount will be safe inside these contracts.

Here if the campaign creator wants to spend the fund he has to create a spending request specifying the reason to spend the fund, to whom the amount goes to (vendors address) and, how much fund is to be released. The investors can vote on this request by approving or can reject the request. Only if the majority is supporting the request the fund is able to release. Here the amount is not directly giving to the campaign creator, but to the vendors address specified in the spending request. The proposed system is a solution to overcome the issues with the existing system.

Objectives:

The main objective of our project is to overcome the problem of security and we are dealing it by using the technology of smart contract which is an application of block chain. In the proposed system the funded amount is kept inside a smart contract and the amount does not directly goes to creator whereas it goes to a vendors address specified by the campaign creator. Before that a spending request must be generated to spend the money kept inside the contract. Within the request the campaign creator need to specify the vendors address, purpose of the spending request and how much money is to be released from the contract. After creating the spending request, investors are given a chance to show their opinion by casting vote whether to sanction the spending request. Approval of majority is mandatory, that 51% of the investor's need to approve the spending request for releasing the amount from the contract to the vendors address. Likewise, the support and interest of the contributors are given importance in this project.

Problem Definition:

Existing system

. that, you may lose or may not. In the existing system, the biggest problem faced is based on security and integrity. With no trouble the current platforms can be subjected to hacking and

alterations. Here once the campaign creator convinces the investors to invest on their ideas and it meets the goal, then the funding amount is directly given to the campaign creator. The investors are unaware of the fund usage and there is no way for them to track the money usage. Their opinions are not taken into consideration while spending the amount. The campaign creator can run away with the amount collected and the investors will never notice this. It will be so late when they come up to know that they were cheated. So there are chances for the occurrences of fraud activities like creators coming up with fake ideas and misleading the investors. The campaign creators will usually offers some rewards in return after their successful project completion to the stakeholders. Expecting these rewards some of them will invest in such project ideas but they might get a low quality product in return or sometimes they will never get anything in return. This is because of the creators buying some cheap and worthless raw materials from the entrepreneurs using the fund. And sometimes there is no terms and policies that supporting the investor's interest and security of the money. These kind of activities cannot be stopped by the investors in the current system. The current system changes their policies according to time and this may affect the investors sometimes. So there is no contracts that the investors can trust on and nowadays investing on the crowd funding is based on the investor's luck

Proposed system

This project is basically an enhancement of the existing crowd funding system. It is developing in a way that overcomes the limitations of the current system. In the proposed system, the campaign creators will post their project ideas in the campaign and the interested people will donate the fund to the project idea. Where it defers from the old crowd funding is that all the money is now digital currencies. All digital coin will be recorded and keep tracks in the block chain. Where the block chain is an immutable ledger. The Donor has control over the funded money. With the Request approval module, the donor has full control over the money they invested. By giving control on invested money the trust is built. Contract is written in such a way that ensures the entire amount funded by the contributors will safely be kept in these contracts so that no one can modify or steal it. If the campaign creator wants to use this amount he/she has to create a spending request. If the majority is voting approving the request the money will be able to release from the contract. The voting system here is decentralized as block chain technology is used in implementing it. This makes it more secure and also cost efficient while guaranteeing the voters privacy. For solving the limitations of the existing system an administrator module is assigned to verify the identity of the users login in to the platform and extra security is given so that to verify user profiles are real and project ideas need to be verified by the admin first to ensure its not scam. In this the security is increased and also the peoples/contributors opinion is taken. It also ensures there is proper communication between the investors and the creators. Here the smart contract is written in a way that ensures the backers would get the benefit of the investing in this project by keeping a fixed amount of money in the contract as backer insurance so that it would not be lost at any context.

Basic functionalities:

USER MODULES:

The project crowd-funding using block chain is implement using python. The application uses the framework flask. My SQL is used in the backend for supporting the system.
The major modules of this project involves:
1. Admin
2. Manager
3. Stakeholder

Admin

The platform administrator verifies the user's identity, verifies the profile of the managers and sanctions the project ideas to publish on the website. Management of the platform is done by the administrator. Admin sets a deadline for the project to reach its goal within which the fund should be collected. After that, only a successfully funded project will be able to collect the fund and the projects that failed to reach the goal within deadline will be rejected and the invested amount will be refunded to

the corresponding shareholders itself. Admin make sure there is less scam in the website by evaluating the projects and the information provided by the campaign creators.

Manager

The person who has to create a new campaign will login to this section. Verified creator account is to be ensured by the administrator so that to prevent fake profiles. Campaign creators need to provide an ID proof ensuring their identity to the admin to get their profile verified. They have to mention the details regarding the project idea they are creating and need to specify the desired amount of fund to be reached for this project. There will be a deadline assigned within which the fund should be raised to meet the goal. If it fails to meet the goal within this deadline then the fund raised would be send back to the wallets of the backers/shareholders. So it isimportant for the creators to create attractive ideas that will make the backers to invest in their ideas. Once the funding goal has reached the managers can create a request for spending the fund. Here is an option for the managers to view the status of the spending request. If it gets 51% of investor's approval the manager can finalize the transaction and the fund is released to the manager's wallet from the contract. The manager has to mention the reason for the release of fund which needs to be convincing for the shareholders.

Stakeholder

The person wishing to support and invest in innovative ideas or need to buy anything from creators will login to this section. The stakeholders can fund the projects and be a shareholder of that project. If there is spending request from the manager then every backers of that project will receive this request and they can either approve or can reject the request. The result of the spending request can be viewed by the shareholders. The balance amount in the project fund will be visible to every investors of that project.

FUNCTIONAL MODULES:

RS RSA is the most common public-key algorithm, named after its inventors Rivest, Shamir, and Adelman. RSA encryption algorithm is a type of public-key encryption algorithm. Public Key encryption algorithm is also called the Asymmetric algorithm. Here both sender and receiver use different keys for encryption and decryption.

Each sender is assigned a pair of keys:

- Public key
- Private key

The public key is used for encryption, and the private key is used for decryption. The two keys are linked, but the private key cannot be derived from the public key. The public key is well known, but the private key is secret and it is known only to the user who owns the key. It means that everybody can send a message to the user using user's public key. But only the user can decrypt the message using his private key.

- The data to be sent is encrypted by sender A using the public key of the intended receiver.
- B decrypts the received cipher text using its private key, which is known only to B. B replies to A encrypting its message using A's public key.
- A decrypts the received cipher text using its private key, which is known only to him

HARDWARE AND SOFTWARE REQUIREMENT

Hardware Requirements

It is recommended that for optimal performance, the following minimum hardware are installed on the server on which the portal is hosted, as well as on clients that access the portal.

1. Processor : Intel Pentium IV

2. Monitor : Min. 14
3. RAM : 256 MB
4. Hard Disk : 80 GB
5. Keyboard : Standard 104 Keys
6. Modem : 56 Kbps
7. Mouse : Serial mouse

Software Requirements

For the proposed system to work properly, it is necessary that following software are installed and running on the server / client.

1. Operating System : Windows 8 or higher
2. Front End Tool : HTML, CSS, python
3. Back End Tool : MY SQL
4. IDE : Pycharm community, Android studio/eclipse
5. Web Browser : All new browsers