

Major Project Report on

# **CERTIFICATE VERIFICATION USING BLOCKCHAIN**

Submitted in partial fulfillment of the requirements for the degree of

BACHELOR OF TECHNOLOGY

in

INFORMATION TECHNOLOGY

by

**Shwetha Jayaprakash M (181IT245)**

**Manish Rathore (191IT229)**

*under the guidance of*

**Dr. Bhawana Rudra**



DEPARTMENT OF INFORMATION TECHNOLOGY  
NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA  
SURATHKAL, MANGALORE - 575025

April, 2023

## DECLARATION

I/We hereby *declare* that the Major Project-IT499 Work Report entitled "***Certificate Verification using Blockchain***", which is being submitted to the **National Institute of Technology Karnataka, Surathkal**, for the award of the Degree of Bachelor of Technology in Information Technology, is a *bonafide report of the work carried out by us*. The material contained in this Major Project-IT499 Report has not been submitted to any University or Institution for the award of any degree.

*Name of the Student (Registration Number) with Signature*

(1) Shwetha Jayaprakash M (181IT245)

(2) Manish Rathore (191IT229)

Department of Information Technology

Place : NITK, Surathkal

Date : 12/04/2023

# CERTIFICATE

This is to *certify* that the Major Project Work Report entitled "***Certificate Verification using Blockchain***" submitted by

*Name of the Student (Registration Number)*

(1) Shwetha Jayaprakash M (181IT245)

(2) Manish Rathore (191IT229)

as the record of the work carried out by them, is *accepted as the B.Tech. Major Project-IT499 work report submission* in partial fulfillment of the requirement for the award of degree of Bachelor of Technology in Information Technology in the Department of Information Technology, NITK Surathkal.

**Dr. Bhawana Rudra**

Professor

Department of Information Technology

NITK Surathkal, Karnataka

**(Chairman - DUGC)**

(Signature with Date)

## **ACKNOWLEDGEMENT**

We would like to take this opportunity to express my deepest sense of gratitude and sincere thanks to everyone who helped me to complete this work successfully. I express my sincere thanks to Dr. Bhawana Rudra, Information Technology, NITK-Surathkal, Karnataka for providing me with all the necessary facilities and support.

# ABSTRACT

Every year lakhs of students are completing higher education and obtaining their certificates that may include results, diplomas, or transcripts during their entire duration of studies. For admission, students need to produce these certificates in institutions or companies. And it is a challenge to track thousands of documents and authenticate. Due to the lack of an efficient anti-forgery mechanism, certificate fraud is frequently discovered. We can solve complex domain that involves various challenges and tedious processes of authentication and make the data more safe and secure. Everything needs to be digitized with the adhering to the concept of Confidentiality, Reliability and Availability. These can all be accomplished with technology named Blockchain. Blockchain is a large open access online distributed ledger that is shared and verified among the nodes of a computer network. Briefly explaining, the system management will consist of a Certificate Authority will upload certificate and after validation, the certificate can be viewed by the student. Each certificate owns a special hash key that can be used to validate the authenticity of the certificate by any organization through the portal. The creation of this system aims to digitally replace the outdated method of submitting transfer certificates in every stage of education system and leaving handwritten records. Today's certificate management methods are cumbersome and time-consuming. The manual entry makes it easy to forge the certificates. This digital certificate system, which is based on cryptography, aims to address the issue of certificate forgery and reduce the risk of losing or damaging a certificate.

**Keywords**— Blockchain, dApps, Ethereum, InterPlanetary File System (IPFS), Metamask, Smart contracts, Solidity.

# CONTENTS

<b>LIST OF FIGURES</b>	<b>iii</b>
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 Overview . . . . .	1
1.2 Motivation . . . . .	2
<b>2 LITERATURE REVIEW</b>	<b>3</b>
2.1 Background and Related Works . . . . .	3
2.2 Outcome of Literature Review . . . . .	4
2.3 Problem Statement . . . . .	4
2.4 Objectives of the Project . . . . .	4
<b>3 PROPOSED METHODOLOGY</b>	<b>6</b>
3.1 Project Description . . . . .	6
3.2 Software Requirements . . . . .	6
3.3 Project Architecture . . . . .	6
3.3.1 Certificate Issuing Module . . . . .	7
3.3.2 Designing and writing Smart Contract . . . . .	7
3.3.3 Procedure of Uploading Document . . . . .	9
3.3.4 Verification Module . . . . .	9
<b>4 RESULTS AND ANALYSIS</b>	<b>11</b>
<b>5 CONCLUSIONS AND FUTURE WORK</b>	<b>15</b>
<b>REFERENCES</b>	<b>16</b>
5.1 BioData: . . . . .	19
5.1.1 Student 1 . . . . .	19
5.1.2 Student 2 . . . . .	19

# LIST OF FIGURES

3.3.1 Only institute can be the modifier . . . . .	8
3.3.2 Smart contract for adding hash and finding document hash . . . . .	8
3.3.3 Flowchart of the website . . . . .	9
4.0.1 Home Page . . . . .	11
4.0.2 Institute Login Page along with address id, chain id and MATIC balance	12
4.0.3 Upload Page done under student address . . . . .	12
4.0.4 Delete Page . . . . .	13
4.0.5 Verify Page . . . . .	14

# CHAPTER 1

## INTRODUCTION

### 1.1 Overview

In the past, there were certain policies like the National Policy on Education and the Programme of Action that were put in place to provide children under the age of 14 with access to free and mandatory education of a higher standard. The student's education life goes from primary, secondary, to high school. After finishing high school, students are required to apply for admission to universities. Similarly, for graduation, they have to switch to another college. This is the standard educational cycle for most students. After graduation, some students might choose to pursue higher education. During this cycle, students are expected to provide all the necessary certificates and documents for validation. However, this process poses a risk of losing or damaging these important certificates. And it is cumbersome and time-consuming for the validator to authenticate each certificate. Consider the population of our country, almost lakhs of students graduate. It is very hard to keep up with manual process to track documents and validate it for such huge amount of records. There are chances of forging the documents. Anti-forgery mechanism has not been efficient in proving the accuracy. It can be quite challenging to differentiate between a fake and an authentic certificate, and it requires a lot of focus and attention to detail. This process can be time-consuming and may end up wasting valuable time.

In order to overcome this drawback, a technology called Blockchain enters our lives as a rescuer. Thus, why utilise Blockchain? Because a Blockchain's data cannot be altered or changed under hypothetical circumstances. Despite data changes, it only takes a moment to alert us to the meddling. In a node or piece of data on the blockchain is only valid when many parties concur on it. The system would be trustworthy and at any time, authentication was possible.



## 1.2 Motivation

Every new invention arises from an effort to address a problem. One such technology that introduces decentralisation is blockchain technology. No single governing body will be in charge of making all the choices. Several issues with conventional systems are resolved by decentralisation. Blockchain technology has unchangeable, distributed, decentralized, consensus-building, and secure mechanism. We may address our issue with certificate forging using this approach. The blockchain adheres to a consensus method, which serves to shield networks against bad conduct and hacking assaults even if a third party tries to change the data. Informing us of the tampering is considerably simpler. The problem of tampering is now resolved.

The next issue is data loss or damage. Blockchain does not have any storage of any its information in a single place. It is highly decentralized. Instead, a network of computers copies and disseminates the blockchain. Every computer in the network updates its blockchain to reflect change whenever a new block is added. As a result, the data loss or damage is handled. There is another problem with regards to time consumption for validation. The system that we will be building will allow verification of certificate by checking if the document's hash is similar to already stored hash.

# CHAPTER 2

## LITERATURE REVIEW

### 2.1 Background and Related Works

The project is focused on developing a blockchain-based system for certificate verification system. We have cited a few previously published articles and works by various authors in this field in order to support this. Our Literature Survey mainly focused on Blockchain Technology, an advanced Storage System IPFS, and Digital Certificate Validations using Ethereum. Our first paper [1] was titled, An overview of blockchain technology. In this paper, they give us extensive knowledge of how Blockchain works including various concepts of hashing , block creation, block structure and key characteristics of blockchain like decentralization, anonymity, persistency, auditability and different types of some typical consensus algorithms i.e., Proof of Work (PoW), Proof of Stake (PoS). Our second paper on IPFS [2], InterPlanetary File System. A file is divided into chunks when it is uploaded to IPFS, with each chunk holding no more than 256 kilobytes of data and/or links to other chunks.. Every chunk is identified by a content identifier. The mentioned links with content identifiers form a Merkle DAG. Due to the Merkle DAG, a file can be determined by looking only at the root hash. The paper [3] was named, Blockchain and Smart Contract for Digital Certificate . There were 3 actors in their design. Institutions came first, followed by students, and then service providers. Their approach had the flaw of employing "one hash as a key," which makes it accessible to everyone who has the hash. In the paper [4], taking advantage of new technology, the authorities grant a e- certificates containing a quick response (QR) code to the graduates whose data have been successfully verified. Each graduate also receives a QR code-enabled certificate file and an inquiry number for the target companies. The companies send inquiries to the system and the QR code enables them to recognize if the certificate has been tampered with or not. The next paper [5], Tamper Proof Birth Certificate, had a design that was essentially identical to the prior study, with the exception that it used the AES algorithm and stored the data in the IPFS. They specifically designed their system for birth certificates. The flaw was that neither the original document nor the ability to create certificates

online were ever saved anywhere.

## **2.2 Outcome of Literature Review**

After seeing the literature review, we can conclude that all the proposed system has some flaws. In the phase of broadcasting the certificate authentication data to the blockchain, the institution should pay a few mining fees for the miner to confirm it on the blockchain. Identifying fraudulent credentials from genuine ones is one of the major challenges for officials. A digital certificate that a business issues on blockchain can be instantaneously confirmed by clicking on the verification link or scanning a QR code. IPFS is a technique that makes use of cryptographic hashes that are conveniently stored on a blockchain. The actual owner, being the only one having the file, can choose to modify it, eventually being able to successfully register as its owner. The successfully hijacked content identifiers serve no purpose, as nodes other than the owner do not have access to the original file. For retrieving a file, if the required permission has been provided, it resembles the chunks to obtain file. If the permission has not been granted, the request will not be answered.

## **2.3 Problem Statement**

In trivial certificate verification systems, a student was needed to keep the records of each and every certificate from primary school to higher education. And sometimes, the certificate would be lost or damaged or forged making it difficult to keep track of. There were a lot of flaws like – lack of security, auditability, integrity, time-consuming and others which can be solved using our proposed method which is Certificate Validation using Blockchain.

## **2.4 Objectives of the Project**

- (1) Create interactive website for better user engagement
- (2) Create a metamask wallet for creating a local blockchain environment

- (3) Deploy our decentralized applications (dApps) and smart contracts on Polygon network
- (4) Add institute block address on Polygon and name of the institute
- (5) Add student block address on Polygon
- (6) Upload the certificate on student address by institute
- (7) Student gets the hash of certificate and can view certificate
- (8) Verifier can verify the certificate

# CHAPTER 3

## PROPOSED METHODOLOGY

### 3.1 Project Description

For the loopholes in our current methodologies, we have proposed our system which will upload certificates as well as verify them. The data will be reliable and unchangeable unless owner modifies it. This section presents our proposed end-to-end solution for transmission and verification of academic document. First let's look at the requirements.

### 3.2 Software Requirements

This proposed framework requires various technologies such as Ganache-cli, which is used for setting up a local blockchain and for testing the decentralized application (dApp), Truffle for designing and developing the decentralized application, Metamask which connects the web application with the Ethereum blockchain and acts as a bridge between them using polygon network. Polygon network helps for easier secure transaction. Next IPFS (Interplanetary File System) which is a file sharing system that allows storing and accessing files using hashes in a decentralized manner. All these technologies combined with front end to give a decent user interface of websites. Further Remix IDE an Ethereum based platform is used to check the functionality of the smart contract.

### 3.3 Project Architecture

- (1) Certificate Issuing Module: College acts as a Certificate issuing authority. This module can be any organization that wishes to issue a certificate. It will also include a phase where the College will upload certificates after authorizing the details. Students will be see and download the digital documents. Students also receive the hash of the document issued for him.

- (2) Verification Module: The third party acts as verifier. The student who applied for college change, can showcase the certificate as a proof of their skill to the verifier of new college who verifies whether the certificate is authentic or not.

### **3.3.1 Certificate Issuing Module**

We consider college as a Degree Certificate Issuing Authority. We have designed web application which needs to be connected into the blockchain smart contract using the ABI of the contract. The following are the main functionalities of the contract:

### **3.3.2 Designing and writing Smart Contract**

Before creating a new smart contract, understand the requirements for the problem. For certificate verification, the structure can be seen as follows:

1. Name of the contract
2. struct studentRecord with blockNumber, minetime, ipfsHash
3. struct instituteRecord with blockNumber, string name
4. Modifiers to check validity and authorization of the owner
5. Functions addDocHash, findDocHash, deleteHash are the main functions of the contract
6. Compile this smart contract in Remix IDE , integrate the ABI into javascript and deploy contract.
7. Test if the contract is working accurately

Below are the figures which show functionalities of the contract

```

modifier onlyOwner() {
    if (msg.sender != owner) {
        revert("Caller is not the owner"); }_; }

modifier validAddress(address _addr) {
    assert(_addr != address(0)); _; }

modifier authorised_institute(bytes32 _doc){

    if (keccak256(abi.encodePacked((institutes[msg.sender].info )))!= keccak256(abi.encodePacked((docHashes[_doc].info))))

    revert("Caller is not authorised to edit this document");

    _; }

modifier canAddHash(){
    require(institutes[msg.sender].blockNumber!=0,"Caller not authorised to add documents"); _; }

```

Figure 3.3.1: Only institute can be the modifier

```

event addHash(address indexed _institute,string _ipfsHash);
function addDocHash (bytes32 hash,string calldata _ipfs) public
canAddHash
{
    assert(docHashes[hash].blockNumber==0 && docHashes[hash].minetime==0);
    Record memory newRecord =
    Record(block.number,block.timestamp,institutes[msg.sender].info,_ipfs);
    docHashes[hash] = newRecord;
    ++count_hashes;
    emit addHash(msg.sender,_ipfs);
}

function findDocHash (bytes32 _hash)
external view returns (uint,uint,string memory,string memory) {

    return (docHashes[_hash].blockNumber,docHashes[_hash].minetime,
    docHashes[_hash].info,docHashes[_hash].ipfs_hash );
}

function deleteHash (bytes32 _hash) public
authorised_institute(_hash)
canAddHash
{
    assert(docHashes[_hash].minetime!=0);
    docHashes[_hash].blockNumber=0;
    docHashes[_hash].minetime=0;

    --count_hashes;
}

function getInstituteInfo(address _add) external view returns(string memory){

    return (institutes[_add].info);
}

```

Figure 3.3.2: Smart contract for adding hash and finding document hash

Incorporate the smart contract into Remix ethereum IDE to generate artifacts. Copy the Application Binary Interface (ABI)—It contains functions that have values for their input and output parameters into Javascript file. Run and deploy the smart contract by selecting Injected Provider - Metamask.

### 3.3.3 Procedure of Uploading Document

Connect to polygon network in metamask wallet for Ethereum-compatible transaction. In the Admin page, connect Institute or Exporter metamask address and add name of the institute thus the institute account is created. Now for uploading the document, in the upload page, connect student block address in metamask wallet. Institute uploads the document in student block address. Document should be hashed and stored in Ipfs. Confirm the transaction fees for uploading. After uploading, it displays the hash of the document along with institute address. Student can view the document with a click. Institute can delete the document from the IPFS if there's any discrepancy on Delete page.

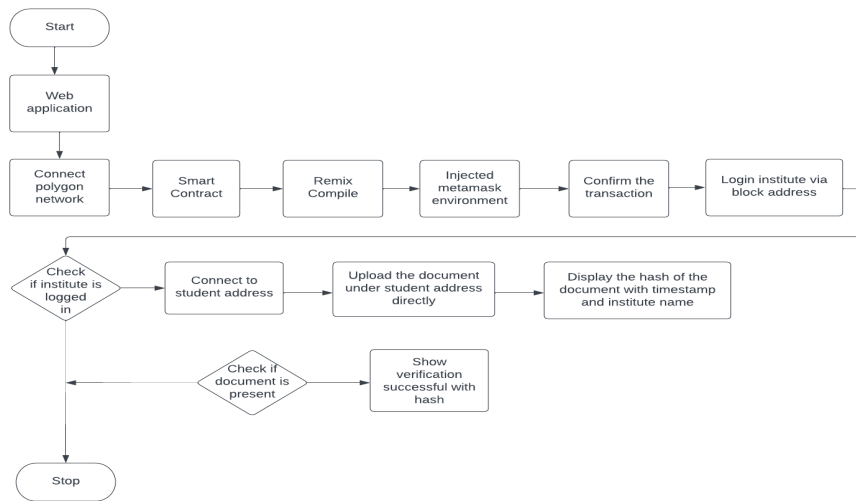


Figure 3.3.3: Flowchart of the website

### 3.3.4 Verification Module

A verify page is created for the verifier which can act as an information desk. The student who applied for college change, can showcase the certificate as a proof of their skill to the verifier of new college/company. This company verifies whether the certificate is authentic or not by uploading the same document to check if it's present in IPFS. There is no third-party involvement in this whole process of verification. So, it eliminates the tampering mechanism.

1. Upload the document of the student and click on verify



2. If present, it displays the hash of the document, Institute address along with timestamp
3. Else it shows document not present

# CHAPTER 4

## RESULTS AND ANALYSIS

We are working on registration of College as a valid certificate issuing authority to avoid tampering of certificates using invalid college identity. Institute logs in via blockchain address. Uploads the document in the student address. Document is then hashed and finally hash of the document is to be displayed.

The various technologies such as Ganache-cli, Truffle, Metamask, IPFS used. Ganache-cli acts as local blockchain and it is used for testing the decentralized application. Remix IDE is used for designing and testing using Ethereum Virtual Machine. Metamask allows us to interact with the Ethereum blockchain ecosystem. IPFS is a file sharing system that allows to store and serve files as a part of a peer-to-peer network relying on cryptographic hashes.

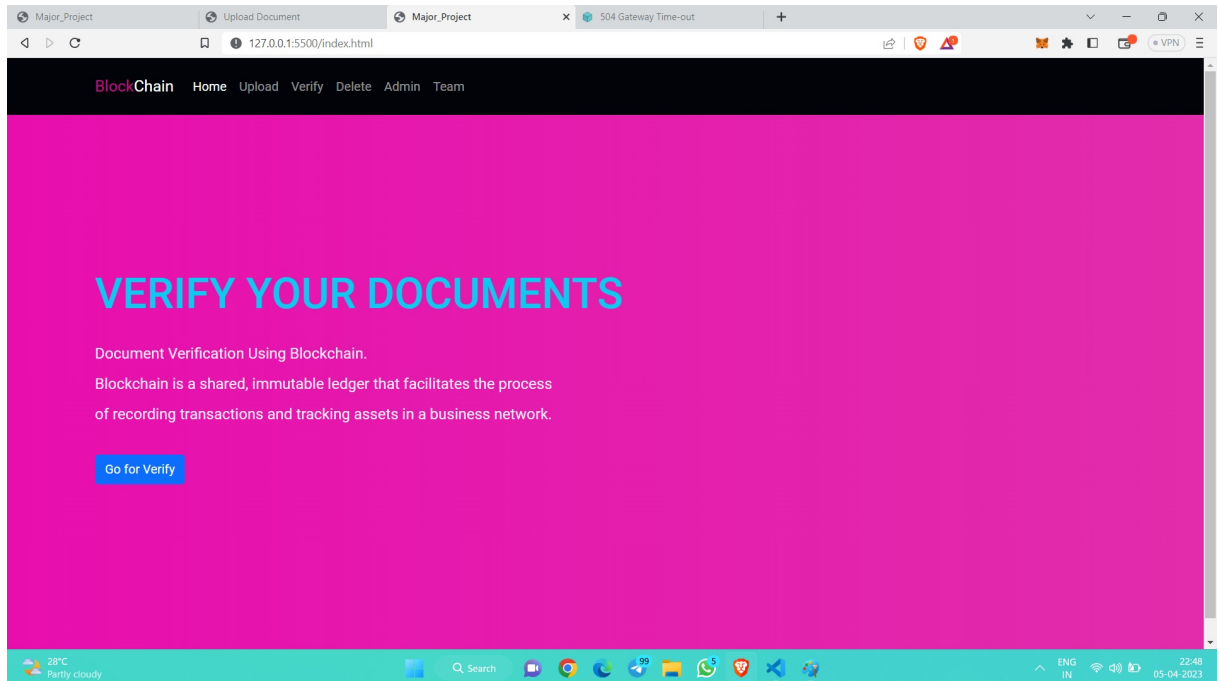


Figure 4.0.1: Home Page

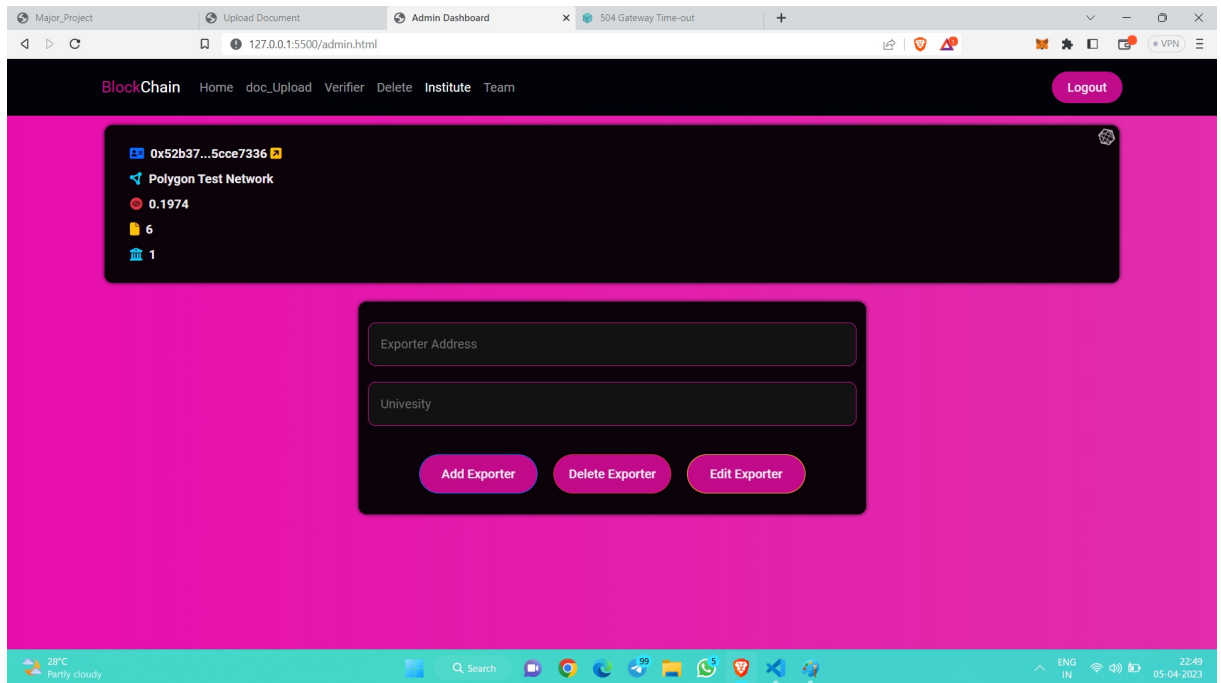


Figure 4.0.2: Institute Login Page along with address id, chain id and MATIC balance

There are functionalities of adding, deleting and modifying the institute/exporter

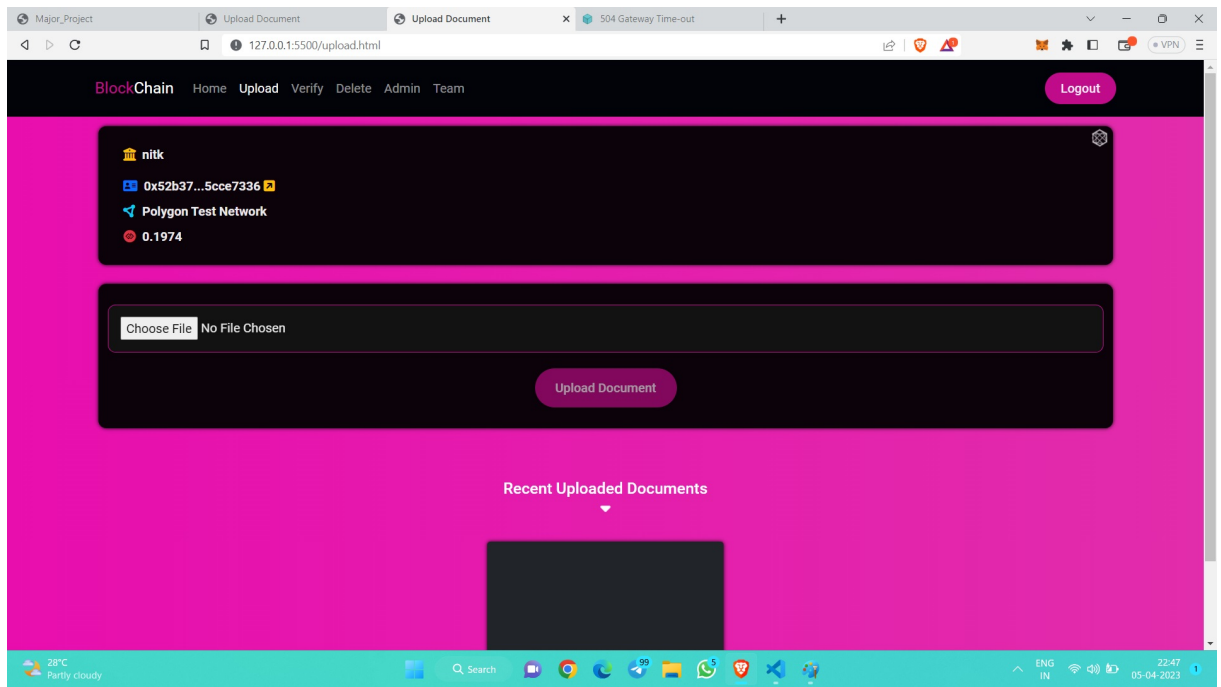


Figure 4.0.3: Upload Page done under student address

Once the logging in of institute is done, go to upload page. Here institute directly uploads the certificate in student's ethereum address. After uploading certificate, hash is generated and displayed with details of which institute, timestamp and transaction ID.

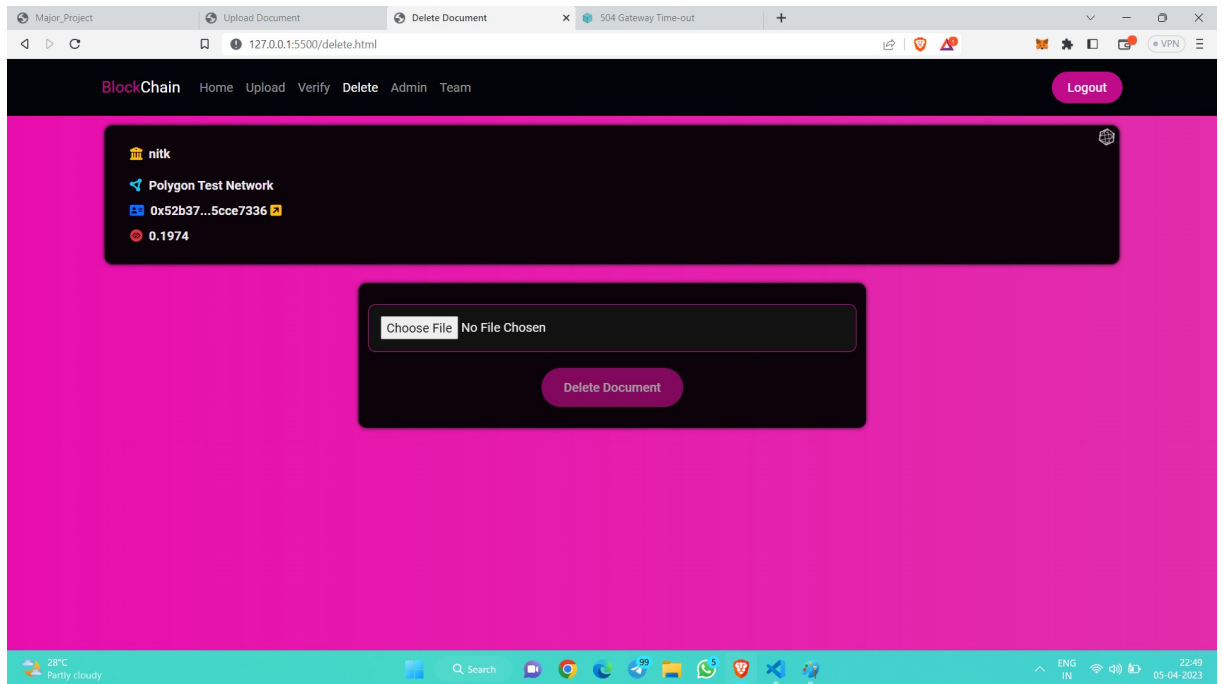


Figure 4.0.4: Delete Page

In the delete page, we can upload the document which we want to delete from the IPFS. Only the exporter/ institute can remove the document.

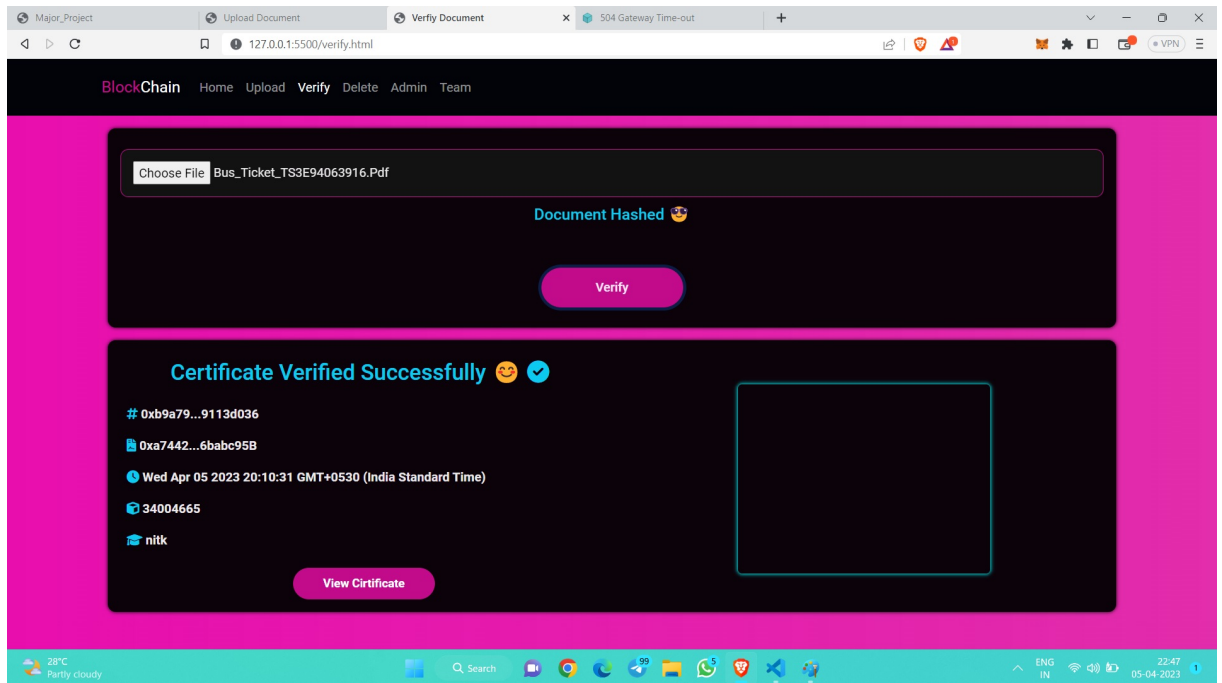


Figure 4.0.5: Verify Page

We know it's hard to remember the hash of the document, so to make the verification process simpler we have included uploading the document and verifying whether it is from an authentic source. Verifier page displays the hash of the document, timestamp, name of the source.

# CHAPTER 5

## CONCLUSIONS AND FUTURE WORK

In this Paper, a blockchain based certificate verification is introduced that a risk of losing and damaging the certificate. The blockchain properties allows us to verify where the certificate is authentic or not without paper work.

A framework is proposed for creation of a decentralized app "Certificate Verification using Blockchain". First task done is to creation of aesthetic user web interface for easier communication , next integrate smart contract with the web interface which is quite challenging. Compile the contract and using the ABI - Application Binary Interface which serves as a standard method for contract-to-contract communication within the Ethereum ecosystem and from outside the blockchain. Smart contract allows different functionalities of adding institute, student, hash, uploading of the document, verifying the document. Utilizing IPFS, storing the certificates is done. All the variables and the method functions are deployed and tested for checking the working of the contract. Thus final contract is deployed.

Now the user interface allows user to enter the details. We have our javascript working such that all details are captured and incorporated with smart contract. All documents are stored and verified accordingly. Only owner has the authorization to add, remove the document. Once the document is removed, the hash is removed from the ipfs. Since IPFS data is stored across a network of computers as a hash/value pair, uses decentralized mechanism. It queries the entire network to determine "who has data associated with the hash" and simultaneously collects bits from numerous computers. The company who acts as the verifier can view the certificate as long as they have the hash.

This project helps students who are willing to showcase their certificate. This certificate will be accessible 24\*7.

The verifier can verify whether the certificate shared by the student is authentic by checking the institute details and minetime. To reduce the complexity of misspelling the hash, we incorporated direct addition of document to check it's validity.

# REFERENCES

- [1] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.
- [2] Y. Chen, H. Li, K. Li and J. Zhang, "An improved P2P file system scheme based on IPFS and Blockchain," 2017 IEEE International Conference on Big Data (Big Data), 2017, pp. 2652-2657, doi: 10.1109/BigData.2017.8258226.
- [3] J. -C. Cheng, N. -Y. Lee, C. Chi and Y. -H. Chen, "Blockchain and smart contract for digital certificate," 2018 IEEE International Conference on Applied System Invention (ICASI), 2018, pp. 1046-1051, doi: 10.1109/ICASI.2018.8394455.
- [4] A. Gayathiri, J. Jayachitra and S. Matilda, "Certificate validation using blockchain," 2020 7th International Conference on Smart Structures and Systems (ICSSS), 2020, pp. 1-4, doi: 10.1109/ICSSS49621.2020.9201988.
- [5] Shraddha S. and Patel, Niraj and Parab, Sukaji and Maurya, Sushil, Blockchain based Tamper Proof Certificates (May 24, 2021). Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021).
- [6] S. Namasudra, P. Sharma, R. G. Crespo and V. Shanmuganathan, "Blockchain-Based Medical Certificate Generation and Verification for IoT-based Healthcare Systems," in IEEE Consumer Electronics Magazine, doi: 10.1109/MCE.2021.3140048.
- [7] G. Zyskind, O. Nathan and A. ' . Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," 2015 IEEE Security and Privacy Workshops, 2015, pp. 180-184, doi: 10.1109/SPW.2015.27.
- [8] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K. -K. R. Choo and M. Aledhari, "Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 8, pp. 2146-2156, Aug. 2020, doi: 10.1109/JBHI.2020.2969648.

- [9] S. Guo, X. Hu, S. Guo, X. Qiu and F. Qi, "Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1972-1983, March 2020, doi: 10.1109/TII.2019.2938001.
- [10] J. Liu and Z. Liu, "A Survey on Security Verification of Blockchain Smart Contracts," in *IEEE Access*, vol. 7, pp. 77894-77904, 2019, doi: 10.1109/ACCESS.2019.2921624.
- [11] Y. Chen, H. Li, K. Li and J. Zhang, "An improved P2P file system scheme based on IPFS and Blockchain," 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 2017, pp. 2652-2657, doi: 10.1109/BigData.2017.8258226.
- [12] J. Jiao, S. Kan, S. -W. Lin, D. Sanan, Y. Liu and J. Sun, "Semantic Understanding of Smart Contracts: Executable Operational Semantics of Solidity," 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2020, pp. 1695-1712, doi: 10.1109/SP40000.2020.00066.
- [13] Nikhil, S. Panday, A. Saini and N. Gupta, "Instigating Decentralized Apps with Smart Contracts," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2022, pp. 1-5, doi: 10.1109/ACCAI53970.2022.9752568.



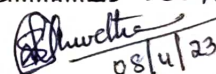
Department of Information Technology  
National Institute of Technology Karnataka, Surathkal-575025

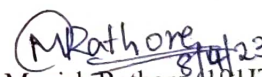
**Permission from Major Project-II Guide to Appear for End Semester Evaluation of  
Major Project-II (IT499)**

I/We student(s) of 8<sup>th</sup> semester B.Tech.(IT) carried out the Major Project-II titled "Certificate Verification using Blockchain" under your guidance of "Dr. Bhawana Rudra" from 02<sup>th</sup> Jan 2023 to 24<sup>th</sup> April 2023. I/we have shown the Major Project-II progress regularly to my major project guide and incorporated all technical suggestions given by my/our Major Project guide in the Major Project-II.

Progress of the my/our Major Project-II in points-wise are as follows:

1. Provide web user interface
2. Deploy verification smart contract on Remix IDE
3. Allow institute to upload the certificate and verify for verification of the certificate

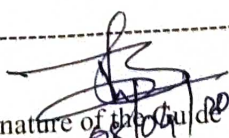
  
08/4/23  
Shwetha Jayaprakash M (181IT245)

  
8/4/23  
Manish Rathore (191IT229)

Aforesaid student(s) shown the progress as well as Report of the Major Project-II (IT499) carried out by him/her/them. Progress is satisfactory. (If progress is not satisfactory strickout this line and write the comments below)

Write comments/remarks if the progress of Major Project-II (IT499) is not satisfactory

-----  
-----

  
(Signature of the Guide with date)  
08/4/2023  
Dr. Bhawana Rudra

## **5.1 BioData:**

### **5.1.1 Student 1**

Name: Shwetha Jayaprakash M

Roll No: 181IT245

Email Id: shwethajp1508@gmail.com

Phone No: 8050985445

Address:

24, c/0 JP Nilaya,

Near BCM Ladies Hostel,

Relable Layout, Puttaswamaiya Palya,

Sira Gate, Tumkur 572106

### **5.1.2 Student 2**

Name: Manish Rathore

Roll No: 191IT229

Phone No: 8349265560

Email id: manish982864@gmail.com

Address: F.e 23 vardhman colony , worker colony budhni distt sehore , pillikarar  
466445 Madhya pradesh