FORGERY DATA DETECTION FOR NATIONAL SECURITY USING BLOCKCHAIN

Major project report
submitted in partial fulfillment of the requirements for the award of

Bachelor of Technology
in
Information Technology

By

YUGANDHAR SURYA (18UTIT0060)

DEPARTMENT OF INFORMATION TECHNOLOGY

SCHOOL OF COMPUTING

VEL TECH RANGARAJAN DR. SAGUNTHALA R&D INSTITUTE OF SCIENCE AND TECHNOLOGY

(Deemed to be University Estd u/s 3 of UGC Act, 1956)
CHENNAI 600062, TAMILNADU, INDIA

JUNE 2022

Vel Tech
Rangarajan Dr. Sagunthala
R&D Institute of Science and Technology
(Deemed to be University Estd. u/s 3 of UGC Act, 1956)

DEPARTMENT OF INFORMATION TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that this Major Project Report is the bonafide work of Yugandhar Surya (18UTIT0060) who carried out the project entitled "FORGERY DATA DETECTION FOR NATIONAL SECURITY USING BLOCKCHAIN" under our supervision from January 2022 to June 2022.

Internal Guide	**Head of the Department**
Mrs. JAYANTHI. K, M.Tech	Dr. C. MAHESH, M.E., Ph.D.

Submitted for Viva Voce Examination held on _____

Internal Examiner	**External Examiner**

Submitted for the partial fulfillment for the award of the degree of Bachelor of Technology in Information Technology from Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology (Deemed to be University, u/s 3 of UGC Act,1956).

DECLARATION

I Ygandhar Surya 18UTIT0060 hereby declare that the Major Project Report entitled "FORGERY DATA DETECTION FOR NATIONAL SECURITY USING BLOCKCHAIN" done by me under the guidance of Mrs. JAYANTHI. K, M.Tech., at Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology , Chennai is submitted in partial fulfillment of the requirements for the award of Bachelor of Technology degree in Information Technology.

Date: / / **Signature of the candidate**

Place: Yugandhar Surya

ACKNOWLEDGEMENT

We express our deepest gratitude to our respected **Founder Chancellor and President Col. Prof. Dr. R. RANGARAJAN B.E. (EEE), B.E. (MECH), M.S (AUTO). DSc., Foundress President Dr. R. SAGUNTHALA RANGARAJAN M.B.B.S.** Chairperson Managing Trustee and Vice President.

We are very much grateful to our beloved **Vice Chancellor Prof. S. SALIVAHANAN,** for providing us with an environment to complete our project successfully.

We are thankful to our esteemed Dean SoC , **Dr.V.SRINIVASA RAO, Ph.D.**, for providing a wonderful environment to complete our project successfully.

We record indebtedness to our **Head, Department of Information Technology Dr. C. MAHESH, M.Tech., Ph.D.,** for immense care and encouragement towards us throughout the course of this project.

A special thanks to our Project Coordinator **Mr. HARIHARAN. R, M.Tech.** for their valuable guidance and support throughout the course of the project.

We also take this opportunity to express our deep sense of gratitude to Our Internal Supervisor **Mrs. JAYANTHI. K, M.Tech,** for her cordial support, valuable information and guidance, which helped us to complete this project through various stages.

We thank our department faculty, supporting staff and friends for their help and guidance to complete this project.

ABSTRACT

One of the most important outlets for exchanging information between social groups is social networking. Not only real news, but also rumours and fake news, are widely disseminated via social media. Users benefit from online platforms since they can simply get news. However, this provides a chance for cyber thieves to distribute bogus news via these channels. Readers read the news and begin to believe it before verifying it. Detecting false news is a significant difficulty since it is not a simple process. To address this issue, blockchain is being utilised to control the spread of misinformation. The suggested system records and analyses disseminated material, limiting the amount of fake news and user manipulation. The system also includes a real-time alert panel that uses user votes to determine the truth of the news.

Once the threshold value is achieved, the news status is continually monitored and adjusted. The false word data collection may be used to identify misleading phrases and stop fake news from spreading. To reduce the consequences of rumours and their uncontrolled spread, all news that reaches the public eye must first be cross-verified by intellects. With the use of block-chain, the proposed initiatives might give governmental entities the capacity to check material and decide whether or not it is authentic enough to be spread among everybody. Because, unlike traditional methods, blockchain tends to share copies of the same data to every individual with hash codes in the system, the certainty that the data cannot be hijacked or corrupted is strong. Along with various characteristics that protect data from cyber-attacks, blockchain technology has the potential to grow service in all areas while maintaining total transparency and intelligence.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

INTRODUCTION

1.1 OUTLINE OF THE PROJECT

Blockchain is basically an storage or electronic ledger which safegaurds the digital data, information, content or currencies with locks in terms of hashes that changes each time if any change in information takes place anywhere in the chain. Change in the hash code keeps all the participants updated with new updates. In near future, Blockchain technology is likely to bring advancements in all sector including banks and online transactions, automobile, automotive, food supplies etc. Smart contract plays very crucial role in the field of blockchain. Smart contracts are similar as contracts but in e-format. Every participants of each chain are connected with each other through smart contracts.Blockchain re-evaluated the requirement of third-parties in trading or transactions and eliminated them which resulted in making the whole process de-centralized and secure.

Forgery in any kind of data or information becomes quite simple, nowadays technology like GANs is being used to generate deep fakes and fake images. The bitter truth is to be captured here is, these thing is being used in creating child sexual abuse material, bullying, financial fraud, revenge porn, fake news, etc.

The main reason behind these forgery data is the invisibility of the creator, mutable data, and insecurity on web2.0. At a saturated level machine or deep learning fails to identify the deep fakes and also to achieve high accuracy, these algorithms need data in bulk to train with, and to store big data high computational database is needed which will cost higher. Using blockchain the data will be transparent, secured, immutable and so the authenticity of data increases.

Figure 1.1: **Image-1**

Figure 1.2: **Image-2**

1.2 LITERATURE REVIEW

[1] L. Zhang et al.(2021).”Peer-to-Peer Networking and Applications” To take action against news and online curated content on the internet which could be inimical to the sovereignty of any nation, the proposed solution being implemented by smart contracts may have the capacity to identify and flag such contenton websites and social media. According to L. Zhang et al.(2021)[1]Fake news, press freedom disputes, advertising fraud, difficulty in digital rights management, flaws in content creation methods, and rumour spreading exacerbated by social media are all challenges that content producers and social media must deal with.All of the difficulties stated above are mostly caused by centralized servers or, to put it another way, management and all of the conceivable decisions made by a single person, allowing anybody to modify data as they choose.Blockchain technology, characterized by decentralization, security, and tamper-proof, offers a brand-new perspective on the above problems. “Blockchain + Media” can give revolutionary results.

[2] P. Fraga-Lamas and T. M. Fernández-Caramés (2020)”Fake News, Disin- formation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality”, fake news raises worries about the Internet and social media’s role in modern democratic countries, which might result in large economic losses or national security problems.This study attempts to investigate the potential of distributed ledger technologies (DLTs) to prevent digital deception by defining the most relevant applications and identifying the main problems they face. Blockchain and other distributed ledger technologies (DLTs) guarantee the provenance and traceability of data by providing a transparent, immutable, and verifiable record of transactions while creating a peer-to-peer secure platform for storing and exchanging information.

[3] S.Cho and C.Jeong (2019) ”A blockchain for media: Survey”, In their study they have stated that We can assure that any type of content is fully secured using blockchain.In their paper, they looked at how to characterise blockchain in digital subjects like media and interactive media as media blockchain. They also stated that a network is made up of devices that are lightweight, such as low storage space and computing performance, and that these issues degrade network security performance. It can be used for tracing and managing right information on content delivery platforms.

[4] S. E. Haddouti, et.al, 2019, ”Analysis of Identity Management Systems Using Blockchain Technology,”. They have investigated and gives us analysis of the most popular Identity Management Systems using Blockchain: uPort, Sovrin, and ShoCard. It then evaluates them under a set of features of digital identity that characterizes the successful of an Identity Management solution.The comparison analysis findings are provided in a clear and straightforward manner, allowing readers to quickly determine which systems meet which standards, allowing them to choose the best system for a given scenario.

[5] Shilpashree B N, et al.(2021),“Counterfeit Detection of Documents using Blockchain” it’s shown that InterPlanetary File System [IPFS] protocol and also a peer-to-peer-network for storing and sharing data in a distributed file system and can make a system that will be more secure and efficient for digital certificate validation.They advocated using blockchain technology to solve the problem of document counterfeiting.The blockchain technology offers the user’s documents with the authentication, authorisation, privacy, secrecy, and ownership that are required attributes of digital documents.

[6] Shovon Paul, Jubair Islam Joy et al.(2019),”Fake News Detection in Social Media using Blockchain,” We’ll talk about how to detect fake news in social media using the benefits of Blockchain’s peer-to-peer network concepts.According to them, use of the concept of decentralization, Ethereum smart contract and use BFS algorithm for calculating proimity of an user.Whenever news has been created, it will be broadcast through the chain by the transaction. Here, we will review only those particular news’ which have surpassed a certain limit of virality. The news will spread over the chain. General users may also get the news, but initially, this news will have no rating. As time passes by, validators will provide their reviews, and then the news will pop up with a rating to the users. This rating represents the correctness/authenticity of particular news.

[7] M. Torky, Emad Nabil, Wael Said,2019, “Proof of Credibility: A Blockchain Approach for Detecting and Blocking Fake News in Social Networks.”Blockchain as a powerful technology can provide a miraculous solution to overcome validating information credibility and reliability for social network platforms due to its immutability, security, tamper-proof, and P2P design.It offers Proof of Credibility (PoC), an innovative blockchain approach for detecting bogus news and preventing its spread on social media. On two datasets of newsworthy tweets obtained from various news sources on Twitter, the PoC protocol’s functionality was simulated.

[8] Yazed Alsaawy et al.(2021), ”Lightweight Chain for Detection of Rumors and Fake News in Social Media”, they proposed modifying the Blockchain’s structure while keeping its core properties. This was accomplished by combining a custom blockchain with the Text Mining (TM) algorithm to generate a Light Weight chain that was updated (LWC). The verification process will be sped up thanks to LWC, which uses proof of good history to assign weights to nodes based on prior posts. They created a basic model to replicate the suggested LWC for detecting fake news while maintaining the standard Blockchain’s properties and functionalities.Because of the widespread availability of the internet and social media in recent years, false information has travelled faster than ever before. Fake news can be more appealing than actual news in some instances. As a result, individuals become misled.

[9] Cohen, K.,(2018),”Before paying with Bitcoins”, The report provides a high-level summary of how blockchain technology works. It also discusses current applications of blockchain technology and possible future applications – in both the context of private transactions and public records. Finally, the report addresses some of the possible economic opportunities connected with blockchain technology as well as risks associated with both the technology and its uses. L. Liu et al.(2021)[2] proposed ”Peer-to-Peer Networking and Applications” to take action against news and online curated content on the internet which could be inimical to the sovereignty of any nation, the proposed solution being implemented by smart contracts may have the capacity to identify and flag such contenton websites and social media.

1.3 PROBLEM DEFINITION

To take action against fake news and online curated content on the internet which could be inimical to the sovereignty of any nation. The proposed solution being implemented by smart contracts may have the capacity to identify and flag such content on websites and social media.The solution may identify such content with reasonable accuracy, which could then be reviewed by the Ministry for taking appropriate action under the Rules. The current system analysis of forgery data is always questionable because there is no transparency and security provided. The blockchain proposed system will have the transparency by which one can fetch details of the user who made any forging in data, after which the officials can assess it and take appropriate action under the Rules.

1.4 OBJECTIVE

Scope of the project is to prevent forgery of data that can spread someone's personal ideologies and can harm the sovereignty of any nation using smart contract. The proposed project will be undoubtedly helpful for detecting fake news. Because of the block-chain's traceable and transparent nature it will be feasible to check the veracity of information or its sources, as well as to develop trust in online news.

Chapter 2

PROJECT DESCRIPTION

2.1 EXISTING SYSTEM

Existing system runs with the help of Machine learning and natural language processing and it tries to aggregate the news and later determine whether the news is real or fake using Support Vector Machine.It has higher data set. The ML based system has centralised access to the data, and it can be easily manipulated by anyone.Because of the multi-dimensional nature of fake news, the recognizing the category of news is not so easy.The proposed strategy is completely made out of Artificial Intelligence which is basic.

Disadvantages

- Require more data and space
- Trust issue
- Depends on accuracy

2.2 PROPOSED SYSTEM

The proposed system tracks and analyzes the news that is shared, thus restricting where it is fake or user manipulated. The system also proposes a real-time alert panel that aims to find out the reality of the news by taking user's votes. The news status is constantly tracked and then eventually modified once the threshold value is reached. The fake word data set can be used to spot misleading terms and prevent the fake news.

Advantages

- Decentralized structure and Trust
- Immutability
- Transparency

2.3 FEASIBILITY OF THE PROJECT

2.3.1 TECHNICAL FEASIBILITY

- IPFS database used for easily accessibility of data.
- ReactJs is used for SPA(Single Page Application).
- User friendly application.

2.3.2 ECONOMIC FEASIBILITY

Economic feasibility deals about the economic impact faced by the industry to implement a brand new system. The proposed system provides an efficient outcome. The whole setup is processed with ethereum based transactions. Cost per usage is least and it provides an safe digital transaction.

- It's very economical as it doesn't need more infrastructure.
- There is some cost for every transaction a user makes which will make it more effecient and effective.

2.3.3 MARKET FEASIBILITY

- The application would be free of cost for users. Prediction and estimation of the budget will be based on size, server, and project maintenance costs. A statistical analysis of the no. of consumers and participating retailers would decide the market scope of the application.
- Type of Software Project: Mobile Application
- Software Development – a new software, involving custom development.
- Size – Medium
- Time Frame – 3 Months

2.3.4 SOCIAL FEASIBILITY

The aspect of social feasibility is to test the amount of acceptance of the system by the user. The project has software installations that are easily accessible and operational to common user. It is an asset to eradicate spread of fake data along web. It is user-friendly after a briefing on the system connections.

2.3.5 SCHEDULING FEASIBILITY

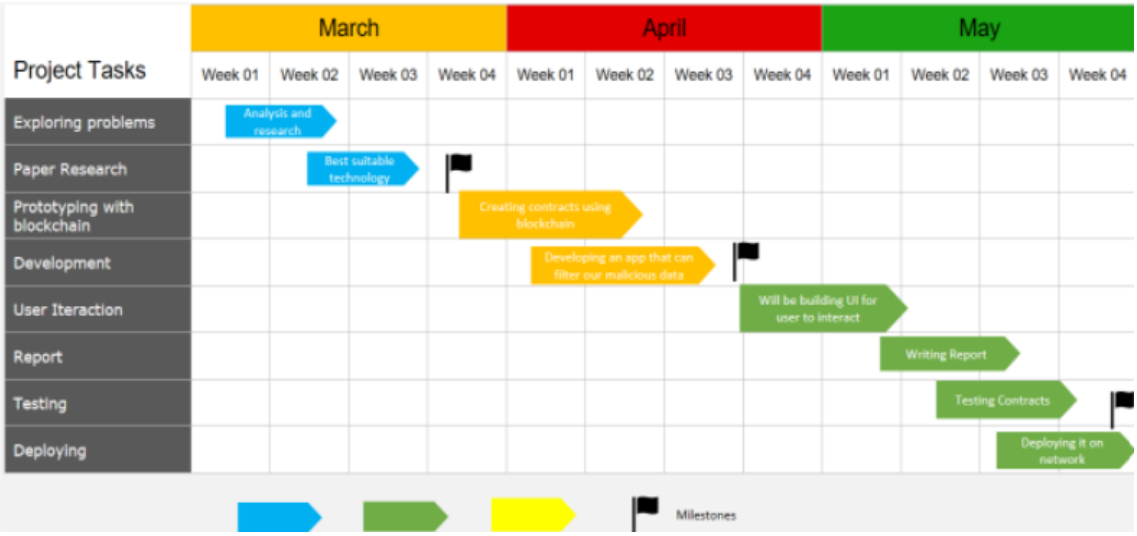

Figure 2.1: **Scheduling Feasibility**

2.4 SYSTEM SPECIFICATION

2.4.1 HARDWARE SPECIFICATION

- SSD :- 256GB
- RAM :- 4GB DDR-SDRAM

2.4.2 SOFTWARE SPECIFICATION

- Operating System: 64bit operating system, x64-based processor
- VScode
- Ethereum IDE, Ganache
- Metamask
- JavaScript
- Solidity
- ReactJs
- JSON

Chapter 3

SYSTEM DESIGN

3.1 ARCHITECTURE

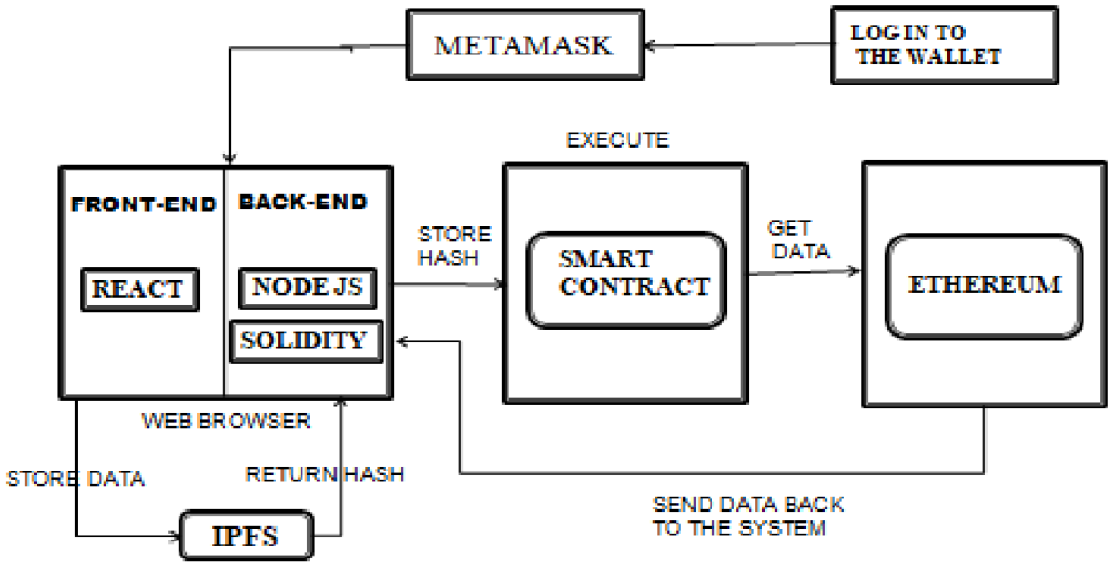

Figure 3.1: **Architecture Diagram**

Given architectural diagram is pictorial representation of step-by-step procedure that we followed to receive desired output.The proposed system has a transactional architecture. It works on the block chain framework.The system uses ganache that provides counterfeit currency to be used in local host and metamask for smart contract based transaction. Ethereum is used for the transactional functioning. The front end is procured using ReactJs and the back-end is managed by solidity. Metamask is the web extension that helps in logging to the crypto wallet and it is used for getting the data and sending it back to the system.

3.2 DESIGN PHASE

3.2.1 DATA FLOW DIAGRAM

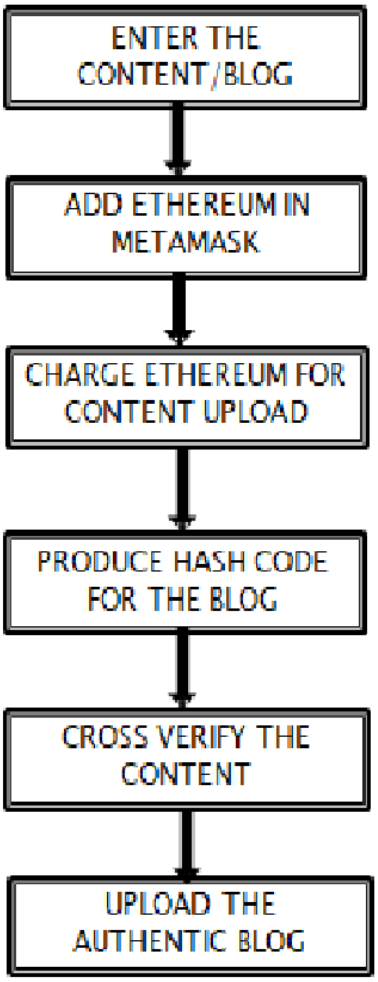

Figure 3.2: **Data Flow Diagram**

This flow diagram illustrates our overall strategy for data transfer and receiving. Once the required software's are installed a block chain based application is created. Before uploading the contents that are to be published user has to sign the smart contract proceedings. Official verification is done and the contents are proportionally filtered. Once done the filtered contents are published along the platform.

3.2.2 USE CASE DIAGRAM

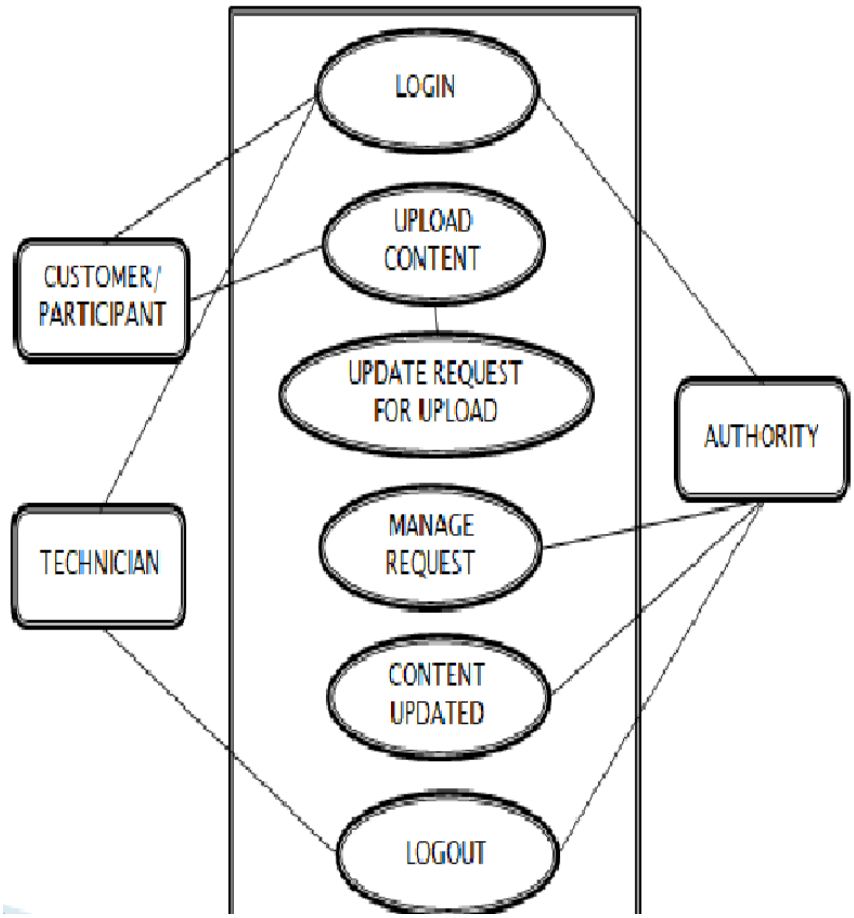

Figure 3.3: **Use Case Diagram**

The project fully look into eradicating forgery data across web. When the user uploads a content into any online platforms or social media websites the system cross checks the content by other nodes in the chain.Only then its finally uploaded. Also if the user wants to delete/edit this content based o the proportional filtration the system intakes an 50 percentage vote to confirm whether the article can be altered or not.

3.2.3 ACTIVITY DIAGRAM

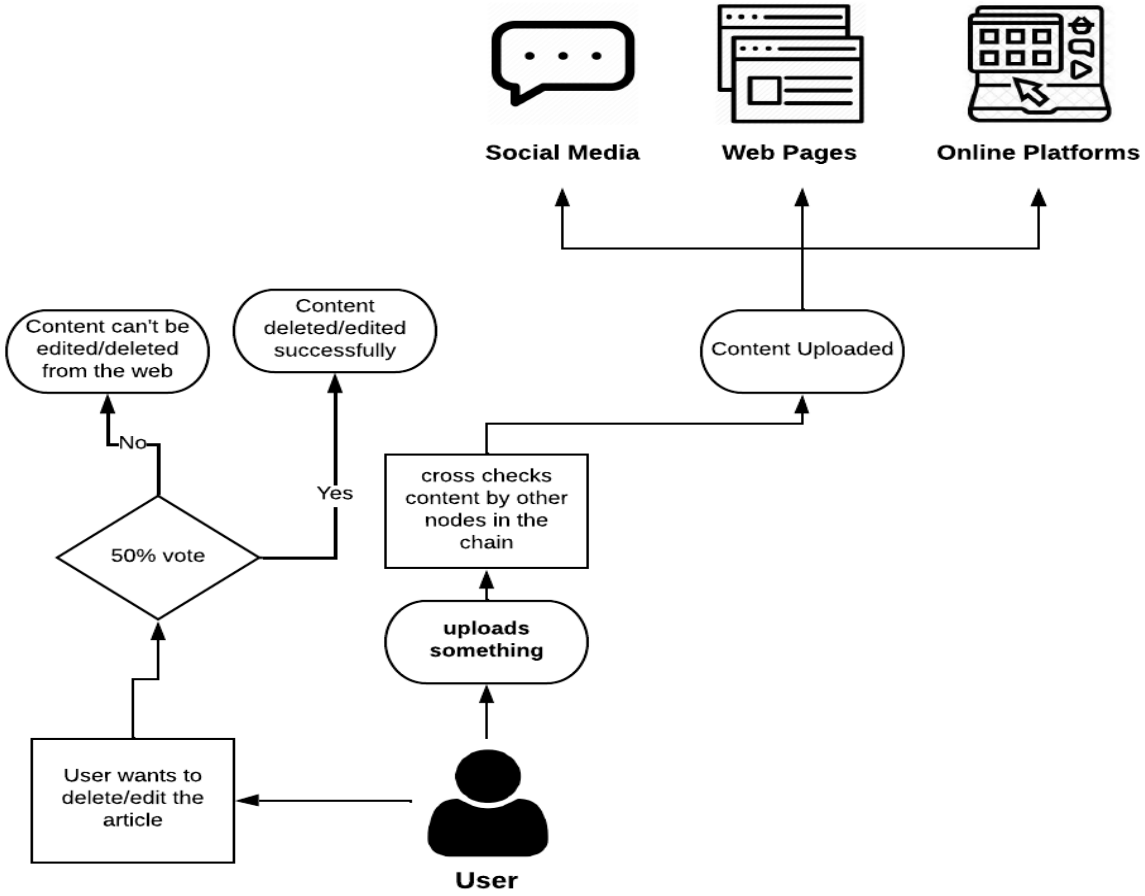

Figure 3.4: **Activity diagram**

The project fully look into eradicating forgery data across web. When the user uploads a content into any online platforms or social media websites the system cross checks the content by other nodes in the chain. Only then its finally uploaded. Also if the user wants to delete/edit this content based o the proportional filtration the system intakes an 50 percentage vote to confirm whether the article can be altered or not.

3.3 MODULE DESCRIPTION

3.3.1 MODULE 1: INITIALIZING THE PROJECT AND CONNECT WITH RINKBEY TEST NETWORKS

- This project have three different application which is then integrated with one another.
- Firstly, I have to install a ReactJs project then to connect with any blockchain network, I have installed contracts using hardhat(i.e. a compiler to compile smart contracts).
- Later we need IPFS file system for that I have used sanity.io.

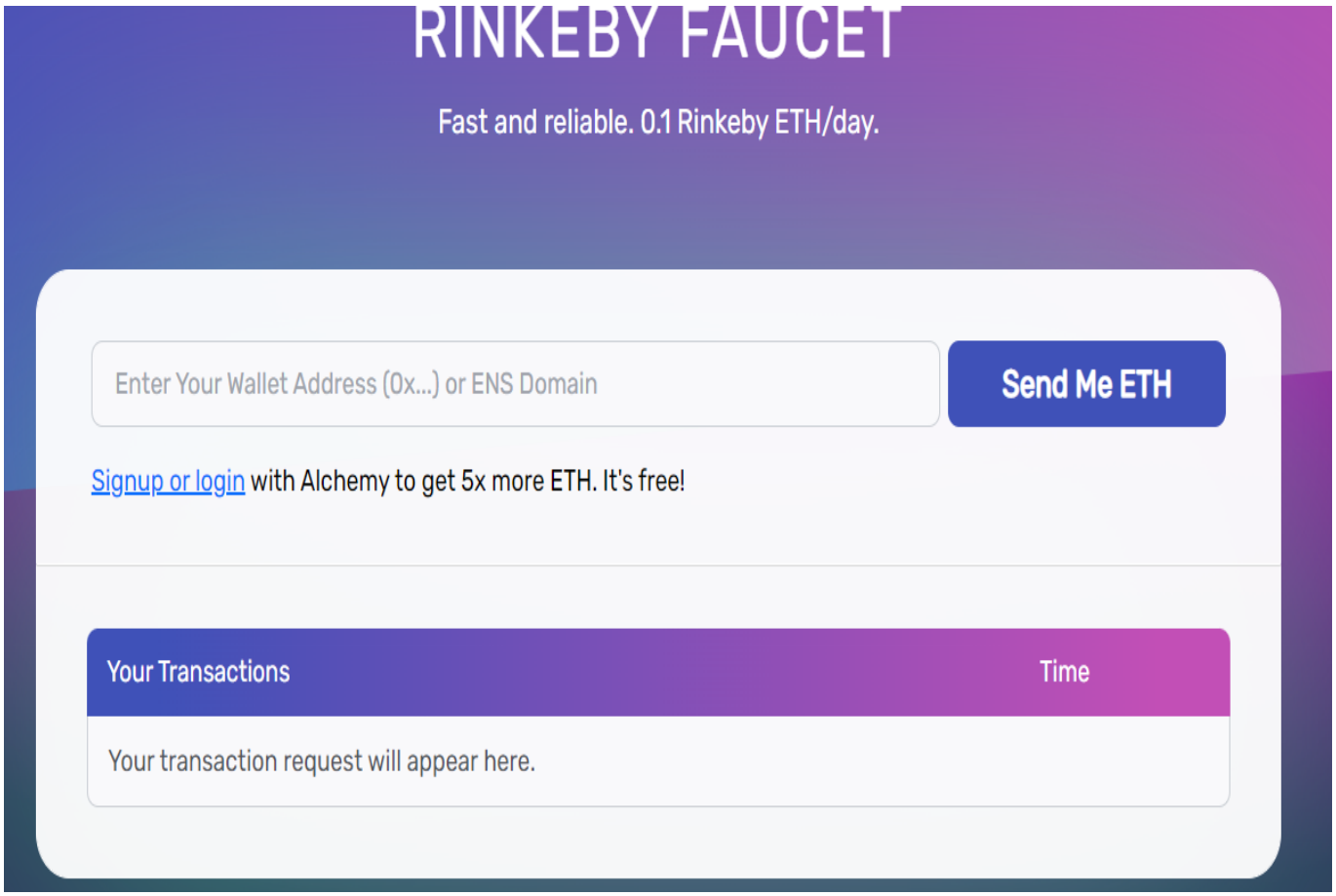

Figure 3.5: **Collection of ETHs**

3.3.2 MODULE 2: PLANNED AND CREATED THE SMART CONTRACT USING SOLIDITY

- Here the functional and class based components are created in VS Code using solidity and define the working of respective components.
- By running this set of code, token IDs are assigned to each content that are supposed to uploaded.

```
function _setTokenURI(uint256 tokenId, string memory _tokenURI) internal {
    _tokenURIs[tokenId] = _tokenURI;
}

function tokenURI(uint256 tokenId) public view virtual override returns (string memory) {
    require(_exists(tokenId),"URI not exist on that ID");
    string memory _RUri =  _tokenURIs[tokenId];
    return _RUri;
}

function getAlltoken() public view returns (RenderToken[] memory){
    uint256 latestId = _tokenIds.current();
    RenderToken[] memory res = new RenderToken[](latestId);
    for(uint256 i = 0; i  <= latestId ; i++){
        if(_exists(i)){
            string memory uri = tokenURI(i);
            res[i] = RenderToken(i,uri," ");
        }
    }
    return res;
}
```

Figure 3.6: **Solidity lag. for smart contract**

3.3.3 MODULE 3: DEPLOYMENT OF CODE ON ETHEREUM NETWORK

- Each post requires ethereums network. After paying for the post, it goes through the verification.
- Adding any article will cost handsome amount, therefore many will avoid sharing fake data uselessly.Authorized and authentic posts next gets selected for getting displayed in the front-end.

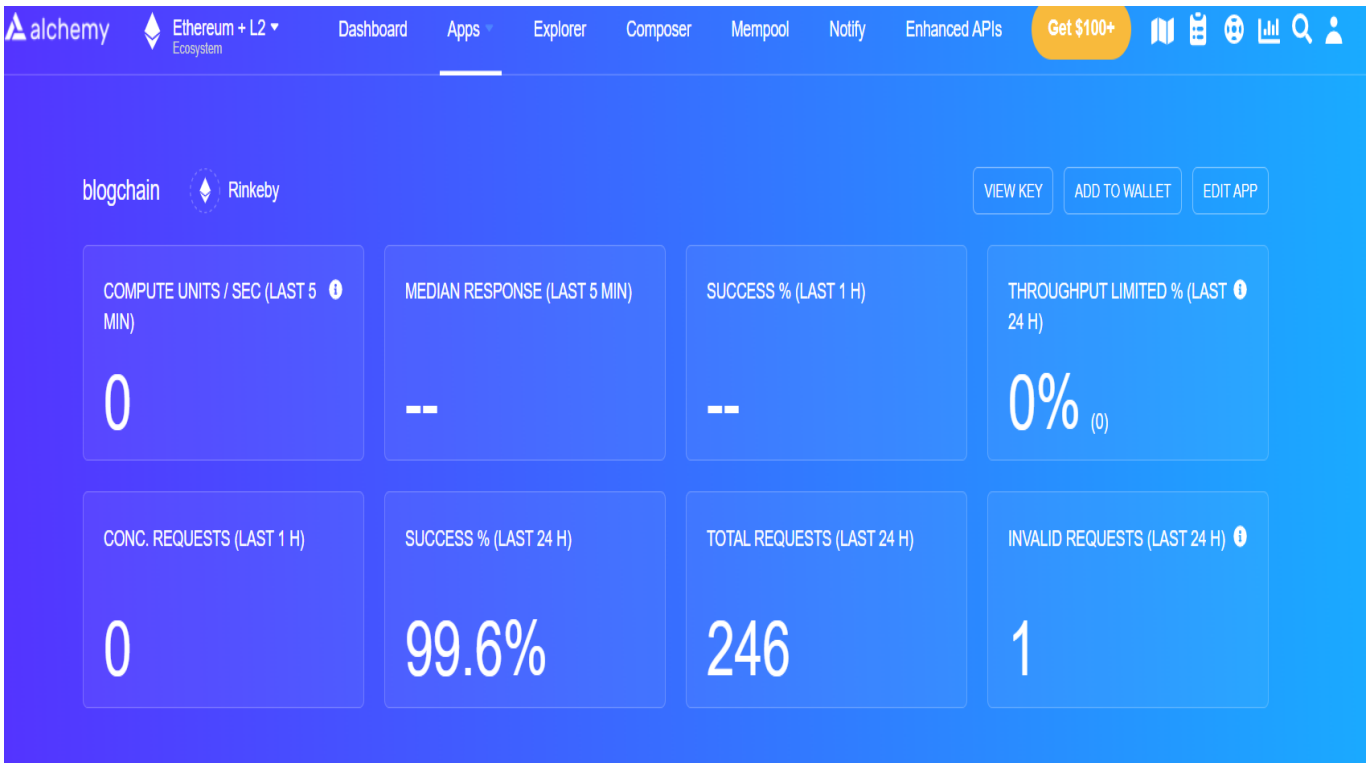

Figure 3.7: **Deployment on alchemy**

3.3.4 MODULE 4: INTEGRATION OF BACK-END AND FRONT-END

- Connect to metamask through any specified network.
- Fetch all the data from the IPFS file system *i.e* Sanity database.
- Display those dynamic data on the front-end.
- Addition of data from front-end which will then pushed to the IPFS file system.

Figure 3.8: **Data fetched from backend**

3.4 STEPS TO EXECUTE / RUN / IMPLEMENT THE PROJECT

3.4.1 STEP 1: CREATING PROJECTS USING REACTJS, SOLIDITY AND SANITY.IO

Before beginning this project I have successfully compiled three different projects that is written using two different language JavaScript and Solidity.

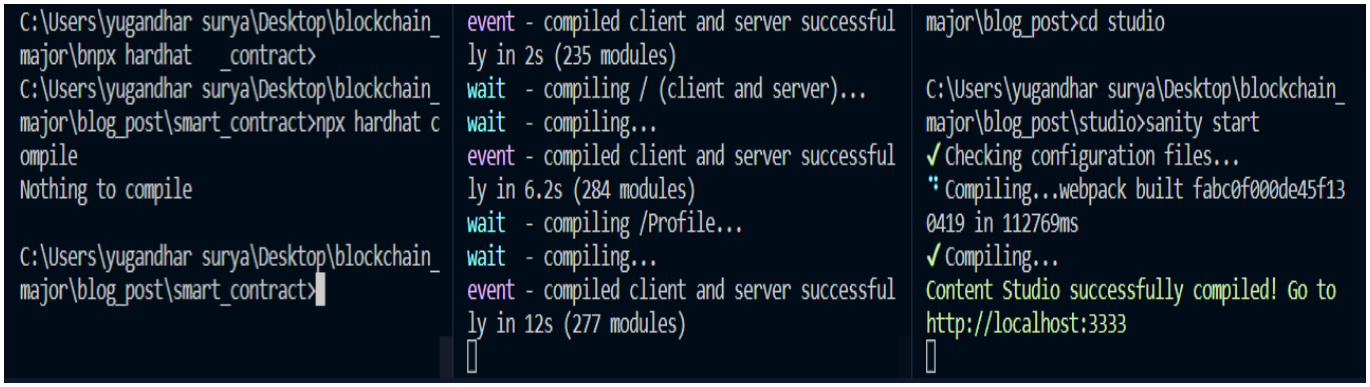

Figure 3.9: **Compiling the diff. projects**

3.4.2 STEP 2: CREATING CONTRACTS AND FUNCTIONAL COMPONENTS USING SOLIDITY

Making use of solidity language I have created some contracts that helped in building projects and connecting my project to the blockchain.

```
function getAlltoken() public view returns (RenderToken[] memory){
    uint256 latestId = _tokenIds.current();
    RenderToken[] memory res = new RenderToken[](latestId);
    for(uint256 i = 0; i  <= latestId ; i++){
        if(_exists(i)){
            string memory uri = tokenURI(i);
            res[i] = RenderToken(i,uri," ");
        }
    }
    return res;
}

function mint(address recipents, string memory _uri) public returns (uint256){
    uint256 newId = _tokenIds.current();
    _mint(recipents,newId);
    _setTokenURI(newId,_uri);
    _tokenIds.increment();
    return newId;
}
```

Figure 3.10: **Created contracts using solidity**

3.4.3 STEP 3: DESIGNING FRONT-END CLASS AND IT'S FUNCTIONAL COMPONENTS USING REACTJS

User experience is one of the main part of my application because creating contracts only have the back-end interaction for the developer but using ReactJs I have integrated front-end and back-end for better experience.

```
function Feed() {
  return (
    <div className={style.wrapper}>
      <div className={style.header}>
        <div className={style.headerTitle}>Home</div>
        <BsStars />
      </div>
      <TweetBox />
      {tweets.map((tweet, index) => (
        <Post
          key={index}
          displayName={tweet.displayName}
          userName={`${tweet.userName.slice(0,4)}...${tweet.userName.slice(-4)}`}
          avatar={tweet.avatar}
          text={tweet.text}
          isProfileImageNft={tweet.isProfileImageNft}
          timestamp={tweet.timestamp}
        />
      ))}
    </div>
  )
```

Figure 3.11: **Front-end using Reactjs**

3.4.4 STEP 4: CREATING SCHEMA USING SANITY DATABASE AND CONNECTING TO PINATA

As in blockchain, IPFS(Inter Planetary File System) type of database is used.In this application, pinata is used as IPFS. With each update in the application, all information related to that post goes to the pinata profile.

```
export const blogSchema = {
  name: "blogs",
  title: "Blogs",
  type: "document",
  fields: [
    {
      name: "blog",
      title: "Blog",
      type: "string",
    },
    {
      name: "timestamp",
      type: "datetime",
      title: "Timestamp",
    },
    {
      name: "author",
      title: "Author",
      type: "reference",
      to: [{ type: "users" }],
    },
  ],
};
```

Figure 3.12: **Schema using sanity and pinata**

3.4.5 STEP 5: CONNECTING BACK-END AND FORNT-END

Integrating solidity with the JavaScript language which is used in ReactJs to create front-end and solidity is used to create back-end of the application.

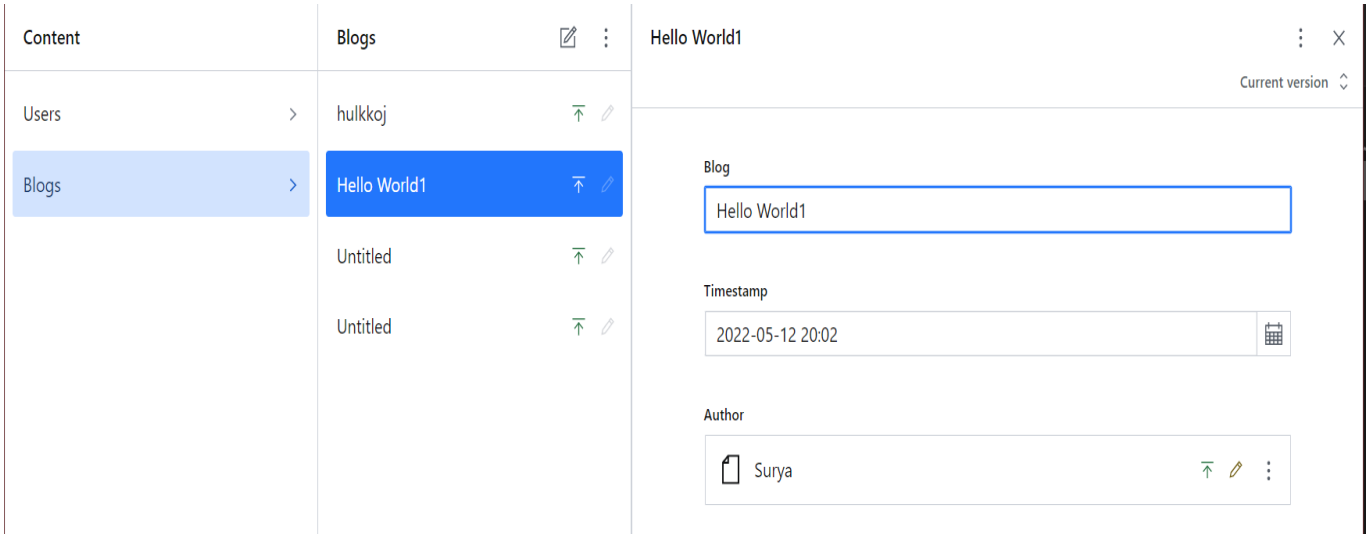

Figure 3.13: **Connecting back-end with front-end**

Chapter 4

IMPLEMENTATION AND TESTING

4.1 SOURCE CODE AND OUTPUT

4.1.1 SOURCE CODE

Creating smart contract using solidity

```
const main = async () => {
  const profileImageFactory = await hre.ethers.getContractFactory(
    "ProfileImageNfts"
  );
  const profileImageContract = await profileImageFactory.deploy();

  await profileImageContract.deployed();

  console.log(
    "Profile Image Minter deployed to:",
    profileImageContract.address
  );
};

(async () => {
  try {
    await main();
    process.exit(0);
  } catch (error) {
    console.error(error);
    process.exit(1);
  }
})();
```

Creating homepage to interact with front-end

```
const Home = () => {
  const { appStatus, connectWallet } = useContext(BlogContext)
  const userLoggedIn = (
    <div className={style.content}>
      <Sidebar initialSelectedIcon={'Home'} />
      <Feed />
      <Widgets />
    </div>
  )
  const noUserFound = (
    <div className={style.loginContainer}>
      <div className={style.walletConnectButton} onClick={() => connectWallet()}>
        Connect Wallet
      </div>
      <div className={style.loginContent}>Connect to Wallet</div>
    </div>
  )
  const error = (
    <div className={style.loginContainer}>
      <Image src={errorImg} width={250} height={250} />
      <div className={style.loginContent}>
        An error occurred. Please try again later or from another browser.
      </div>
    </div>
  )
  const noMetaMaskFound = (
    <div className={style.loginContainer}>
      <Image src={metamaskLogo} height={200} width={200} />
      <div className={style.loginContent}>
        <a
          target="_blank"
          rel="noreferrer"
          href={`https://metamask.io/download.html`}
        >
          You must install Metamask,<br />a virtual Ethereum wallet, in your
          browser.
        </a>
      </div>
    </div>
  )
  return (
    <div className={style.wrapper}>
      {app(appStatus)}
    </div>
  )
}
```

Uploading documents to the IPFS database

```
const ProfileImageMinter = () => {

  const [status,setStatus] = useState('initial')


  const { currentAccount, setAppStatus } = useContext(BlogContext)
  const router = useRouter()

  const [name, setName] = useState('')
  const [description, setDescription] = useState('')
  const [profileImage, setProfileImage] = useState()


  const minter = async () => {
    if (!name || !description || !profileImage) return
    setStatus('loading')

    const pinataMetaData = {
      name: `${name} - ${description}`,
    }

    const ipfsImageHash = await pinFileToIPFS(profileImage, pinataMetaData)

    await client
      .patch(currentAccount)
      .set({ profileImage: ipfsImageHash })
      .set({ isProfileImageNft: true })
      .commit()

    const imageMetaData = {
      name: name,
      description: description,
      image: `ipfs://${ipfsImageHash}`,
    }

    const ipfsJsonHash = await pinJSONToIPFS(imageMetaData,pinataMetaData)


    const contract = await getEthereumContract()
    // console.log(ipfsJsonHash)

    const transactionParameters = {
      to: contractAddress,
      from: currentAccount,
      data: await contract.mint(currentAccount, `ipfs://${ipfsJsonHash}`),
    }

    try {
      await metamask.request({
```

```
        method: 'eth_sendTransaction',
        params: [transactionParameters],
      })

      setStatus('finished')
    } catch (error) {
      console.log(error)
      setStatus('finished')
    }
  }


  const modalChildren = (modalStatus = status) => {
    switch (modalStatus) {
      case 'initial':
        return (
          <InitialState
            profileImage={profileImage}
            setProfileImage={setProfileImage}
            name={name}
            setName={setName}
            description={description}
            setDescription={setDescription}
            minter={minter}
          />
        )
      case 'loading':
        return <LoadingState />
      case 'finished':
        return <FinishedState />
      default:
        router.push('/')
        setAppStatus('error')
        break;
    }
  }

  return (
    <>{modalChildren(status)}</>
  )
}
```

Fetching data from server to the profile page

```
const ProfileHeader = () => {
  const { currentAccount, currentUser } = useContext(BlogContext)
  const router = useRouter()
  return (
    <div className={style.wrapper}>
      <div className={style.header}>
        <div onClick={() => router.push('/')} className={style.backButton}>
          <BsArrowLeftShort />
        </div>
        <div className={style.details}>
          <div className={style.primary}>{currentUser.name}</div>
          <div className={style.secondary}>
            {currentUser.blogs?.length}{' '}
            {currentUser.blogs?.length === 1 ? 'Blog' : 'Blogs'}
          </div>
        </div>
      </div>
      <div className={style.coverPhotoContainer}>
        <img
          src={currentUser.coverImage}
          alt="cover"
          className={style.coverPhoto}
        />
      </div>
      <div className={style.profileImageContainer}>
        <div
          className={
            currentUser.isProfileImageNft ? 'hex' : style.profileImageContainer
          }
        >
          <img
            src={currentUser.profileImage}
            alt={currentUser.walletAddress}
            className={
              currentUser.isProfileImageNft
                ? style.profileImageNft
                : style.profileImage
            }
          />
        </div>
      </div>
      <div className={style.details}>
        <div>
          <div className={style.primary}>{currentUser.name}</div>
        </div>
        <div className={style.secondary}>
          {currentAccount && (
            <>
              @{currentAccount.slice(0, 8)}...{currentAccount.slice(37)}
```

```
            </>
          )}
        </div>
      </div>
      <div className={style.nav}>
        <div className={style.activeNav}>Tweets</div>
        <div>Tweets & Replies</div>
        <div>Media</div>
        <div>Likes</div>
      </div>
    </div>
  )
}
```

Creating schema for the database

```
export const userSchema = {
  name: "users",
  type: "document",
  title: "Users",
  fields: [
    {
      name: "name",
      type: "string",
      title: "Name",
    },
    {
      name: "walletAddress",
      type: "string",
      title: "Wallet Address",
    },
    {
      name: "profileImage",
      type: "string",
      title: "Profile Image",
    },
    {
      name: "isProfileImageNft",
      title: "Is Profile Image NFT",
      type: "boolean",
    },
    {
      name: "coverImage",
      type: "string",
      title: "Cover Image",
    },
    {
      name: "blogs",
      title: "Blogs",
```

```
      type: "array",
      of: [
        {
          type: "reference",
          to: [{ type: "blogs" }],
        },
      ],
    },
  ],
};
```

Showing data uploaded to IPFS successfully.

```
const FinishedState = () => {
  const router = useRouter()
  const { getCurrentUserDetails } = useContext(BlogContext)

  useEffect(() => {
    getCurrentUserDetails()
  })

  return (
    <div className={style.wrapper}>
      <div className={style.title}>Minting Successful!</div>
      <Image src={checkMark} alt="checkmark" height={100} width={100} />
      <div onClick={() => router.push('/')} className={style.closeButton}>
        Close
      </div>
    </div>
  )
}
```

4.1.2 OUTPUT

Fetching details from sanity.io database and IPFS database(Pinata)

Figure 4.1: **Home Page Layout**

Single user data fetched from database

Figure 4.2: **Profile Page Layout**

Uploading data(Profile Image, Title, Description) to the pinata

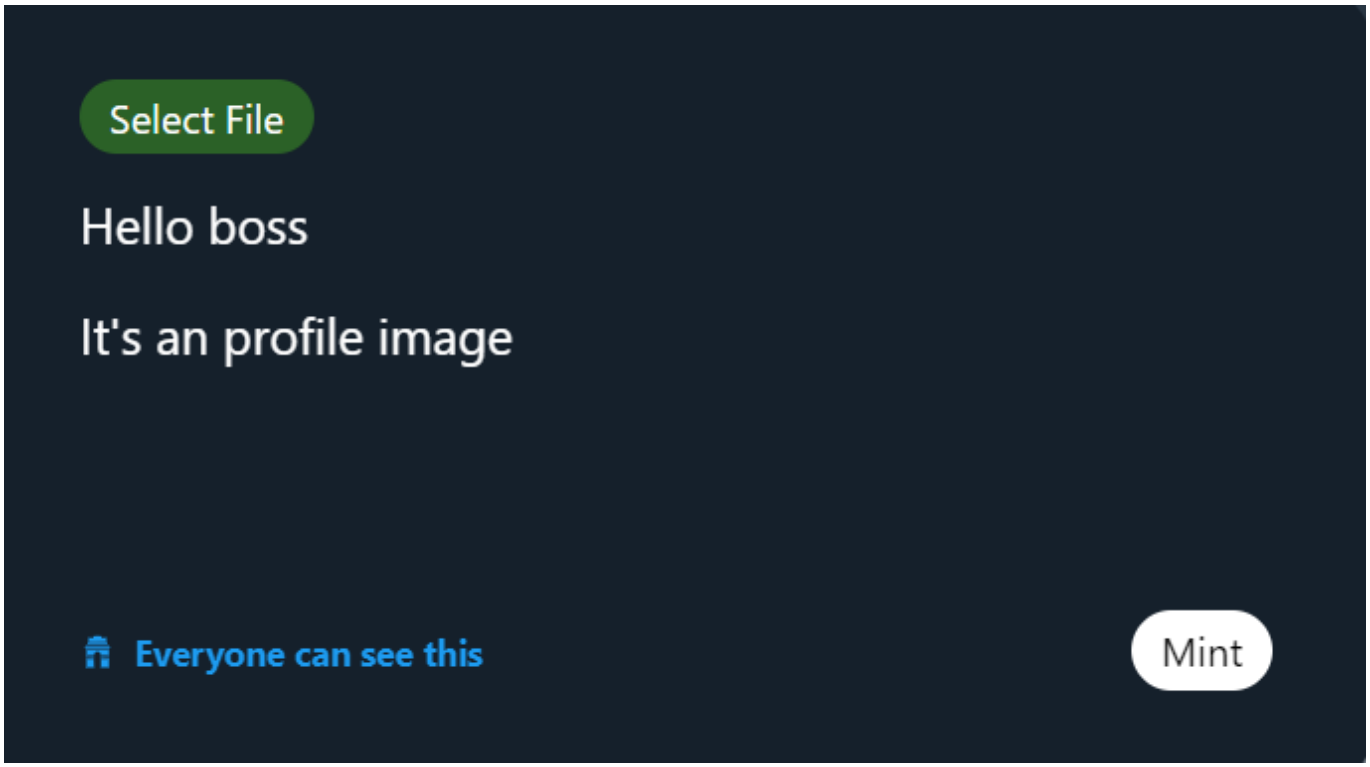

Figure 4.3: **Minting Layout**

Processing to upload the data's on the IPFS database

Figure 4.4: **Progressing Layout**

Successfully uploaded all the data to the pinata

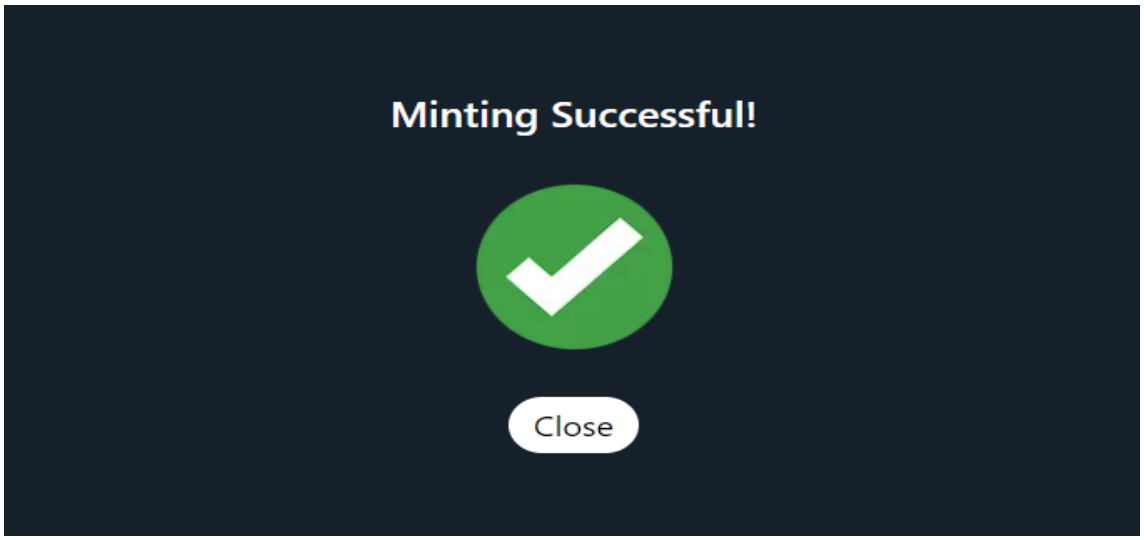

Figure 4.5: **Successful Layout**

Giving money to publish my data on the blockchain network

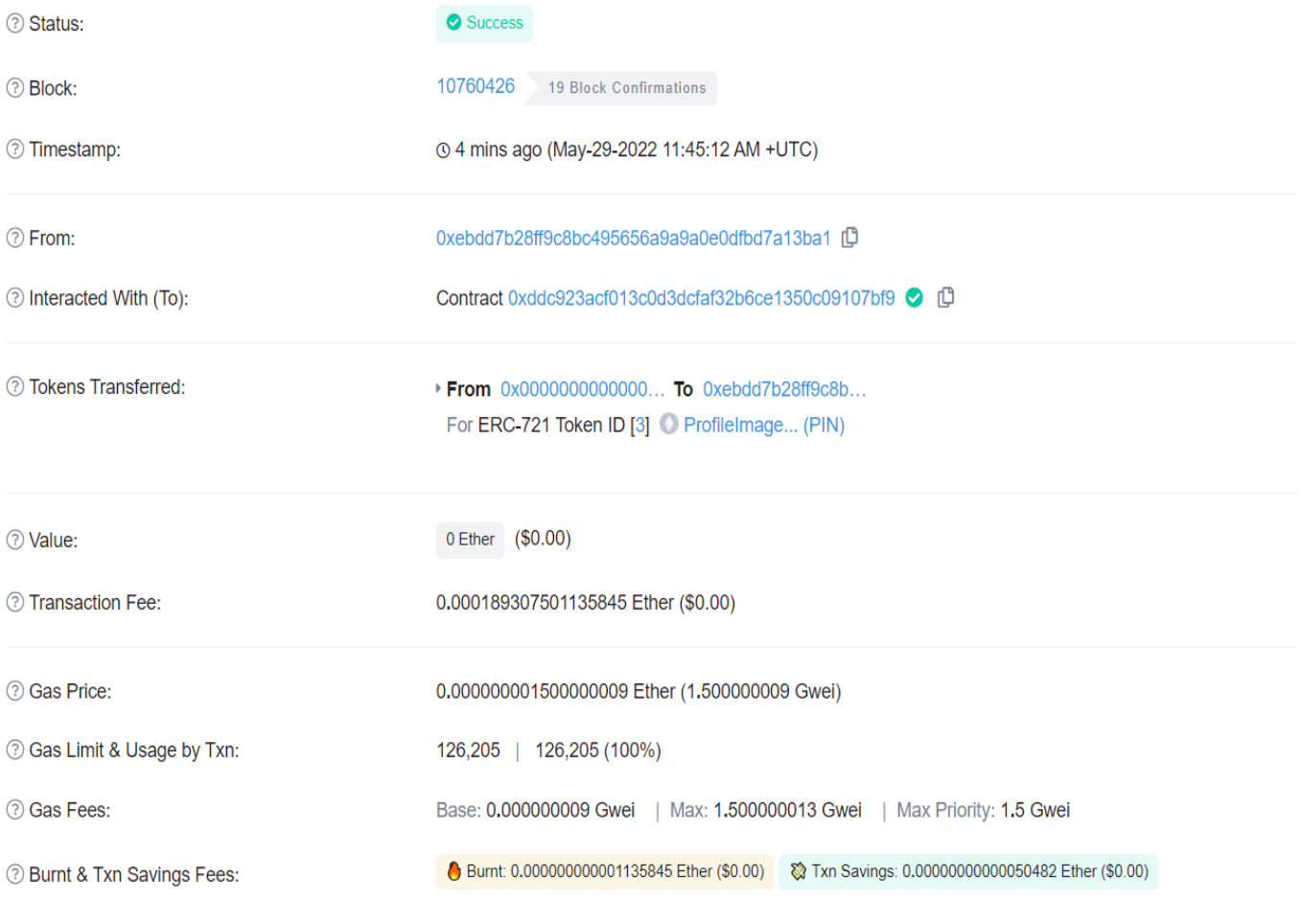

Figure 4.6: **Metamask**

4.2 TESTING

4.3 TYPES OF TESTING

Software testing is an important aspect of the process. The testing procedure ensures that the developed product meets the specifications for which it was created. Building test cases against which the product must be tested is an important part of the testing process.The various testing procedures like unit,integral and functional testing procedures implemented on applicational level testing.

4.3.1 UNIT TESTING

Unit testing is conducting to verify the functional performance of each modular component of the application. Unit testing focuses on the smallest unit of the application design. This project underwent a progressive examination of unit testing and I tested all the packages that constitute the model and I have found out that these packages were self independent and was able to yield the required result at all instances.

Input

```
const CheckIfWalletIsLoggedIn = async () => {
  if (!window.ethereum) return
  try {
    const addressArray = await window.ethereum.request({
      method: 'eth_accounts',
    })
    if (addressArray.length > 0) {
      setAppStatus('connected')
      setCurrentAccount(addressArray[0])
      createUserAccount(addressArray[0])
    } else {
      router.push('/')
      setAppStatus('notConnected')
    }
  } catch (error) {
    console.log(error)
    router.push('/')
    setAppStatus('error')
  }
}
```

Figure 4.7: **Unit Testing**

Figure 4.8: **Homepage**

4.3.2 INTEGRATION TESTING

Integration testing is a systematic technique for construction the program structure while at the same time conducting tests to uncover errors associated with interfacing. Integration testing is the complete testing of the set of modules which makes up the product. For this project a sequential analysis of integration testing was done.

Input

```
const { blogs } = useContext(BlogContext)


return (
  <div className={style.wrapper}>
    <div className={style.header}>
      <div className={style.headerTitle}>Home</div>
      <BsStars />
    </div>
    <TweetBox />
    {blogs.map((tweet, index) => (
      <Post
        key={index}
        displayName={
          tweet.author.name === 'Unnamed'
            ? `${tweet.author.walletAddress.slice(
                0,
                4
              )}...${tweet.author.walletAddress.slice(41)}`
            : tweet.author.name
```

Figure 4.9: **Integration Testing**

Figure 4.10: **Image of uploaded tweets**

4.3.3 FUNCTIONAL TESTING

Functional testing is a quality assurance (QA) process and a type of black-box testing that bases its test cases on the applications of the software component under test. Functions are tested by feeding them input and examining the output and internal program structure is rarely considered (unlike white box-testing). It is basically defined as a type of testing which verifies that each function of the software application works in conformance with the requirement and specification. This testing is not concerned about the source code of the application. Each functionality of the software application is tested by providing appropriate test input, expecting the output and comparing the actual output with the expected output.

Input

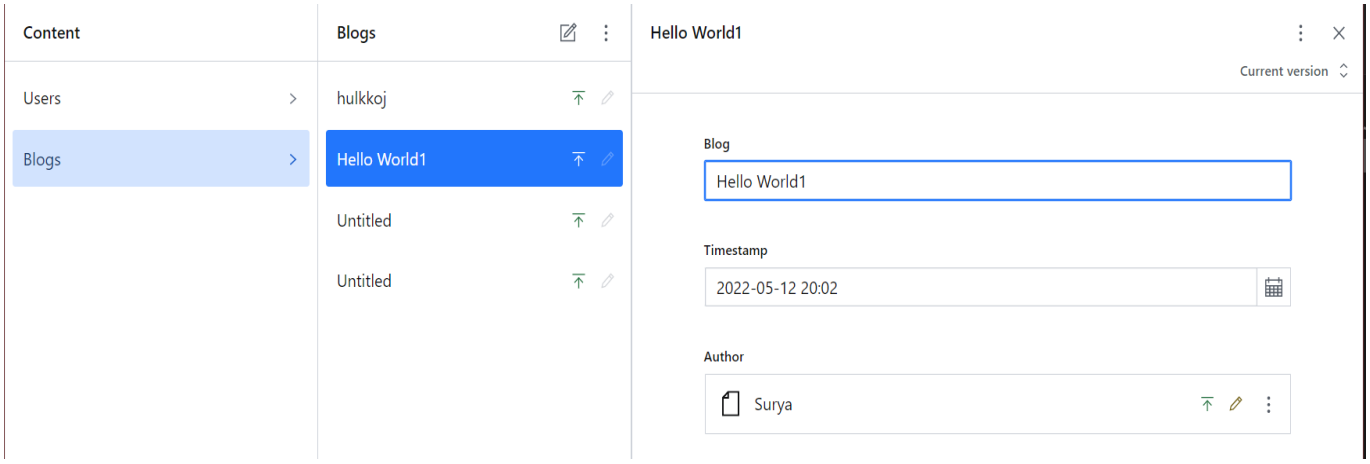

Figure 4.11: **Functional Testing**

Whenever someone uploads any content on my application, content identifier(CID) is getting generated from pinata which acts as an IPFS database.

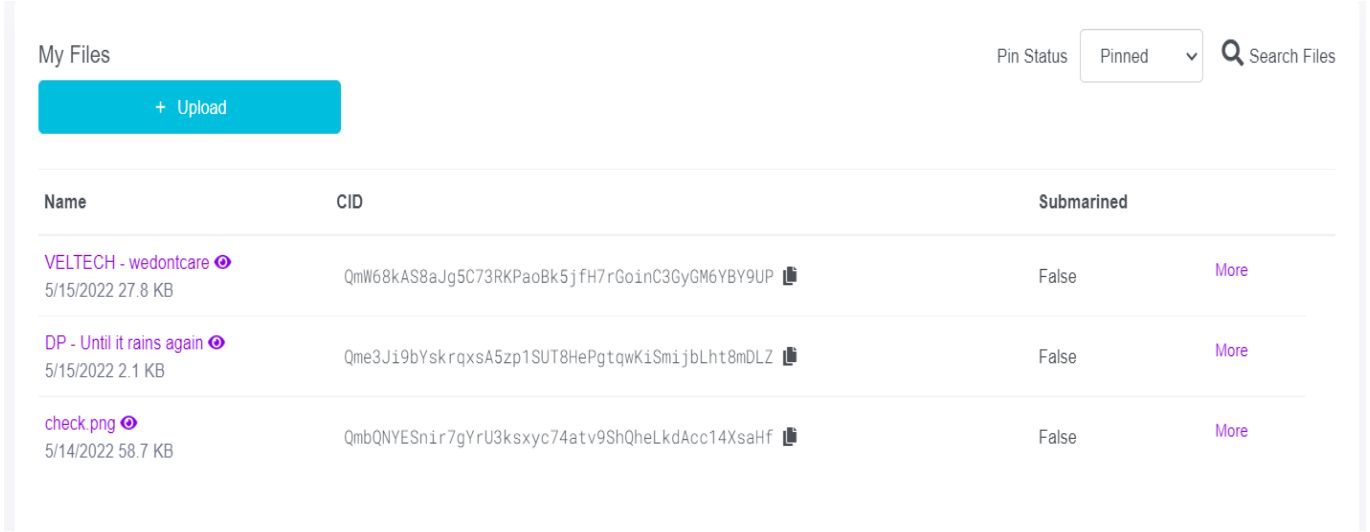

Figure 4.12: **TokenId generated in pinata**

4.3.4 TEST RESULTS

From the above image, it is confirmed that sanity is successfully connected to the localhost and localhost is fetching all required data from sanity.

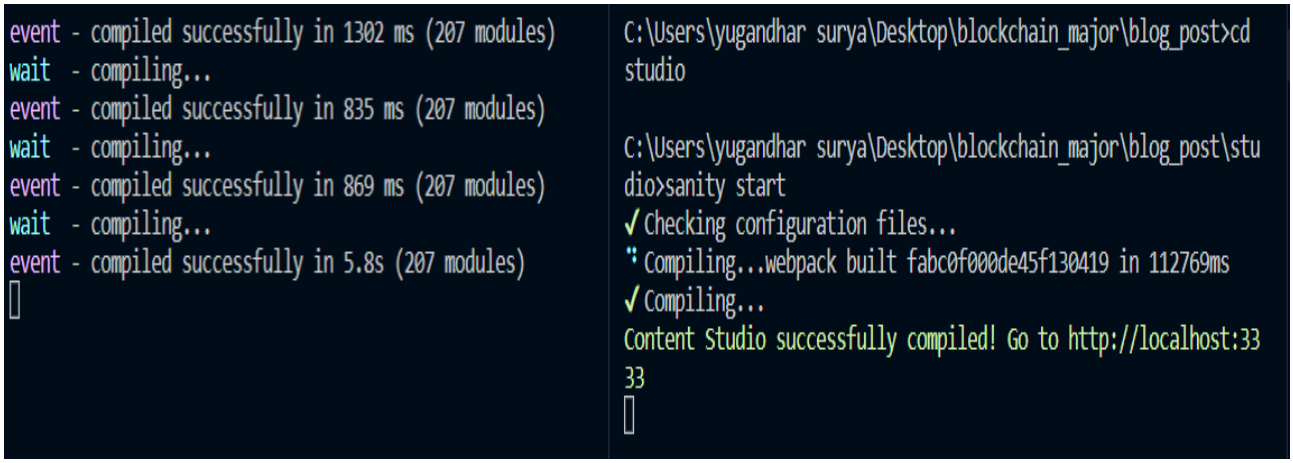

Figure 4.13: **Connected to localhost and sanity**

Created some test cases that verifies my application is working securely. As it passes all the test cases, it is confirmed that my application is working fine.

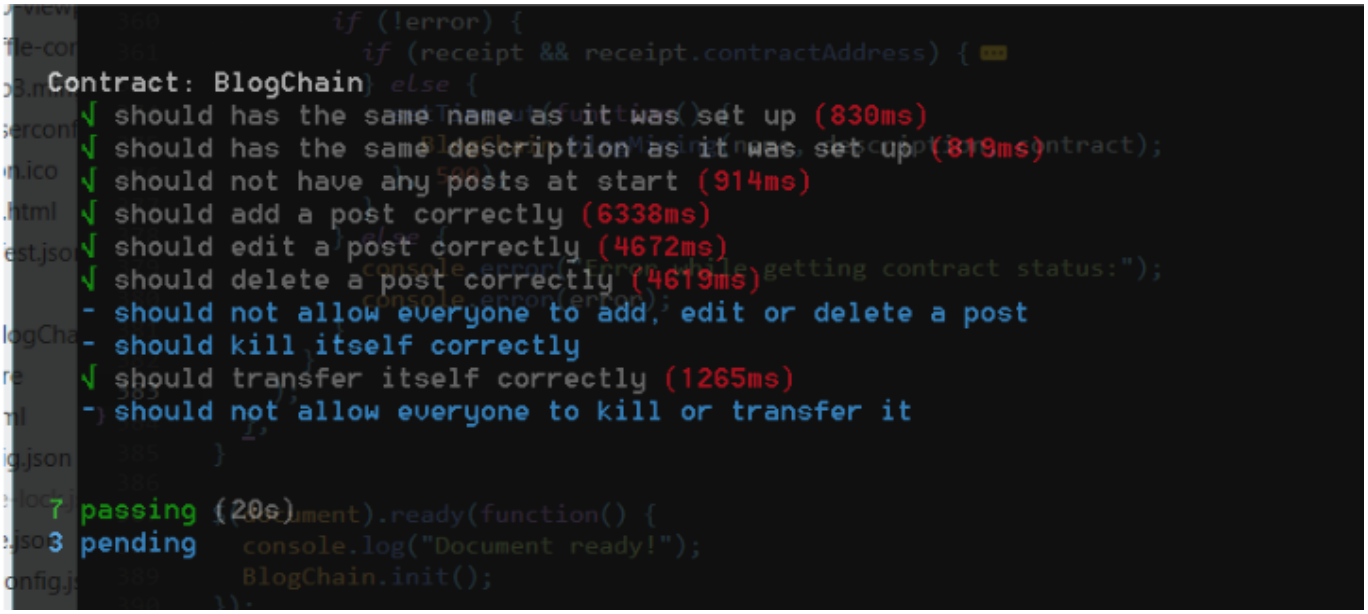

Figure 4.14: **Successfully verified all test cases**

Chapter 5

RESULTS

5.1 EFFICIENCY OF THE PROPOSED SYSTEM

The proposed system is tentatively safe, secure and transparent for the user. The distribution of counterfeit goods has become widespread in recent years. In today's supply chain, there are numerous phoney products. Fake product cases have increased in recent years, according to the research. Customers or users must be able to examine all of the product's details so that they can determine whether the goods is genuine or not. There is currently no system in place in India to detect counterfeit goods. As a result, the solution entails a simple QR code-based identification that allows the end-user or customer to scan and verify the product's authenticity using a smartphone.

5.2 COMPARISON OF EXISTING AND PROPOSED SYSTEM

5.2.1 EXISTING SYSTEM

Existing machine learning and deep learning methods are focused on detecting news of particular types (such as political). Accordingly, they developed their models and designed features for specific datasets that match their topic of interest. These approaches might suffer from dataset bias and perform poorly on news of another topic. Hence, it is important to study if these are sufficient for different types of news published in online media by evaluating various models on different diverse datasets and comparing their performances. However, the existing comparative studies on fake news detection methods also focused on a specific type of dataset or explored a limited number of models.However, the length of this dataset is not sufficient for neural network based advanced models, and some models were found to suffer from overfitting.

5.2.2 PROPOSED SYSTEM

The proposed system tracks and analyzes the news that is shared, thus restricting where it is fake or user manipulated. The system also proposes a real-time alert panel that aims to find out the reality of the news by taking user's votes. The news status is constantly tracked and then eventually modified once the threshold value is reached. The fake word data set can be used to spot misleading terms and prevent the fake news.When a user tries to find a blog using their address, our function is checking if the address is matched with any existing address or not. Verified that all the functionality of this project works as expected.The proposed systems make use of block-chain technology for verifying the source and content of the news. Using block chain makes it secure and efficient as it identifies the user's malicious intent and hence prevents it from spreading fake news.

5.3 SAMPLE CODE

```
function SidebarOption({ text, Icon, isActive, setSelected, redirect }) {
  const router = useRouter()

  const handleClick = (buttonText = text) => {
    if (buttonText !== 'More' && setSelected) {
      setSelected(buttonText)
    } else return
  }

  return (
    <div
      className={style.wrapper}
      onClick={() => {
        handleClick(text)
        if (redirect) {
          router.push(redirect)
        } else return
      }}
    >

  )
}
```

5.3.1 OUTPUT

It is a profile page which contains all information about the user like name, hash code, image(checks if NFT or not), number of blogs and timestamp. These data are fetched from sanity and pinata.

Figure 5.1: **Personal Information of participant**

In sanity.io, all information about the user/participant such as name, who uploads the blog is saved

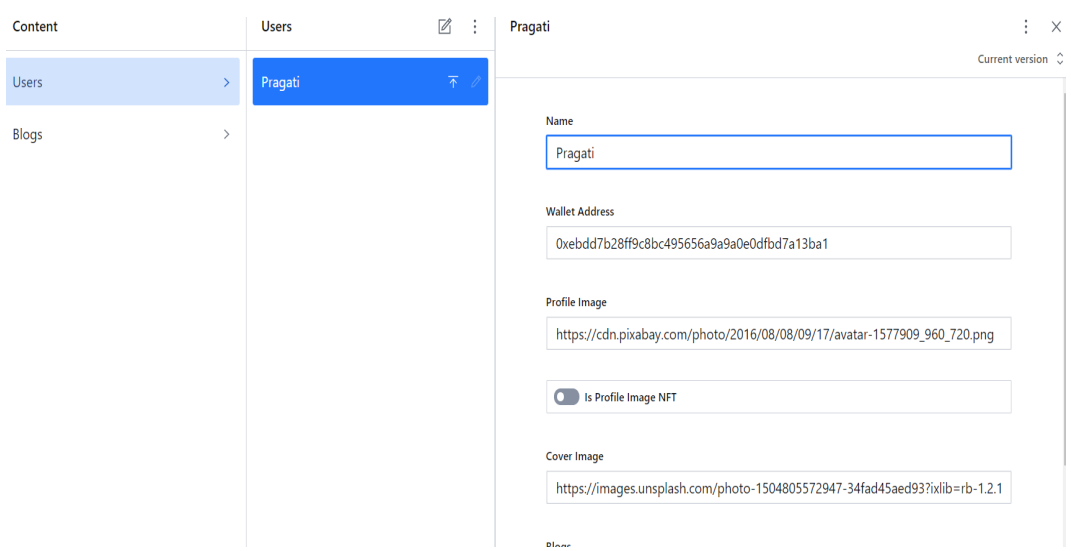

Figure 5.2: **User Verification on Sanity**

This section of sanity contains content of the blog which is being uploaded from front-end.

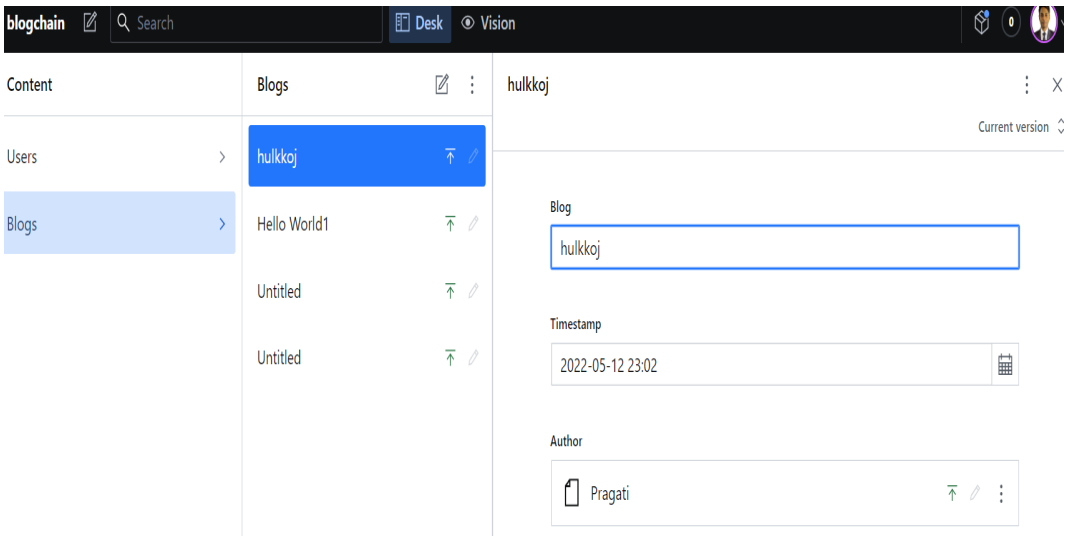

Figure 5.3: **Blog/Content Verification on Sanity**

This page fetches all the required data from sanity database and displays all data.

Figure 5.4: **Uploaded Contents**

Chapter 6

CONCLUSION AND FUTURE ENHANCEMENTS

6.1 CONCLUSION

A new system is proposed to detect and avoid further spreading of fake news and validate the information from origin. The proposed systems make use of block-chain technology for verifying the source and content of the news. Using block chain makes it secure, transparent, smart and efficient as it identifies the user's malicious intent (if any) and hence prevents it from spreading fake news. It also restricts any further change in the content ones uploaded and reduces the chance to escape after creating a havoc. RTAP (Real Time Alert Panel) keeps track of the live news and constantly updates news status. Block chain based forgery data detection preserves the interest and sterility of the readers.

6.2 FUTURE ENHANCEMENTS

This research looked into the current state of the block chain technology landscape. This included a general review of block chain technology as well as a more in-depth look at existing research publications and potential study fields. As a result, the goal of this project was to improve understanding of the technologies, as well as to spur further research and uncover knowledge gaps. From our perspective, the future of block chain technologies is incredibly promising, but there are issues and obstacles that must be addressed before widespread adoption. For example, 51 percent attacks, authentication, data malleability, latency, throughput, size, and bandwidth are all difficulties in security. But also in terms of personal privacy, personal data, the right to be forgotten. In its initial form, block chains are also incredibly energy inefficient. We need to use various forms of consensus and byzantine fault tolerance instead of POW. There are also issues on the developer side, as there is now no clear front runner among the various products available. There is also no agreement on the usefulness of block chains, developer support, end user support, or how they should be linked into other systems. This causes problems with chain versions, forks, numerous chains, side chains, and so forth. Finally, block chain systems rely heavily on hash puzzles and asymmetric encryption that are now available. If one of these fails, or if a flaw is revealed, the chain becomes untrustworthy and useless.

REFERENCES

[1] Liqun Liu, Weihan Zhang, Cunqi Han,2021, ”A survey for the application of blockchain technology in the media”, Peer-to-Peer Networking and Applications, Issue 5, May 2021

[2] P. Fraga-Lamas and T. M. Fernández-Caramés, 2020, ”Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality,” in IT Professional, vol. 22, no. 2, pg no. 53-59, Issue March-April 2020.

[3] S. Cho and C. Jeong, 2019, ”A blockchain for media: Survey”, 2019 International Conference on Electronics, Information, and Communication (ICEIC), Issue Jan 2019, pg no. 1-2.

[4] S. E. Haddouti and M. D. Ech-Cherif El Kettani, 2019, ”Analysis of Identity Management Systems Using Blockchain Technology,” 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), Issue April 2019, pg no. 1-7.

[5] Shilpashree B N, Rohini Krishna Mohite, Sahana S, Rajesha, Rakesh K R, 2021, “Counterfeit Detection of Documents using Blockchain”, International Journal of Engineering Research Technology,Volume 10, Issue 07 ,July 2021.

[6] S. Paul, J. I. Joy, S. Sarker, A. -. A. -. H. Shakib, S. Ahmed and A. K. Das, ”Fake News Detection in Social Media using Blockchain,” 2019, 7th International Conference on Smart Computing Communications (ICSCC), pp. 1-5, September 2019.

[7] M. Torky, Emad Nabil, Wael Said,2019, “Proof of Credibility: A Blockchain Approach for Detecting and Blocking Fake News in Social Networks.” International Journal of Advanced Computer Science and Applications (2019),Vol. 10, Issue No. 12.

[8] Yazed Alsaawy, Ahmad Alkhodre, Nour Mahmoud Bahbouh, Adnan Abi Sen, Adnan Nadeem Al Hassan, 2021, ”Lightweight Chain for Detection of Rumors and Fake News in Social Media”,International Journal of Advanced Computer Science and Applications, August 2021.

[9] McKinsey Company, 2019,"Beyond the Hype: Blockchains in Capital Markets",Corporate Investment Banking / No 12,March 2019.

[10] Cohen, K.,2018,"Before paying with Bitcoins", Retrieved from FTC Consumer Information Theory, 22(6),644-654, June 22, 2019.