BACHELOR OF SCIENCE IN COMPUTER SCIENCE AND ENGINEERING

Decentralized Social Network using Blockchain (Dinke-Din)

Supervised by :

Mohammad Sazid Zaman Khan
Lecturer, Dept. of CSE, IIUC
Department of Computer Science and Engineering , IIUC

Prepared by :

Jamshedul Alam
ID: C171029
Mohammed Raihan
ID: C163069

Submitted To:

Department of Computer Science and Engineering ,
International Islamic University Chittagong
Kumira, Sitakunda, Chittagong – 4318

JAMSHEDUL ALAM (C171029)
MOHAMMED RAIHAN (C163069)

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
B. SC. IN COMPUTER SCIENCE AND ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CSE)
INTERNATIONAL ISLAMIC UNIVERSITY CHITTAGONG (IIUC)
CHITTAGONG, BANGLADESH

DECLARATION

We hereby declare that Dinke-din is our original creation, and we strive to add knowledge to previous Blockchain-based knowledge.

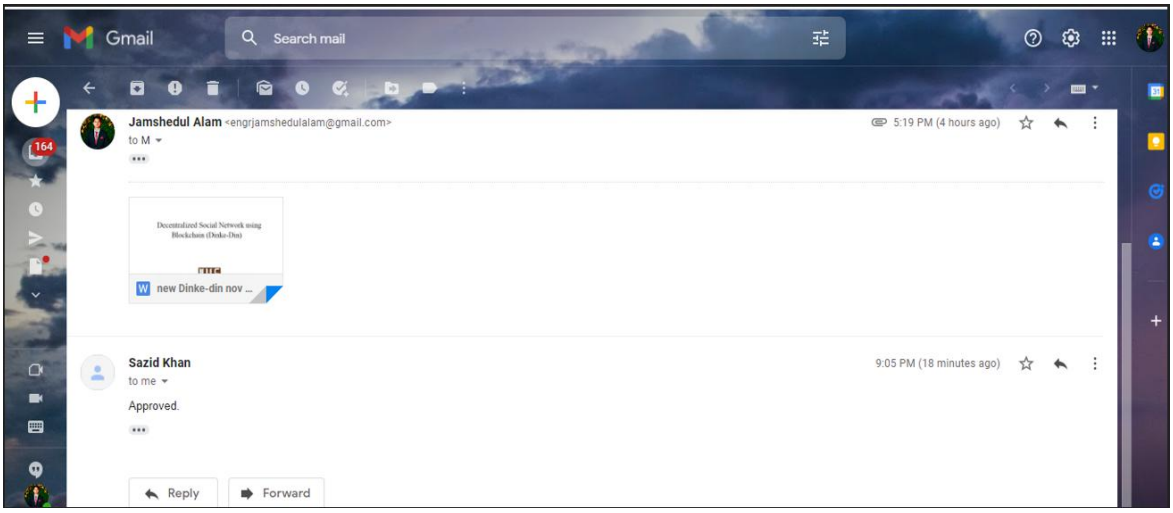
11 November 2021

JAMSHEDUL ALAM
C171029

MOHAMMED RAIHAN
C163069

DECLARATION OF SUPERVISOR

I thus declare that I have read this thesis and that, in my judgment, it is suitable in scope and quality for the award of a Bachelor of Science in Computer Science and Engineering degree.



Date : 11/11/2021

SAZID ZAMAN KHAN
Lecturer, Dept. of CSE, IIUC

DECLARATION ABOUT PROJECT REPORT AND COPYRIGHT

PROJECT TITLE:

Decentralized Social Network using Blockchain (Link-din)

AUTHORS:

SL	NAME	ID	SIGNATURE
i			
ii			
NAME OF SUPERVISOR:Mohammad SAZID ZAMAN KHAN SIGNATURE OF SUPERVISOR:			

We declare

1. Our thesis will be a Open Source Paper for IIUC database store .

2. CSE Department of IIUC also belonging as follows:

i. The thesis is the asset of Department of CSE, IIUC.

ii.The IIUC library has the right to print the paper only on Research purpose .

ACKNOWLEDGEMENT

Thanks to Almighty Allah for giving us Barakah to reach the end of Dinke-din project accomplishment .Without Allah's Barakah it was impossible for us to reach the end of our Dinke-din project .

We feel proud about our Supervisor Sazid Zaman Khan . Who helps to us to become the best version of ourselves .He is very helpful .However , we are grateful to all of the IIUC Teacher , Authority , staffs .

JAMSHEDUL ALAM

MOHAMMED RAIHAN

ABSTRACT

We all heard about Blockchain .But we have a curiosity to calm our mind what is actually Blockchain does ? what it provide to the humanity ? let's comes to the motto of the Blockchain ,"To store the digital data so that not to get modified"[17]. it actually works as a open source database.

In our Dinke-din we are going to explore the Blockchain world so that in social network uses can be safe and it's owner can keep the data in safe .We all are familiar with sharing post to social media .We all feel insecure about data that we are sharing to the online social network (OSN) system.What will happen to our life if any of the data are hacked or modified or shared to any corrupt person .Then our daily life's becomes a hard one to live .Dinke-din is the place where we explore the Blockchain and it's most eye charming technology IPFS(Inter Planetary File system). In the Dinke-din , we used the Blockchain hash ,the most buzzing word we always listen to secure the data , is like fingerprint for digital data [17]. In our Dinke-din we uses different hashing algorithm.

Index of Dinke-din

CHAPTER I

INTRODUCTION

1.1 BACKGROUND OF THE DINKE-DIN PROJECT

Online social networks have exploded in popularity, allowing users to exchange images, videos, and other content with their peers. Facebook, for example, has more than two billion members.

At the same time, consumer's privacy in online social networks(OSN) has been discovered to be easily compromised . Although members of Online Social Networks (OSN) can alter privacy settings to limit who has access and who does not, We don't have any effective technical solutions to provide access or prevent them from disclosing user data to third parties in this case. The New York Times reported in March 2018 that a business fraudulently got information from more than 50 million Facebook users .[19] The primary cause of these incidents is that present OSN's with centralized structures can completely comprehend all user data..

The solution is a decentralized online social network based on Blockchain (OSN).

1.2 PROBLEM STATEMENT

When we post content to an OSN, we worry that our account will be hacked or blocked, and we'll lose all control over it. The most pressing concern on our minds is how to keep our data safe. Instead of giving the main copy of data to OSN, what if we

had a system where we stored data and just gave OSN system an authorized hash value?.

1.3 MOTIVATION

From professional to social worker , every one are uses social network . We all are there for long time and our most of the data are in social network not safe . Nowadays hacker and evil personality in the social network have been increased at a alarming rate . What if we in such social network where we will have a shared cloud system to store the users data and full system data .What if we are not dependent on the centralization of the Social network storage rather we are thinking about decentralize system .if we can make a dapps where users data will not be stored in the direct storage of owner of social network.

1.4 OBJECTIVE OF DINKE-DIN

1. The purpose of this Social Network is to safeguard an OSN user's personal data from being accessed and being lost in the OSN platform.

The following are the desired goals:

1.1. Protecting User Account .

1.2. To keep personal data access as secure as possible.

1.3. To store all resources in a separate cloud storage, the OSN will communicate with that cloud storage to retrieve the desired data based on the user's rights and public key.

Organization of the Dinke-din

Chapter One :

In this components , we demonstration a big picture of our Dinke-din , why we choose this topics and why we make dinke-din as our final project . We discuss about the background of our dinke-din . In there we talk about why dinke-din can be the ultimate solution of our problem that try to solve in this project .

Chapter two :

To make our statement more strong and to find proper background of existing work , we discuss about lots of existing work like us. We compared each of them with ours dinke-din and find the limitation. We studied about Blockchain , Image encryption , IPFS blockchain technology uses in different software. We also have great discussion here about Decentralized system .

Chapter Three :

In the previous chapter we have conversation and mining about the existing work that exist. After that we have to come up with the specific requirements of the Dinke-din . To answer the question of what should be the requirements of Dinke-din and How we overcome the limitations of the Existing work .

Chapter four:

As we specified the requirements , now we need a methodology to make the project executable . We choose spiral model as Software development life cycle . We dig deep on the question of How right software development model have big impact on the Dinke-din project creation .

Chapter five :

In this part of the Dinke-din report components , As we fixed spiral model as software development life cycle , Now we have to design our systems different parts elements .Like All heard about facebook system design and whatsapp system design. In there we design a workable system to make Dinke-din work in real life . We design Restful API for our Dinke-din and also design our systems User panel , Dinke-din Owner Panel and other part of the Dinke-din .

Chapter SIx:

As we successfully design our Dinke-din system , now it's time for Implementing the system .In this stage we create the website front-end with JavaScript Library React js , to handshake with the blockchain we uses Solidity with web3.js . To make a back-end of the

Dinke-din we uses PHP framework Laravel . After the implementation of the system we check every corner case of the Dinke-din to overcome the failure of the Dinke-din . We use multiple test cases to check whether our project is optimized and efficient or will cause problem in the future .

Chapter Seven :

In this components , we conclude the Dinke-din project with having conversation about contribution of work and what we are planning to add new feature in the upcoming future .

CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

The first step in our Dinke-din would be the literature review. We have to carry out the Literature survey of others project to find out what others have been done on the same theme of the Dinke-din and identify the gaps and what to do next .

It helps us :

1 . To see how our research work is original and provides something new .

2 .To make sure that our work isn't redundant or merely reproducing knowledge that's already been done by others .

2.1 EXISTING WORK REVIEW

Traffic Police Assistant System[1] is a Blockchain based system used India . It offers several features of protecting the Traffic data and other handy data. But It fails to reduce the cost of implementing and designing smart contract . which is an important part of an Blockchain based system.

Medical image sharing system [2] Blockchain based image sharing system . It has features like zero trust principles, role based authentication etc. It also offers data encryption features. Since each transaction requires peer-to-peer verification , it becomes time consuming especially in a public Blockchain with many nodes .

IdM system [3] is based on Single Sign-On services . SP validates the identity and credentials with an Idp , preventing the user needs to enter it's identifier and password to access the services. But it has some authentication layer left risky.

Decentralized Copyright Protection system [4] is based on decentalised concept of Blockchain . If any one rotate , crop or gray the image to avoid the copyright validation , and upload the image to system , it will detect the copyright violation . But it is not storing the user data a compormise database.

Patient Centric Image Management [5] , it enables the patient to sharing and storing a big medical data in a trustless environment . It uses the IPFS to storing image for decentralized storage . But it has some lack in authentication of patient in this system.

Industrial Image security [6] is all about peer-to-peer image sharing system .it actually detect if anyone modify the image frames compression and change frame speed manupulaiton . In the contraty to us it uses pHash in their system.

Internet of vehicles [7] is system(IoV) to improved traffic safety in road using Blockchain technology . It has features to send messages in real time . it will reward the block generator by crytocurrency . But it has misses the uses of IPFS in the system.

Color Image encryption [8] , it uses Henon-zigzag map and chaotic restricted Boltzmann (CRBM) to encrypt the image data .it uses Henon-zigzag to get 2 new pseudo random number sequence which are provided by Henon map . But we recommend for uses of IPFS to encrypt the image.

Fast Image encryption system [9] uses the permutation and diffusion to encrypt the image .they used permutation algorithms including sorting-based permutation algorithm .They emphaiss on using of parrallelism of diffusion to get quality full result on image encryption .

Medical Image encryption [10] system encode the plain image message in elliptic curve coordinate by kolitz encoding algorithm . it has some problem in image data expansion issue .

Digital Image watermarking by phase shifting interferometry [11] it also uses authentication system to protect unauthorized reveivers to get the shared image .It uses interferograms and hidden the image from users .it uses specific algorithm to get the image owner . It is can be used only on remote secret transmission of data via the internet . In our Dinke-din we uses IPFS to secure our image which is more suitable for a user.

Virtual disk based centralized enterprise management [12] it uses distributed ,diskless and centralized data management .theier paradigm was a system without disk and use of decentralition concept .But didn't uses the Blockchain system to make the system decentralized .

Blockchain-based image stenography for COVID-19 data [13], it uses Blockchain PSO algorithm and hash function to protect the image data and covid-19 data from malicious user . In this system they have 3 phases like pre-hiding , data-hiding and 3rd Transmission phase . it uses hash funciton to hide secret medical COVID-19 data from hospital platform .

jPeg-Blockchain for Glam services [14] it uses a special Blockchain framework to protect the image in decentralized way . They used low bit-rate compression to check

every Blockchain record which are linked to a unique transaction hash. Where we used IPFS in our Dinke-din system .

Tweetchain [15] it actually same as Blockchain application .This paper try to overcome some drawbacks of blockchian .They try to use meshed chain in their system .they used proof of concept instead of verified by miners what we mostly used in Blockchain system.

2.2 LIMITATION OF THE EXISTING WORKS

1. Most of the applications have Complexity in using Image encryption and decentralization the system .They have some problem in implementing decentralized system successfully in their system .As a example some of the system uses different algorithm to decentralized the system .

2. They have limitations in combining authentication and Blockchain in same system.From our Study we found that a lot of good working system doesn't implement user authentication in blockchian system .They ignore the Authentication of a user in the system .

3. Some of the existing Application are not with full social Network system. Most of the system are mainly focused on providing a secure system on their own system. They mostly ignore the question , what if a malicious user are going to enter in the system and take control of the system .

2.3 PROBLEMS THAT ARE FOCUSED FROM STUDY

1. This system needs a cloud system where any user's post can be stored in database system . From where a OSN provider securely pull the request of the data for OSN system.

2. In the Application real-time data showing and posting to cloud with same time posting it to ipfs Blockchain is must need . which will make the OSN more user-friendly.

3. A well-secured authentication and data security is needed fo better data safeguarding .

2.4 SUMMARY

After mining the research paper about Dinke-din ,we got some interesting information between Dinke-din and other previous work:

- The basic security layer's is a Must have thing.
- The main limitations of previous Blockchain based system that must have to overcome.
- After the brief study , we finally figure out our OSN system's features.

CHAPTER III

REQUIREMENT SPECIFICATION & ANALYSIS

Requirement Analysis is very critical to the success or failure of a software project. It enables our team to figure out full process to reach the end of the project .As it is very important to create a good set of requirements to ensure that project have a good chance of success .

We have to think about some point in this stage:

1) Will this requirement be too big??

2) How likely that it'll take too long to achieve ?

3) How likely is it that it will not be possible ?

4) How likely that it won't be very reliable?

3.1 Dinke-din Requirements Analysis from Existing OSN

From our literature review and study of similar project paper we got some Requirements to fulfill to overcome the limitaitons of the existing project. In our Dinke-din we try to overcome the limitaitons . In lots of case we saw that our digital Image encryption is not secure enough . We overcome this problem by Using IPFS which is a Blockchain technology to encrypt the digital image .Most of the image stored in the digital platform are also not safe .IPFS aslo solve this problem too.

We overcome the problem of account security , As we Import the account from the Blockchian from Ganache with a Private key . Those Private key's privacy level is so high. We also implement a cloud storage compromised by user and Dinke-din owner to secure the data in Dinke-din system .

3.2.1 User functionality

- OSN User
- Administrator

3.3 SYSTEM REQUIREMENTS

- Our Dinke-din are developed in web Application.
- As we create back-end API it can be also implement in any native application

3.3.1 Web Application

1) Solidity (Programming language for Decentralize app development)
2) Laravel (Framework for back-end API building)
3) React js (JavaScript framework for front-end development)

3.3.2 Database for the System

1) PhpMyAdmin(Sql)

3.4 FEASIBILITY STUDY

Feasibility study keeps us from expending time and racecourses on a project which we will be unable to successfully completed .it helps us to think carefully before

deciding to start the project . it is similar to the most used proverb for decision making the - look before leap .In this stages we have to find answers of few questions such as :

1. Can it be done?

2. Will it be acceptable?

3. What are the alternatives?

4. Is it affordable ?

Economic Feasibility:

Our Dinke-din is in affordable .

- A user can afford the cost to participate in the smart contract .
- We used here ether-um .

Technical Feasibility:

The technical viability of our project relates to whether the project is likely to succeed or is too difficult to attempt. This may depend on how easy the materials are to work with or if there are weaknesses in the design or engineering of our project, is the technical aspects.

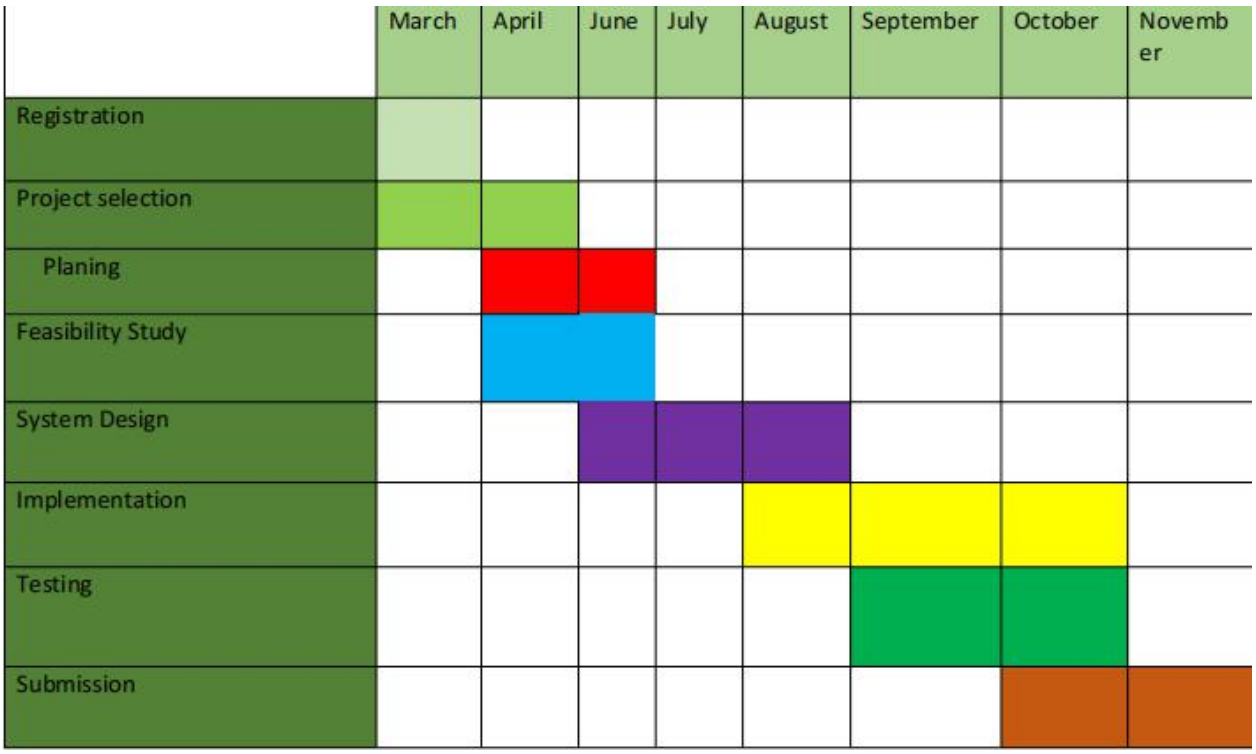
Operational Feasibility:

This is about how a selected framework will be survive in the challenges and How it will beneficiary to our project.

Schedule Feasibility:

We try our best to ensure that our deadline of our specific task wasn't missed . We try to use Force efficiency to meet the deadline of the project work .

Gantt Chart of Thesis/Project



CHAPTER IV

METHODOLOGY

A software development methodology is similar to a cooking recipe. A software development methodology, like a recipe, tells Us how to build a software. The ultimate goal of software methodology is to create high-quality, maintainable software in a reasonable time frame and at a reasonable cost. A successful software development methodology describes how all of our tools, techniques, and practices work together to create a winning Project.

4.1 PROCESS MODEL

Software process have to include main functionalities of the software and the constrains (Specification) .Software needs to be designed and programmed . A software must meet the specifications and to cope up in the software competion we need to evaluate our software .

4.2 DIFFERENT SOFTWARE PROCESS MODELS

1. Waterfall Model.
2. V-model
3. Iterative and Incremental Model
4. Spiral Model

5. Iterative Development Model
6. Agile Model
7. Big Bang Model
8. DevOps Model

4.3 WHY WE CHOOSE SPIRAL MODEL (SDM) ?

The spiral model combines iterative project development from evolutionary implementation of a prototype model with the systematic and controlled features of the sequential waterfall model. The spiral model is better suited for large-scale projects that require consistent improvement and refinement with each iteration around the spiral.The output of one iteration's specific activities is a small proof-of-concept (POC) prototype, which is part of the larger software and is used to gather user feedback. The same activities are repeated in subsequent spirals, with refinement of the POC prototype, to produce a working model of the software called build with a version ID/number. Each version ohf the build is distributed to users in order to gather feedback for future enhancements in the next version until the final system is developed.

The difficulty in calculating the Gas price, the cost of running a smart contract on a public Blockchain such as the Ethereum platform, is particularly high for large-scale projects with complex smart contract coding.

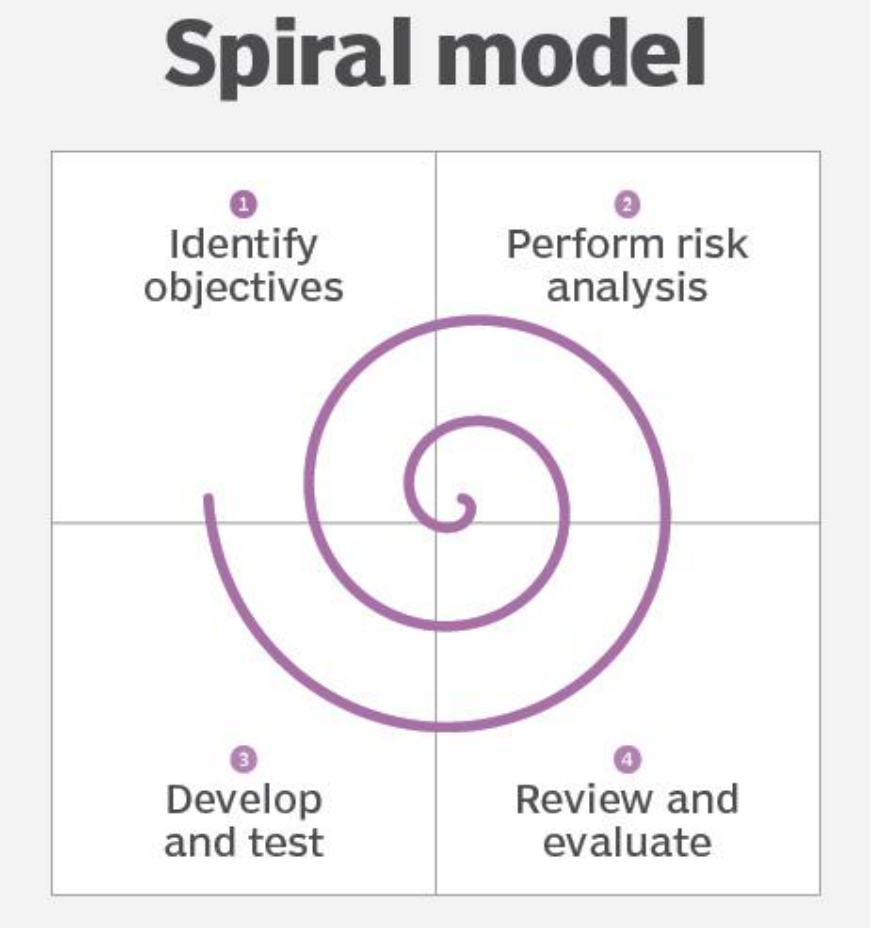


Figure4.1 Spiral Model

4.4 SPIRAL MODEL IMPLEMENTATION

As we used spiral approach in our project. We completed the phases properly one after another to avoid conflict in development. The phases are described below in detail:

4.4.1 Requirements

It is the primary period of the development where every one of the prerequisites accumulated and documented. For our project we have examined previous related systems and the users. After that we have finalized our system features.

4.4.2 Design

As we are finished the testing and requirement analysis of our project .Now it's time for designing's the front-end part . In that stage we use React js , the JavaScript framework , to develop a dynamic front-end part. To make our project eye catching we used Material UI , Bootstrap, React js Styled Components to style different parts of page components .

4.4.3 Implementation

As we achieving the product requirements and design , It's time for starting our implementation or development stage in web development terminology we can say we are now going to Back-end system development.

In this phase we strictly follow the spiral model . It helps us to be on track of project requirement and takes us to next steps. We hard coded a function and then test it and optimize it and then we this function for our final figured function .

We implement user backend using solidity and web3.js and admin back-end using Laravel with phpMyAdmin .

4.4.4 Testing

As testing is very important for Sdlc model . We first test our wallet connection by Ethereum Tester and Ganache .In Blockchain as everything is node , we node test to keep everything smooth. For Admin Backend we Test our Api .

We observe every error and failed response in our project . Then we debug it and also pay attention to corner stage for which the error are causing.

We also checked our project using White Box testing and Truffle Migration testing in white box approach .We will presenting system testing in chapter 6 'System Implementation and Testing".

4.4.5 Deployment

As we are now in the Deployment stage , we previously debug and log to console bar to detect any hiding error. And Then Now our project is ready for Deployment.Once it is Deployed to production ,Now It is ready for everyone to use in website .

4.4.6 Review & Maintenance

We regularly keep an eye on Maintenance so that we can provide our visitors with the best possible user experience.keeping Updated with valuable information, fixing broken links, removing duplicate pages to boost our website traffic.

Figure 4.2 Spiral Model for Software Development

4.5 LIMITATIONS OF SPIRAL MODEL

There are some limitations of using Spiral model in porject -

1) Difficulty in time management. As the number of phases is unknown at the start of the project, so time estimation is very difficult.

2) A large number of intermediate stages necessitate an abundance of documentation.

3) Spiral development is best suited for large projects and necessitates risk assessment expertise.

CHAPTER V

SYSTEM ANALYS7IS

5.1 DINKE-DIN SYSTEM ANALYSIS

System analysis is the technique of studying a system or its components in order to identify its objectives. .A system is a special design that is physical and functional need. System analysis is performed to investigate a system or its elements of the system in order to determine its goals.

5.2 DATA FLOW OF DINKE-DIN APP

Data flow is which is the way of sending data to server and receive them to android application. The process is figured out below:

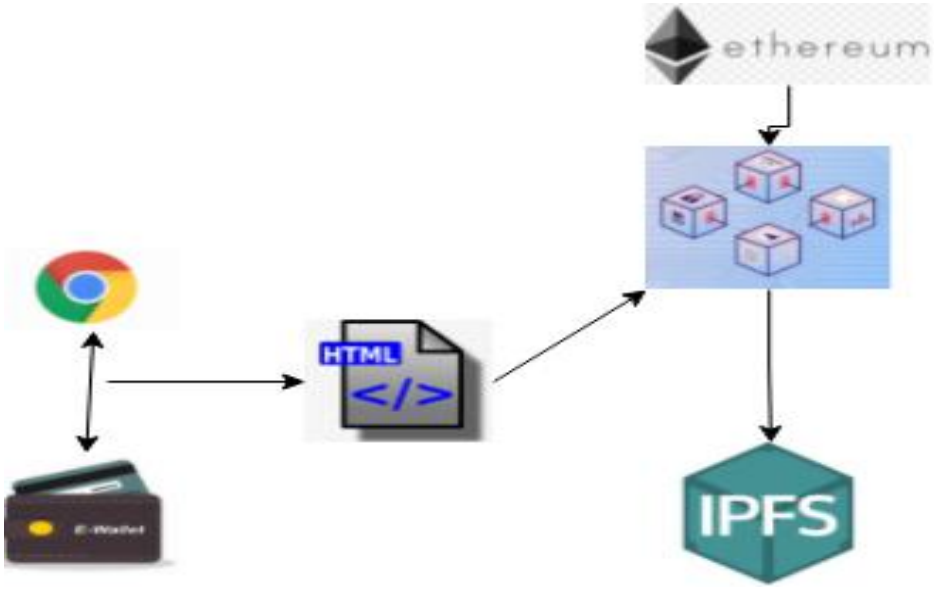


Figure 5.1: System Data Flow of Decentralized Social Network

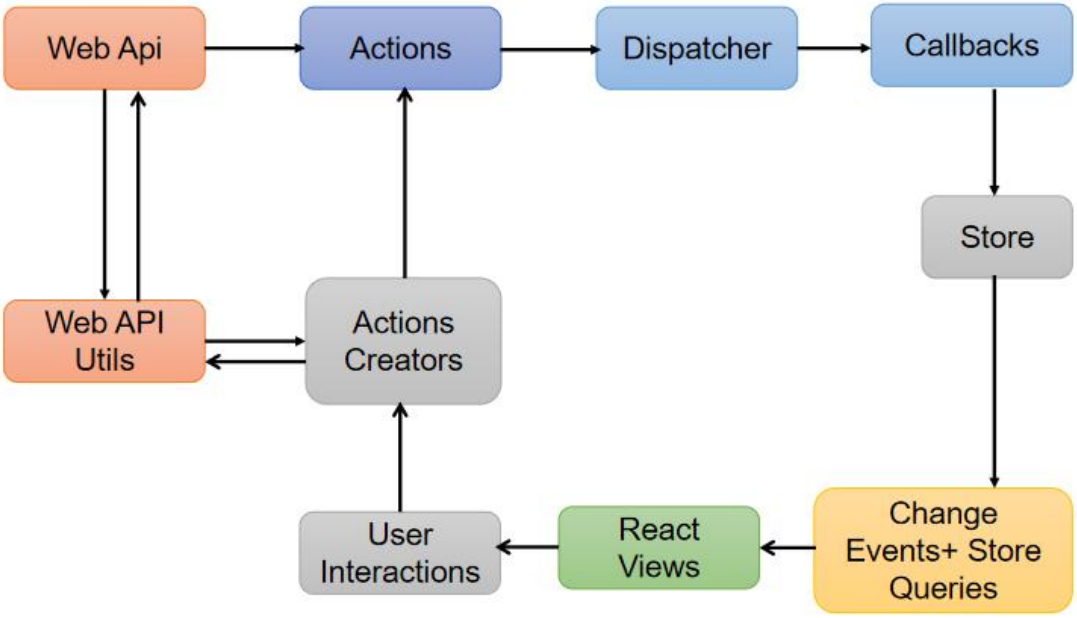


Figure 5.2: General Model of Software Design Process of Dinke-din

5.3 DATA VIEW

In Our Dapps we show post of user using grid view. In a post there is two part one is text and other is image .As we request for user data , then the post of every user will be appeared in Grid view. In our Dapps we followed a excellent view of post so that grid view will be responsible.

5.4 SECURITY

In our Dapps we try to maintain best security practices. When ever a user try to post he/she must have to pay some gas fee and he must have to be connected with his meta mask Ethereum wallet. So if any user will not connect his meta mask account he will not get the facility to post and even unable to see the post of others. We store the User Post data to IPFS(Interplanetary File System) [18] to secure the user Shared data .And IPFS will not give the main copy of the data rather it will give it a url hash

value which is generated by IPFS system. To secure the user data to be shared by OSN system admin we used JSON Web Token (JWT) . Whenever a OSN admin pull all user data he/she must have to show a badge given the jwt authentication system . If he shared the data and jwt token to others ,the surprising part of jwt token is that in every different login a different token will be given to admin .So there is no benefit of sharing every data to others, other's will not get the data.

5.5 VERSION SUPPORT

As we building this website with the help of framework , we try to keep up to date of our every frameworks version up to date. Laravel 8, and solidity 0.5.0 version and web3.js version are supported by most of the web browser.

5.8 FLOW CHART DIAGRAM

5.8.1 Flow Chart Diagram for Posts List

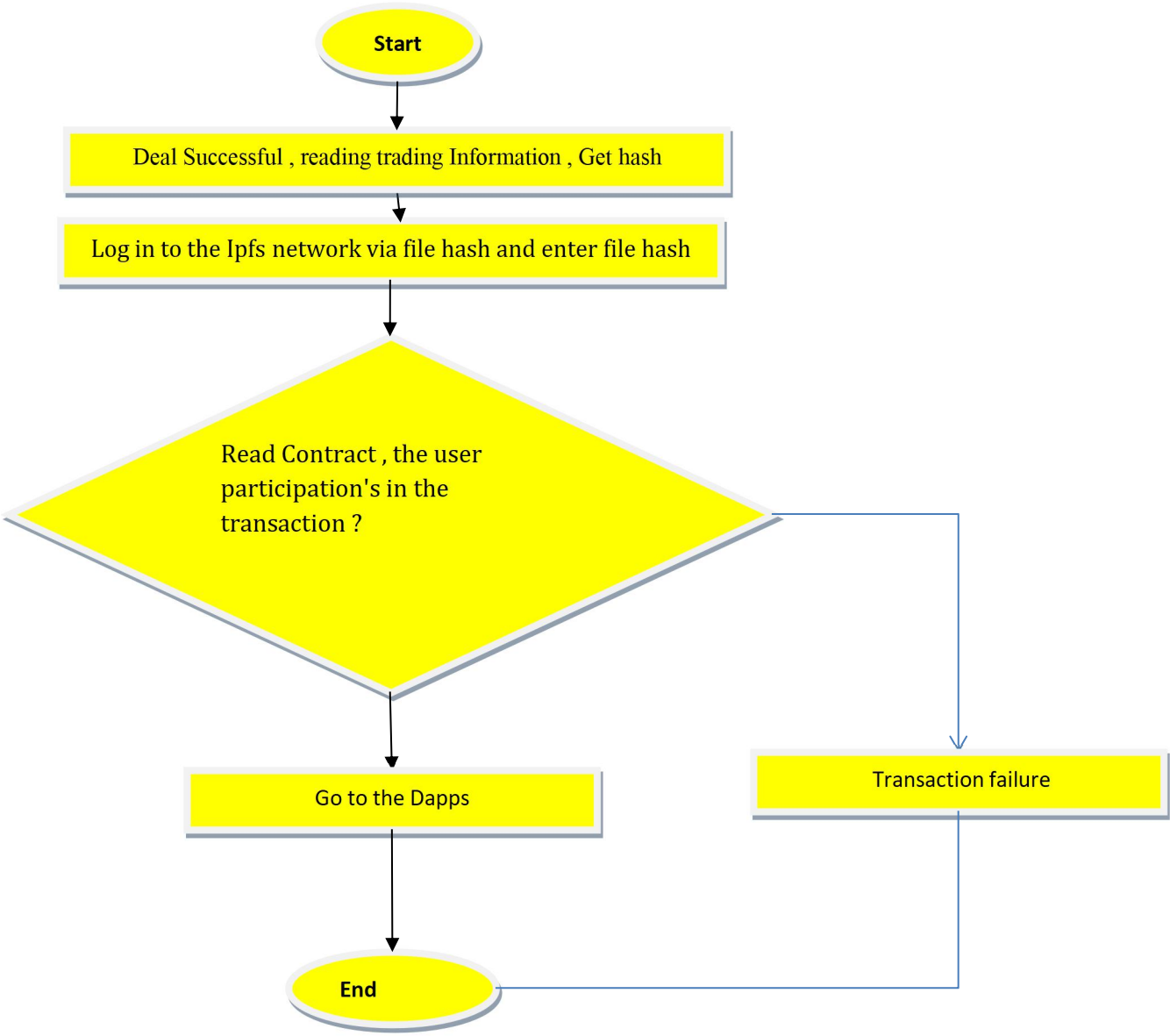


Figure 5.3: User Activity diagram of the system.

5.8.2 Flow Chart Diagram for User Posting panel

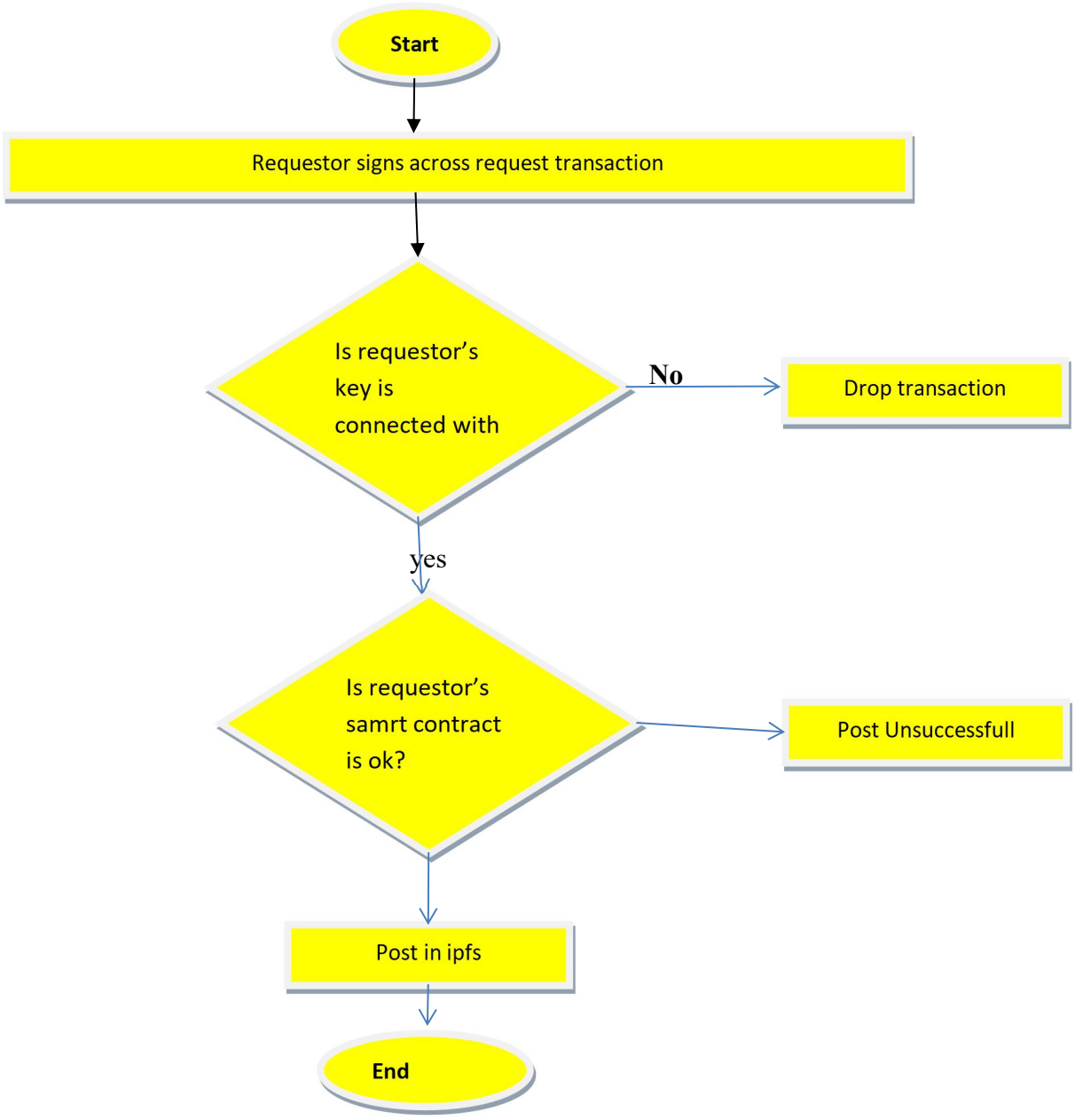


Figure 5.4:User Posting Activity diagram of the system.

5.8.3 Flow Chart Diagram for Admin Panel

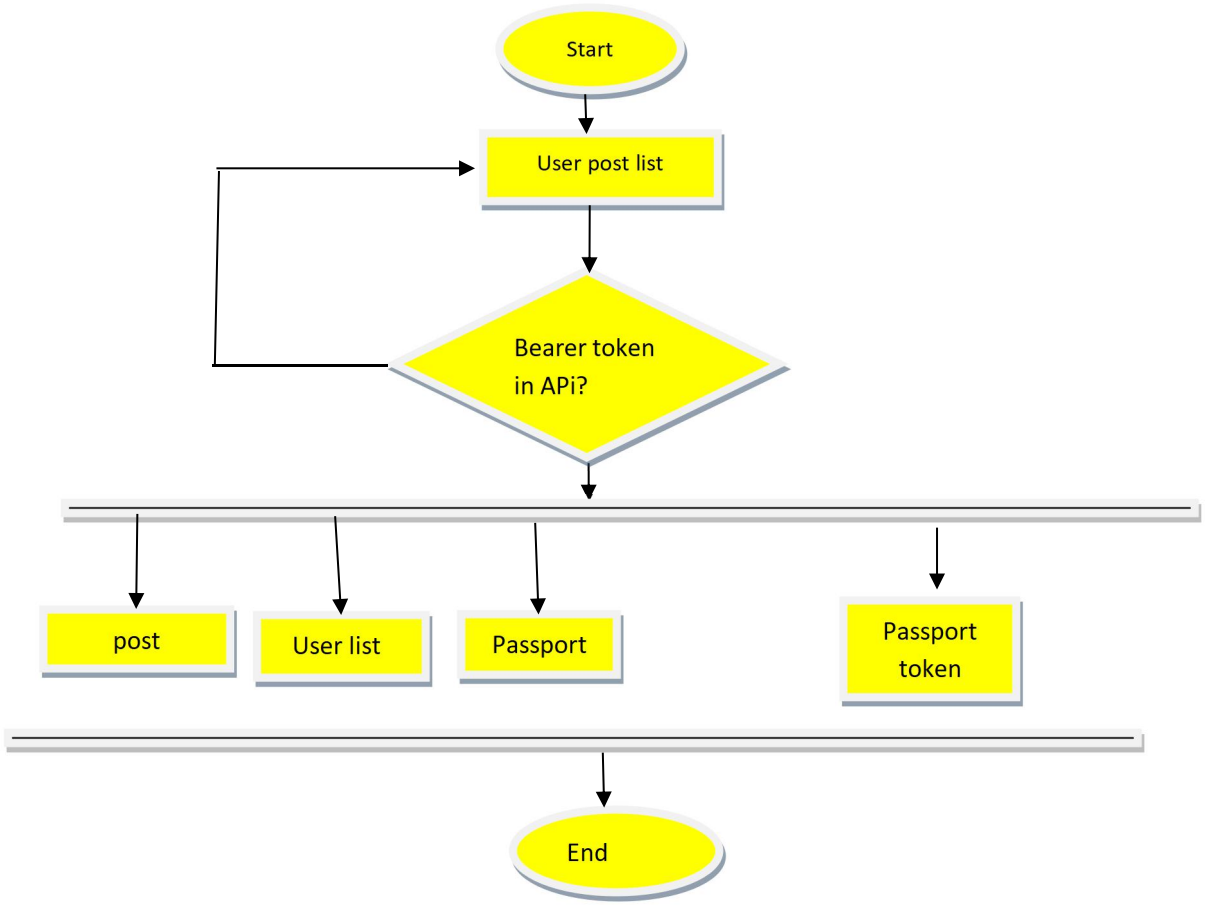


Figure 5.5: Admin Activity diagram of the system.

5.9 USE CASE DIAGRAM

5.9.1 Use Case Diagram for Post Insert Panel

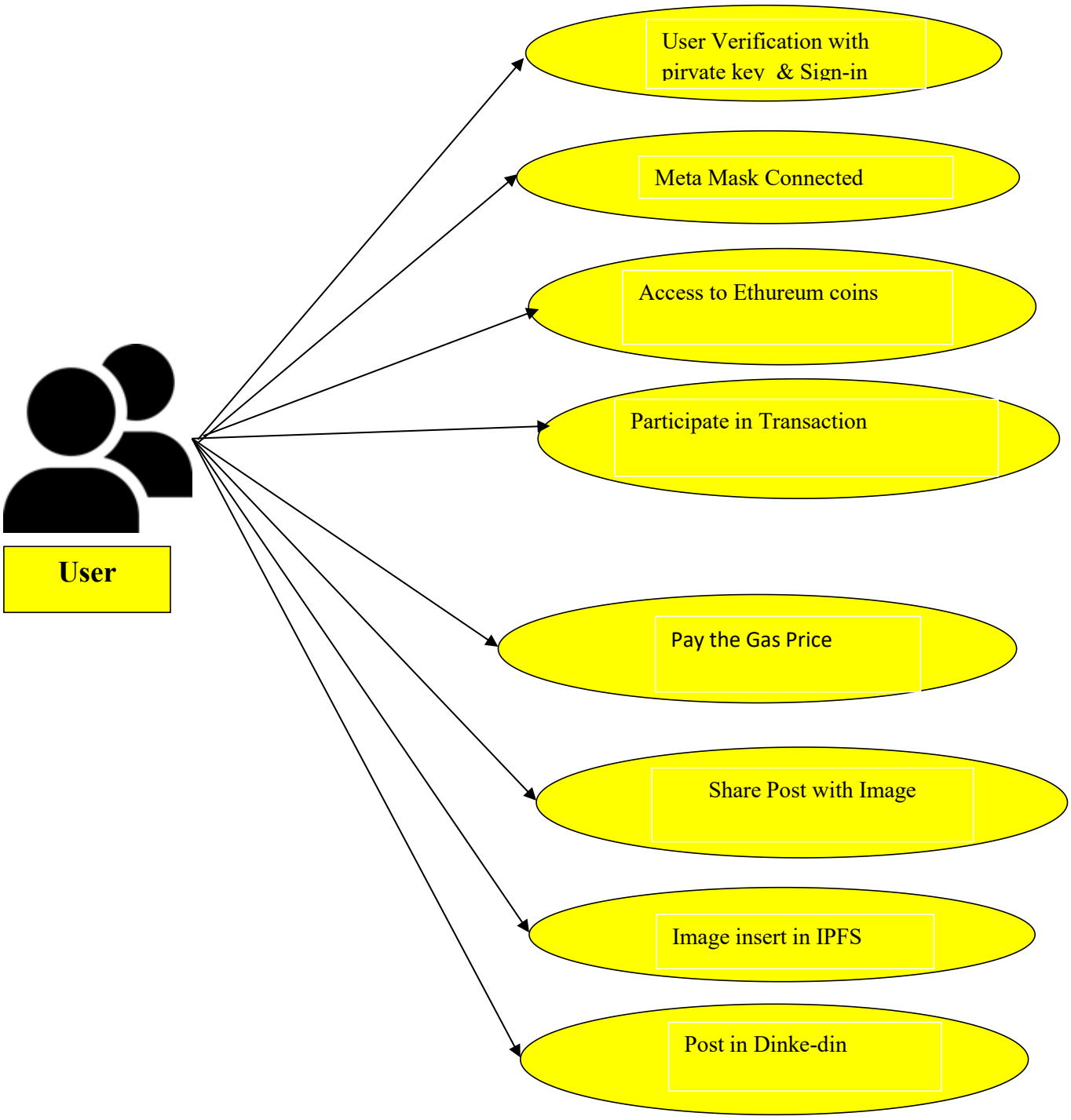


Figure 5.6: Use Case for Dinke-din User

5.9.3 Use Case Diagram for Dinke-din Admin

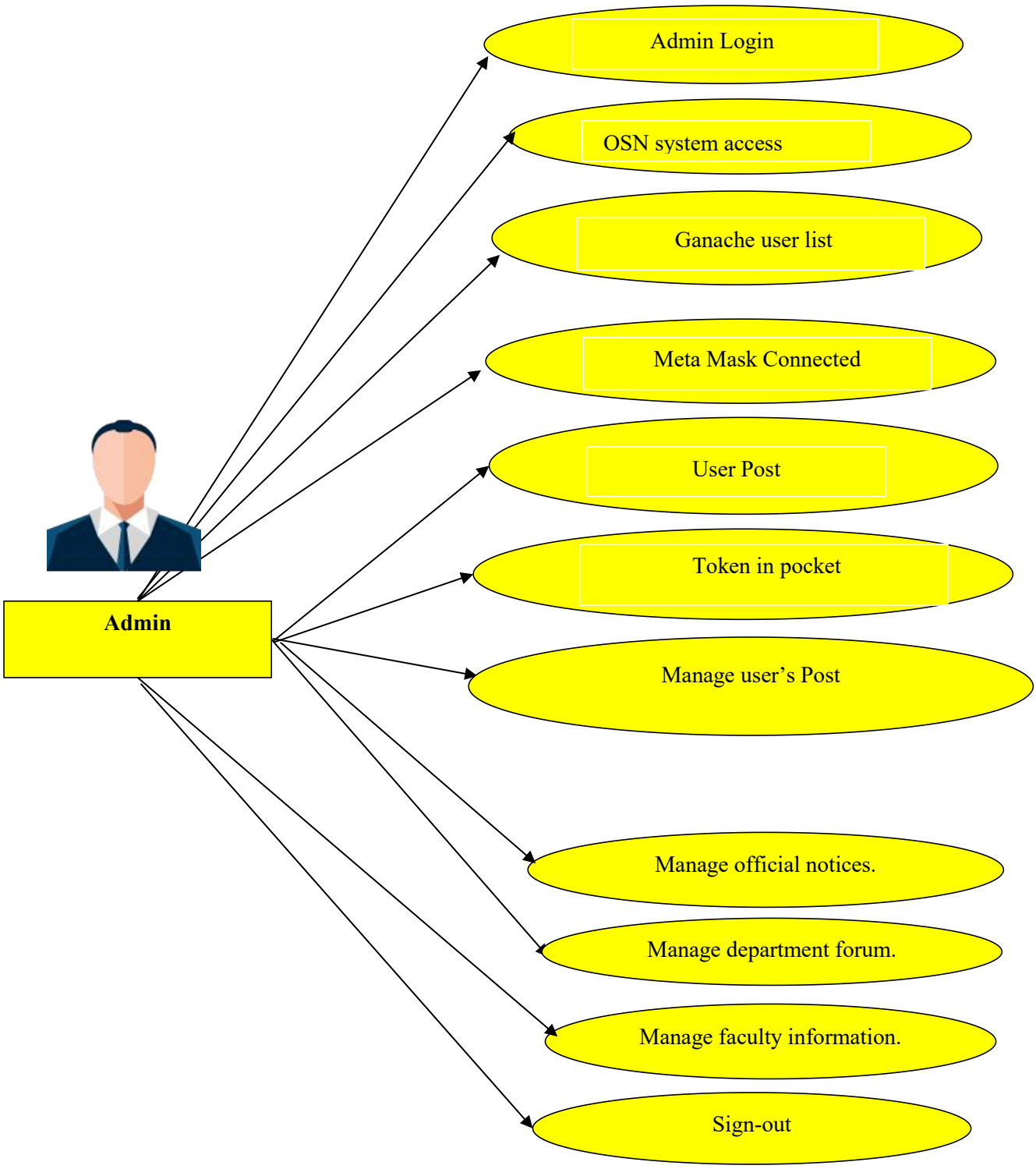


Figure 5.7: Use Case diagram for Admin

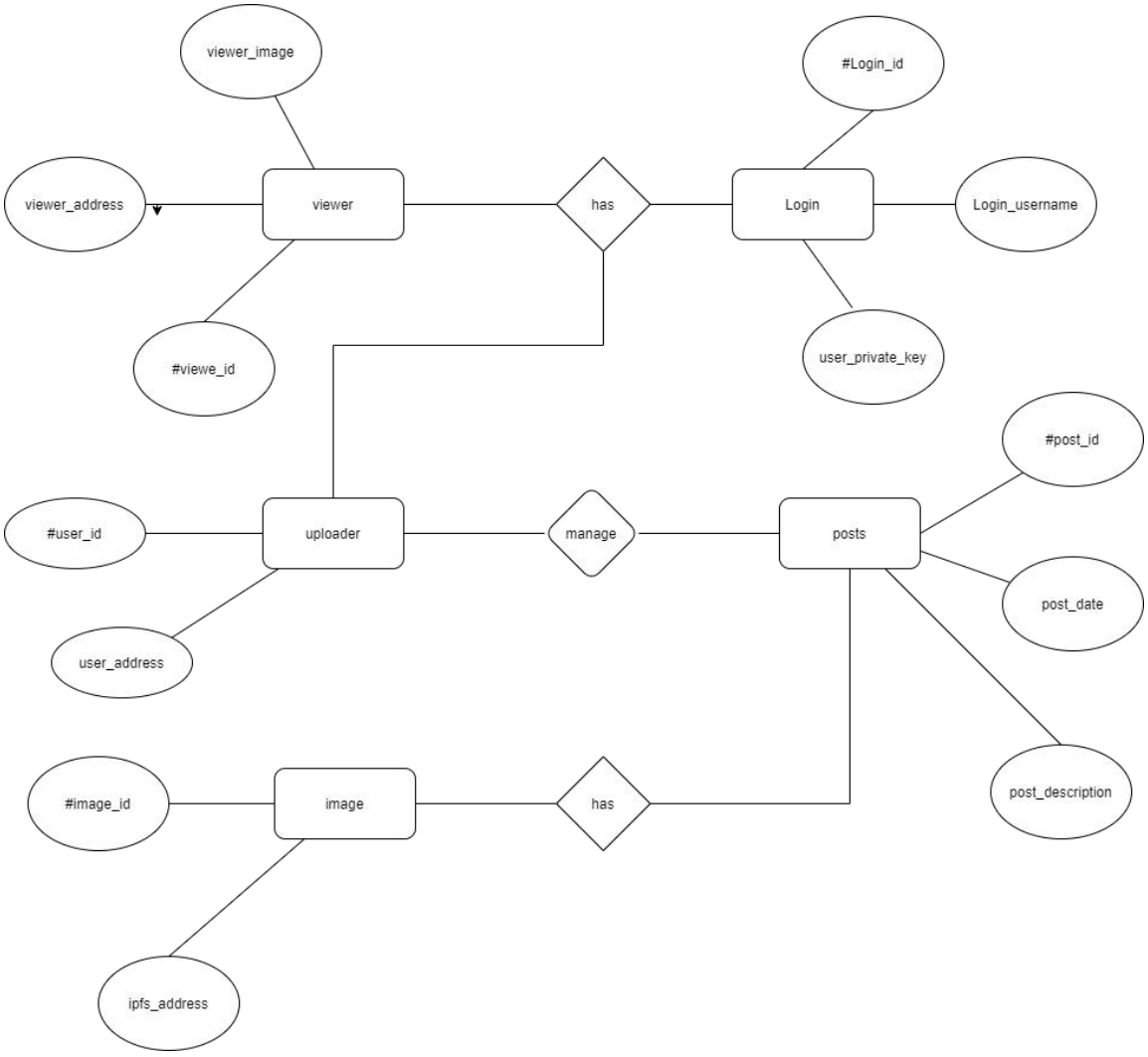


Figure 5.8: Entity Relationship Diagram

5.10.1 Logical Schema

- admin (id, name , email, password , Bearer Token)
- User (id, name , email, email_verified_at , password , remember token , created at , updated at)
- Post(id, user_id , title , image , created at , updated at)

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	id	bigint(20)		UNSIGNED	No	None		AUTO_INCREMENT	Change Drop More
2	name	varchar(255)	utf8mb4_unicode_ci		No	None			Change Drop More
3	email	varchar(255)	utf8mb4_unicode_ci		No	None			Change Drop More
4	email_verified_at	timestamp			Yes	NULL			Change Drop More
5	password	varchar(255)	utf8mb4_unicode_ci		No	None			Change Drop More
6	remember_token	varchar(100)	utf8mb4_unicode_ci		Yes	NULL			Change Drop More
7	created_at	timestamp			Yes	NULL			Change Drop More
8	updated_at	timestamp			Yes	NULL			Change Drop More

Fig 5.9 : Table (Admin)

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	id	bigint(20)		UNSIGNED	No	None		AUTO_INCREMENT	Change Drop More
2	user_id	varchar(255)	utf8mb4_unicode_ci		No	None			Change Drop More
3	title	varchar(255)	utf8mb4_unicode_ci		No	None			Change Drop More
4	image	varchar(255)	utf8mb4_unicode_ci		No	None			Change Drop More
5	created_at	timestamp			Yes	NULL			Change Drop More
6	updated_at	timestamp			Yes	NULL			Change Drop More

Fig 5.10 : Table (Posts)

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	id	bigint(20)		UNSIGNED	No	None		AUTO_INCREMENT	Change Drop More
2	tokenable_type	varchar(255)	utf8mb4_unicode_ci		No	None			Change Drop More
3	tokenable_id	bigint(20)		UNSIGNED	No	None			Change Drop More
4	name	varchar(255)	utf8mb4_unicode_ci		No	None			Change Drop More
5	token	varchar(64)	utf8mb4_unicode_ci		No	None			Change Drop More
6	abilities	text	utf8mb4_unicode_ci		Yes	NULL			Change Drop More
7	last_used_at	timestamp			Yes	NULL			Change Drop More
8	created_at	timestamp			Yes	NULL			Change Drop More
9	updated_at	timestamp			Yes	NULL			Change Drop More

Fig 5.11 : Table (Admin access tokens)

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	id	varchar(100)	utf8mb4_unicode_ci		No	None			Change Drop More
2	access_token_id	varchar(100)	utf8mb4_unicode_ci		No	None			Change Drop More
3	revoked	tinyint(1)			No	None			Change Drop More
4	expires_at	datetime			Yes	NULL			Change Drop More

Fig 5.12 : Table (Admin Token refresh)

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	email	varchar(255)	utf8mb4_unicode_ci		No	None			Change Drop More
2	token	varchar(255)	utf8mb4_unicode_ci		No	None			Change Drop More
3	created_at	timestamp			Yes	NULL			Change Drop More

Fig 5.13: Table (Admin Password reset)

5.11 DIAGRAM OF DATA FLOW

5.11.1 Level 0

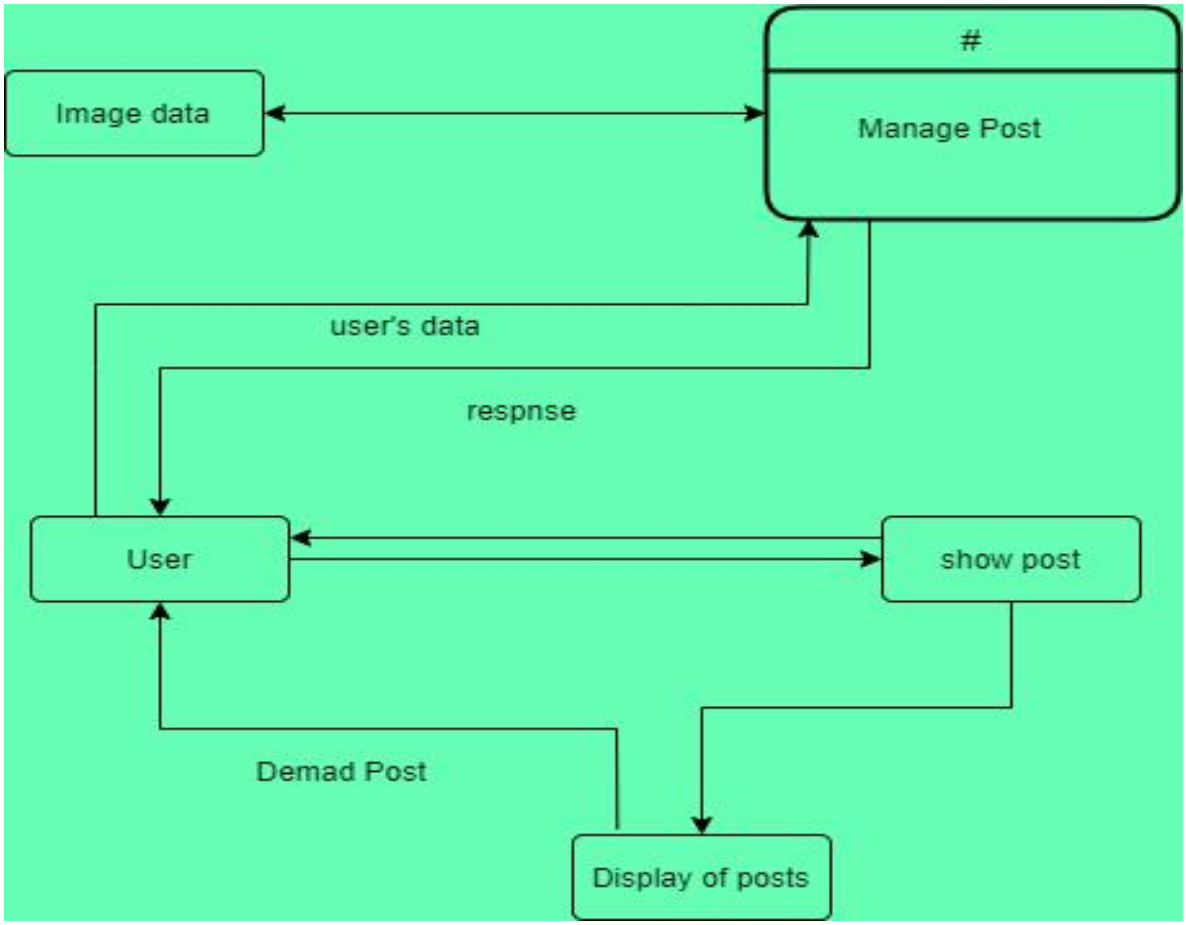


Figure 5.14 : Level 0 Data Flow Diagram .

11.2 Level 1

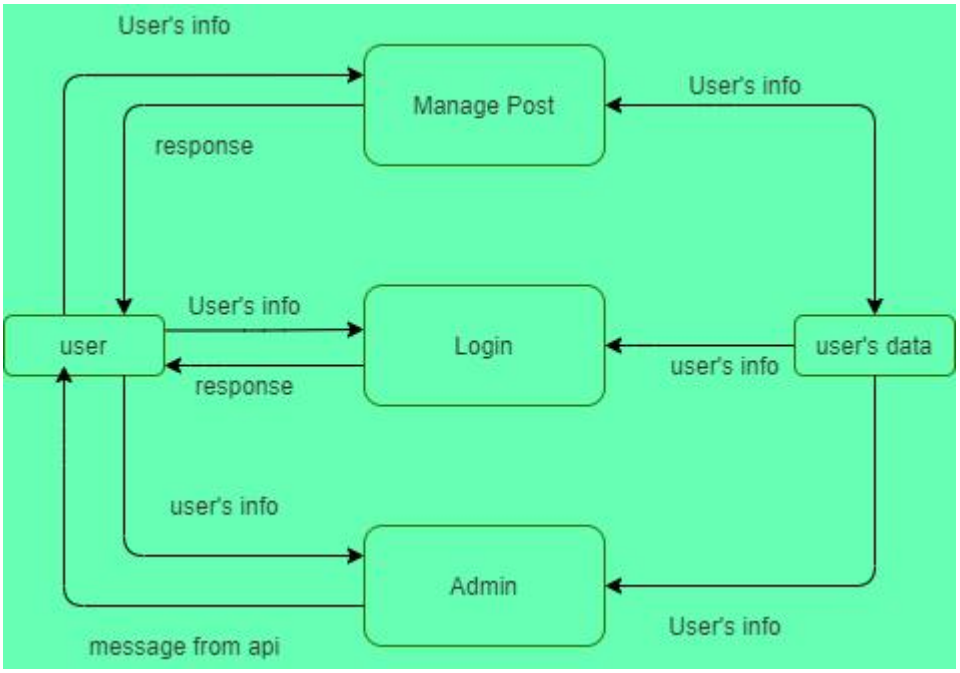


Figure 5.15 : Level 1 Data Flow Diagram for Admin .

5.11.3

Level 1 DFD for User

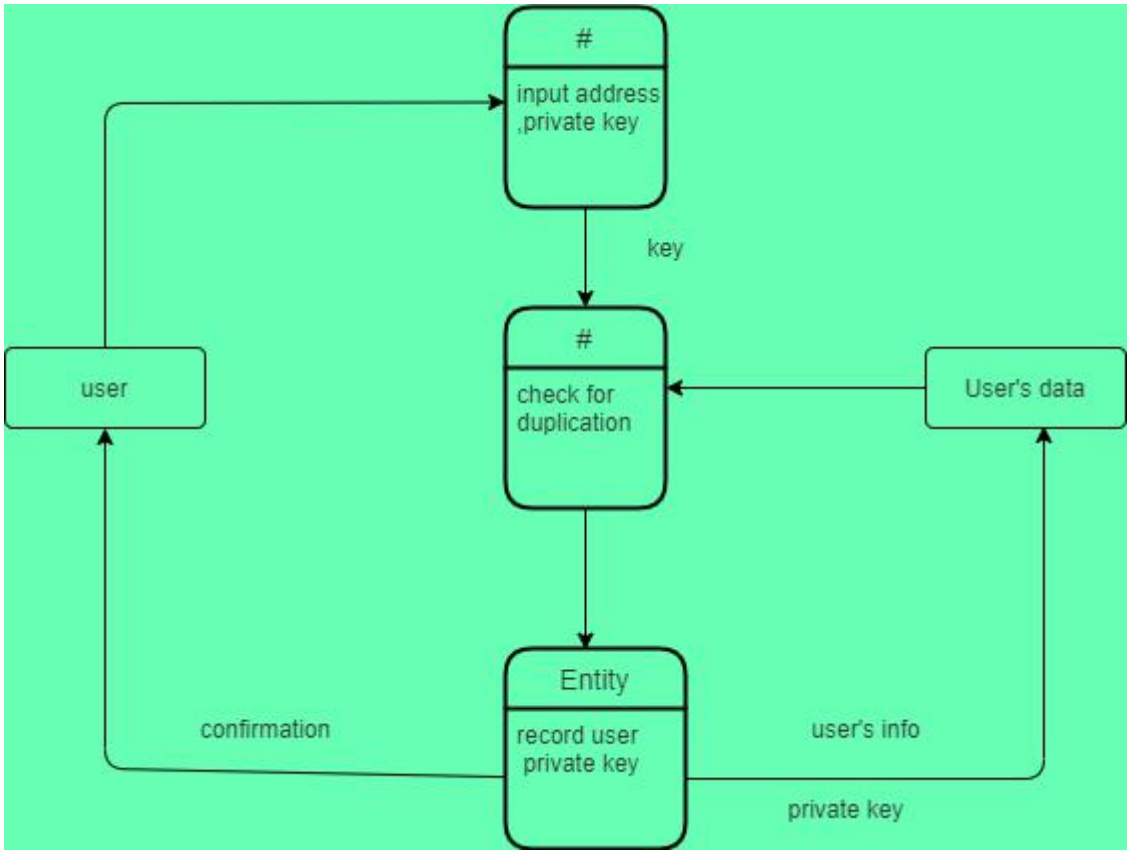


Figure 5.16 : Level 1 Data Flow Diagram for User

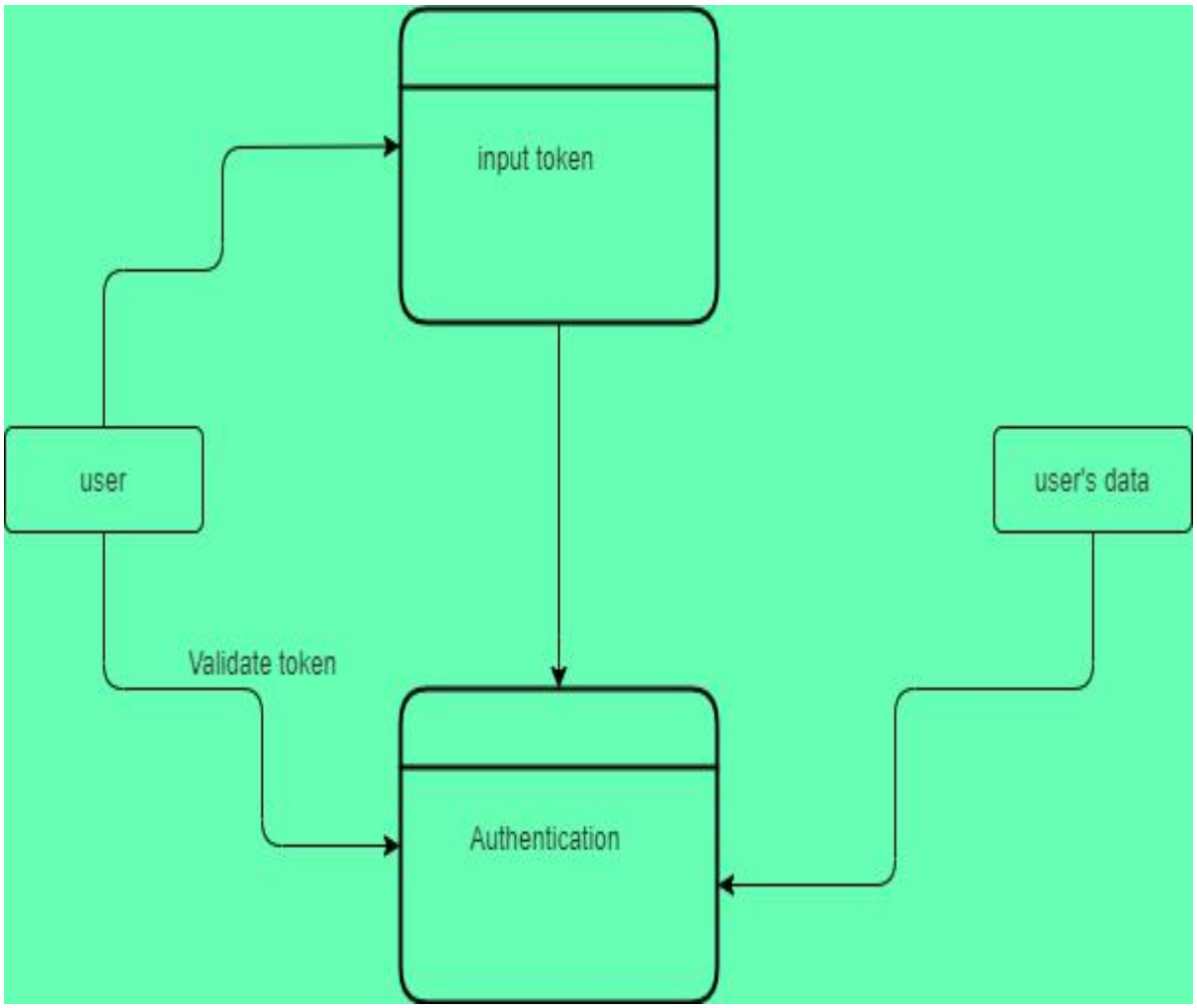


Figure 5.17 : Level 1 Data Flow Diagram for User

CHAPTER VI

SYSTEM IMPLEMENTATION & TESTING

In ensuring security in Social network , People always want a secure and decentralize platform . As day by day Blockchain becoming a very trusted technology to adopt in securing the social network . By using Blockchain technology we make our Dinke-din a place for trust , hope for social network user .

6.1 SYSTEM IMPLEMENTATION IN DETAILS

In OSN system there are 2 panels.

- User Panel
- OSN Owner Panel

6.1.1 User Panel

To use the User panel user must need to first open the Blockchain server provided by Ganache .Without opening the Ganache the user database provided by Blockchain terminal will not be accessed . When Ganache will be open it will create a connection

between Ganache and Meta mask in browser .Then user signing in meta mask by putting Private key mentioned in Account information in Ganache . When a user import his Account to meta mask by putting by private key , then account imported done . Now user has access to user panel . In our PWA user can able to do:

- **Share Post**
  - All Posts – Every user can post in OSN system and they have to pay some gas fee to continue the post to be inserted in the system . whenever a user post in system his data will be uploaded in IPFS system .
  - My Posts – The previous given post will be shown here. Can delete or modify any post.
- **Tip Amount** – Can as in normal OSN system user's post are promoted by likes and comment .In our Blockchain system we provide user to promote other's post by giving coin to other , we can call it Tip amount .

6.1.2 Dinke-din Owner Panel

This panel provides the unique facility to the Admin to control all the aspects of the whole system .This panel provide a user-secured data flow within the system. Viewing and managing all old data .it consists of the sub panel activity

- **Post Control**
  - All Post --

    Admin can get all posts control with passing some security pathway to confirm that admin are not a malicious user to stole the data. Admin can get all data of user and post data in this panel . He can delete the data too. .

6.2 UI DESIGN IMPLEMENTATION

Here we will describe the UI Implementation into two main parts. These are:

1. User Panel
2. OSN Admin Panel

6.2.1 User Panel

User is the main attention in our Dinke-din system. User can register and sign in by setting up Meta mask account . Once the Meta mask is setup our system will count the meta mask account as a user . If anything wrong or not registered he will not able to start the Dinke-din system .

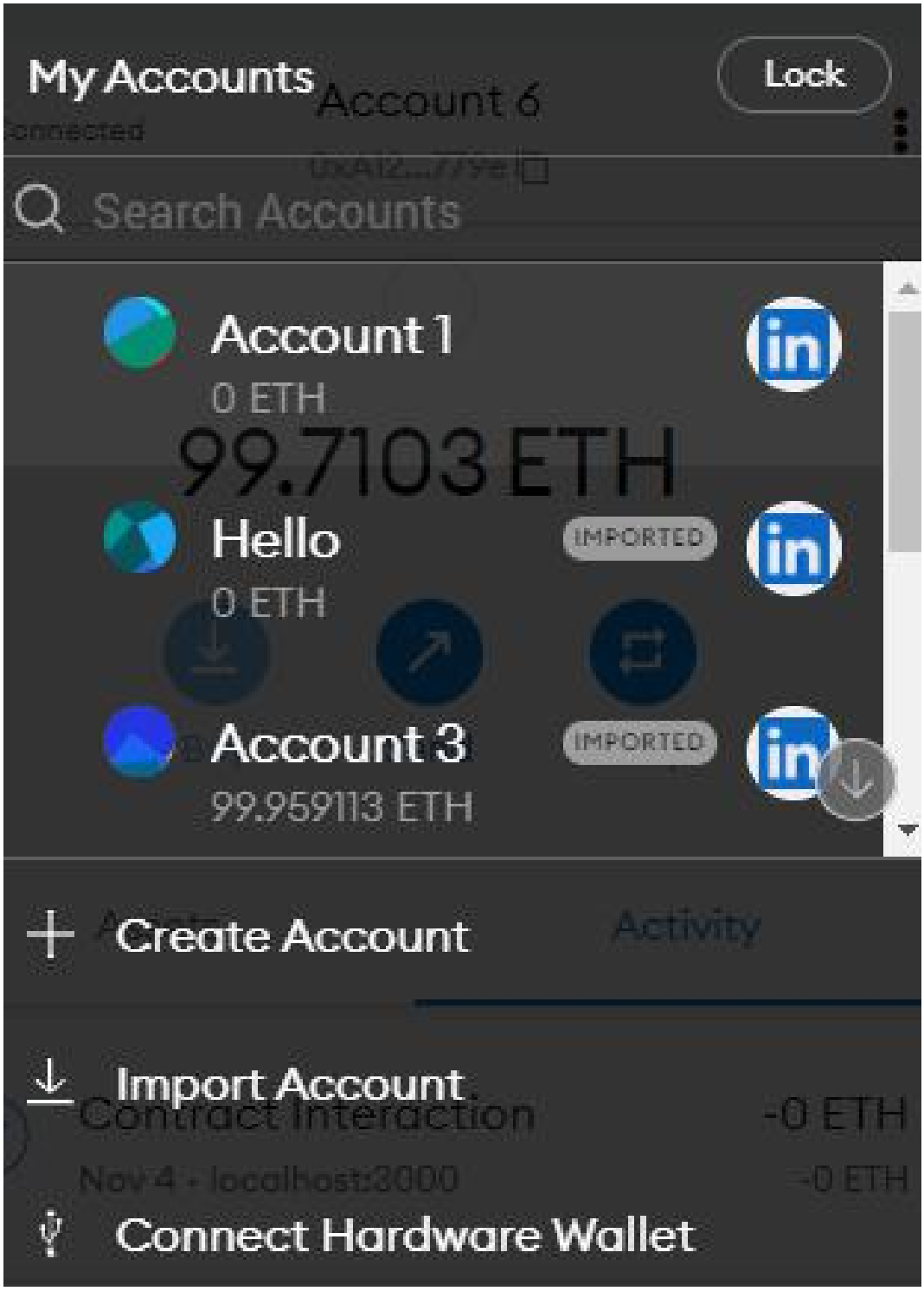


Fig 6.1:User Account in Meta Mask

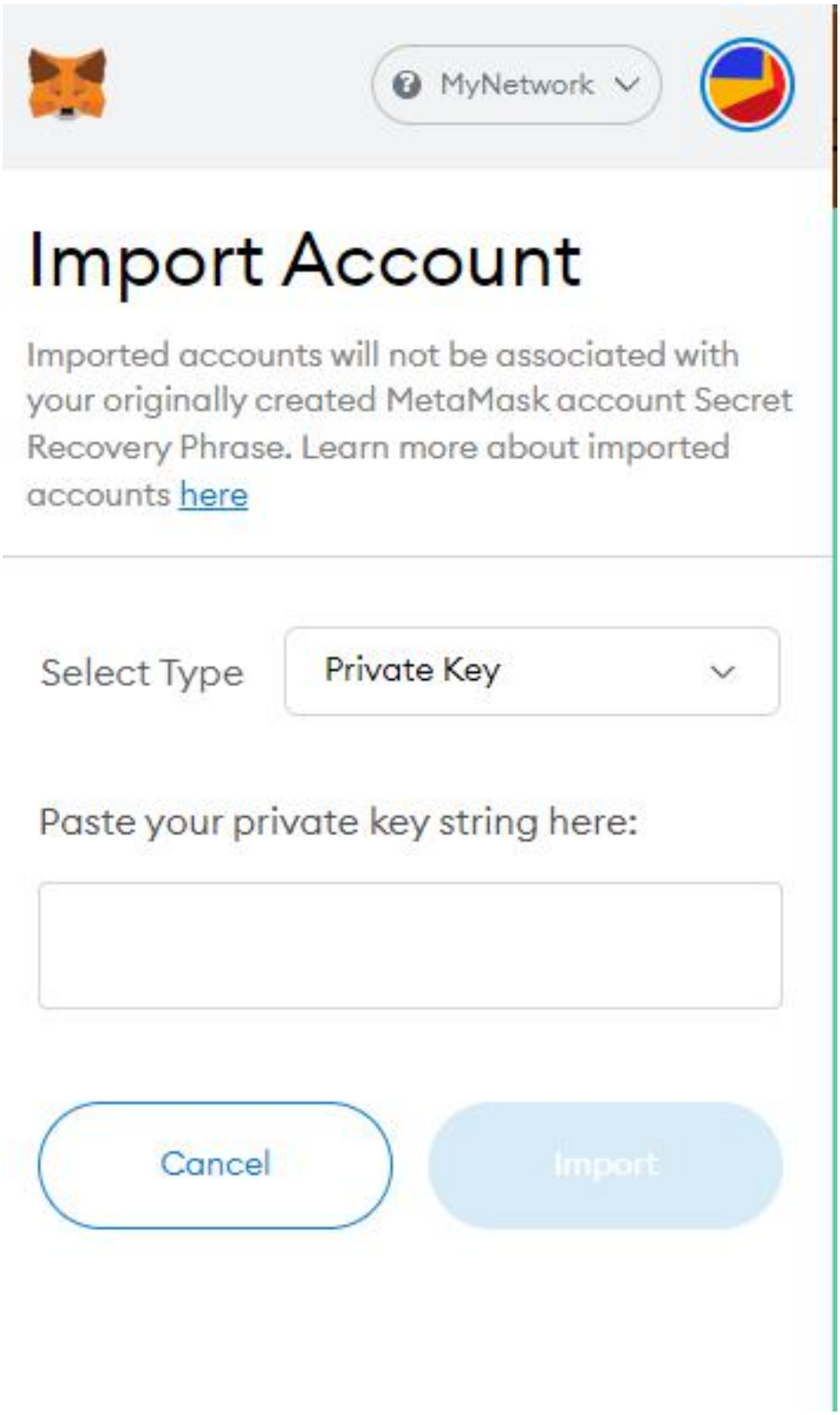


Fig 6.2 :User Account import panel

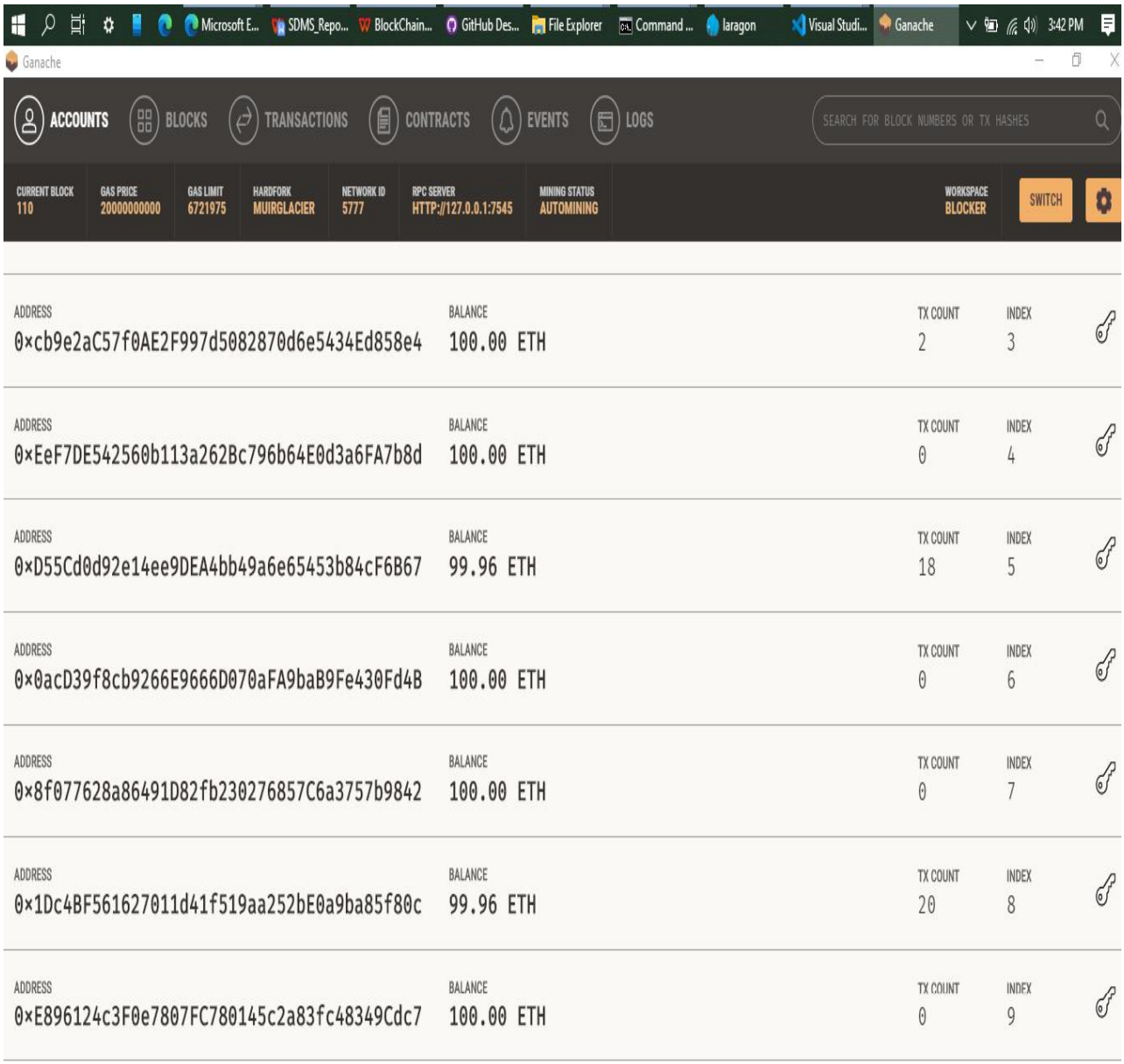


Fig 6.3 :User Account provided by Blockchain

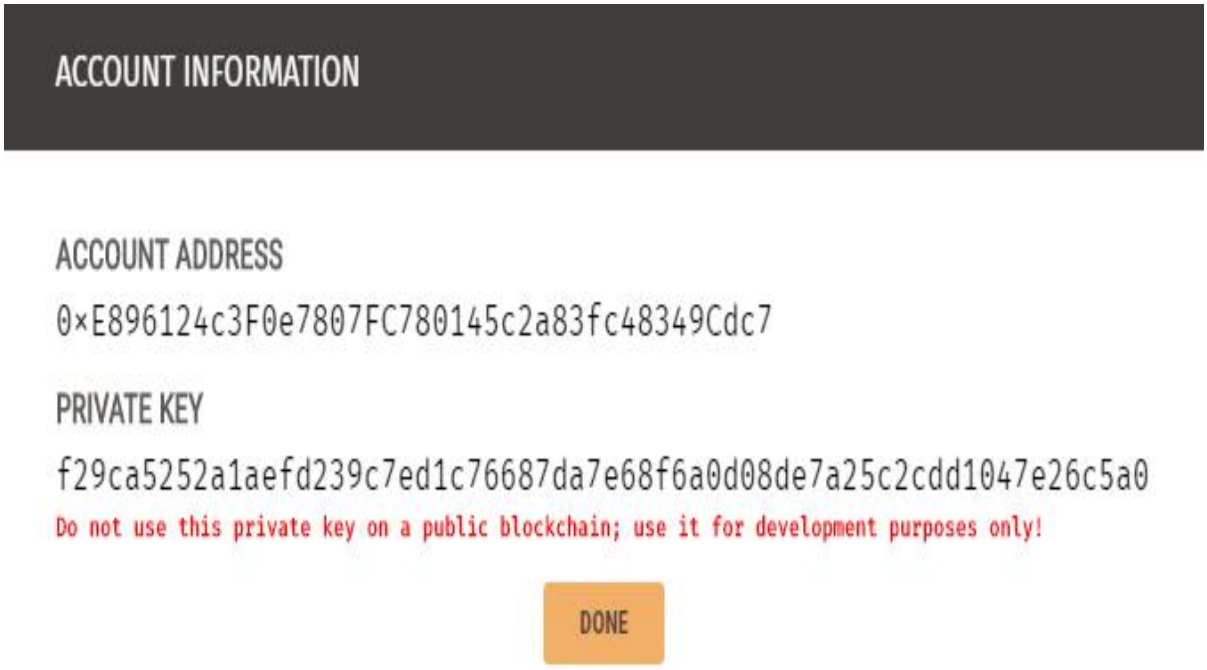


Fig 6.4 : User Account Address in BlockChain

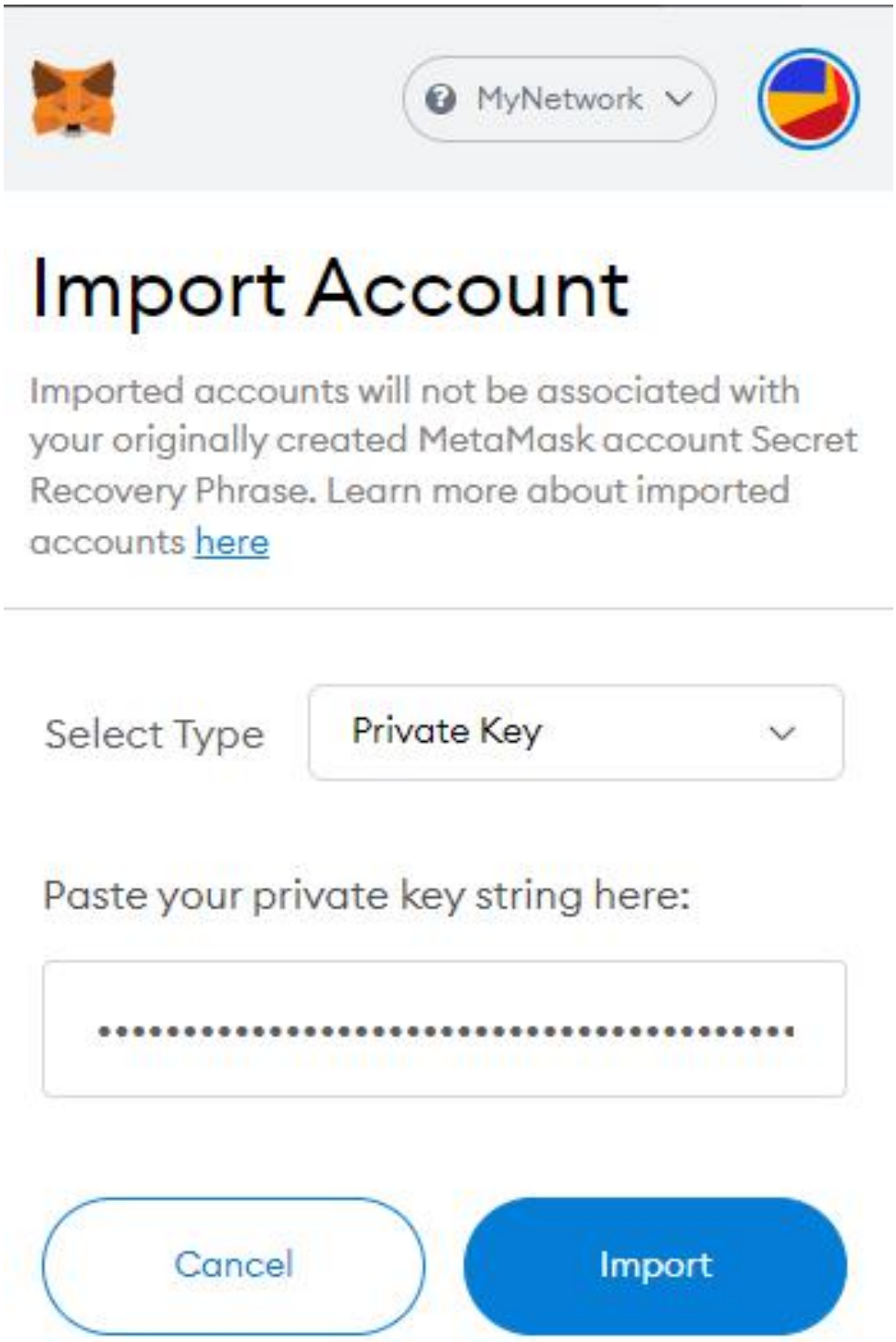


Fig 6.5 : User Account Imported

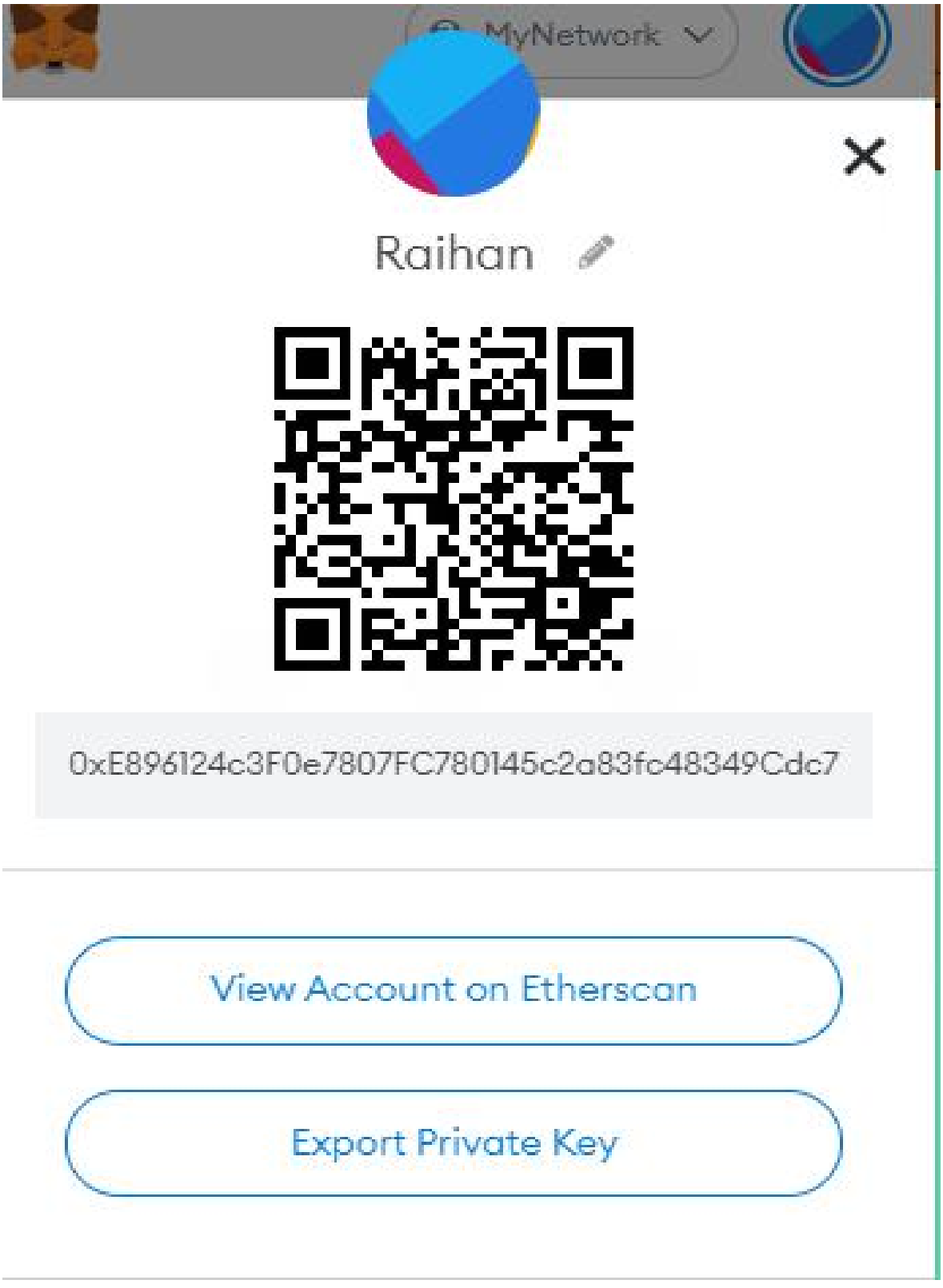


Fig 6.6 : Account Details of User

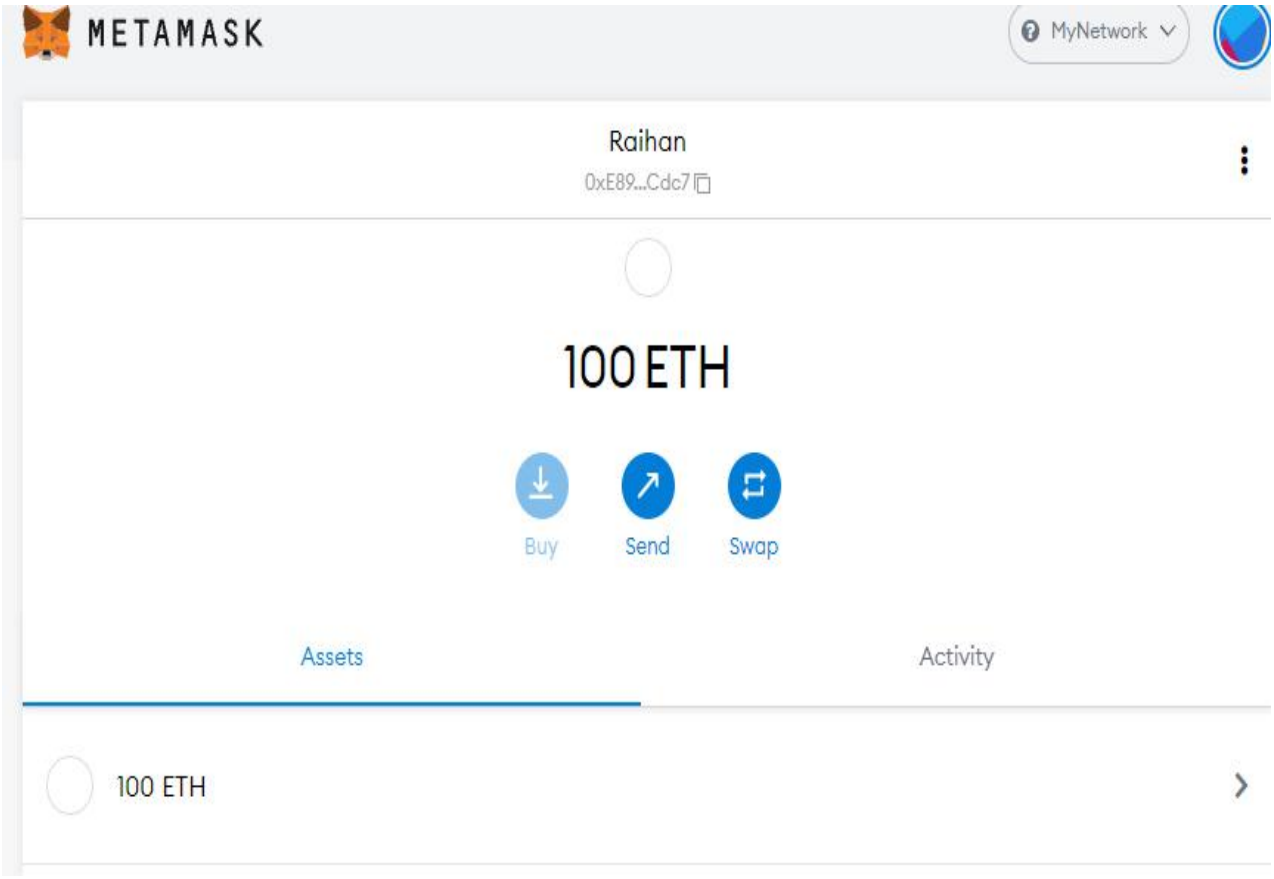


Fig 6.7 :User Smart Wallet

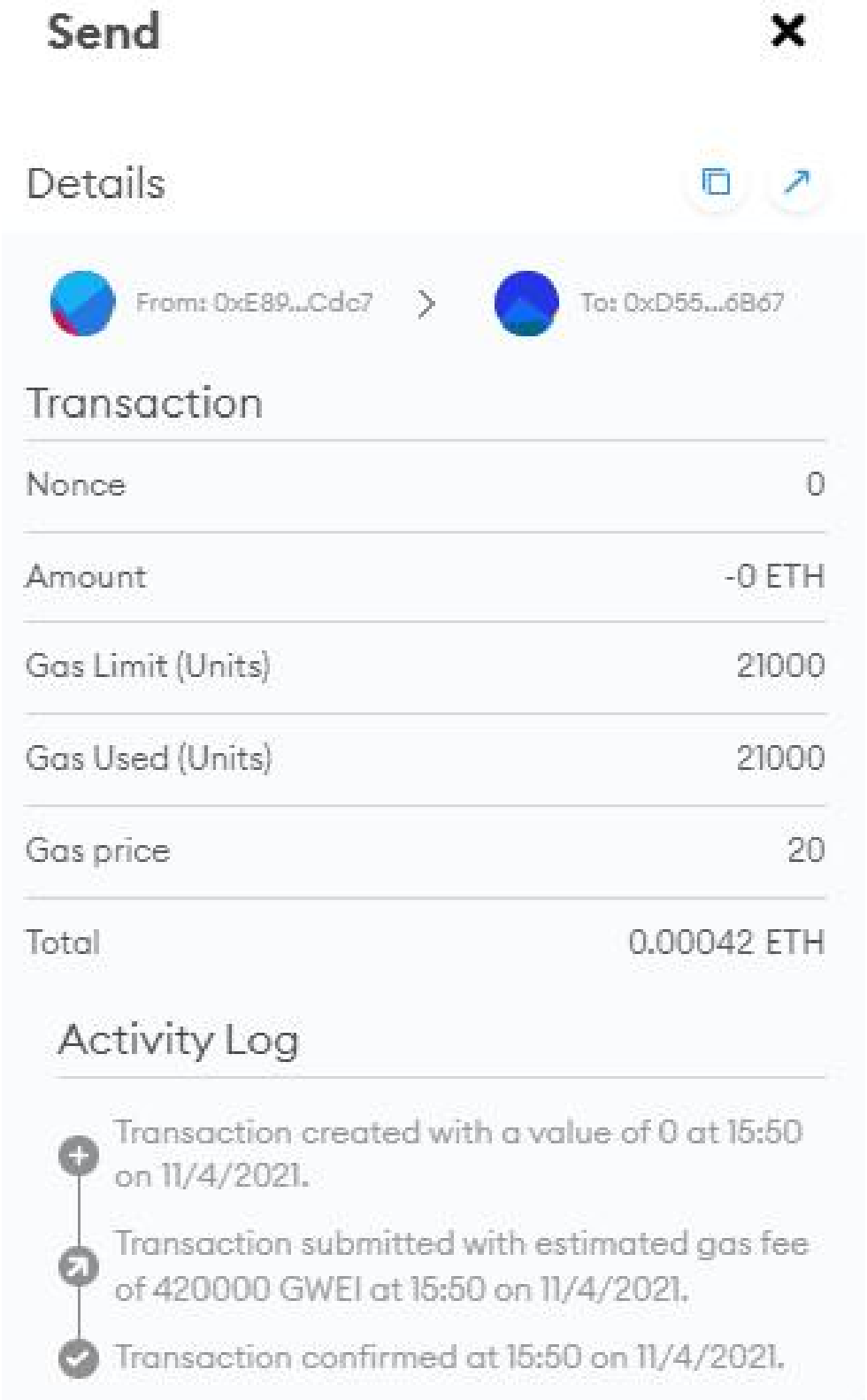


Fig 6.8 :User's Transaction with etherum

Fig 6.9 :Dinke-din’s landing page

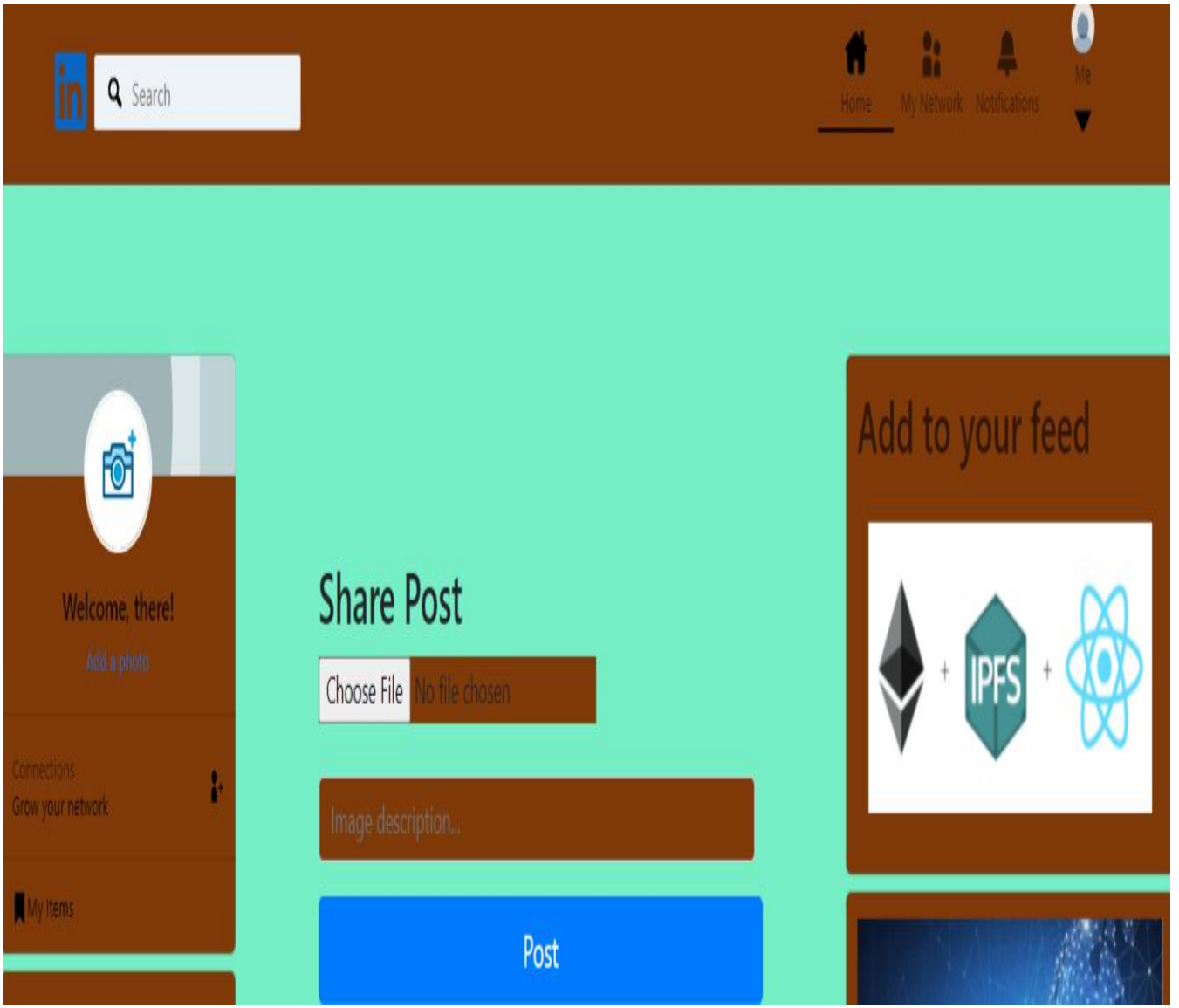


Fig 6.10 :User post share options

Fig 6.11:Shared post in Dinke-din

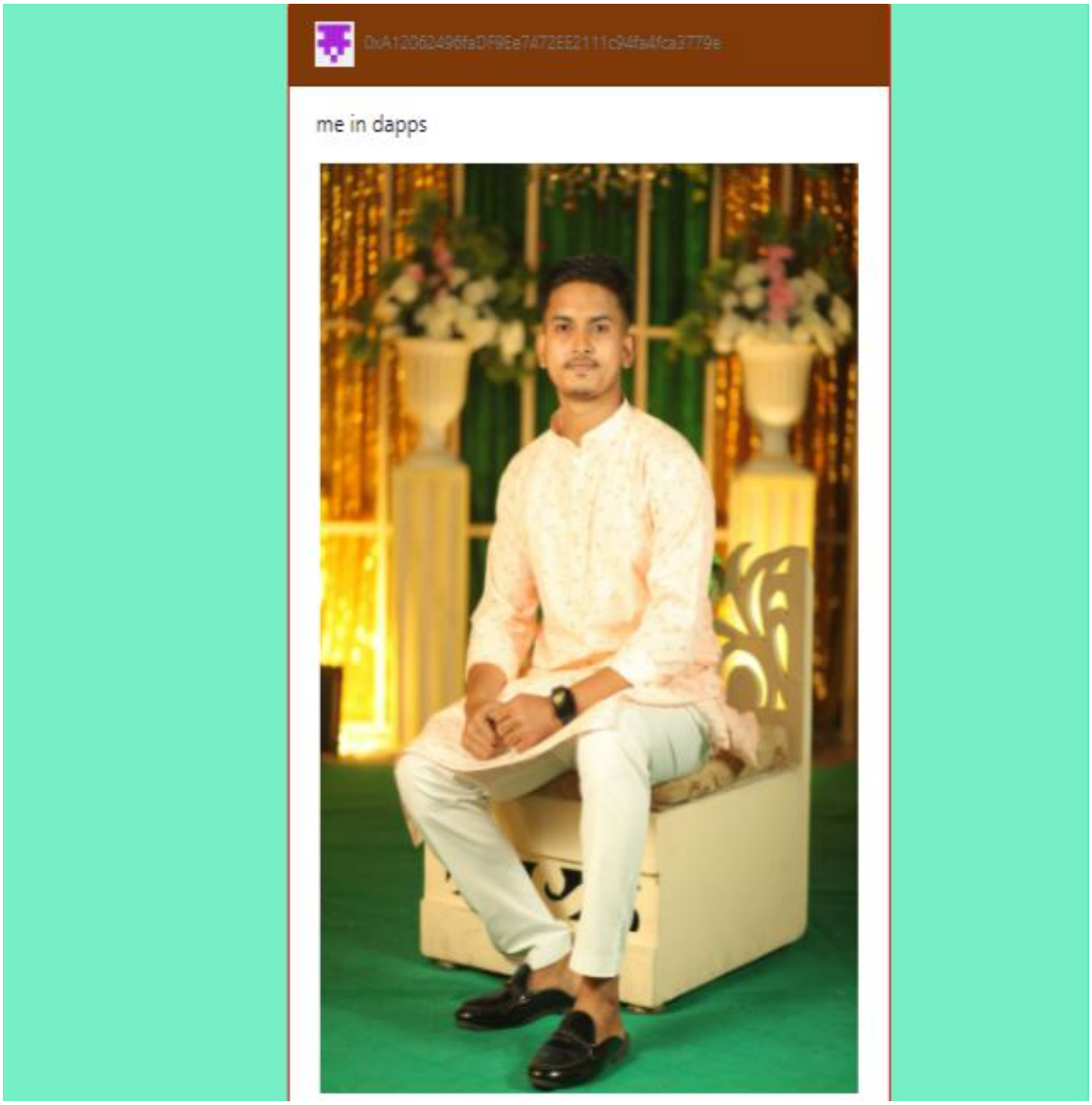


Fig 6.12 :Shared post in Dinke-din

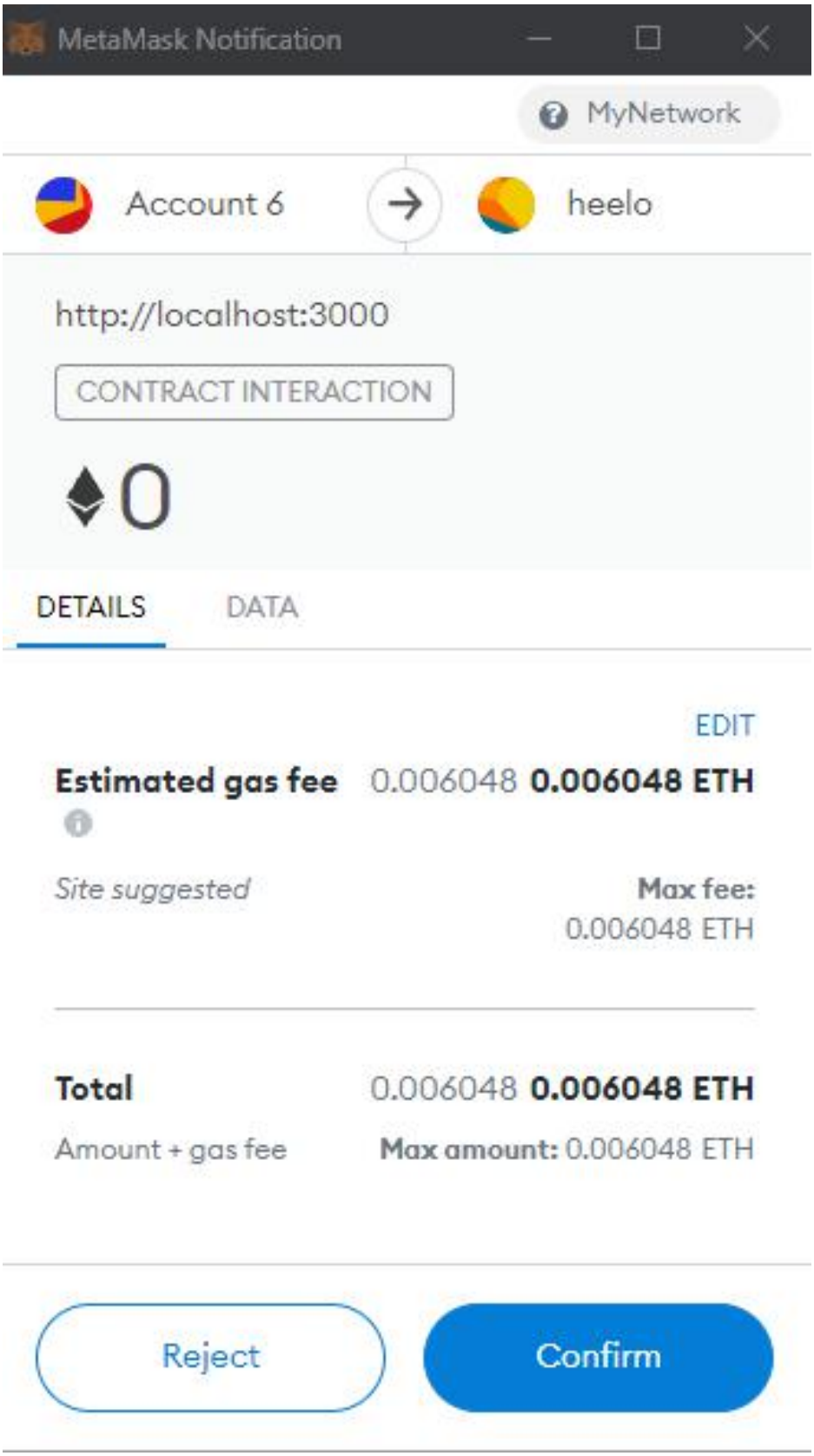


Fig 6.13 :Confirmation of sharing post to Dinke-din with smart contract

Admin of Dinke-din system:

Admin panel is in our Dinke-din system is like the role of Mark Zukerbark in Facebook system . To get the data of all user Owner of Dinke-din system must have to have the Bearer Token to get the all data in the own system .

```
{
  "success": true,
  "message": "Login Successful",
  "data": {
    "id": 2,
    "name": "Jamshedul Alam",
    "email": "jamshedulalam@gmail.com",
    "email_verified_at": null,
    "created_at": "2021-11-04T10:07:58.000000Z",
    "updated_at": "2021-11-04T10:07:58.000000Z"
  },
  "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9
      .eyJhdWQiOiIxIiwianRpIjoiZmY5OWEwYzBmZjg2ZDUzNjFiMTdmMWU5YjA4YTM0MGE3YWUzN2Y0MDkzNjZlYjkyYjZjZGZjM2JmZDdhMWFhZGFlY2U1ZWNlYzllZTE5YmMi
      LCJpYXQiOjE2MzYwMjA3MDQuMjMxODQsIm5iZiI6MTYzNjAyMDcwNC4yMzE4NDYsImV4cCI6MTY2NzU1NjcwMy44ODA2MjUsInN1YiI6IjIiLCJzY29wZXMiOltdfQ
      .YxmengP4exDNPnz_nnzbt5gWN49mhQT9
      -73y170kHgSYdWSN1snk95hZ4C3jbbyDZuA69HQig28LDlXGu_Itn0rsAsZYxEdVd_3OXFYINSCpEAFRnIolrL1ev6eNdNbzcJxWt6XNArXEjnFgfh_vbJUoPKAs_6Q33a-nB
      -l1YNDIxj8edWf2Q-bjErRY9je5ncyxQfH6XbcZtniyqnaEzV2isi8nh_SXf4kjIe3m-DLk671FRlrpbBiw450MJaumL74_ynpImP
      -btmxpe49yndKUxW1TCNJdQg4lsVxOxMXkFjhuk2Ho36jPa3hHaBqo1mXbfC_2fuc57GdjfxQ1CDQNK5mB33iaz6plJcbma61jYxXL1j83ptnhy_saax_LvczxFldkwZd1cvZ
      wL7TXPQfVNPOCyOPdF4SEJTV_6-yT6mXghKdiChzgkK8Ani36BoyASH5cQSfS25Ju65lCapr5C1j1sqtL9_Q7ye_IE598L9hJS4GcqvAkkrw33O7zUavJX3uiKmzPVs59fvkD
      _BsM-SuKBHfJa2uxhWR4FWqCLfwyOGka2FugV74sVOZiR6eCT-4ytrmfWgv9ayGsvwiKi8tfpuJgZenn7OWsPuY2wKzo9EKvj7BPJub3dNi_ZqTCvdKnpkOGg
      -a1LhkJKyXYQeyqErmsoLE5IXZixZs",
  "token_type": "bearer"
}
```


Fig 6.14 :Admin Data pull from database using bearer Token

In there whenever a owner of Dinke-din system call for any user data he must have to fullfill the requirements setup in api call to be safe from data loss with the permission of owner of Dinke-din system.

user	title	image	created at
0xA12062496faDF9Ee7472EE2111c94fa4fca3779e	I am Jamshedul Alam. I work as a Frontend Developer in this work.	QmYhTeDFSJYDwuwCzBqMepjQBBWBuyBFhqReKo5745gAU4	19 minutes ago
0xA12062496faDF9Ee7472EE2111c94fa4fca3779e	Our sir , our inspiration	QmVs8jFUyUdoGDCQhqBUwdaRUEBfaAxy1kpqPHyyySb4LW	15 minutes ago
0xA12062496faDF9Ee7472EE2111c94fa4fca3779e	We are preparing for presentation.	QmaANq6REAV7LEqUzjH66yk4MizPKUWWAdGoqjLoYWPrvg	13 minutes ago
0xA12062496faDF9Ee7472EE2111c94fa4fca3779e	Our sir , our inspiration	QmVs8jFUyUdoGDCQhqBUwdaRUEBfaAxy1kpqPHyyySb4LW	5 minutes ago
0xA12062496faDF9Ee7472EE2111c94fa4fca3779e	I am Jamshedul Alam. I work as a Frontend Developer in this work.	QmYhTeDFSJYDwuwCzBqMepjQBBWBuyBFhqReKo5745gAU4	3 minutes ago

Fig 6.15 :Admin’s All post show in Dinke-din

6.3 TESTING

Software testing is a process where in the software is evaluated to find the difference between the given input and expected output.Software testing is performed to determine whether or not the software is performing as expected or deviates from the original expectations.. Accordingly to the SWEBOK: “Software testing is the dynamic verification that a program performs as expected on a finite set of test cases chosen from the normally infinite execution domain.. “[20] .

6.3.1 Objectives of Testing

There have some different goals and objectives in software testing. The main objectives are as follows -

1. To find failures and defects. .
2. Increase the likelihood that the test application will meet all of the requirements described
3. Increase the likelihood that the application intended for testing will work correctly under all circumstances
4. Helps to ensure that product is safe and secure for end-user/customer.

6.3.2Testing Details

The testing methodologies are provided below:

a)Unit testing with white testing

b)Black box testing

1.12.1Unit Testing:

Test Case	Output	Expected Result
posts?id=`id`-10	As we send Get Method to the api back-end , it give us error .	As there is no such routes in our system it should return a routes error.

- We have debugged all inputs which are mandatory as user inputs. We have tested another important field, file input. If file upload manager accepts all file type without specific one, then it can cause security issue to our database and server. We got error exception in debugger while checked with invalid or unknown file types.

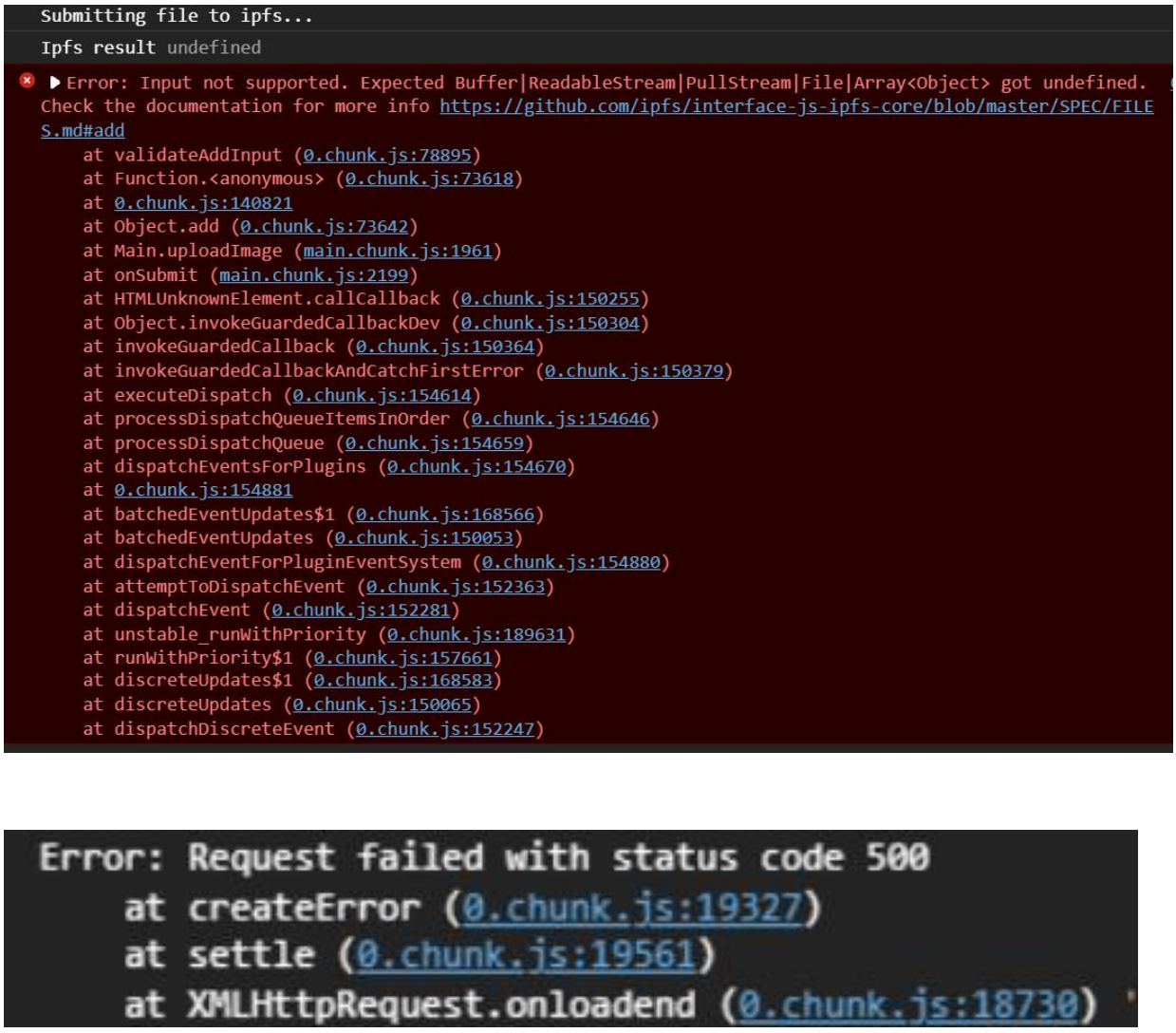


Fig 6.16 : connection request execution testing output

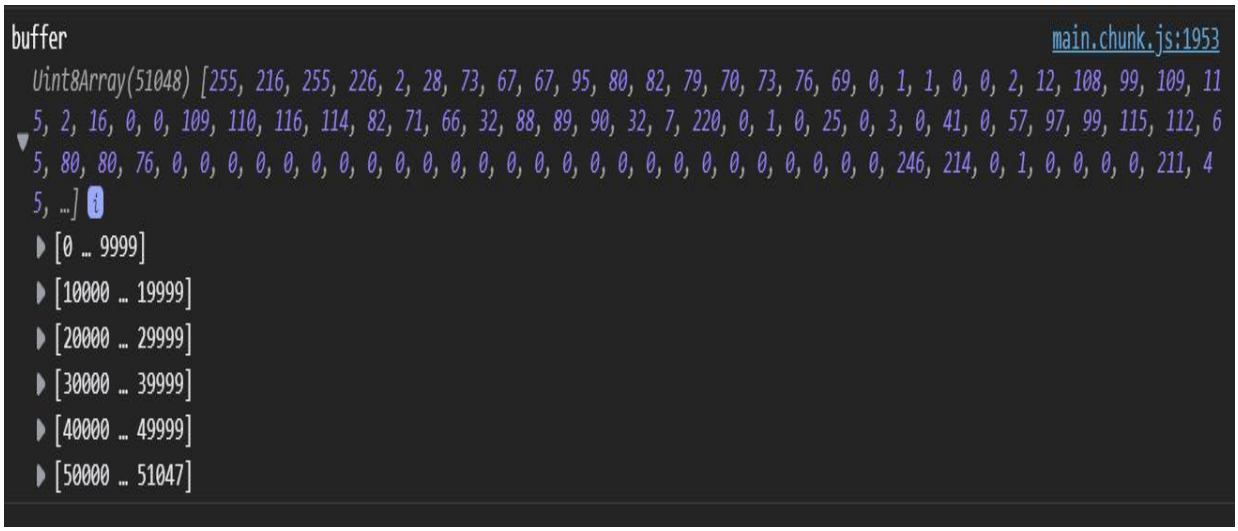
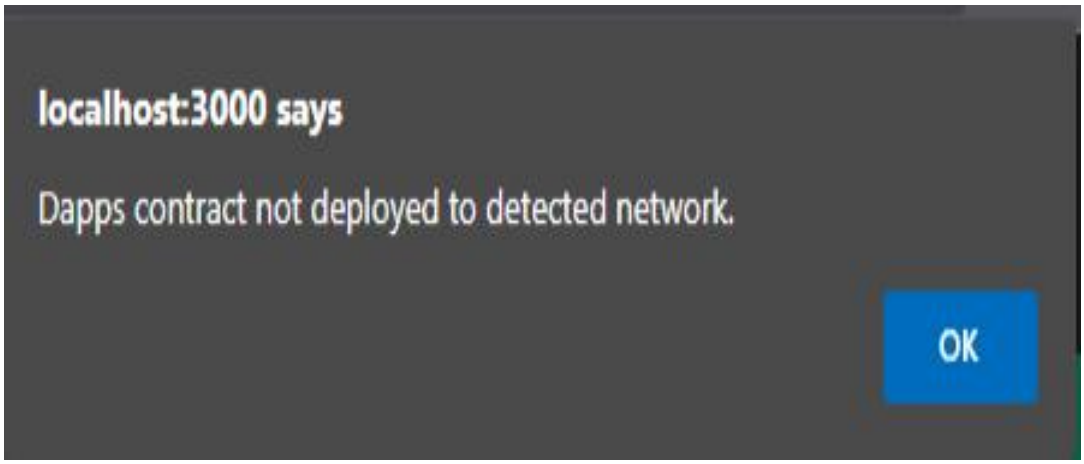


Fig 6.17 : File type checking output

- if the website will not deploy to Blockchain , then the error will showed in there to notify the user .



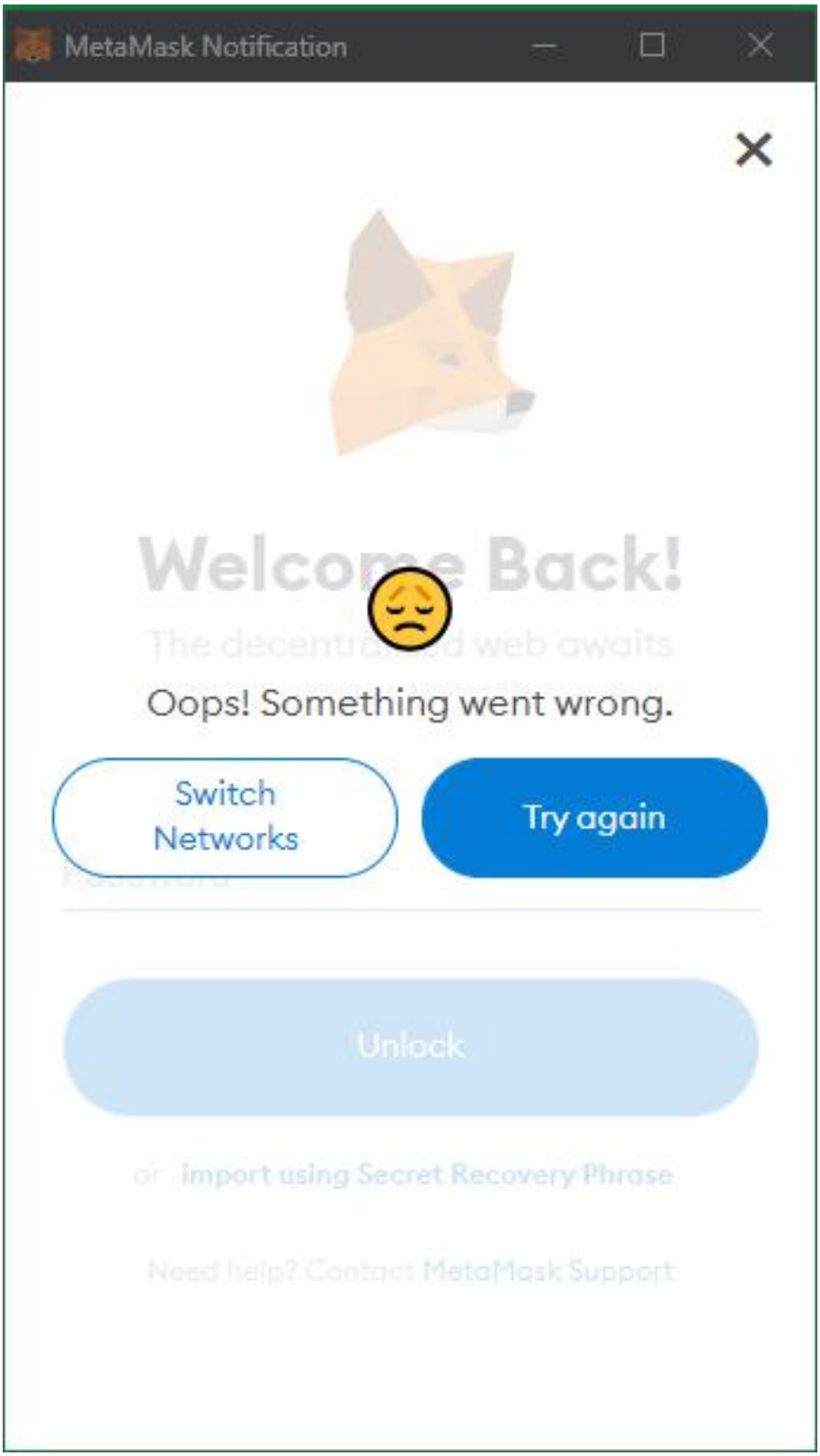


Fig 6.18 : Output of manual connection check of application

Testing Black Box

Test Case	Output	Expected Result
posts?id=10	Http Get will be sent and it is returning about post	It should be retuning with data.
User = admin Pass = admin	Http post method was sent and then it is returning a success messages .	Should return in ok from back-end .

/posts	Request for all post in return .	Should return all data about posts.
Header: user.token	It is allowing the user to take control of the data and admin panel .	Should recongnize as a familiar user.

CHAPTER VII

CONCLUSION & FUTURE PLAN

7.1 CONCLUSION

Our Dinke-din was a product to ensure our security in online social network as a sample we choose Linke-din. Our Dinke-din is a solution to the social network data losing and data corruption .In Dinke-din , we try to solve the most debating talk we always have with each other about what we sharing in the Dinke-din is it safe? Will Dinke-din Owner share the all user data and user info to the thrid party ?

To solve this problem in our Dinke-din we uses IPFS Blockchain system .

7.2 CONTRIBUTION OF THE PROJECT

,Blockchain helps to solve the security problem about user's shared data and user data. But we make a separate cloud system where we stored the ipfs returned hash value in database .In this cloud system whenever a user post in our Dinke-din , this post account address , image ipfs hash address , description of the post and date of the post will be stored in the database . The most interesting thing about that is that it is a place

for user and owner of Dinke-din .Here if any party want the post data or user data he must have to bearer token in his hand , without that he will be detected as a evil user.

7.3 FUTURE PLAN

- We have plan to make the Dinke-din platform more secured for the user.
- We are planning to add new feature to the Dinke-din so that Dinke-din becomes the best version of it.

REFERENCES

[1] Pawade, Dipti, and Avani Sakhapara. "Blockchain Based Secure Traffic Police Assistant System." (2020).

[2] Sultana, Maliha, et al. "Towards developing a secure medical image sharing system based on zero trust principles and Blockchain technology." BMC Medical Informatics and Decision Making 20.1 (2020): 1-10.

[3] Adriano Witkowski and Altair Santin "An IdM and Key-Based Authentication Method for Providing Single Sign-On in IoT ".

[4] R. Mehta, N. Kapoor, S. Sourav and R. Shorey, "Decentralised Image Sharing and Copyright Protection using Blockchain and Perceptual Hashes," 2019 11th International Conference on Communication Systems & Networks (COMSNETS), 2019, pp. 1-6, doi: 10.1109/COMSNETS.2019.8711440.

[5] Jabarulla, Mohamed Y., and Heung-No Lee. 2021. "Blockchain-Based Distributed Patient-Centric Image Management System" Applied Sciences 11, no. 1: 196. https://doi.org/10.3390/app11010196

[6] Kumar, Randhir, et al. "A secured distributed detection system based on IPFS and Blockchain for industrial image and video data security." Journal of Parallel and Distributed Computing 152 (2021): 128-143.

[7] Zhang, Lei, Mingxing Luo, Jiangtao Li, Man Ho Au, Kim-Kwang Raymond Choo, Tong Chen, and Shengwei Tian. "Blockchain based secure data sharing system for Internet of vehicles: A position paper." Vehicular Communications 16 (2019): 85-93.

[8] Feixiang, Zhao, Liu Mingzhe, Wang Kun, and Zhang Hong. "Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over Blockchain." Optics & Laser Technology 135 (2021): 106610.

[9] Wang, Xingyuan, Le Feng, and Hongyu Zhao. "Fast image encryption algorithm based on parallel computing system." Information Sciences 486 (2019): 340-358.

[10] Laiphrakpam, Dolendro Singh, and Manglem Singh Khumanthem. "Medical image encryption based on improved ElGamal encryption technique." Optik 147 (2017): 88-102.

[11] Cai, Lu-Zhong, Ming-Zhao He, Qing Liu, and Xiu-Lun Yang. "Digital image encryption and watermarking by phase-shifting interferometry." Applied optics 43, no. 15 (2004): 3078-3084.

[12] Zhou, Yuezhi, Yaoxue Zhang, and Yinglian Xie. "Virtual disk based centralized management for enterprise networks." In

Proceedings of the 2006 SIGCOMM workshop on Internet network management, pp. 23-28. 2006.

[13] Mohsin, A. H., A. A. Zaidan, B. B. Zaidan, K. I. Mohammed, Osamah Shihab Albahri, Ahmed Shihab Albahri, and M. A. Alsalem. "PSO-Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture." Multimedia tools and applications 80, no. 9 (2021): 14137-14161.

[14] Bhowmik, D., Natu, A., Ishikawa, T., Feng, T., & Abhayaratne, C. (2018, July). The Jpeg-Blockchain framework for glam services. In 2018 IEEE International Conference on Multimedia & Expo Workshops (ICMEW) (pp. 1-6). IEEE.

[15] [19]Buccafurri, F., Lax, G., Nicolazzo, S., & Nocera, A. (2017, June). Tweetchain: An alternative to Blockchain for crowd-based applications. In International Conference on Web Engineering (pp. 386-393). Springer, Cham.

[16] Swapnil Ninawe and Pallapa Venkataram “Authentication schemes for social network users: a review ”.

[17] What is Blockchain ? what is the future of it 8 Reasons Why Blockchain Technology Is the Future | upGrad blog

[18] Zheng, Qiuhong, Yi Li, Ping Chen, and Xinghua Dong. "An innovative IPFS-based storage model for blockchain." In 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), pp. 704-708. IEEE, 2018.

[19] Kozlowska, Iga. "Facebook and data privacy in the age of Cambridge Analytica." Seattle, WA: The University of Washington. Retrieved August 1 (2018): 2019.

[20] What is testing What is software testing? - Quora

The End