CROWD-FUNDING USING BLOCK CHAIN & CRYPTOCURRENCY

NAME: RINSHA AP

ROLL NO: 40

PRODUCT OWNER: DR.GEEVAR.C ZACHARIAS

Table of contents

1. Introduction
2. Modules
3. Methodology
4. Project Plan
5. User Story
6. Product backlog
7. Sprint plans
8. Sprint Actual

INTRODUCTION

- Crowd funding is the practice of funding a project orventure 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 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 Kick starter, Indiegogo etc. which are helping people for getting the required funding and thereby making their dreams come true.
- 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.

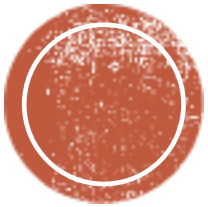
- People with intention to make money easily will use this platform in a wrong way by coming up with fake ideas and the investors will end up losing all the money invested. Even though there are digital contracts available, they are not ensuring the investor's interest or security.So, investing in these 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.
- Acryptocurrency,crypto-currency,orcryptoisacollectionofbinarydatawhichisdesignedto workasamedium ofexchange.Individualcoinownershiprecordsarestoredinaledger,which isacomputerizeddatabaseusingstrongcryptographytosecuretransactionrecords,tocontrol thecreationofadditionalcoins,andtoverifythetransferofcoinownership

- Cryptocurrencies are generally fiat currencies,as they are not backed by or convertible into commodity.Some crypto schem esuse validators to maintain the cryptocurrency.In a proof-of stakemodel,owners put up their tokens as collateral.In return,they get authority over the token in proportion to the amount they stake. Generally,these tokens take rs get additional ownership in the token over time viane tworkfees,newly minted tokens or other such reward mechanisms.
- Cryptocurrency does not exist in physical form (likepapermoney)an distypically not issued by a central authority. Cryptocurrencies typically used ecentralized control a s opposed to a central bank digital currency(CBDC).
- The main objective of our project is to over come the problem of security and we are Dealing it by using the technology of smartcontract which is an application of blockchain. In the proposed system the funded amount in the form of cryptocurrency is kept inside a smart Contract and the amount does not directly goes to creator where as it goes to avendors address specified by the campaign creator.
- Before that as pending request must be generated to spend the money kept in side the contract. Within the request the campaign creator need to specify the vendors address, purpose of the spending request an dhow 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 releaprojecte Amount from the contract to the vendors address.Like wise,the support and interest of the Contribut or sare given importance in this project.

METHODOLOGY

MODULES



1. Admin
   - Login
   - Add and manage managers
   - Manage stakeholder
   - Manage projects
2. Manager
   - Login
   - Create new project
   - View project status
   - Create spending request
   - View spending request status
3. Stakeholder
   - Registration
   - Login
   - View project details
   - Fund project
   - View request
   - Vote for request

DEVELOPING ENVIRONMENT

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

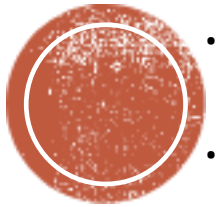
RSA ALGORITHM

- The RSA algorithm is an asymmetric cryptography algorithm; this means that it uses a public key and a private key (i.e two different, mathematically linked keys). As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.
- The RSA algorithm involves four steps: key generation, key distribution,encryption, and decryption.

SHA-256 ALGORITHM

- The SHA-256 algorithm is one flavor of SHA-2 (Secure Hash Algorithm 2), which was created by the National Security Agency in 2001 as a successor to SHA-1. SHA-256 is a patented cryptographic hash function that outputs a value that is 256 bits long.
- In encryption, data is transformed into a secure format that is unreadable unless the recipient has a key.
- In its encrypted form, the data may be of unlimited size, often just as long as when unencrypted. In hashing, by contrast, data of arbitrary size is mapped to data of fixed size. For example, a 512-bit string of data would be transformed into a 256-bit string through SHA-256 hashing.

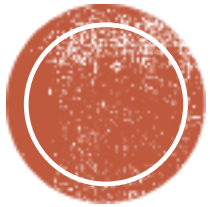
BLOCKCHAIN



- All the Voting information's are stored in block chain. Block chain is a record-keeping technology designed to make it impossible to hack the system or forget the data stored on it, thereby making it secure and immutable. It is a type of distributed ledger technology (DLT), a digital system for recording transactions and related data in multiple places at the same time.
- Once the information stored in block chain it is not possible to manipulate the stored information .
- It consists of an expanding list of transactions or records stored in the blocks and uses peer to peer networks. The blocks in the block chain are connected as a chain with the use of hashing algorithms.
- Blocks are stored in a decentralized network where all the blocks are present in multiple nodes. As data is decentralized the chances of data tampering and data loss is less which makes block chain more secure and transparent.
- Each block of the block chain consist of the previous block's hash value, nonce, a timestamp, the records of the block and the hash of the current block.
- The main advantages of using block chain are decentralization, security , transparency, and immutability.

CONFIGURATION OF BLOCKCHAIN

Truffle

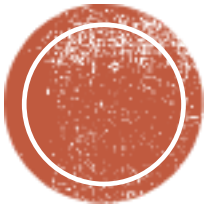


- Truffle is the most popular development tooling for Ethereum programmers. Easily deploy smart contracts and communicate with their underlying state without heavy client side programming. An especially useful library for the testing and iteration of Ethereum smart contracts.
- It is used to create configuration files and compile block chain.
- First install node to create files for block chain automatically. Through this create contract that contain sol files. Sol files contain the information that we want to pass into the block chain. This concept is called smart contracting.

Ganache

- Ganache is a high-end development tool used to run your own local block chain for both Ethereum and Cordad App development. It act as a server to see the info that pass to the block chain.

CRYPTOCURRENCY



- Cryptocurrencies are digital currencies that use blockchain technology to record and secure every transaction. A cryptocurrency (forexample,Bitcoin) can be used as a digital form of cash to pay for everything from every day items to larger purchases like cars and homes .It can be bought using one of several digital wallet sortrading platforms,thendigitally transferred up on purchase of anitem,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,time stamped 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 thous and different cryptocurrencies in the world,and many see them as the key to a fairer future economy.

TABLE DESIGN

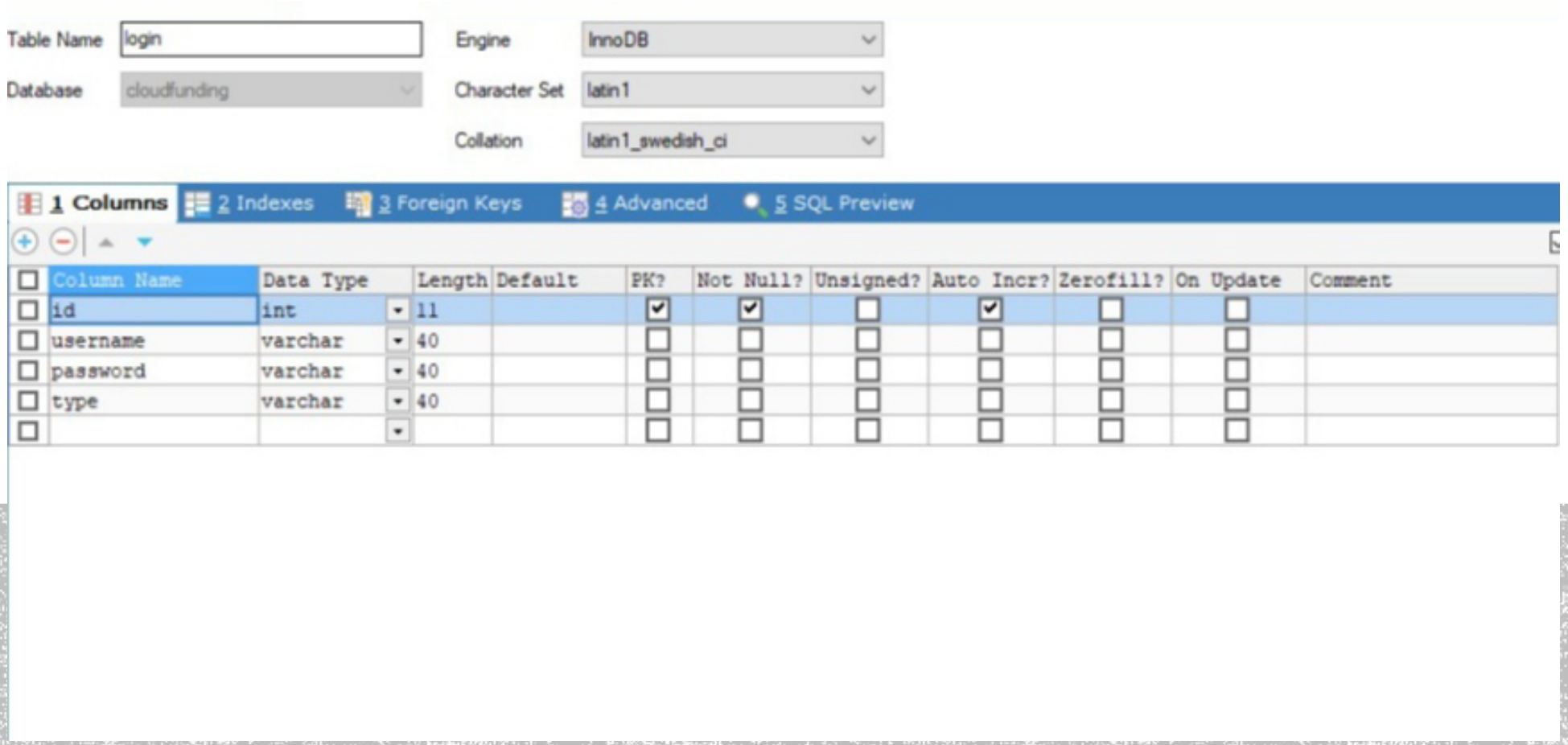


Table design

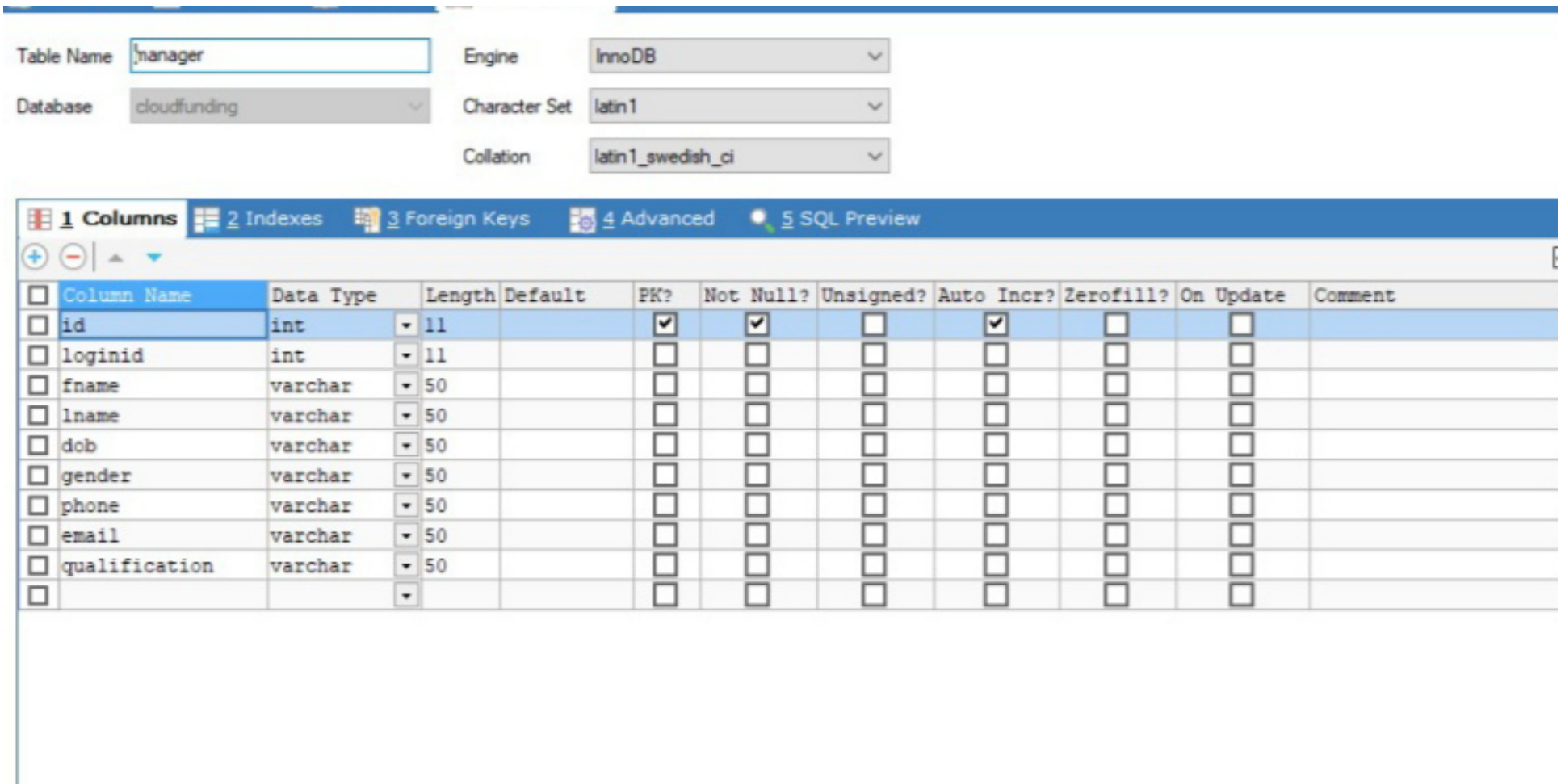


Table Name: manager
Engine: InnoDB
Database: cloudfunding
Character Set: latin1
Collation: latin1_swedish_ci

1 Columns | 2 Indexes | 3 Foreign Keys | 4 Advanced | 5 SQL Preview

Column Name	Data Type	Length	Default	PK?	Not Null?	Unsigned?	Auto Incr?	Zerofill?	On Update	Comment
id	int	11		☑	☑	☐	☑	☐	☐	
loginid	int	11		☐	☐	☐	☐	☐	☐	
fname	varchar	50		☐	☐	☐	☐	☐	☐	
lname	varchar	50		☐	☐	☐	☐	☐	☐	
dob	varchar	50		☐	☐	☐	☐	☐	☐	
gender	varchar	50		☐	☐	☐	☐	☐	☐	
phone	varchar	50		☐	☐	☐	☐	☐	☐	
email	varchar	50		☐	☐	☐	☐	☐	☐	
qualification	varchar	50		☐	☐	☐	☐	☐	☐	
				☐	☐	☐	☐	☐	☐	

Table design

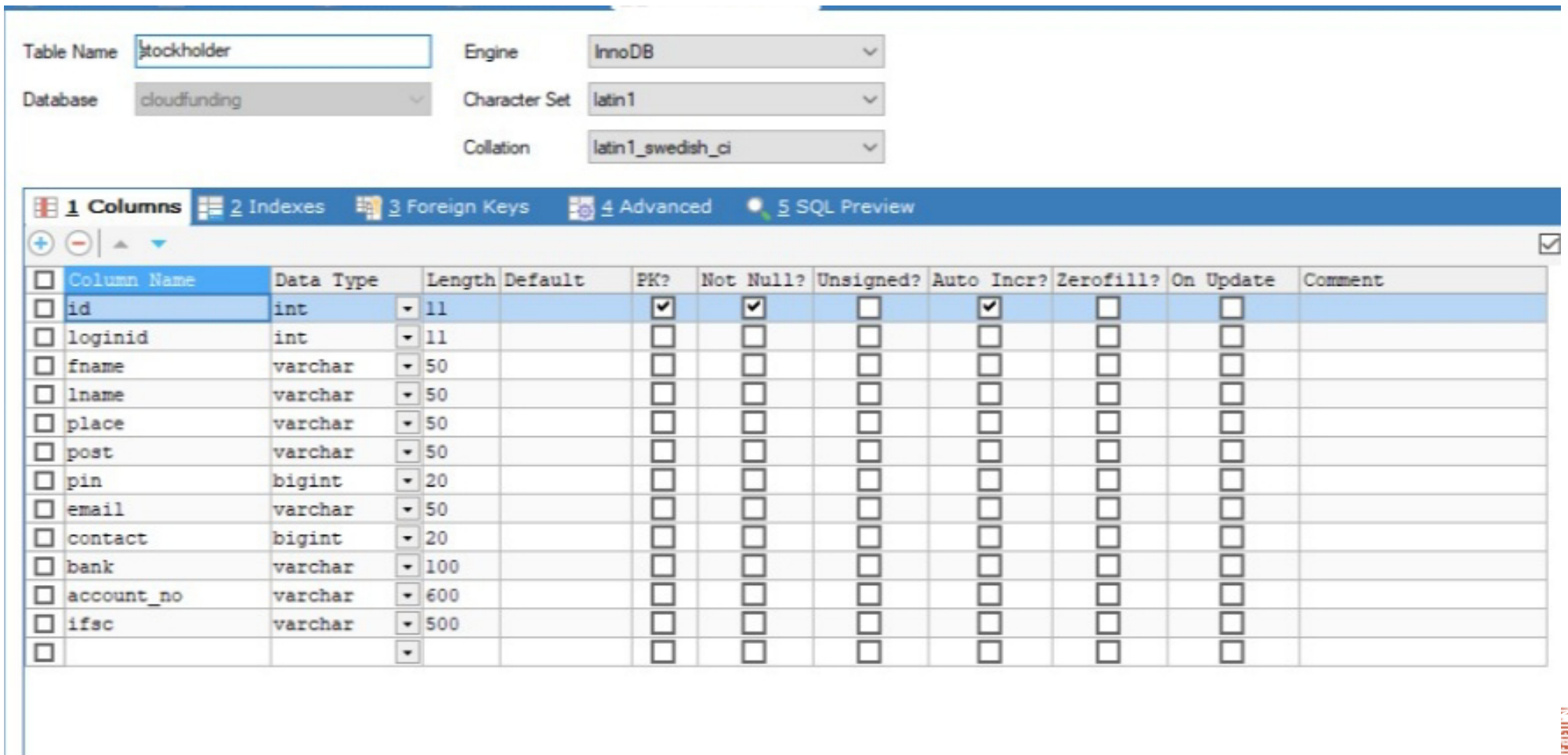


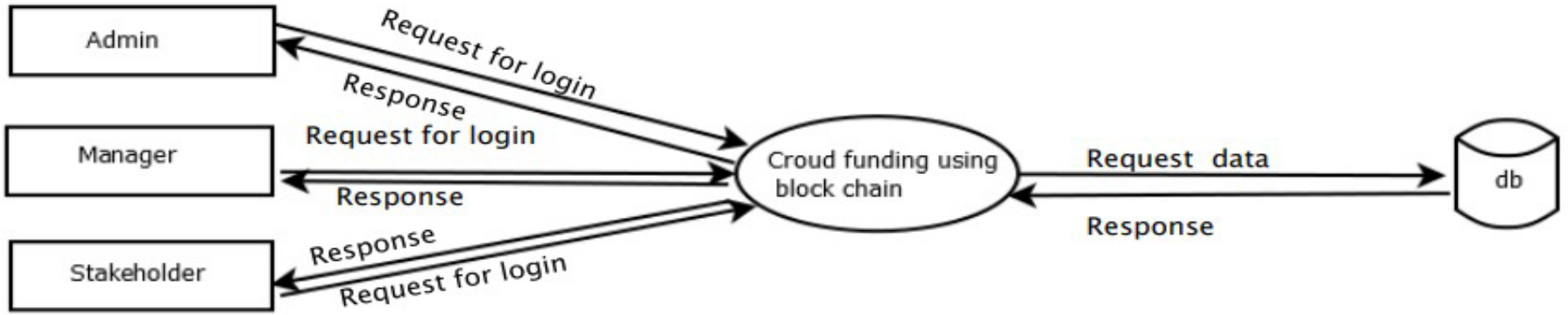
Table Name: stockholder
Engine: InnoDB
Database: cloudfunding
Character Set: latin1
Collation: latin1_swedish_ci

1 Columns | 2 Indexes | 3 Foreign Keys | 4 Advanced | 5 SQL Preview

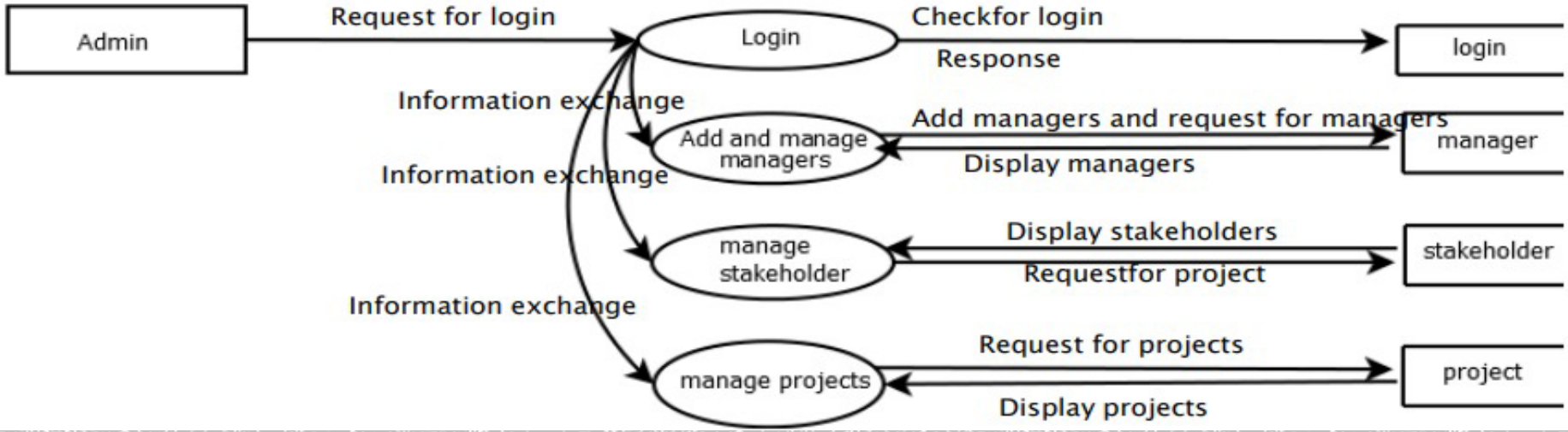
Column Name	Data Type	Length	Default	PK?	Not Null?	Unsigned?	Auto Incr?	Zerofill?	On Update	Comment
id	int	11		☑	☑	☐	☑	☐	☐	
loginid	int	11		☐	☐	☐	☐	☐	☐	
fname	varchar	50		☐	☐	☐	☐	☐	☐	
lname	varchar	50		☐	☐	☐	☐	☐	☐	
place	varchar	50		☐	☐	☐	☐	☐	☐	
post	varchar	50		☐	☐	☐	☐	☐	☐	
pin	bigint	20		☐	☐	☐	☐	☐	☐	
email	varchar	50		☐	☐	☐	☐	☐	☐	
contact	bigint	20		☐	☐	☐	☐	☐	☐	
bank	varchar	100		☐	☐	☐	☐	☐	☐	
account_no	varchar	600		☐	☐	☐	☐	☐	☐	
ifsc	varchar	500		☐	☐	☐	☐	☐	☐	
				☐	☐	☐	☐	☐	☐	

DATA FOLW DIAGRAM

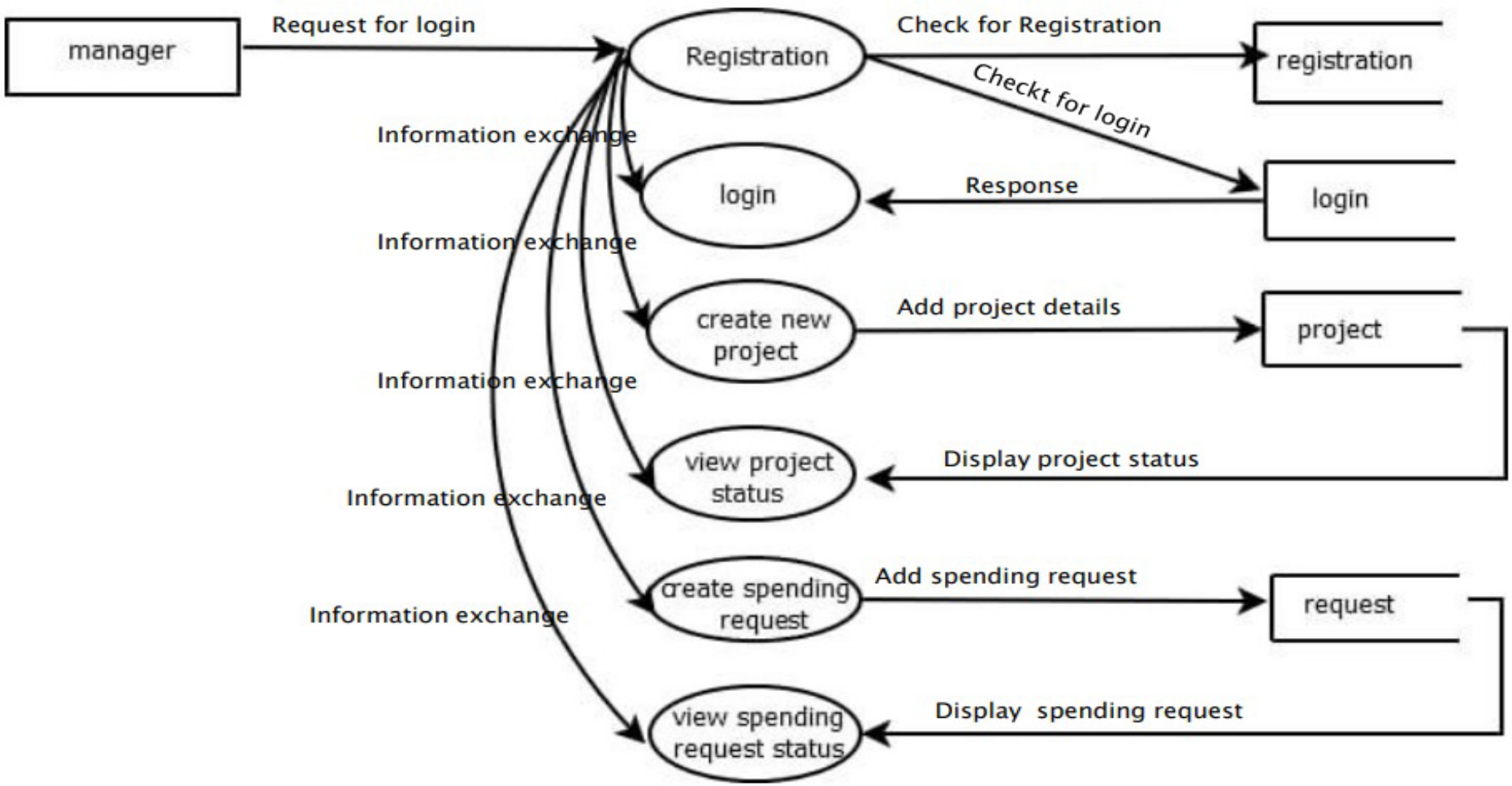
Level 0



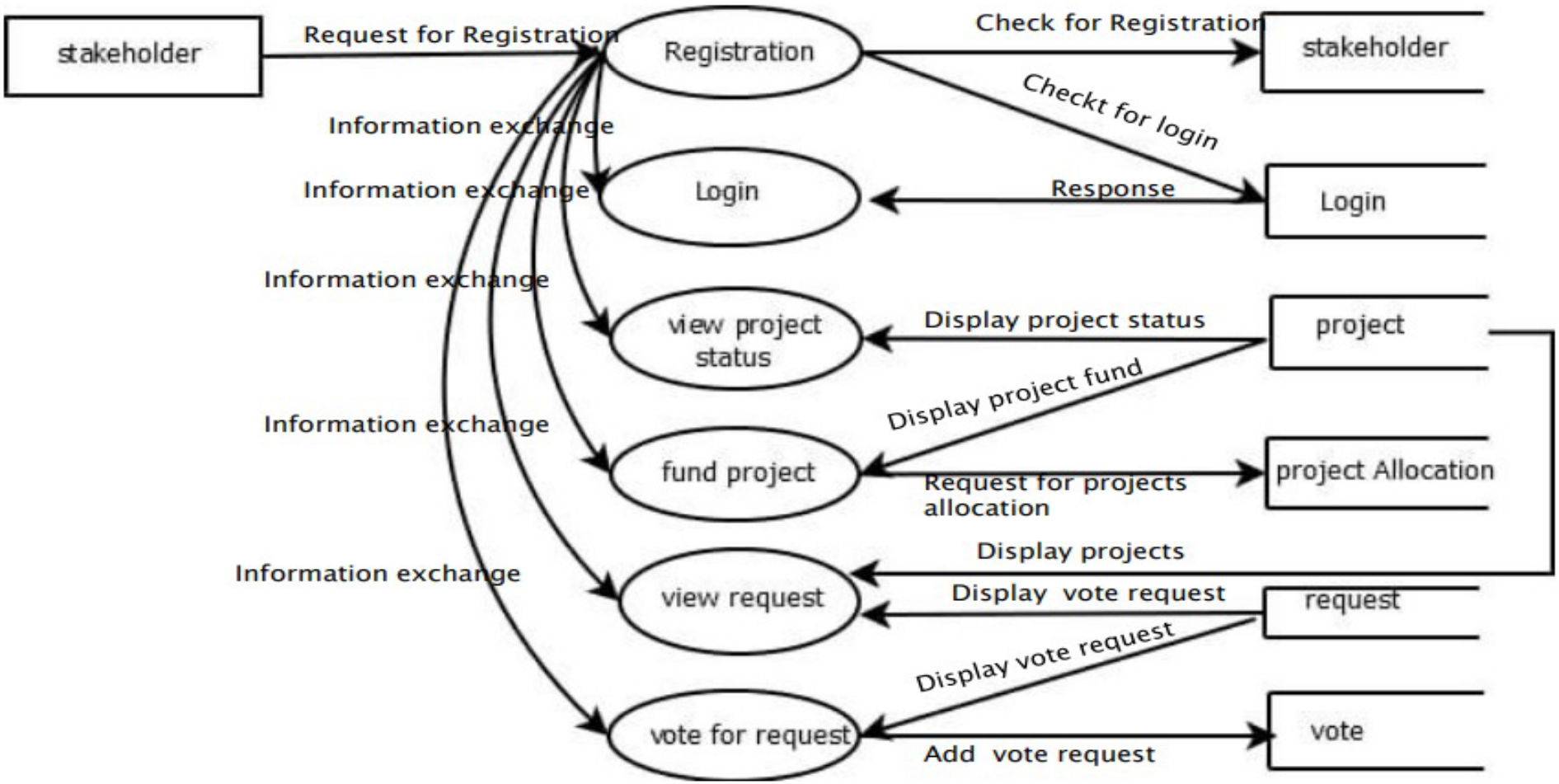
Level 1.



Data folw diagram



Data folw diagram



USER STORIES

User story id	As a<type of user>	I want to	So that I can
1	Admin	Login	Login successful with correct username and password
2	Admin	Manage stakeholder	View stakeholders and accept reject managers
3	Admin	Manage managers	View managers and accept reject managers
4	Admin	Manage projects	Approve or reject project ideas
5	Manager	Registration	Registration by user details
6	Manager	Create new project	Add new project ideas
7	Manager	View project status	View project current status

USER STORIES

User story id	As a<type of user>	I want to	So that I can
8	Manager	Create spending request	Create spending request with amount reason
9	Manager	View status	View status of spending request(accept or reject)
10	Stakeholder	Registration	Registered by using details
11	Stakeholder	login	Login by user name & password
12	Stakeholder	View projectdetails	View project info from manager
13	Stakeholder	Fund project	Send fund amount to a project
14	Stakeholder	View request	View spending request
15	Stakeholder	Vote for request	Accept/reject spending request

PRODUCT BACKLOG

User story id	Priority<High/ Medium/Low>	Size (hours)	Sprit (#)	Status<Planned/in progress/ Completed>	Release date	Release goal
1	Medium	8	1	Completed	1/05/2022	Create table transaction
2	High	10	2	Completed	15/05/2022	View The Transfer amount
3	High	6	3	Completed	28/05/2022	Block chain management , create block chain , truffle management
4	Medium	5		Completed	1/06/2022	Contract creation , blockchain implementation.
5	High	5	4	Completed	5/06/2022	Add & manage blocks to blockchain , create block ,node module , add to block
6	High		5	Completed		Cryptocurrencies exchange through blockchain

PROJECT PLAN

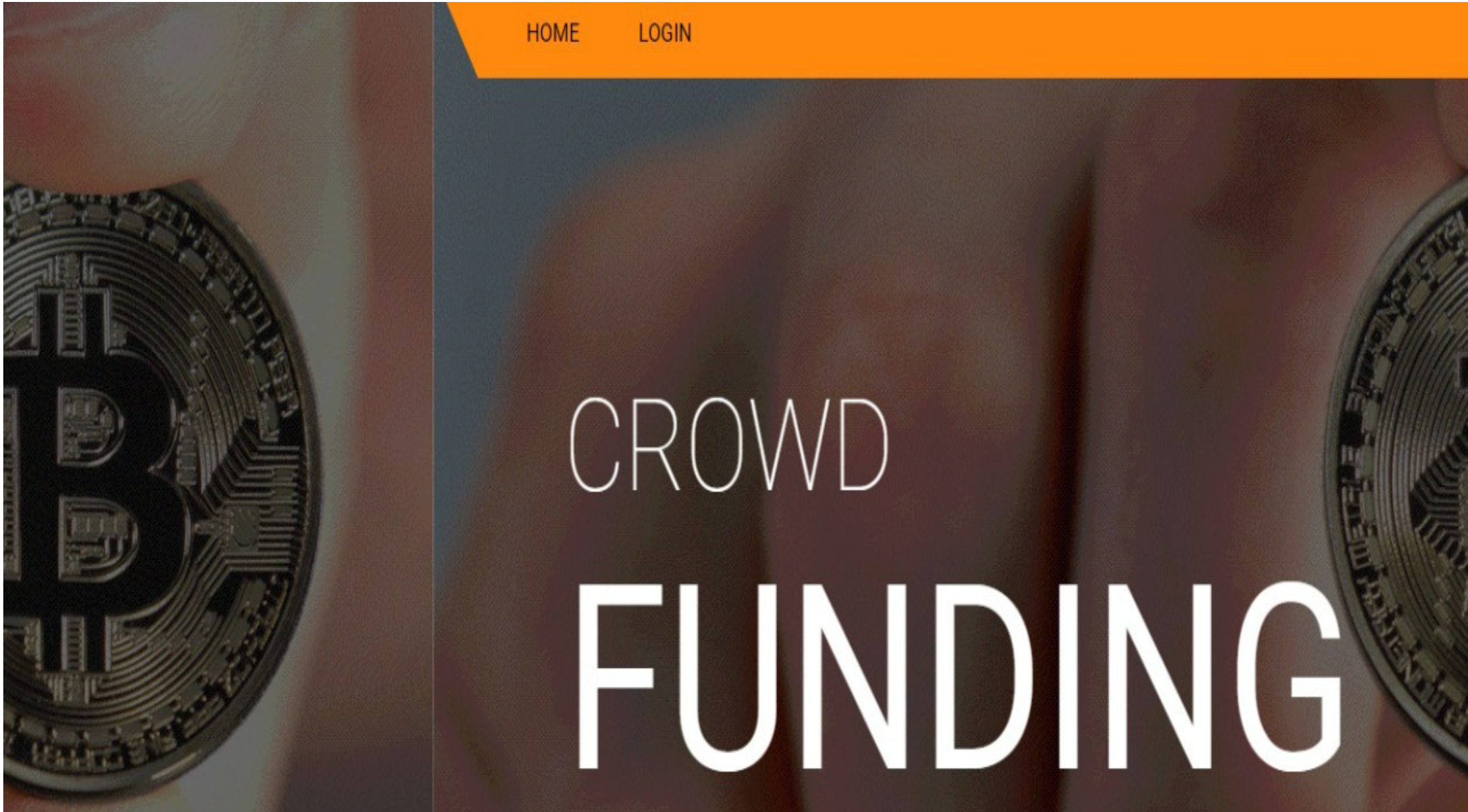
User story id	Task Name	Start date	End date	Hours	Status
1	Sprint 1	20/04/2022	1/05/2022	18	Completed
2	Sprint 2	4/05/2022	15/05/2022		Completed
3	Sprint 3	17/05/2022	28/05/2022	11	Completed
4		29/05/2022	1/06/2022		Completed
5	Sprint 4	2/06/2022	5/06/2022	5	Completed
7	Sprint 5	8/06/2022	10/06/2022	6	Completed

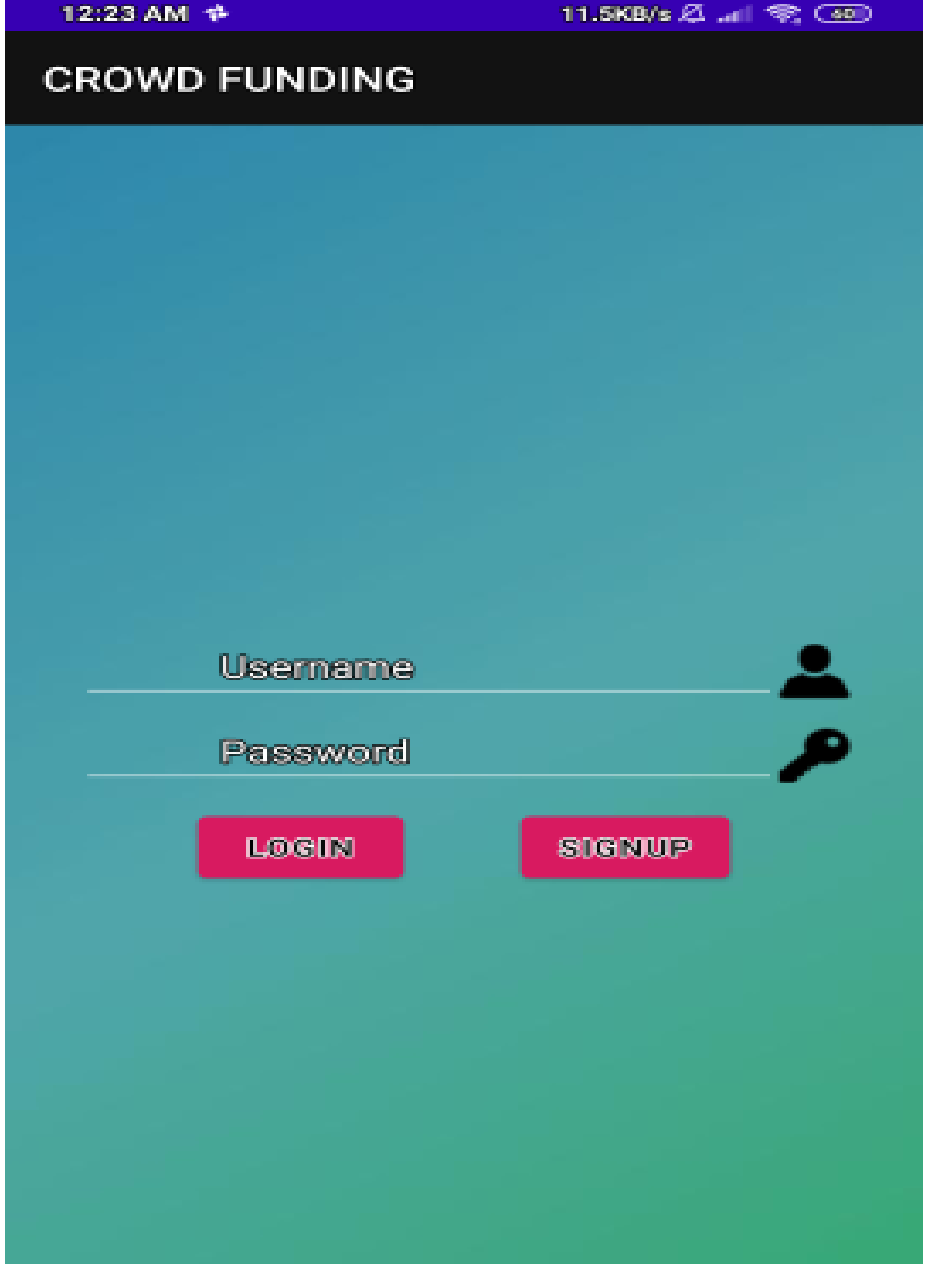
SPRINT BACKLOG PLAN

Backlog Item	Status And Completion Date	Original Estimation in Hours	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7	Day 8	Day 9	Day 10	Day 11	Day 12	Day 13	Day 14
UserStory#1,#2																
Create table transaction	1/05/22	8	1	1	1	2	0	1	1	0	1	0	0	0	0	0
View the transfer amount	15/05/2022	10	1	3	0	1	1	0	1	0	0	3	0	0	0	0
UserStory#3,#4																
Block chain management	28/05/2022	6	1	1	0	1	1	2	0	0	0	0	0	0	0	0
Blockchain implementation	1/06/2022	5	0	4	1	0	0	0	0	0	0	0	0	0	0	0
Add and manage blocks	5/06/2022	3	0	0	0	0	2	1	0	0	0	0	0	0	0	0
UserStory#5																
Cryptocurrencies	10/06/2022	6	0	0	0	0	0	0	0	0	0	0	3	3	0	0

ACTUAL SPRINT

Backlog Item	Status And Completion Date	Original Estimation in Hours	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7	Day 8	Day 9	Day 10	Day 11	Day 12	Day 13	Day 14
UserStory#1,#2																
Create table transaction	1/05/22	8	1	1	1	2	0	1	1	0	1	0	0	0	0	0
View the transfer amount	15/05/2022	10	1	3	0	1	1	0	1	0	0	3	0	0	0	0
UserStory#3,#4																
Block chain management	28/05/2022	6	1	1	0	1	1	2	0	0	0	0	0	0	0	0
Blockchain implementation	1/06/2022	5	0	4	1	0	0	0	0	0	0	0	0	0	0	0
Add and manage blocks	5/06/2022	3	0	0	0	0	2	1	0	0	0	0	0	0	0	0
UserStory#5																
Cryptocurrencies	10/06/2022	6	0	0	0	0	0	0	0	0	0	0	3	3	0	0


HOME
LOGIN
CROWD
FUNDING


12:23 AM
11.5KB/s
CROWD FUNDING
Username
Password
LOGIN
SIGNUP


1:23 PM
0.2KB/s
CROWD FUNDING
VIEW PROJECTS
VOTE REQUEST
REQUEST STATUS
LOGOUT

THANK YOU