MES COLLEGE OF ENGINEERING, KUTTIPPURAM
DEPARTMENT OF COMPUTER APPLICATIONS
20MCA246 – MAIN PROJECT

PRO FORMA FOR THE APPROVAL OF THE FOURTH SEMESTER MAIN 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.)

Main Project Proposal No : ____1____ _______

Academic Year : 2021- 22
Year of Admission : 2020

1. Title of the Project : CROWD FUNDING USING BLOCKCHAIN
2. Name of the Guide : Dr. Geevar C Zacharias
3. Student Details (in BLOCK LETTERS)

Name	Register Number	Signature
RINSHA AP	MES20MCA-2039	__________________

Date:

Approval Status : Approved / Not Approved

Signature of
Committee Members }

Comments of the 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

Introduction & Objectives:

Crowdfunding 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 crowdfunding were started people would really struggle to get funding for startups. It was difficult for people to convince investors to invest in their ideas. But now there is no need of such struggle as many crowdfunding platforms have evolved like Kickstarter, Indiegogo etc. which are helping people for getting the required funding and thereby making their dreams come true. In the existing system of crowdfunding platform like Kickstarter 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 kinds of platforms are highly risky and depends on luck. So, our project focuses on increasing the security with the help of blockchain 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.

A cryptocurrency, crypto-currency, or crypto is a collection of binary data which is designed to work as a medium of exchange. Individual coin ownership records are stored in a ledger, which is a computerized database using strong cryptography to secure transaction records, to control the creation of additional coins, and to verify the transfer of coin ownership.

Cryptocurrencies are generally fiat currencies, as they are not backed by or convertible into a commodity. Some crypto schemes use validators to maintain the cryptocurrency. In a proof-of-stake model, owners put up their tokens as collateral. In return, they get authority over the token in proportion to the amount they stake. Generally, these token stakers get additional ownership in the token over time via network fees, newly minted tokens or other such reward mechanisms.

Cryptocurrency does not exist in physical form (like paper money) and is typically not issued by a central authority. Cryptocurrencies typically use decentralized control as opposed to a central bank digital currency (CBDC). When a cryptocurrency is minted or created prior to issuance or issued by a single issuer, it is generally considered centralized. When implemented with decentralized control, each cryptocurrency works through distributed ledger technology, typically a blockchain, that serves as a public financial transaction database.

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 blockchain. In the proposed system the funded amount in the form of crypto currency 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:

EXISTING SYSTEM:

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 offer 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 kinds 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 crowdfunding is based on the investor’s luck that, you may lose or may not.

Proposed System:

This project is basically an enhancement of the existing crowdfunding 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. The fund is mainly donated in the form crypto currency so that the invested amount will be protected from inflation and it's easier to transfer fund in a secure way. Where it defers from the old crowdfunding is that all the money is now digital currencies. All digital coin will be recorded and keep tracks in the blockchain. Where the blockchain 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 blockchain 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 user's 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/contributor's 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

RSA KEY ENCRYPTION ALGORITHM:

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 decrypt the received cipher text using its private key, which is known only to him.

BLOCKCHAIN:

A blockchain is a growing list of records, called blocks, that are linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree). The timestamp proves that the transaction data existed when the block was published in order to get into its hash. As blocks each contain information about the block previous to it, they form a chain, with each additional block reinforcing the ones before it. Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.
Blockchains are typically managed by a peer-to-peer network for use as a publicly distributed ledger, where nodes collectively adhere to a protocol to communicate and validate new blocks. Although blockchain records are not unalterable as forks are possible, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance.
The blockchain was popularized by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin, based on work by Stuart Haber, W. Scott Stornetta, and Dave Bayer. The identity of Satoshi Nakamoto remains unknown to date. The implementation of the blockchain within bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications and blockchains that are readable by the public and are widely used by cryptocurrencies. The blockchain is considered a type of payment rail. Private blockchains have been proposed for business use but Computerworld called the marketing of such privatized blockchains without a proper security model "snake oil". However, others have argued that permissioned blockchains, if carefully designed, may be more decentralized and therefore more secure in practice than permissionless ones.

CRYPTO CURRENCY:

Cryptocurrencies are digital currencies that use blockchain technology to record and secure every transaction. A cryptocurrency (for example, Bitcoin) can be used as a digital form of cash to pay for everything from everyday items to larger purchases like cars and homes. It can be

bought using one of several digital wallets or trading platforms, then digitally transferred upon purchase of an item, with the blockchain recording the transaction and the new owner. The appeal of cryptocurrencies is that everything is recorded in a public ledger and secured using cryptography, making an irrefutable, timestamped and secure record of every payment.
A cryptocurrency is a tradable digital asset or digital form of money, built on blockchain technology that only exists online. Cryptocurrencies use encryption to authenticate and protect transactions, hence their name. There are currently over a thousand different cryptocurrencies in the world, and many see them as the key to a fairer future economy.

User Modules:

The project crowd-funding using blockchain is implement using python. The application uses the framework flask. MySQL is used in the backend for supporting the system.

The major modules of this project involve:

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.

Admin

- Login
- Add and Manage managers

- Manage stakeholder
- Manage projects

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 is important 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.

Manager

- Login
- Create new project
- View project status
- Create spending request
- View spending request status

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 backer 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 investor of that project.

Stakeholder

- Registration
- Login
- View project details
- Fund project
- View request
- Vote for request

HARDWARE AND SOFTWARE REQUIREMENT

This specifies the hardware and the support software required to carry out the development.

HARDWARE REQUIREMENTS:

The selection of hardware is very important in the existence and proper working of any

software. Then selection hardware, the size and capacity requirements are also important.

- Processor - Intel x86
- Speed - 1.1 GHz
- RAM - 700 MB (min)
- Hard Disk - 150 MB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVG

SOFTWARE REQUIREMENTS:

One of the most difficult tasks is selecting software for the system, once the system requirements is found out then we have to determine whether a particular software package fits for those system requirements. The application requirement:

- Operating System - Windows 7 or Above, Android
- Technology - Python, Java
- Backend - MySQL
- Platform used - JetBrains, PyCharm, Android Studio
- Web Browser - Google Chrome, Fire fox, Microsoft Edge
- Front End - HTML, CSS, JAVASCRIPT
- Frame work - Flask