CERTIFICATE REGISTRATION AND VERIFICATION USING BLOCKCHAIN

TEAM MEMBERS
19BCE2127: VEERA VIJAYAPRASAD C
19BCE2537: SAMYOGITA BHANDARI
19BCE2552: OJASHWI PAUDEL

PROBLEM STATEMENT

The number of certificate counterfeits in our society has become challenging and prevalent. Today, forging certificates has become a business tumbling from the need/want of the people for employment. Graduates with legitimate certificates/degrees are denied job opportunities by the holders of these forged credentials. To address this problem, many researchers have proposed a certificate verification system. Although the existing systems can solve some of the major problems such as accessing student's records with the provision of a central database to manage these records electronically. However, the system can easily be hacked and manipulated since it is mostly available on centralized servers.

OBJECTIVES

- To research, design and develop a system for dynamic and secure e-certificate generation system using smart contracts in the blockchain domain.
- Implement a custom mining strategy in the smart contract.
- Allow a private user base to validate the minted certificates.
- The system will include a frontend and IPFS for hosting, which offers decentralized and free backend for the data storage.
- Moralis is used to leverage the above stated technology and for deployment. It is the main integration tool.

LITERATURE SURVEY

Blockchain for Industry 4.0: A Comprehensive Review

Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone

Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company, or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published. This document provides a high-level technical overview of blockchain technology. The purpose is to help readers understand how blockchain technology works.

A survey on the security of blockchain system

Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, QiaoyanWen

Since its inception, blockchain technology has demonstrated promising application prospects. From the first cryptocurrency to the current smart contract, the blockchain has been used in many fields. Although there are some studies on blockchain security and privacy issues, there is no systematic review of blockchain system security. In this paper, we conduct a systematic study of security threats in the blockchain and examine real-life concurrent attacks by exploring popular blockchain systems. The writers were also reviewing blockchain security solutions, which could be used to develop various blockchain systems, and propose future guidelines to promote research efforts in this area.

Understanding Security Issues in the NFT Ecosystem

D*ipanjan Das, Priyanka Bose, Nicola Ruaro, Christopher Kruegel, Giovanni Vigna*

Non-Fungible Tokens (NFTs) have emerged as a way to collect digital art and an investment vehicle. Despite their recent publicity, NFT markets have seen high (and high value) sales as well as a dramatic increase in trading value over the past year. Unfortunately, these markets have not yet received much security analysis. In this paper, they first present a comprehensive overview of how the NFT ecosystem operates, and identify three main actors: markets, foreign businesses, and users. The authors conducted an in-depth analysis of the top 8 markets (listed on the volume of the production) to identify potential problems related to such markets. Many of these problems lead to significant financial losses. They also collected a large amount of goods and event data related to NFTs sold in the tested markets. they automatically analyze this data to understand how non-blockchain businesses are able to disrupt NFT markets, lead to critical outcomes, and measure the violent trading behavior of users under the guise of anonymity.

A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities

Ahmed Afif Monrat; Olov Schelén; Karl Andersson

In this paper, the opportunities and benefits of blockchain and its trading are discussed in comparative experimental research. In addition, the transaction process, system building, application areas and blockchain compliance methods are also described. There are still many open issues that need to be further researched and analyzed in order to build effective and efficient industrial applications that can fully benefit from blockchain implementation and achieve the intended goals. Examples of these open-ended issues include security, privacy, rating, power issues, and integration with other systems and, most importantly, control issues. Future work in this field is needed to address these issues and to fill the gaps in the highly efficient, manageable and secure blockchain industry applications.

A Decentralized Framework for Patents and Intellectual Property as NFT in Blockchain Networks

Seyed Mojtaba Hosseini Bamakan , Nasim Nezhadsistani , Omid Bodaghi

This paper provided a conceptual framework for presenting an NFT-based patent with a comprehensive discussion of many aspects: background, model components, token standards to application areas, and research challenges. The proposed framework includes five main layers: Storage Layer, Authentication Layer, Verification Layer, Blockchain Layer, and Application. The main purpose of this patent framework was to provide an NFT-based concept that could be used to patent a decentralized, anti-tamper, and reliable network for trade and exchange around the world. Finally, we addressed several open challenges to NFT-based inventions. Blockchain technology enables creating a transparent, distributed, cost-effective, and resilient environment that is open to all and where each transaction is auditable. When these intrinsic characteristics of blockchain technology are applied to the IP domain, it helps copyrights.

Identifying Security Risks in NFT Platforms

Yash Gupta, Jayanth Kumar, Dr. Andrew Reifers

This paper examines the effects of natural hazards on emerging mold-free tokens technology and proposes a set of practical solutions for participants in this ecosystem and spectators. Web3 and NFTs are a fast-growing $ 300 billion economy with a clear, highly publicized impact that has emerged recently. They come to a collection of solutions that are a combination of processes that must be adopted, as well as changes or technological improvements that need to be integrated into the ecosystem, in order to be used to reduce risk. By linking mitigation to individual risks, they are confident that their recommendations will enhance the maturity and security of the growing Web3 ecosystem. The authors do not recommend, or recommend any particular product or service in thier solution set. Nor do they compensate or get influenced in any way by these companies for writing these products in their research.

Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges

Qin Wang, Rujia Li, Qi Wang, Shiping Chen

The Non-Fungible Token (NFT) market is booming in recent years. The concept of NFT originally came from the Ethereum token standard, which aims to distinguish each token with distinctive symbols. This type of token can be tied to physical / digital objects as their unique identifier. The development of the NFT ecosystem is still in its infancy, and the NFTs technology is maturing prematurely. Newcomers may get lost in their unusual evolution due to the lack of formal summaries. In this technical report, the writers have examined NFT ecosystems in a number of areas. They start with an overview of NFT solutions, and then provide their technical components, agreements, standards, and eligibility requirements. After that, they offer the emergence of security, and discussions about the ideas of models in their design, opportunities, and challenges.

Towards the Tokenization of Business Process Models using the Blockchain Technology and Smart Contracts

Andrii Kopp and Dmytro Orlovskyi

In this research paper, the authors have suggested how to make tokens for a business-based process blockchain technology and smart contracts. Based on modern research conducted, BPMN business process model notification has been selected to define business process models for tokens as the most widely used and considered standard in the BPM industry. The essence of the blockchain the technology was considered to prove the coherence of the modeling of the business process model, as well as the importance of smart contracts and international applications were also reviewed. Two standards for tokens - ERC20 and ERC721, representing token frustration and unstable token respectively consider selecting the appropriate token standard for BPMN drawings. Based on the features of the NFTs, the ERC721 standard had been selected, with Ethereum as a pioneer and still leading smartly the contract field had been selected for use.

Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity

KB Wilson, A Karg, H Ghaderi

In this paper, they have define NFTs and look at how they fit with blockchain and cryptocurrencies, how they are used by various industries, and the opportunities and risks they present. They disscuss key contribution is a conceptual map of an initial NFT ecosystem. In doing so, they provide relational mapping between and among key stakeholders: content creators, core and related technical and business intermediaries, consumers, investors, and speculators. they also highlight implications for managers and tie them to conceptual exploration and exploitation frameworks.

A Technical Deep Dive Into and Implementation of Non-Fungible Tokens in a Practical Setting

Julia Martin, Carrie Hay Kellar

This paper has laid out the technical details of how NFTs are created and how they are implemented on two of their most popular platforms: Ethereum and Solana. Italso went into the difference between the two, and showed a physical implementation of an NFT on Solana, and deployed onto the platform. This paper shows how easy it is for regular users to create and deploy their own NFTs, thus interacting with the market and greater blockchain community as a whole.

From Trade-only to Zero-Value NFTs: The Asset Proxy NFT Paradigm in Web3.

Denis Avrilionis, Thomas Hardjono

The massive implementation of smart contracts found in the NFT markets today allows for the conversion of NFT token attributes, without any particular way of controlling off-chain metadata compliance. The authors believe this is a weakness in the overall formation of the NFTs today. They propose a calculation model called the NFT Estate Agent that ensures consistency between the NFT (on-chain) token and the off-chain asset associated metadata. Generally, the proposed model can be used for any type of NFT that requires statistical or statistically controlled metadata. A second contribution to this paper is an NFT design patterns concept that recognizes the need for a coherent framework for dealing with mixed materials, and that in the use of a particular mixed material, appropriate technical components should be used under the framework.

Efficient Plan for Art Transaction Through Non Fongible Token(NFT)

K*yoohoon Jo1 , Jeongmin Ko2*

This study is aimed to examine how art works are traded through Non Fongible Token(NFT) that are different from the existing trade methods such as galleries, auctions, and art fairs in art trade. It also analyzes how art trades such as game items are traded through NFT. Furthermore, it is intended to place appropriate values to the works created through NFT, have clear ownership, and avoid hacking when collectors try to buy at NFT exchanges. Lastly, in relation to the environment, is to closely monitor whether or not it causes environmental problems like the existing virtual currency, and to achieve 'efficient art trade' with a more eco-friendly system. As for the research method, the data were qualitatively investigated and analyzed through interviews with major related companies, literature study and case analysis, and legal review of the supervisory body

METHODOLOGY

Frontend Module:

- It gets the user input for authentication and local file input.
- It is the user interface.

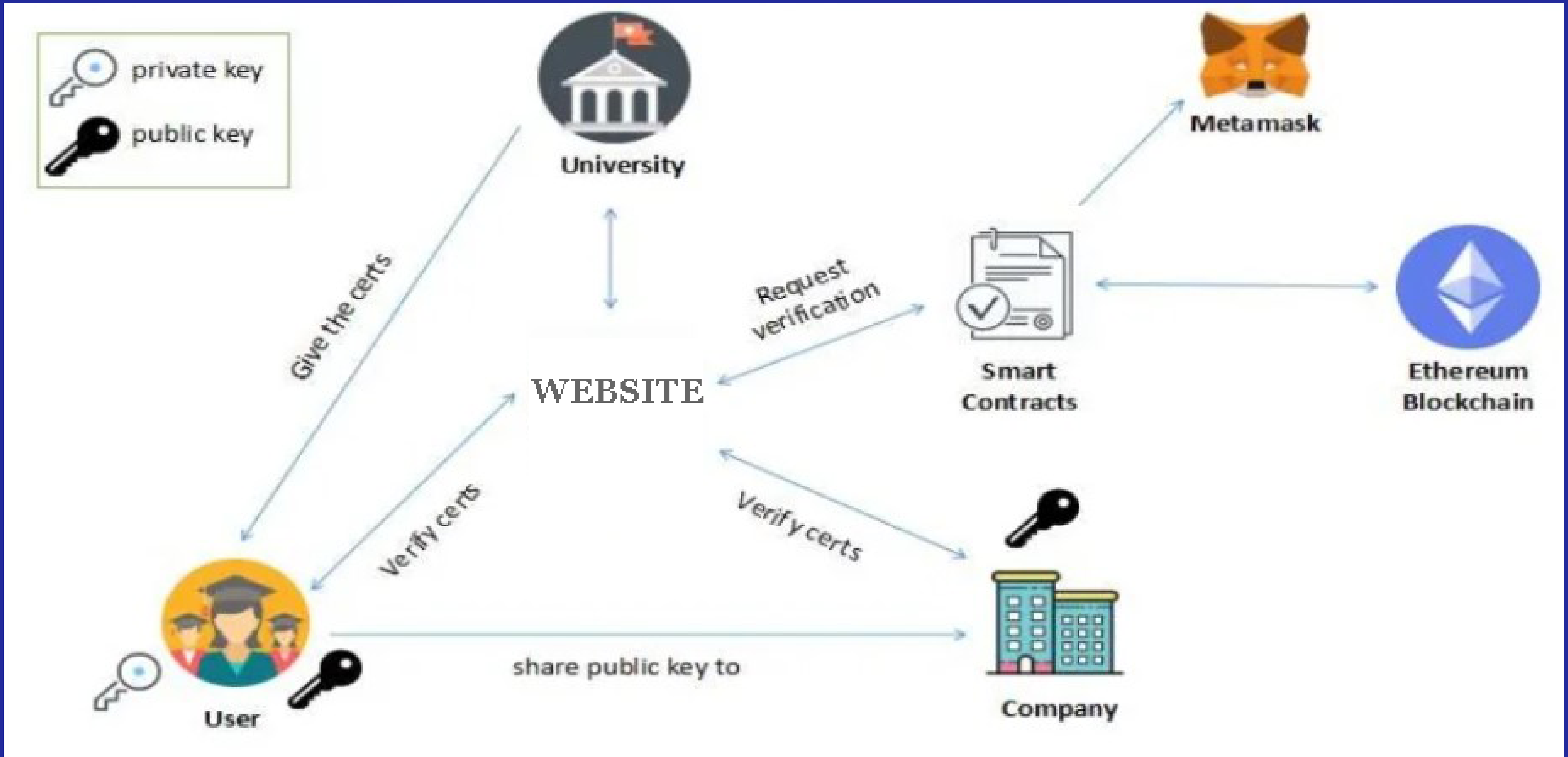
Backend Module:

- It accesses the smart contract using Moralis Integration.
- It is written in javascript.
- The json is created here and sent to the smart contract.
- The crypto wallets are accessed and queried through this.

Decentralized Storage Module:

- It accesses the IPFS using Moralis Integration.
- It is written in javascript.
- The Image hash is created here.The json hash is created here.

WORK FLOW DIAGRAM

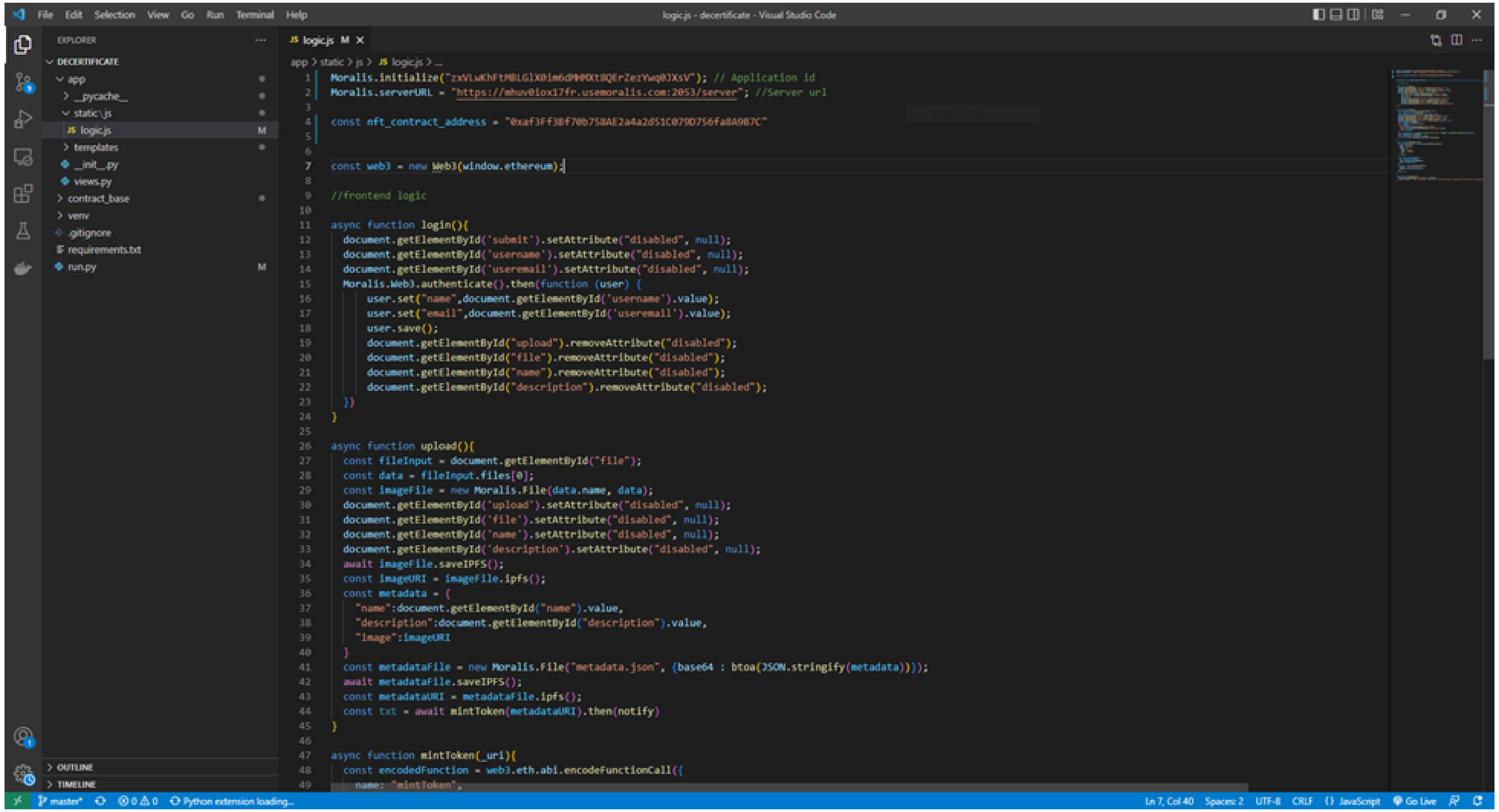


IMPLEMENTATION

BACKEND

- JAVASCRIPT AND MORALIS

  MORALIS IS USED FOR SMART CONTRACT INTERACTION AND IPFS ACCESS

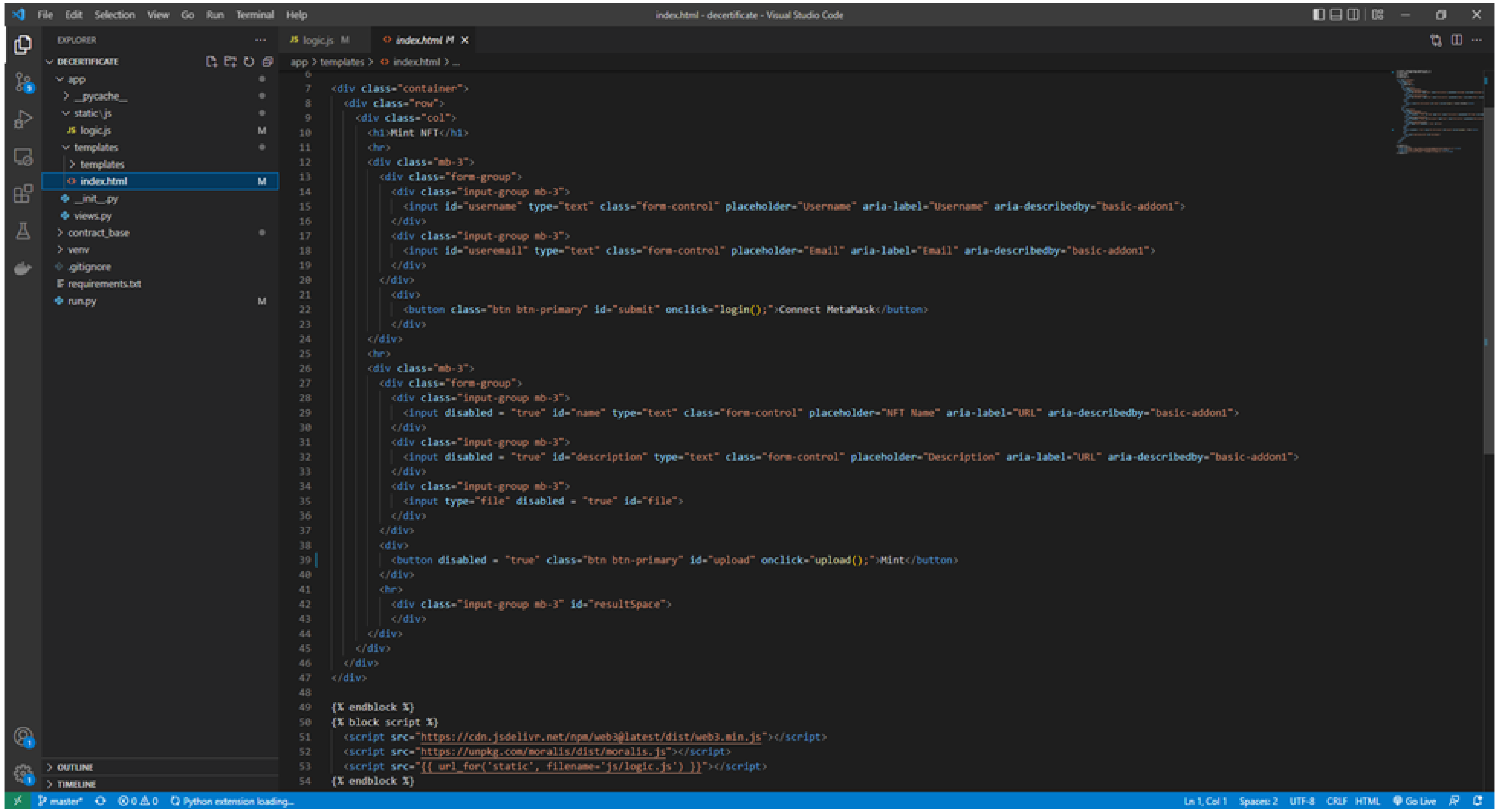

File Edit Selection View Go Run Terminal Help
logic.js - decertificate - Visual Studio Code
EXPLORER
DECERTIFICATE
app
__pycache__
static\js
logic.js M
templates
__init__.py
views.py
contract_base
venv
.gitignore
requirements.txt
run.py M
OUTLINE
TIMELINE
logic.js M
app > static > js > logic.js > ...
master*
⊗ 0 ⚠ 0
Python extension loading...
Ln 7, Col 40 Spaces: 2 UTF-8 CRLF {} JavaScript Go Live

```
Moralis.initialize("zxVLwKhFtMBLGlX0im6dMHMXt8QErZezYwq0JXsV"); // Application id
Moralis.serverURL = "https://mhuv0iox17fr.usemoralis.com:2053/server"; //Server url

const nft_contract_address = "0xaf3Ff3Bf70b758AE2a4a2d51C079D756fa8A987C"


const web3 = new Web3(window.ethereum);

//frontend logic

async function login(){
  document.getElementById('submit').setAttribute("disabled", null);
  document.getElementById('username').setAttribute("disabled", null);
  document.getElementById('useremail').setAttribute("disabled", null);
  Moralis.Web3.authenticate().then(function (user) {
      user.set("name",document.getElementById('username').value);
      user.set("email",document.getElementById('useremail').value);
      user.save();
      document.getElementById("upload").removeAttribute("disabled");
      document.getElementById("file").removeAttribute("disabled");
      document.getElementById("name").removeAttribute("disabled");
      document.getElementById("description").removeAttribute("disabled");
  })
}

async function upload(){
  const fileInput = document.getElementById("file");
  const data = fileInput.files[0];
  const imageFile = new Moralis.File(data.name, data);
  document.getElementById('upload').setAttribute("disabled", null);
  document.getElementById('file').setAttribute("disabled", null);
  document.getElementById('name').setAttribute("disabled", null);
  document.getElementById('description').setAttribute("disabled", null);
  await imageFile.saveIPFS();
  const imageURI = imageFile.ipfs();
  const metadata = {
    "name":document.getElementById("name").value,
    "description":document.getElementById("description").value,
    "image":imageURI
  }
  const metadataFile = new Moralis.File("metadata.json", {base64 : btoa(JSON.stringify(metadata))});
  await metadataFile.saveIPFS();
  const metadataURI = metadataFile.ipfs();
  const txt = await mintToken(metadataURI).then(notify)
}

async function mintToken(_uri){
  const encodedFunction = web3.eth.abi.encodeFunctionCall({
    name: "mintToken",
```

FRONTEND

- HTML FLASK

THE FRONTEND IS DONE USING THE ABOVE-MENTIONED TECH STACK IT IS MAINLY FOR INTEGRATION AND TESTING PURPOSES


File Edit Selection View Go Run Terminal Help
index.html - decertificate - Visual Studio Code
EXPLORER
DECERTIFICATE
app
__pycache__
static\js
logic.js M
templates
templates
index.html M
__init__.py
views.py
contract_base
venv
.gitignore
requirements.txt
run.py M
OUTLINE
TIMELINE
logic.js M
index.html M
app > templates > index.html > ...
master* ⊗ 0 ⚠ 0 Python extension loading...
Ln 1, Col 1 Spaces: 2 UTF-8 CRLF HTML Go Live

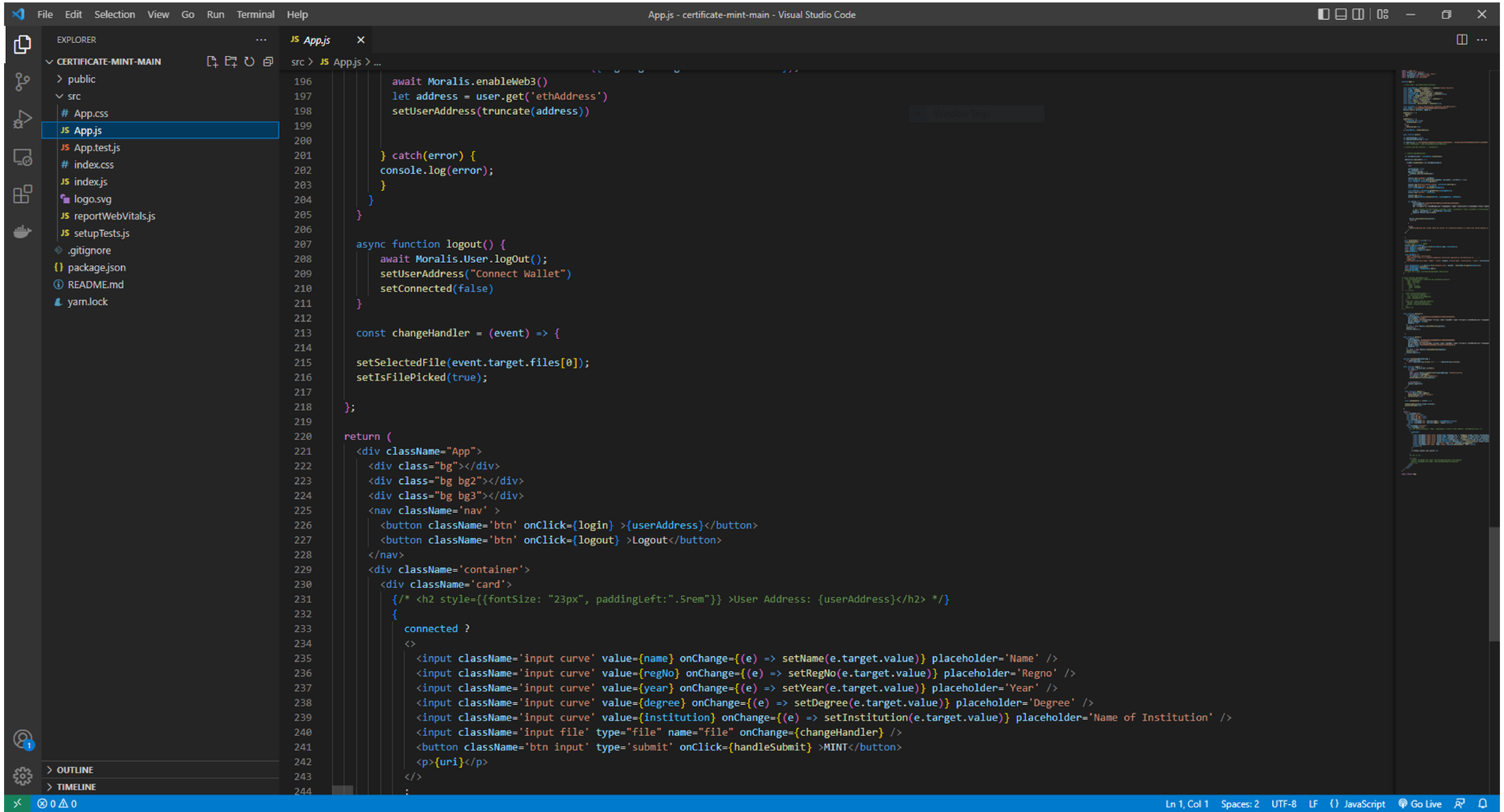
```html
<div class="container">
  <div class="row">
    <div class="col">
      <h1>Mint NFT</h1>
      <hr>
      <div class="mb-3">
        <div class="form-group">
          <div class="input-group mb-3">
            <input id="username" type="text" class="form-control" placeholder="Username" aria-label="Username" aria-describedby="basic-addon1">
          </div>
          <div class="input-group mb-3">
            <input id="useremail" type="text" class="form-control" placeholder="Email" aria-label="Email" aria-describedby="basic-addon1">
          </div>
        </div>
          <div>
            <button class="btn btn-primary" id="submit" onclick="login();">Connect MetaMask</button>
          </div>
      </div>
      <hr>
      <div class="mb-3">
        <div class="form-group">
          <div class="input-group mb-3">
            <input disabled = "true" id="name" type="text" class="form-control" placeholder="NFT Name" aria-label="URL" aria-describedby="basic-addon1">
          </div>
          <div class="input-group mb-3">
            <input disabled = "true" id="description" type="text" class="form-control" placeholder="Description" aria-label="URL" aria-describedby="basic-addon1">
          </div>
          <div class="input-group mb-3">
            <input type="file" disabled = "true" id="file">
          </div>
        </div>
        <div>
          <button disabled = "true" class="btn btn-primary" id="upload" onclick="upload();">Mint</button>
        </div>
        <hr>
          <div class="input-group mb-3" id="resultSpace">
          </div>
      </div>
    </div>
  </div>
</div>

{% endblock %}
{% block script %}
  <script src="https://cdn.jsdelivr.net/npm/web3@latest/dist/web3.min.js"></script>
  <script src="https://unpkg.com/moralis/dist/moralis.js"></script>
  <script src="{{ url_for('static', filename='js/logic.js') }}"></script>
{% endblock %}
```

FRONTEND

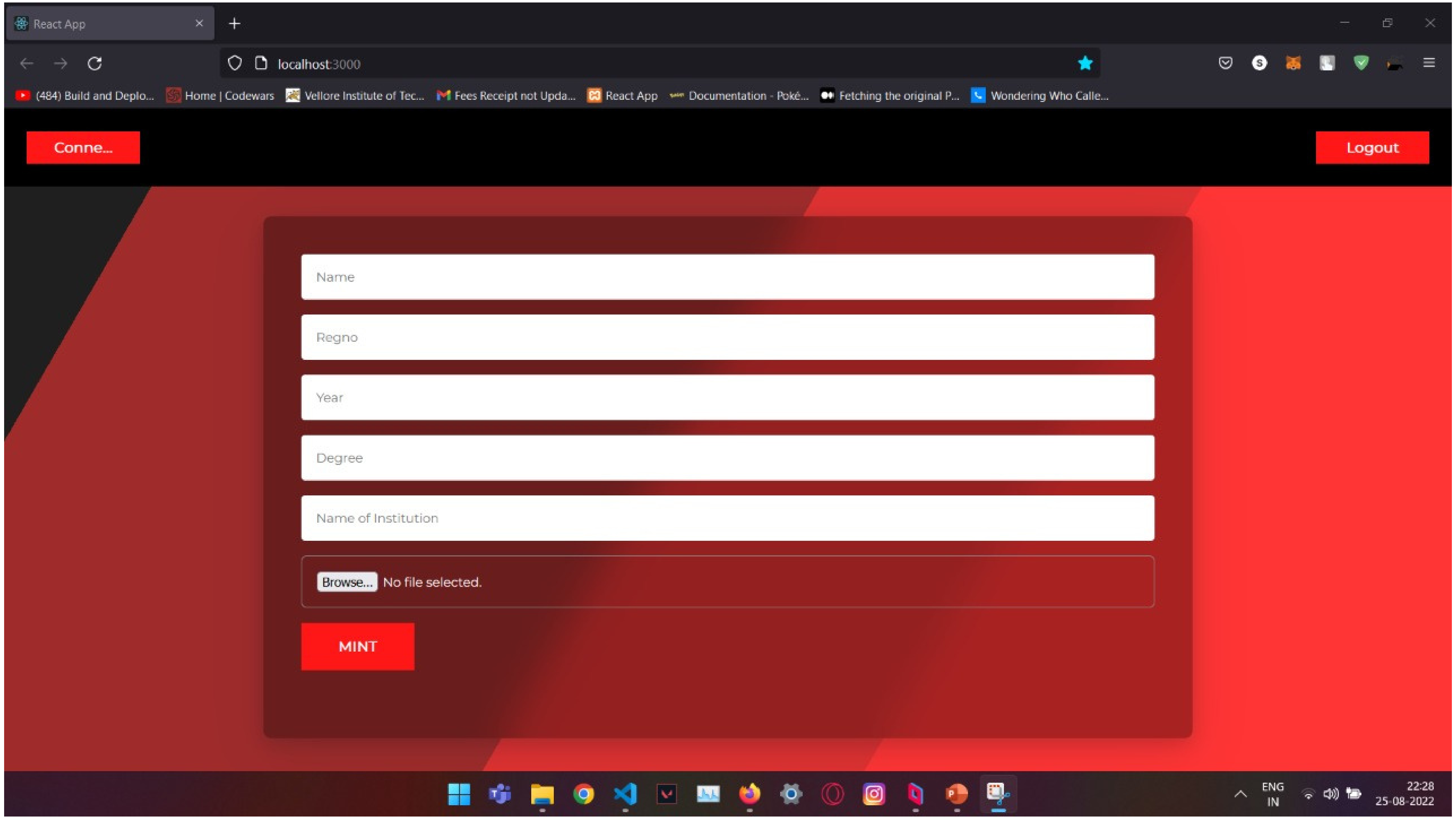
- REACT

THE NEW AND UPDATED FRONTEND IS DONE USING REACT

IT IS THE FINAL END USER ITERATION



```
          await Moralis.enableWeb3()
          let address = user.get('ethAddress')
          setUserAddress(truncate(address))


        } catch(error) {
        console.log(error);
        }
      }
    }

    async function logout() {
        await Moralis.User.logOut();
        setUserAddress("Connect Wallet")
        setConnected(false)
    }

    const changeHandler = (event) => {

    setSelectedFile(event.target.files[0]);
    setIsFilePicked(true);

  };

  return (
    <div className="App">
      <div class="bg"></div>
      <div class="bg bg2"></div>
      <div class="bg bg3"></div>
      <nav className='nav' >
        <button className='btn' onClick={login} >{userAddress}</button>
        <button className='btn' onClick={logout} >Logout</button>
      </nav>
      <div className='container'>
        <div className='card'>
          {/* <h2 style={{fontSize: "23px", paddingLeft:".5rem"}} >User Address: {userAddress}</h2> */}
          {
            connected ?
            <>
              <input className='input curve' value={name} onChange={(e) => setName(e.target.value)} placeholder='Name' />
              <input className='input curve' value={regNo} onChange={(e) => setRegNo(e.target.value)} placeholder='Regno' />
              <input className='input curve' value={year} onChange={(e) => setYear(e.target.value)} placeholder='Year' />
              <input className='input curve' value={degree} onChange={(e) => setDegree(e.target.value)} placeholder='Degree' />
              <input className='input curve' value={institution} onChange={(e) => setInstitution(e.target.value)} placeholder='Name of Institution' />
              <input className='input file' type="file" name="file" onChange={changeHandler} />
              <button className='btn input' type='submit' onClick={handleSubmit} >MINT</button>
              <p>{uri}</p>
            </>
            :
```

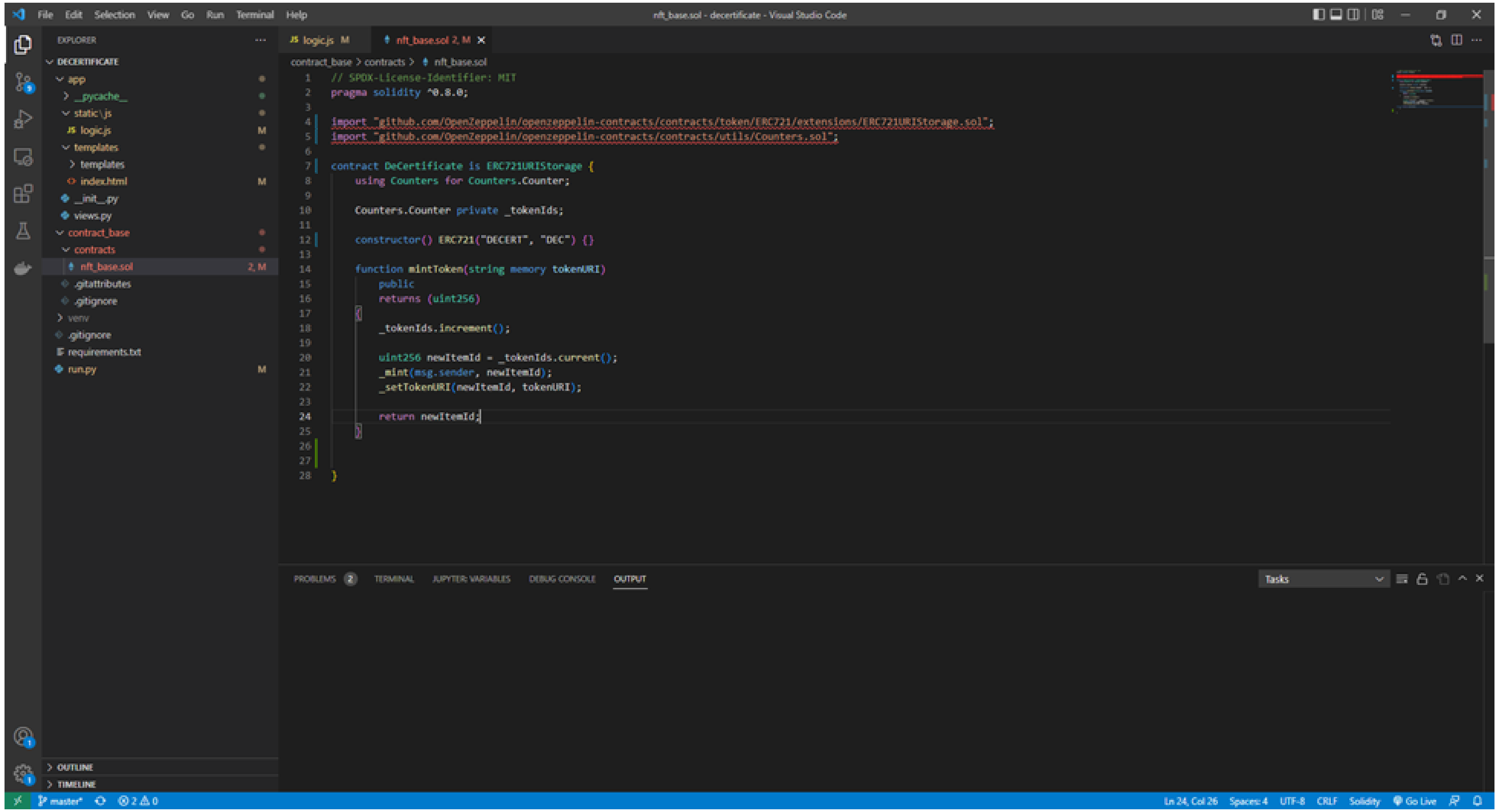

React App
localhost:3000
(484) Build and Deplo...
Home | Codewars
Vellore Institute of Tec...
Fees Receipt not Upda...
React App
Documentation - Poké...
Fetching the original P...
Wondering Who Calle...
Conne...
Logout
Name
Regno
Year
Degree
Name of Institution
Browse... No file selected.
MINT
ENG
IN
22:28
25-08-2022

SMART CONTRACT

- SOLIDITY

  AN ERC721 STANDARD SMART CONTRACT IS USED

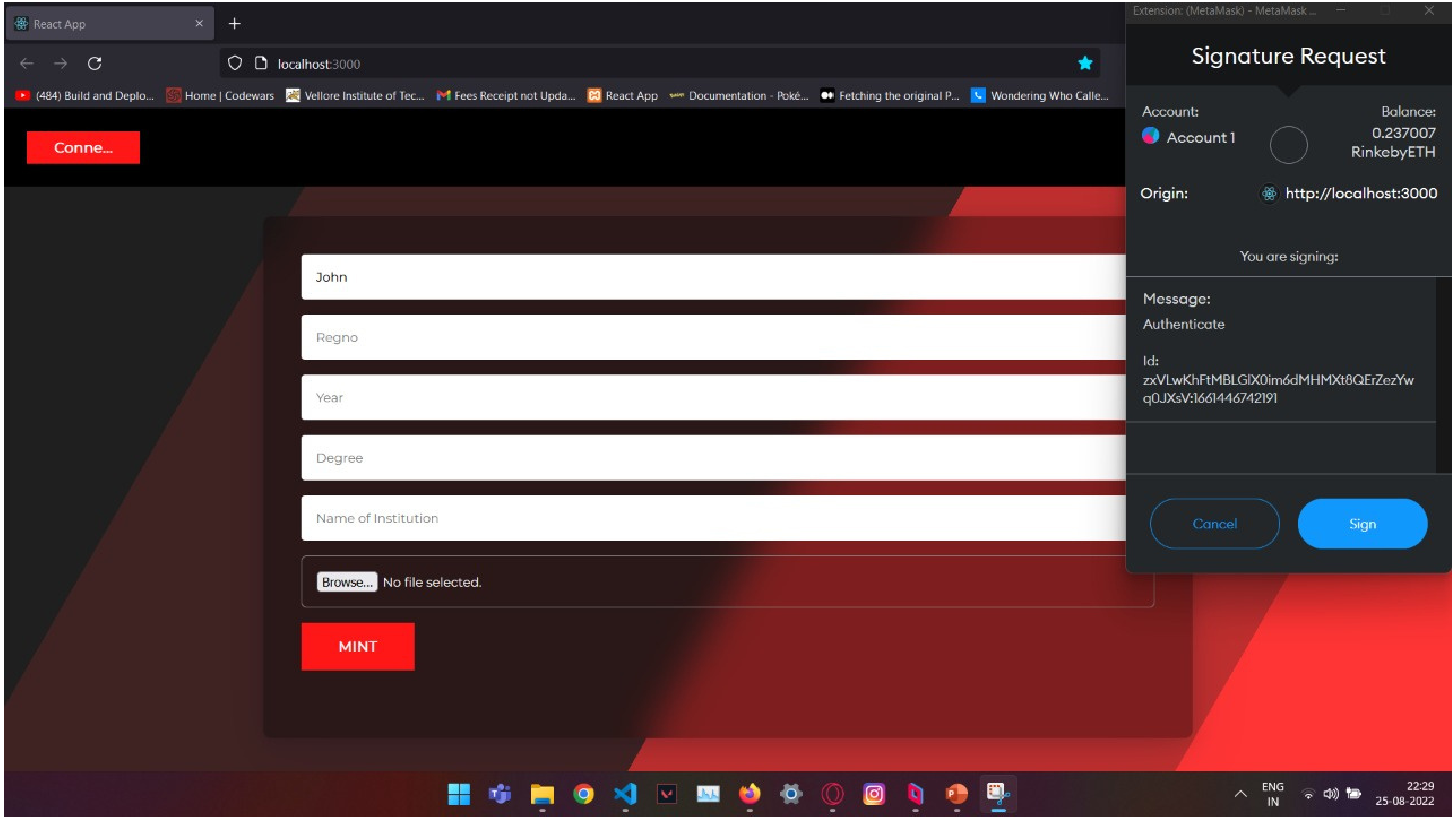
  THE SMART CONTRACT IS BEING UPDATED/UPGRADED FOR INCLUDING THE PROVISON OF A PRIVATE USERBASE OF ADMINS



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "github.com/OpenZeppelin/openzeppelin-contracts/contracts/token/ERC721/extensions/ERC721URIStorage.sol";
import "github.com/OpenZeppelin/openzeppelin-contracts/contracts/utils/Counters.sol";

contract DeCertificate is ERC721URIStorage {
    using Counters for Counters.Counter;

    Counters.Counter private _tokenIds;

    constructor() ERC721("DECERT", "DEC") {}

    function mintToken(string memory tokenURI)
        public
        returns (uint256)
    {

        _tokenIds.increment();

        uint256 newItemId = _tokenIds.current();
        _mint(msg.sender, newItemId);
        _setTokenURI(newItemId, tokenURI);

        return newItemId;
    }


}
```

FLOW/PROCESS

- THIS DEMONSTATES THE FLOW/PROCESS OF MINTING A CERTIFICATE
- THIS IS ALSO VERIFIES THE EXPECTED END RESULT/OUTPUT



John

Signature Request

Account: Account 1

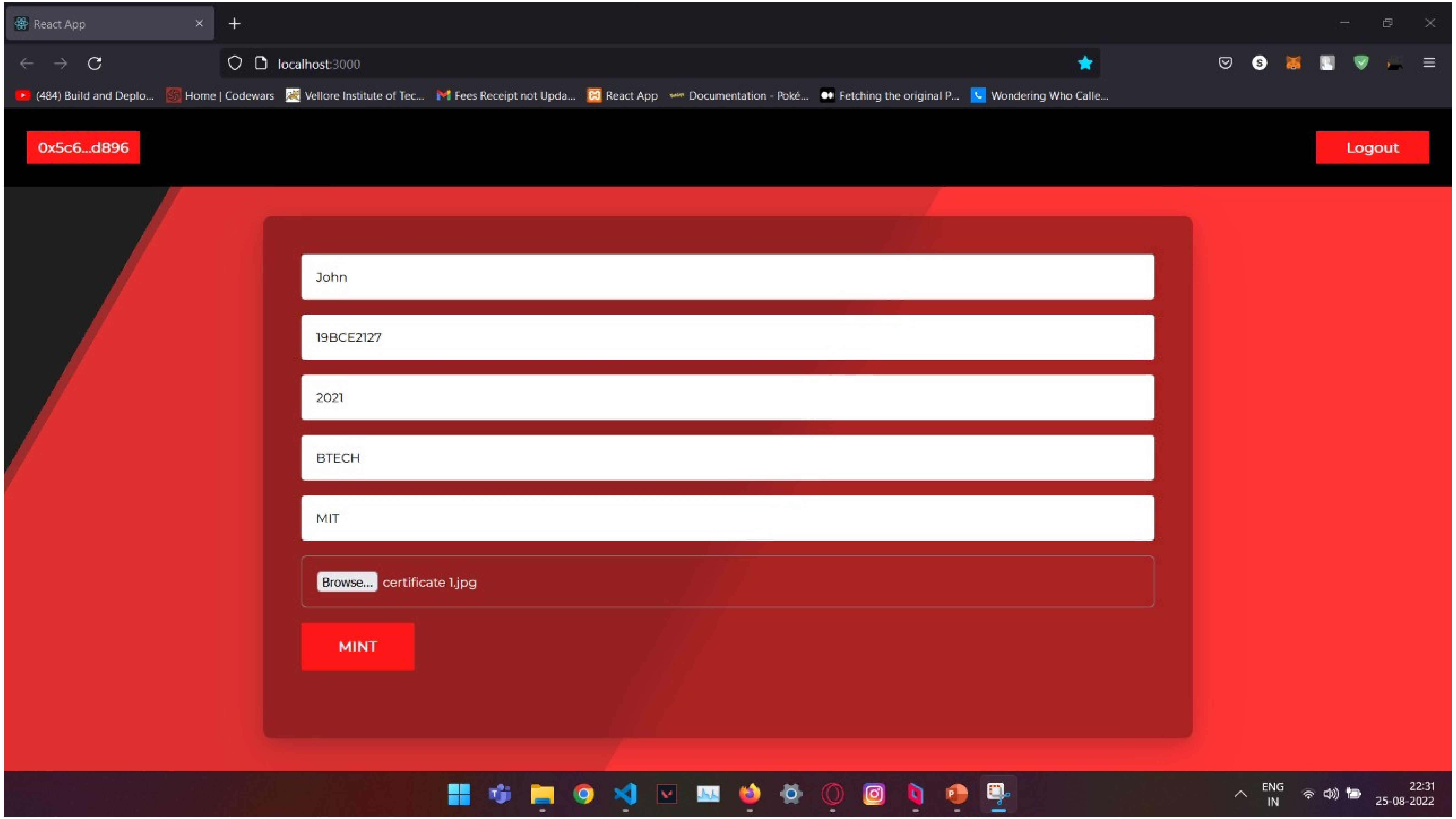
Balance: 0.237007 RinkebyETH

Origin: http://localhost:3000

You are signing:

Message:
Authenticate

Id:
zxVLwKhFtMBLGlX0im6dMHMXt8QErZezYwq0JXsV:1661446742191



John

19BCE2127

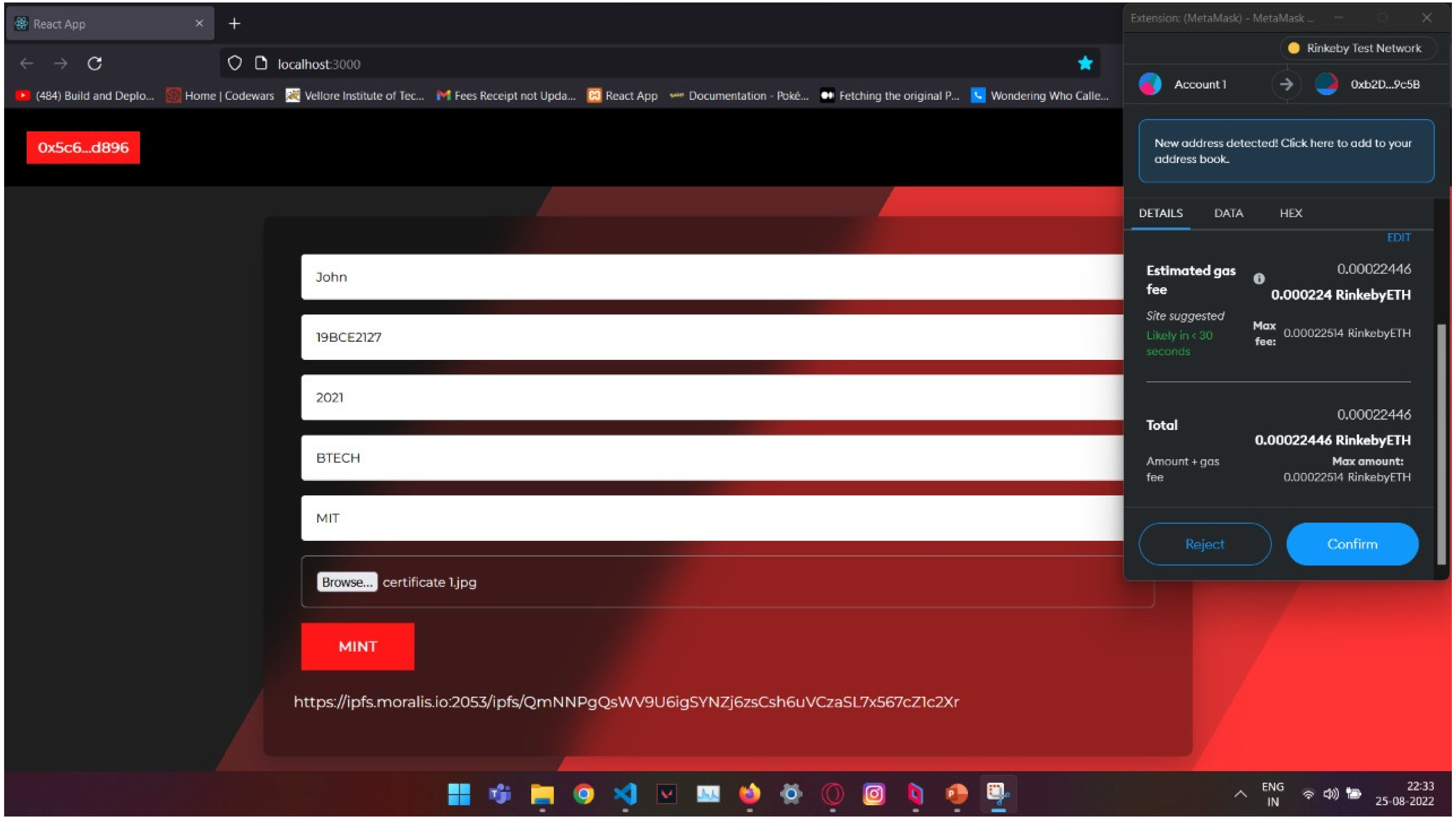
2021

BTECH

MIT

Browse... certificate 1.jpg

Fig: New React Frontend



John

19BCE2127

2021

BTECH

MIT

certificate 1.jpg

https://ipfs.moralis.io:2053/ipfs/QmNNPgQsWV9U6igSYNZj6zsCsh6uVCzaSL7x567cZ1c2Xr

New address detected! Click here to add to your address book.

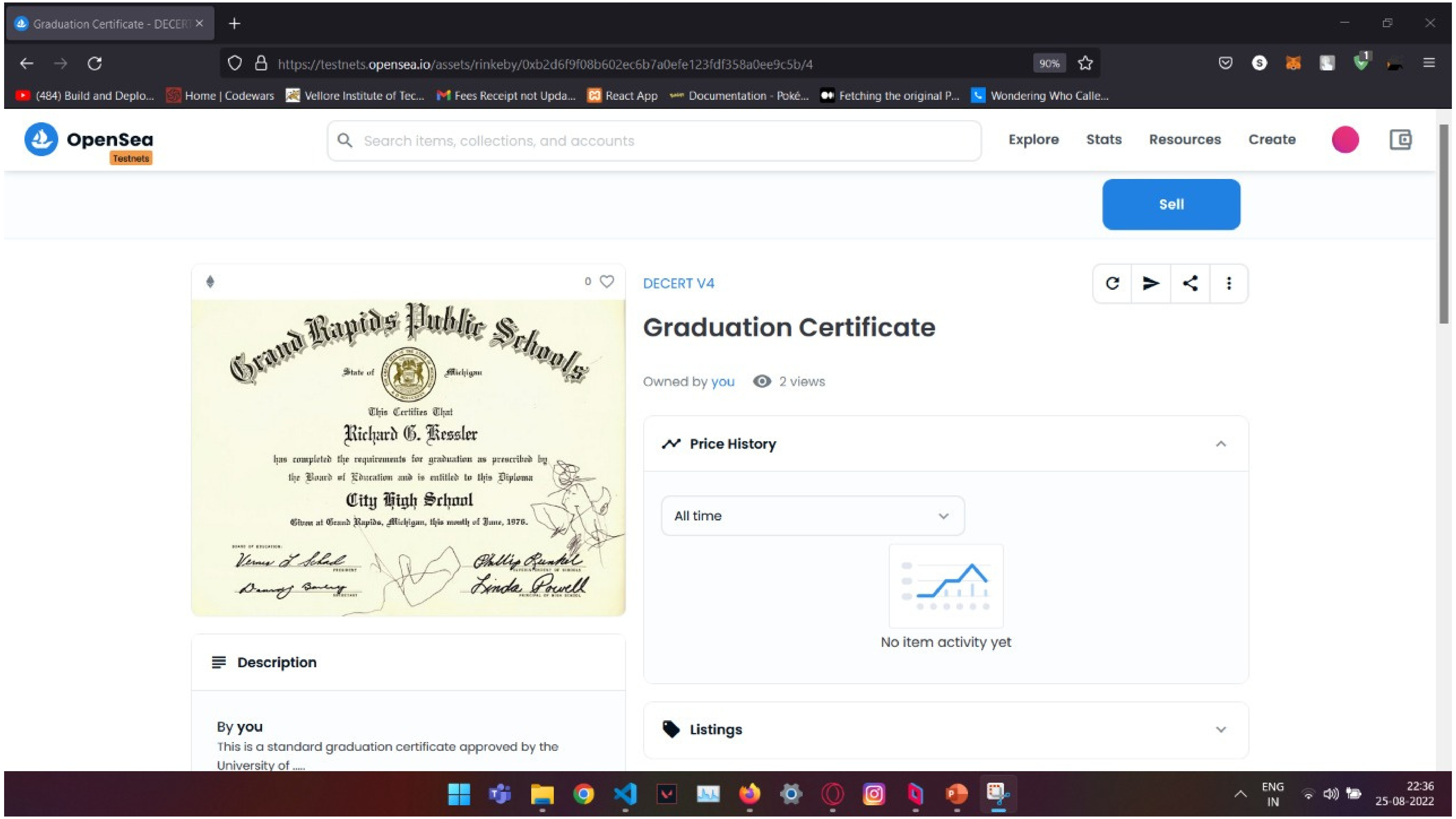
Estimated gas fee 0.00022446
0.000224 RinkebyETH

Site suggested
Likely in < 30 seconds
Max fee: 0.00022514 RinkebyETH

Total 0.00022446
0.00022446 RinkebyETH

Amount + gas fee
Max amount: 0.00022514 RinkebyETH

Fig: Authentication (Only Authorized Used Allowed To Mint)


Graduation Certificate - DECERT
https://testnets.opensea.io/assets/rinkeby/0xb2d6f9f08b602ec6b7a0efe123fdf358a0ee9c5b/4
90%
(484) Build and Deplo...
Home | Codewars
Vellore Institute of Tec...
Fees Receipt not Upda...
React App
Documentation - Poké...
Fetching the original P...
Wondering Who Calle...
OpenSea
Testnets
Search items, collections, and accounts
Explore
Stats
Resources
Create
Sell
0
ENG
IN
22:36
25-08-2022

DECERT V4

Graduation Certificate

Owned by you 2 views

Price History

All time

No item activity yet

Listings

Grand Rapids Public Schools

State of Michigan

This Certifies That

Richard G. Kessler

has completed the requirements for graduation as prescribed by the Board of Education and is entitled to this Diploma

City High School

Given at Grand Rapids, Michigan, this month of June, 1976.

Phillip Runkel

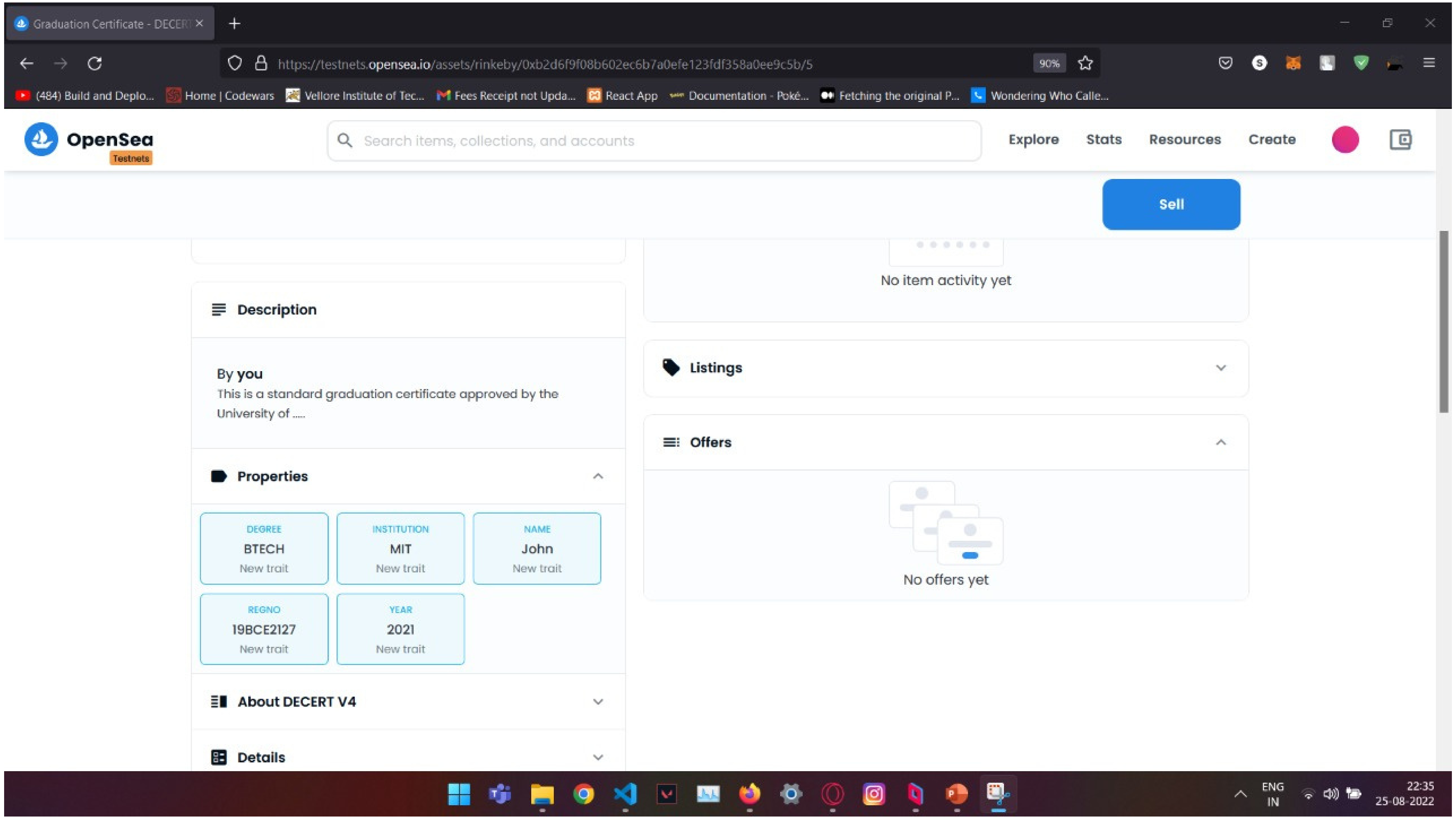
Linda Powell

Description

By you

This is a standard graduation certificate approved by the University of .....

Fig: Minted Certificate with A Default Certificate Image (Rinkeby Testnet)



No item activity yet

Description

By you

This is a standard graduation certificate approved by the University of .....

Properties

DEGREE
BTECH
New trait

INSTITUTION
MIT
New trait

NAME
John
New trait

REGNO
19BCE2127
New trait

YEAR
2021
New trait

No offers yet

Fig: Certificate Details Shown As Attributes And Not In The Description

Conclusion and Future Scope

This was a successful project with positive results. This can be further developed and deployed. Future work in this area includes the development of the decentralized marketplace and exchange for NFTs, The Decentralized application should evolve into the full-scale where NFTs could be traded and swapped in the same way it could be done with cryptocurrency nowadays.

THANK YOU