PROJECT REPORT

Date	25/11/2023
Team ID	**au622420121032**
Project Name	Ethereum Decentralized Identity Smart Contract

CHAPTER 1

INTRODUCTION

1.1 PROJECT OVERVIEW

Traditional paper certificates and electronic certificates are difficult to handle and preserve, may need third parties to authenticate the certificate, take a lot of time, and have a potential of being tampered with. People routinely fabricate certificates to represent their credentials and degrees. A false certificate created by a skilled con artist is never easy to spot and address as the real one. As a result, it is imperative to enhance the certification and verification procedure. So, to avoid such issues, we want to develop a project where we can use blockchain technology for verification of certificates. Initially University will enter the students roll number and upload their college certificate and it will be stored on Interplanetary File System (IPFS) by generating a hash which uniquely identifies that block. Now any person like the student or recruiter or an administrator can fetch and verify the college certificate by providing a unique hash value and roll number of the student. And we can also validate the certificate by providing the certificate and roll number of the student in case we forget the generated hash value. This can result in increased security, lower costs, and a quicker platform for verifying educational certificates.

Keywords: Ethereum · IPFS · Smart Contracts · MetaMask

1.2.PURPOSE

The fundamental pattern of a student's education in India is to enroll in kindergarten, then transferring to a different school for elementary, middle, and high school courses. After graduating from secondary school, pupils must now apply for admission to junior college. For students, this is the basic cycle of the academic year. This cycle has the drawback of requiring a student to submit all the certifications for approval at each stage. This could result in the certificate being broken or lost. Also, the validator finds it time-consuming to authenticate each certificate. It is quite difficult to maintain track of and certify such a large number of records due to the country's massive population. Certificate manipulation and the creation of false certificates consequently turn into negative occurrences. As technology advances, it becomes easier to create fake certifications. It will need a lot of focus to distinguish between a real certificate and a phoney one, which will waste time. Finding a clear solution necessitates a major investment of time, money, and resources.

CHAPTER 2

LITERATURE SURVEY

2.1.EXISTING PROBLEM

The problem arises with the student certificates in each stage of student's life for validation. As the data is huge, sometimes the data may be lost or tampered. The validator finds it challenging to authenticate each

certificate. The production of false certifications is getting simpler as technology develops. Differentiating between authentic and fraudulent certifications takes a lot of labor, which takes time. Because of centralization and digitization, the issue of fraudulent credentials has become a headache for both colleges and recruitment firms. Innocent people's lives might be lost as a result of false buildings planned by false engineers and false medical care provided by false physicians. At the very least, it is necessary to properly validate the certificates before allowing someone to join the organization.

2.2.REFERENCES

1. A. Badr, L. Rafferty, Q. H. Mahmoud, K. Elgazzar and P. C. K. Hung, "A Permissioned Blockchain-Based System for Verification of Academic Records," 10th IFIP International

2. Conference on New Technologies, Mobility and Security (NTMS), CANARY ISLANDS, Spain, 2019, pp. 1–5.

3. Aisong Zhang and Xinxin Ma, "Decentralized Digital Certificate Revocation System Based on Blockchain", Journal of Physics: Conference Series, Volume 1069, 3rd Annual International Conference on Information System and Artificial Intelligence (ISAI2018) 22–24 June 2018, Suzhou.

4. Emmanuel Nyaletey, Reza M. Parizi, Kim-Kwang Raymond Choo, "BlockIPFS - Blockchainenabled Interplanetary File System for Forensic and Trusted Data Traceability", Published on IEEE International Conference on Blockchain, 2019.

5. Gunit Malik, Sai Prasanth Reddy, Dr. Seema Shah, "Blockchain Based Identity Verification Model", International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 2019.

6. Izuchukwu Chijioke Emele, Stanley Ikechukwu Oguoma, Kanayo Kizito Uka, Emeka Christian Nwaoha “An Enhanced Web Base Certificate Verification System”. Decentralized Smart Contract 461
7. Iftekher Toufique Imam, Yamin Arafat, Kazi Saeed Alam and Shaikh Akib Shahriya,“DOC BLOCK: A Blockchain Based Authentication System for Digital Documents” Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021) , Volume-7, Issue-03, March 2021.
8. J. Cheng, N. Lee, C. Chi and Y. Chen, “Blockchain and smart contract for digital certificate,” IEEE ICASI, Chiba, 2018, pp. 1046–1051
. 9. Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, “Blockchain and Smart Contract for Digital Certificate,” IEEE International Conference on Applied System Innovation 2018.
10. Meerja vali Shaik, Ch. Rupa,M N S Koundinya, Rohith Gadde, Harish Donepudi, “Blockchain based Certificate Issuing System using Smart Contracts” IJITEE, Volume-9, Issue-7, May 2020

2.3.PROBLEM STATEMENT DEFINITION

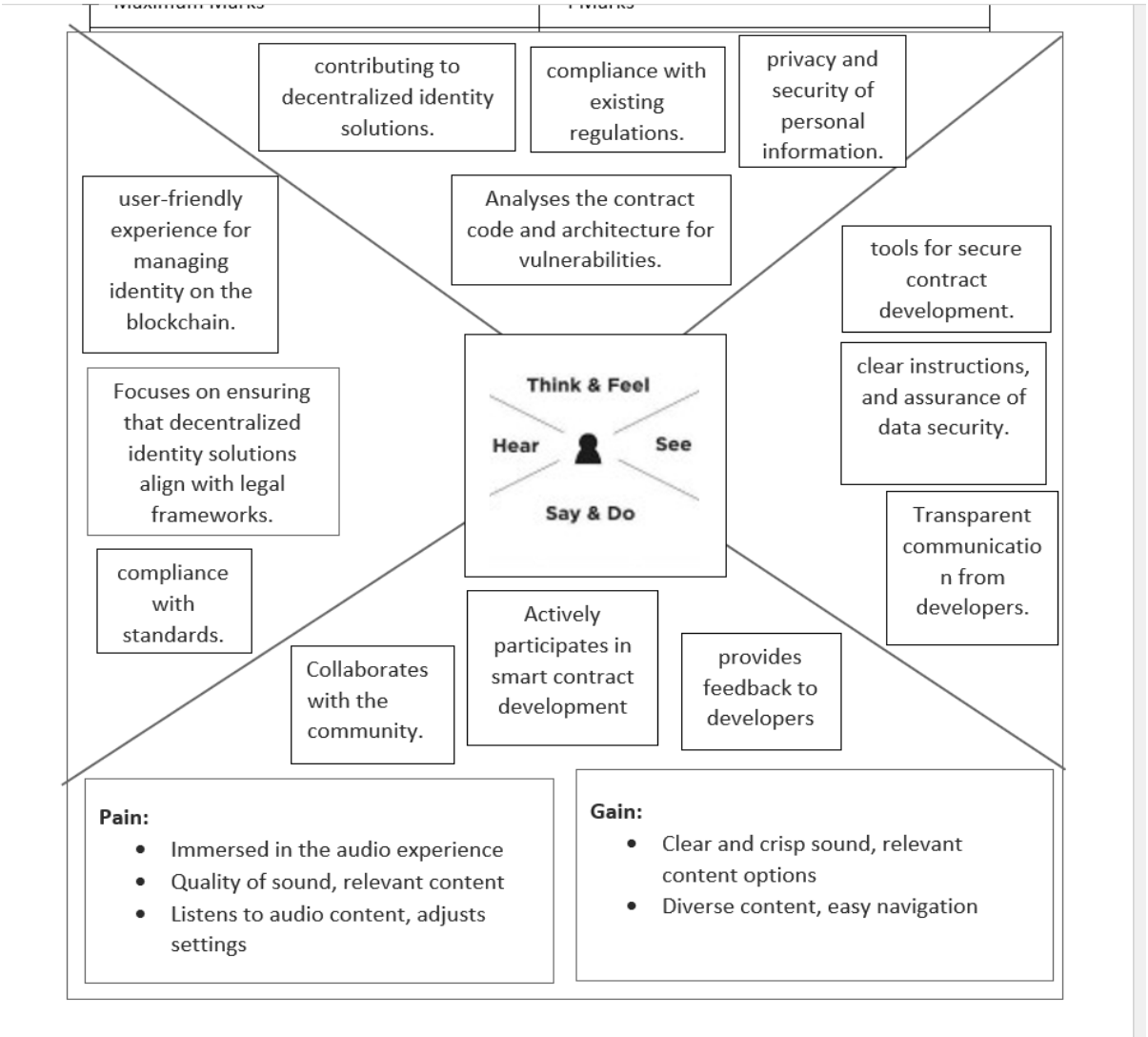
Every person’s identity document must be issued and verified in a rapid, dependable, and secure manner. The mechanisms already in place are operational, but because the procedure often takes several weeks, the efficiency and security need to be increased. This is not just a hassle and a waste of time, but it’s also costly financially and environmentally. The solution for this problem is to detect fake certificates, store certificates and make organizations certificate verification easier without the help of third party. Creating a website using Ethereum blockchain technology that doesn’t allow data tampering and which makes storage and validation of certificates

easier is a way to create a system that facilitates all the requirements and makes the process of verification and storage simpler.

CHAPTER 3

IDEATION &PROPOSED SOLUTION

3.1 EMPATHY MAP CANVA



3.2. IDEATION&BRAINSTROMING

2

Brainstorm

Write down any ideas that come to mind that address your problem statement.

10 minutes

TIP

You can select a sticky note and hit the pencil [switch to sketch] icon to start drawing!

Person 1

Person 2

Person 3

Person 4

Person 5

Person 6

Person 7

Person 8

4

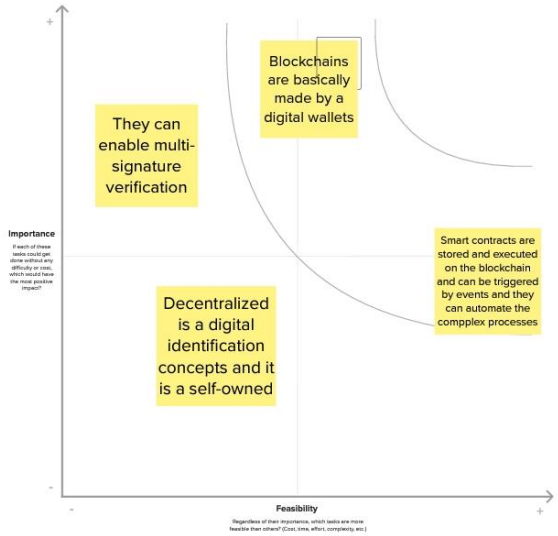
Prioritize

Your team should all be on the same page about what's important moving forward. Place your ideas on this grid to determine which ideas are important and which are feasible.

20 minutes

TIP

Participants can use their cursors to point at where sticky notes should go on the grid. The facilitator can confirm the spot by using the laser pointer holding the **H key** on the keyboard.



CHAPTER 4

REQUIREMENT ANALYSIS

4.1.FUNCTIONAL REQUIREMENT

The following are the main contributions to the research work: In order to verify certificates without use of third party or central authority, we had developed a website which uses SHA-256 algorithm to generate hash for the certificate which is stored in blockchain. This hash is unique and irreversible. It minimizes manual work required for their verification and ensures security. The remaining part of the paper follows the same format. By describing current methodologies and systems, Sect. 2 illustrates the relevant research on existing certificate verification systems. Section 3 presents the suggested approach for verification 454 K. V Raghavender of certificates using Ethereum Blockchain Technology. Section 4 of the proposal finishes with a presentation of the results together with any limitations and any future recommendations.To recognize false documents and certifications, both in paper form and digital form, research has been ongoing. The project focuses on developing a mechanism for both storing immutable certificates and validating them. The following techniques have been suggested to reduce the use of fraudulent documents and publications. Blockchain technology and digital certificate validations were the main topics of the survey. An Enhanced Web Base Certificate Verification System [5] was the title of our first paper. It used the object-oriented and design methodology (OOADM), with HTML5, CSS3, Bootstrap, and PHP5 as the frontend and backend programming languages, respectively. The fact that it is centralized, requires a third party, and involves manual verification is a major drawback.

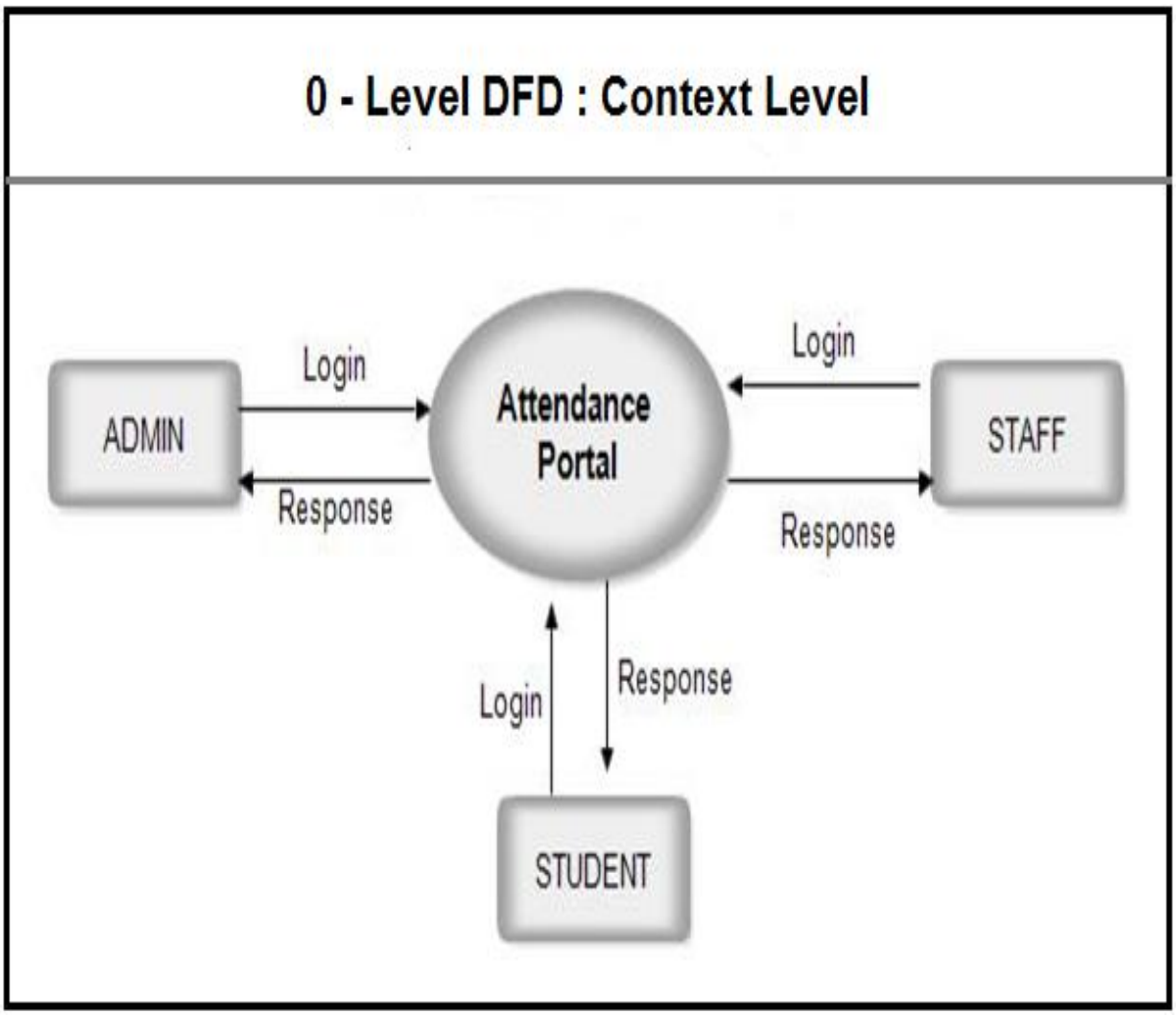
4.2.NON-FUNCTIONAL REQUIREMENT

The second publication, An Overview of Blockchain Technology [15], gave further information about Blockchain. It defined a number of words related to this technology, including the most crucial idea known as a smart contract. The Blockchain generates a long chain of nodes and stores the data's hash in the block before it. When data is changed, its hash will modify and cease to correspond to the value recorded in the preceding block, alerting us to the change. Blockchain and Smart Contract for Digital Certificate was the title of the third paper. There were 3 actors in their design. Institutions came first, followed by students, and then service providers. Their strategy had the drawback of using "one hash as a key," making it available to anyone with the hash. Next up is our tamper-proof birth certificate document. With the exception of using the AES technique and IPFS to store the data, their concept was essentially identical to that of the second paper. They specifically designed their system for birth certificates. The problem was that neither the original document nor the capability to create certificates online were ever stored anywhere. We investigated a distinct paper with the title BlockIPFS (Blockchain enabled Interplanetary File System for Forensic and Trusted Data Traceability) to address the issue of document storage.

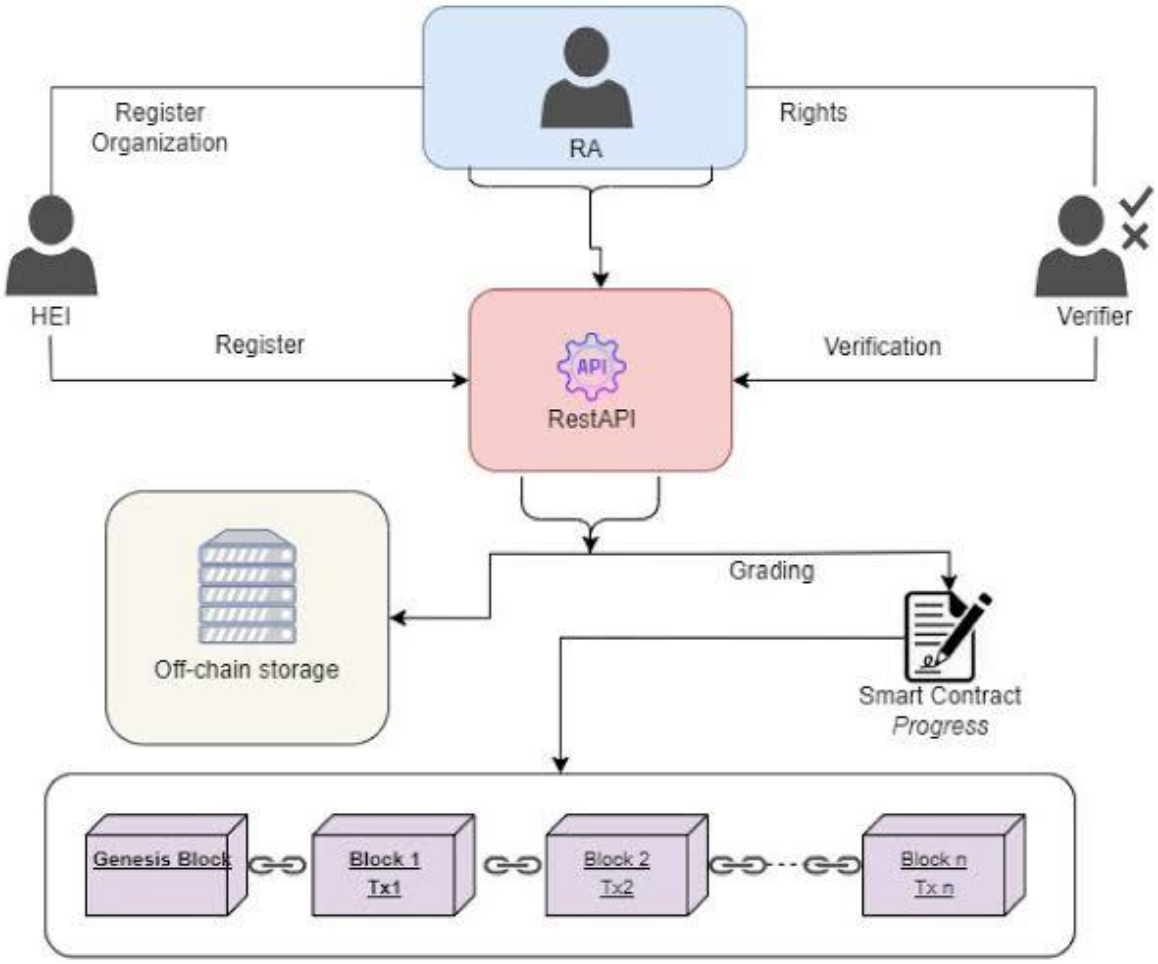
CHAPTER 5

PROJECT DESIGN

5.1.DATA FLOW DIAGRAM



5.2.SOLUTION ARCHITECTURE



CHAPTER 6

PROJECT PLANNING AND SCHEDULING

6.1 TECHNICAL ARCHITECTURE

To recognize false documents and certifications, both in paper form and digital form, research has been ongoing. The project focuses on developing a mechanism for both storing immutable certificates and validating them. The following techniques have been suggested to reduce the use of fraudulent

documents and publications. Blockchain technology and digital certificate validations were the main topics of the survey. An Enhanced Web Base Certificate Verification System [5] was the title of our first paper. It used the object-oriented and design methodology (OOADM), with HTML5, CSS3, Bootstrap, and PHP5 as the frontend and backend programming languages, respectively. The fact that it is centralized, requires a third party, and involves manual verification is a major drawback. The second publication, An Overview of Blockchain Technology [15], gave further information about Blockchain. It defined a number of words related to this technology, including the most crucial idea known as a smart contract. The Blockchain generates a long chain of nodes and stores the data's hash in the block before it. When data is changed, its hash will modify and cease to correspond to the value recorded in the preceding block, alerting us to the change. Blockchain and Smart Contract for Digital Certificate was the title of the third paper [8]. There were 3 actors in their design. Institutions came first, followed by students, and then service providers. Their strategy had the drawback of using "one hash as a key," making it available to anyone with the hash. Next up is our tamper-proof birth certificate [11] document.

CHAPTER 7

CODING&SOLUTION

7.1 FEATURE 1

VS CODE

```
{
// Use IntelliSense to learn about possible attributes.
// Hover to view descriptions of existing attributes.
```

```
// For more information, visit: https://go.microsoft.com/fwlink/?linkid=830387
"version": "0.2.0",
"configurations": [
 {
  "type": "node",
  "request": "launch",
  "name": "Jest All",
  "program": "${workspaceFolder}/node_modules/.bin/jest",
  "args": ["--runInBand"],
  "console": "integratedTerminal",
  "internalConsoleOptions": "neverOpen",
  "windows": {
   "program": "${workspaceFolder}/node_modules/jest/bin/jest"
    }
  },
  {
    "type": "node",
   "request": "launch",
   "name": "Jest Current File",
   "program": "${workspaceFolder}/node_modules/.bin/jest",
   "args": ["${relativeFile}", "--detectOpenHandles"],
```

```
  "console": "integratedTerminal",
  "internalConsoleOptions": "neverOpen",
  "windows": {
    "program": "${workspaceFolder}/node_modules/jest/bin/jest"
  }
},
{
  "type": "node",
  "request": "launch",
  "name": "Launch Program",
  "skipFiles": ["<node_internals>/**"],
  "program": "${workspaceFolder}/lib/index.js",
  "preLaunchTask": "tsc: build - tsconfig.json",
  "outFiles": ["${workspaceFolder}/lib/**/*.js"]
},
{
  "type": "node",
  "request": "launch",
  "name": "test revoker",
  "skipFiles": ["<node_internals>/**"],
  "program": "${workspaceFolder}/node_modules/.bin/jest",
  "args": ["revokerTests"]
```

```
    },
    {
      "type": "node",
      "request": "launch",
      "name": "test basic",
      "skipFiles": ["<node_internals>/**"],
      "program": "${workspaceFolder}/node_modules/.bin/jest",
      "args": ["basic"]
    }
  ]
}
```

7.2 FEATURE 2

GITHUB

```
name: Build, Test and Publish
on:
  workflow_dispatch:
  push:
 branches:
- 'master'
- 'alpha'
jobs:
  build-test-publish:
```

```
runs-on: ubuntu-22.04
steps:
  - uses: actions/checkout@v4
    with:
      fetch-depth: 0
      token: ${{ secrets.GH_TOKEN }}

  - name: "Setup node with cache"
    uses: actions/setup-node@v4
    with:
      node-version: 18
      cache: 'yarn'

  - run: yarn install --frozen-lockfile
  - run: yarn run build

  - name: "Setup git coordinates"
    run: |
      git config user.name ${{ secrets.GH_USER }}
      git config user.email ${{ secrets.GH_EMAIL }}

  - name: "Run semantic-release"
```

env:

GH_TOKEN: ${{secrets.GH_TOKEN}}

NPM_TOKEN: ${{secrets.NPM_TOKEN}}

if: github.ref == 'refs/heads/master' || github.ref == 'refs/heads/alpha'

run: yarn run relea

CHAPTER 8

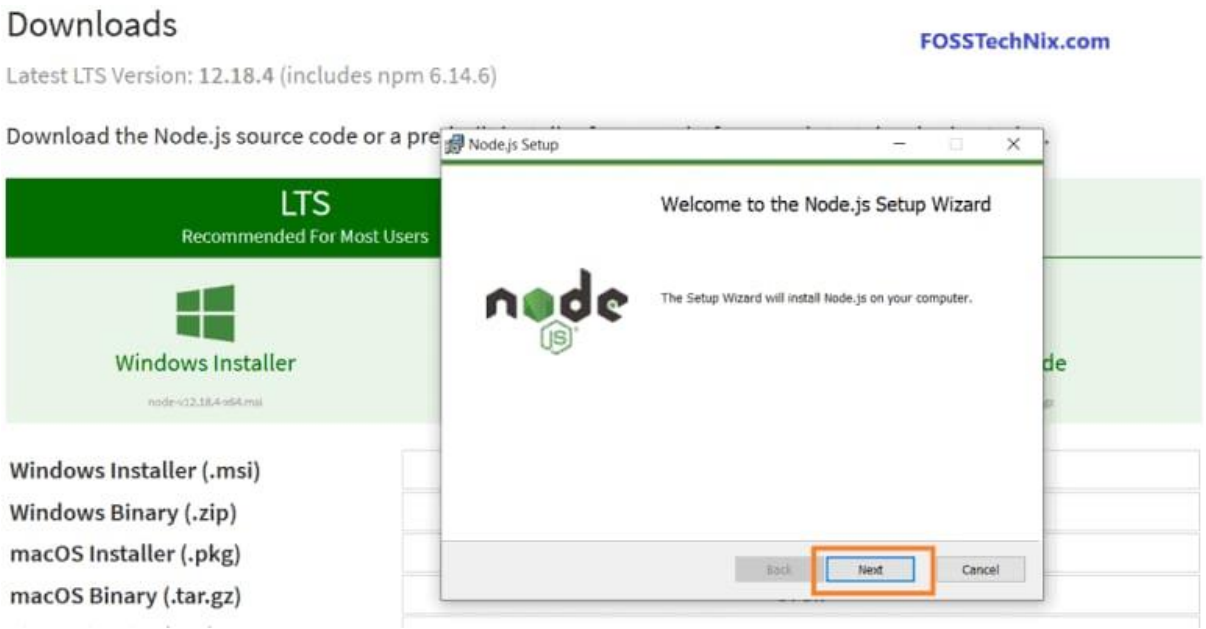
PERFORMANCE TESTING

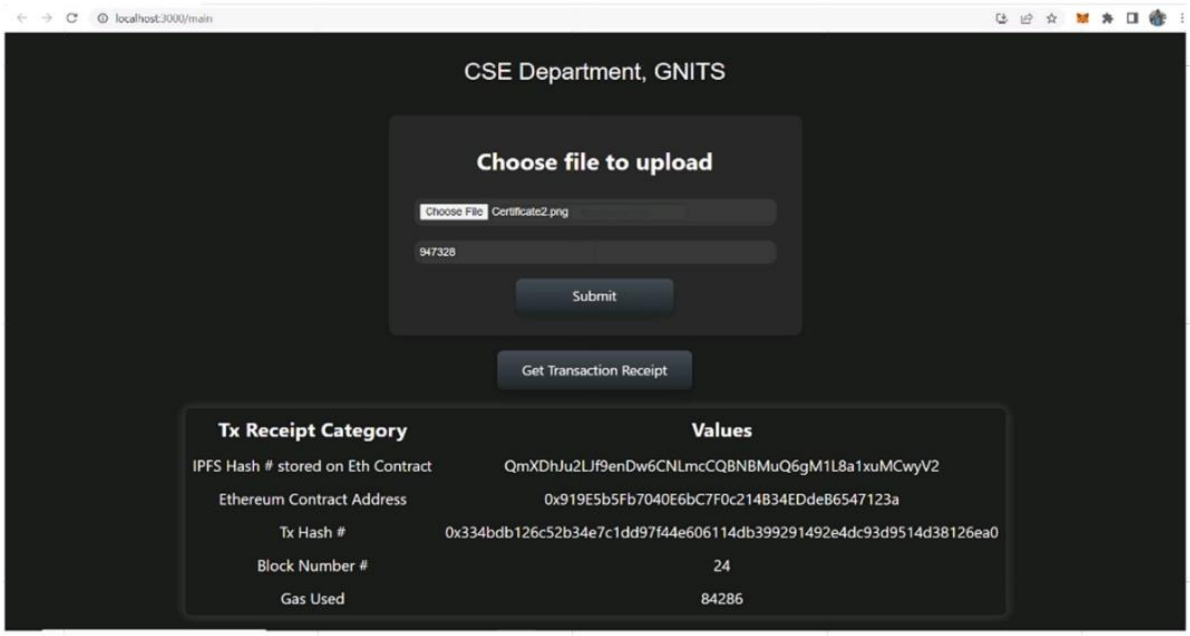
When IPFS receives this data, it uses its SHA2–256 hashing algorithm to process it. SHA-256 may transform large input data into a fixed-size hash code of 256 bits (32 bytes). Hashing is always a one-way process. As a result, finding a hash function's input is computationally impossible based on the hash output. Large amounts of storage space are needed to store the original files in the database. Therefore, a method is required to identify documents in a way that are lesser than their actual size. To complete this task, a hashing method must be employed. Along with the original Document, this generated hash is kept in the IPFS and it needs to be stored in the Blockchain. For this, some generation charges in MetaMask must be approved by the issuer. This hash is then saved in the Blockchain and cannot be normally modified after that. Even in the unlikely event that the data is altered, the Blockchain's other nodes will alert you. It only takes a few seconds for us to be informed if data is changed. A specific certificate ID is assigned to each certificate that serves as the distinctive ID required for verification. For this process, we need MetaMask extension in the browser, ganache and truffle framework using NPM and also local ipfs needs to be installed through command line. Here

truffle will be used to set up the ReactJS application using “truffle unbox react” command. Then smart contracts need to be created using solidity language inside contracts folder.

CHAPTER 9

9.1 OUTPUT SCREENSHOTS





CHAPTER 10

CONCLUTION

Here only college admin has access to upload the certificate. Admin has to upload the certificate and student roll number and when he clicks on submit button then certificate is uploaded to local IPFS and it runs its SHA-256 hashing algorithm to get IPFS Hash and it will be stored. The identical hash will be transmitted to the Blockchain Node, where the administrator must first accept the charges in MetaMask before they can be stored to the Blockchain. After MetaMask approval, some gas fee is utilized to store IPFS Hash into the local blockchain ganache. Then a transaction hash is generated after interacting with the contract and then a new block is created in the blockchain

CHAPTER 11

FUTURE SCOPE

The proposed solution entails creating a federated blockchain amongst businesses, academic institutions, and students. Universities typically add student certificates first, and then businesses or other verifiers can check the

credentials using the certificate. No one will be able to alter the data contained in a blockchain or incorporate fresh transactions that are backdated. All universities and colleges are able to use this system to add 460 K. V Raghavender Fig. 8. Verification using certificate itself additional protection to the certificates and student data. The System makes it easier to submit certificates while reducing the quantity of manual effort needed to verify them. And students also have a relatively low risk of losing their credentials. By using the SHA2–256 hashing algorithm, we minimize the quantity of data that has been changed. The Inter Planetary File System will hold the actual document, while the blockchain will retain the certificate's hash. This allows us to maintain data and ensure transparency. The following are some potential future directions for the work: (i) Development of a terminal-based document authentication system that allows for multiple file uploads and incorporates additional usability elements. (ii) This can be extended to ensure the integrity of all kinds of documents, not just in education field, but in government sectors where digital time stamping of documents is necessary. (iii) To develop a feature that gets rid of the fraudulent certificates that are already present in society.