

**A
Project Report
on**

**DOQFY: DIGITAL DOCUMENT VERIFICATION USING
BLOCKCHAIN AND IPFS**

Submitted to

Sant Gadge Baba Amravati University, Amravati

**Submitted in partial fulfilment of
the requirements for the Degree of
Bachelor of Engineering in
Computer Science and Engineering**

Submitted by

Mr. Pratik Ganesh Ekhande

(PRN: 203120374)

Mr. Yash Kumar Sugandhi

(PRN:203120341)

Under the Guidance of

**Dr. J. M. Patil
HOD, CSE Dept.**



**Department of Computer Science and Engineering
Shri Sant Gajanan Maharaj College of Engineering,
Shegaon – 444 203 (M.S.)
Session 2023-2024**

SHRI SANT GAJANAN MAHARAJ COLLEGE OF ENGINEERING,
SHEGAON – 444 203 (M.S.)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING



CERTIFICATE

This is to certify that **Mr. Pratik Ganesh Ekhande and Mr. Yash Kumar Sugandhi** students of final year Bachelor of Engineering in the academic year 2023-24 of Computer Science and Engineering Department of this institute have completed the project work entitled **“DOQFY: DIGITAL DOCUMENT VERIFICATION USING BLOCKCHAIN AND IPFS”** and submitted a satisfactory work in this report. Hence recommended for the partial fulfilment of degree of Bachelor of Engineering in Computer Science and Engineering.

Dr. J. M. Patil
Project Guide

Dr. J. M. Patil
Head of Department

Dr. S. B. Somani
Principal
SSGMCE, Shegaon

SHRI SANT GAJANAN MAHARAJ COLLEGE OF ENGINEERING,

SHEGAON – 444 203 (M.S.)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING



CERTIFICATE

This is to certify that **Mr. Pratik Ganesh Ekhande and Mr. Yash Kumar Sugandhi** students of final year Bachelor of Engineering in the academic year 2023-24 of Computer Science and Engineering Department of this institute have completed the project work entitled **“DOQFY: DIGITAL DOCUMENT VERIFICATION USING BLOCKCHAIN AND IPFS”** and submitted a satisfactory work in this report. Hence recommended for the partial fulfillment of degree of Bachelor of Engineering in Computer Science and Engineering.

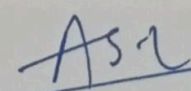

Internal Examiner

Dr - J. M. Patil

Name and Signature

Date: 10/5/24

External Examiner


Name and Signature

Date: 10/5/24

Acknowledgement

It is our utmost duty and desire to express gratitude to various people who have rendered valuable guidance during our project work. We would have never succeeded in completing our task without the cooperation, encouragement and help provided to us by them. There are a number of people who deserve recognition for their unwavering support and guidance throughout this report.

We are highly indebted to our guide **Dr. J. M. Patil** for his guidance and constant supervision as well as for providing necessary information from time to time. We would like to take this opportunity to express our sincere thanks, for his esteemed guidance and encouragement. His suggestions broaden our vision and guided us to succeed in this work.

We are sincerely thankful to **Dr. J. M. Patil** (HOD, CSE Department, SSGMCE, Shegaon), and to **Dr. S B Somani** (Principal, SSGMCE, Shegaon) who always has been kind to extend their support and help whenever needed.

We would like to thank all teaching and non-teaching staff of the department for their cooperation and help. Our deepest thank to our parents and friends who have consistently assisted us towards successful completion of our work.

Pratik Ganesh Ekhande
Yash Kumar Sugandhi

Contents

Abstract	i
List of Abbreviations	ii
List of Figures	iii
List of Screenshots	iv
List of Tables	v
1. Introduction	1
1.1 Preface	1
1.2 Motivation	2
1.3 Problem Statement	3
1.4 Objectives	3
1.5 Scope of Project	3
1.6 Organization of Project	4
2. Literature Review	7
2.1 Introduction to Proposed System	7
2.2 Stakeholders and Roles	7
2.3 Encryption and Decentralised Storage	7
2.4 Large Data Handling	8
2.5 Cost Concerns and alternative Solutions	8
2.6 Integration of Insights	8

3. Methodology

10

3.1 Blockchain 10

3.2 Proposed System 10

3.3 System Model 11

3.4 Modules 11

3.5 Entities in the System 16

4. Implementation

20

4.1 Smart Contract 20

4.2 IPFS Integration 21

4.3 Ether.js & Contract Interaction 21

4.4 User Authentication 21

5. Result and Discussion

23

5.1 Authentication 23

5.2 Owner 23

5.3 Student 24

5.4 University 24

5.5 Company 25

5.6 Result 25

5.7 Gas Usage Metrics	26
-----------------------	----

6. Conclusion	28
----------------------	-----------

6.1 Conclusion	28
----------------	----

6.2 Future Scope	28
------------------	----

References	30
-------------------	-----------

Abstract

Every year, millions of students enrol in Indian higher education institutions, generating numerous certificates such as marksheets, certificates, appreciation cards, and diplomas throughout their academic journey. For admissions or job applications, students are required to submit these documents to institutes or companies. However, manually tracking and validating the authenticity of these certificates becomes a tedious task. In the era of AI tools and smart editing technologies, the risk of modifying scores on scorecards or forging someone else's documents has increased. Manual document verification is not only time-consuming but also incurs paper costs and poses challenges to managing old records. There is a pressing need to address this issue and streamline the document verification process, ensuring confidentiality, reliability, and data availability. This paper suggests creating a verification system based on blockchain technology aimed at preserving data integrity.

Keywords: Blockchain· Manual verification· QR code· Confidentiality· Reliability· Data availability.

List of Abbreviations

Abbreviation	Description
IPFS	Inter Planetary File System
DApp	Decentralized Application
ETH	Ethereum
OOP	Object Oriented Programming
EVM	Ethereum Virtual Machine
CLI	Command Line Interface
SSR	Server Side Rendering
SEO	Search Engine Optimization
LTS	Long Term Support
NPM	Node Packet Manager
API	Application Programming Interface

List of Figures

Figure No.	Description
Figure 3.1	Proposed System Model
Figure 3.2	System Work Flow

List of Screenshot

Screenshot No.	Description
Screenshot 5.1	Authentication Page
Screenshot 5.2	Owner Page
Screenshot 5.3	Student Page
Screenshot 5.4	University Page
Screenshot 5.5	Company Page
Screenshot 5.6	Verified Document

List of Tables

Table No.	Description
Table I	Upload Document Gas Cost
Table II	Verify Document Gas Cost

CHAPTER 1
INTRODUCTION

INTRODUCTION

1.1 PREFACE

In India, the basic cycle of education involves students being promoted to higher classes each year. After completing higher secondary education, students seek admission to junior college. For undergraduate education, there is yet another transition to a different college, and some may pursue postgraduate studies or opt for job placements.

However, a significant challenge arises as students need to present all their certificates at each stage for validation. This manual verification process becomes tedious for validators, requiring them to meticulously check each document detail against the original copies they maintain. Moreover, this process involves record-keeping and incurs paper costs. Another concern is the counterfeiting of documents, which is prevalent at a mass level. In India, obtaining a white-collar job without academic credentials is nearly impossible, leading some students with lower scores to resort to illegal means. Various methods are employed, including:

- 1) Degree Mills: Where fake degrees are generated and sold to clients.
- 2) Modified Documents: Involving alterations to original documents, such as changes in name or scores.
- 3) In-House Produced: Involving the creation of fake documents with the assistance of corrupt officials within institutions.

Even if the documents are genuine, the traditional verification process demands the submission of documents to the company, leading to a waste of time for the student, the university, and the company.

To address these challenges and mitigate the issues, blockchain technology emerges as a viable solution. Blockchain ensures data integrity since the information stored in it cannot be altered. With this technology, data validation occurs only when a consensus is reached. Every transaction within the blockchain is interconnected within a chain, guaranteeing that all participants possess the most recent ledger version. The concept of a distributed ledger involves duplicating and storing transactional data across

multiple nodes. Because blockchain operates as a peer-to-peer network, there's no reliance on third party providers for transaction validation.

This approach to record-keeping ensures resistance to tampering, with each peer retaining a complete ledger copy. The incorporation of new transactions necessitates consensus from the majority of peers or compliance with predetermined rules. This transformative approach not only addresses document verification challenges but also revolutionizes the process. By implementing blockchain in the education system, the need for physical document submission is eliminated. Instead of conventional approaches, academic certificates and accomplishments find secure storage on the blockchain, presenting a decentralized and transparent method for institutions and businesses to authenticate their validity. This not only amplifies security and operational efficiency but also mitigates the hazards associated with manual document management, ensuring a dependable and efficient verification process for all stakeholders engaged.

1.2 MOTIVATION

To address the issue of the distribution and verification of certificates, we propose a decentralized application that does the digital certificate generation and certificate verification processes. An effective solution by integrating the concepts of blockchain, ipfs and QR codes has been proposed. The system saves paper, cuts management costs, prevents forgery, and provides accurate and reliable information about certificates. Components

Blockchain technology provides a potential solution to these problems by providing a secure and immutable way to Digitally verify document. The use of blockchain for document authentication can help to prevent counterfeiting and protect document safety by enabling consumers to verify the authenticity of a document with ease.

This project's specific motivation is to develop a practical and efficient product authentication system using blockchain technology that can be easily implemented by Owners and adopted by universities and third parties. The proposed system aims to address the limitations of existing authentication methods by providing a tamper-proof and transparent way to digitally validate document journey from the university to the students and companies.

In addition to addressing the problems of forgery and document safety, the proposed system also has the potential to provide significant benefits to students. By ensuring the authenticity of their documents, universities can protect their brand reputation, reduce the risk of documents tampering, and enhance their relationship with companies.

1.3 PROBLEM STATEMENT

Universities and Institutes: They have to validate and verify each student's document and keep records for a longer period of time, and the next issue is the time consumption for validation

Companies and organizations: The tampering and production of fake or duplicate certificates is a problem for companies. They have to verify each document from the respective university, or institute this takes a lot of time to request and verify the document

The student: has to visit the university personally to attest the document, and they are also worried about losing or damaging the certificate in the validation process.

1.4 OBJECTIVES

- 1) To Enhanced Certificate Security
- 2) To make Efficient Validation process
- 3) To Generate Digital Certificate
- 4) To Eliminate Hidden Scams
- 5) To Reduced Administrative Burden

1.5 SCOPE OF PROJECT

- 1) Utilizing blockchain technology and QR codes to protection in the digital document verification process.
- 2) Ensuring the authenticity of document information by securely storing its complete source chain and ownership histories within the blockchain system.
- 3) Preventing unauthorized alterations to document data through robust blockchain encryption methods.
- 4) Development of a user-friendly application to facilitate easy access to the blockchain record of each document, streamlining the verification process for users.

1.6 ORGANIZATION OF PROJECT

Chapter 1: It gives an Introduction of the project. A blockchain-based digital document verification system leverages the immutable nature of blockchain technology to securely authenticate and validate the integrity of digital documents. By anchoring document hashes onto a distributed ledger, it ensures tamper-proof records, enhancing trust and reliability in document management processes.

Chapter 2: A literature survey involves conducting a comprehensive review of existing research papers relevant to a specific project to gain insights into the previous work done in that field. In the context of a blockchain-based digital document verification system, this survey would delve into academic papers, journal articles, conference proceedings, and other scholarly sources that explore topics such as blockchain technology, digital document authentication, cryptography, and related fields.

Chapter 3: the methodology for executing the project involves several key steps. Firstly, defining clear objectives and research questions based on insights gained from the literature review. Next, designing and implementing the technical architecture of the blockchain-based digital document verification system, including selecting the appropriate blockchain platform, developing smart contracts for document verification, and integrating necessary cryptographic techniques for data security.

Chapter 4: we delve into the intricate implementation details crucial to the successful completion of our project. This section elucidates the methodologies, algorithms, and technical frameworks employed, offering readers a comprehensive understanding of the development process. First and foremost, we outline the methodologies adopted during the development lifecycle, shedding light on our strategic approach to project management, collaboration, and iteration. This includes insights into agile methodologies such as Scrum or Kanban, as well as any custom methodologies tailored to the specific needs of our project.

Next, we elucidate the algorithms utilized to address various computational tasks and challenges encountered throughout the development process. Whether it be data processing, optimization problems, machine learning algorithms, or cryptographic protocols, we provide detailed explanations of the underlying algorithms and their implementations.

Chapter 5: In the results and discussion section of the project on organization, the culmination of meticulous planning and execution unfolds. Quantitative data, such as timelines met and budget adherence, intertwine with qualitative insights on team dynamics and stakeholder satisfaction, offering a comprehensive view of the project's performance. Through critical analysis, key successes emerge, underpinned by effective communication strategies and agile adaptation to challenges. Moreover, this section delves into the implications of the findings, highlighting areas for improvement and offering actionable recommendations to enhance future project endeavors..

Chapter 6: we draw conclusions derived from the culmination of our project. Through rigorous analysis and reflection, we explore the implications, insights, and potential future directions stemming from our work, providing valuable takeaways for both practitioners and researchers alike.

CHAPTER 2
LITERATURE
REVIEW

LITERATURE REVIEW

2.1 INTRODUCTION TO PROPOSED SYSTEM

To address issues in the current document verification process, the paper proposes a system that automatically generates and verifies certificates, leveraging decentralized document storage and record-keeping in an immutable distributed ledger such as the Ethereum blockchain given in [1]. This also enhances understanding of blockchain, transactions, and data storage in interconnected blocks. If data in any block changes, its hash is altered, indicating tampering. By harnessing blockchain's decentralized nature, every certificate issued becomes securely stored within a network of interconnected blocks, ensuring tamper-proof verification and eliminating the need for centralized authority. Furthermore, this initiative not only streamlines the verification process but also serves as a practical educational tool, enhancing understanding of blockchain principles, transactions, and data storage mechanisms among stakeholders.

2.2 STAKEHOLDERS AND ROLES

Broadly, the system involves three primary stakeholders: students, universities, and companies as found in [2]. This paper introduces a significant role, the owner, responsible for verifying and granting permissions to universities and companies to eliminate fake registrations. However, a pivotal addition introduced in this paper is the concept of an "owner" entity, tasked with a critical role in the verification process and the authorization of permissions granted to universities and companies. This owner role serves as the linchpin for ensuring the authenticity of registrations and certificates, effectively eliminating the prevalence of fraudulent activities within the system. By centralizing the responsibility for verification and permission management, the owner entity adds an extra layer of security and oversight, bolstering trust and confidence among all stakeholders involved.

2.3 ENCRYPTION AND DECENTRALISED STORAGE

The encryption algorithm used for data is AES, as proposed in [3], which also eliminates reliance on centralized systems for file storage by incorporating decentralized storage, IPFS. However, a drawback is identified: using the 'document hash' as a key, publicly available on the chain, poses challenges in future larger implementations.

2.4 LARGE DATA HANDLING

The platform SkillCheck, outlined in [4], awards crypto tokens to evaluators, relying entirely on blockchain and employing technologies like Ganache, Truffle, and the Metamask wallet for transactions, simplifying testing. The system efficiently manages a large number of students with minimal teaching staff. This innovative system relies entirely on blockchain infrastructure, utilizing specialized technologies such as Ganache, Truffle, and the Metamask wallet for seamless and secure transactions. By harnessing the decentralized nature of blockchain, SkillCheck simplifies the testing process while ensuring transparency and reliability in evaluating student performance. Moreover, the platform's architecture enables the efficient management of a large volume of students with minimal reliance on teaching staff, thereby optimizing resource allocation and scalability.

2.5 COST CONCERNS AND ALTERNATIVE SOLUTIONS

. A potential cost concern arises if documents are converted into binary and stored on the blockchain compared to the current centralized system. Paper [5] proposes an alternative, suggesting storing documents in a decentralized manner using IPFS, enhancing data resilience and accessibility by breaking files into smaller chunks distributed across a node network. Each file is referenced using content-based addressing, reducing dependence on servers compared to traditional storage systems. Paper addresses potential cost concerns by proposing an alternative to storing documents on the blockchain. It suggests using IPFS to decentralize document storage, breaking files into smaller, distributed chunks, thus enhancing resilience and accessibility while reducing reliance on centralized servers.

2.6 INTEGRATION OF INSIGHTS

By combining the insights from all these references, a system can be built that utilizes decentralized storage (IPFS) and the Ethereum blockchain for the verification of document identity, as detailed in [6]. This paper addresses the problems and drawbacks identified in the previously proposed methodologies

CHAPTER 3
METHODOLOGY

METHODOLOGY

3.1 BLOCKCHAIN

It is the bedrock of numerous innovative projects, serving as a steadfast digital ledger that underpins their functionality. At its core, it functions as an immutable record-keeping system, meticulously documenting every transaction and event within its network. Unlike traditional ledgers that are prone to manipulation or tampering, blockchain operates on a decentralized architecture, distributing copies of the ledger across a network of nodes. This decentralization ensures that no single entity has control over the entirety of the ledger, enhancing its security and reliability.

Every action recorded on the blockchain is transparent and verifiable by all participants, fostering a level of trust and accountability unparalleled in traditional systems. Through cryptographic techniques such as hashing and consensus algorithms like Proof of Work or Proof of Stake, blockchain ensures the integrity and immutability of its data. Once a transaction is added to the blockchain, it becomes virtually impossible to alter or erase, providing a permanent and auditable record of all activities.

Beyond its role as a ledger, blockchain has the potential to revolutionize various industries by enabling new forms of peer-to-peer transactions, smart contracts, and decentralized applications. Its transparent and tamper-proof nature opens doors to applications in finance, supply chain management, healthcare, and beyond, promising greater efficiency, transparency, and trust in an increasingly digital world. As the foundation of countless projects and initiatives, blockchain continues to evolve, reshaping the way we conceptualize and interact with data and transactions in the digital age.

3.2 PROPOSED SYSTEM

To address existing flaws in current verification methods, this system introduces an automatic certificate verification System Design process, complemented by QR codes for seamless sharing and validation. This ensures authenticated, reliable, and unalterable data. The following sections provide an in-depth explanation of the system design and functionality

3.3 SYSTEM MODEL

The proposed application system aims to combat the increasing Tampering of documents by utilizing blockchain and QR codes. The system will store the documents source chain and maintain histories, allowing students to access comprehensive documents details. QR codes will be used to validate documents and add information, while blockchain technology ensures the integrity of the stored data, preventing unauthorized alterations. By leveraging these technologies, the system will effectively identify invalid documents, enhancing trust and transparency in the educational sector.

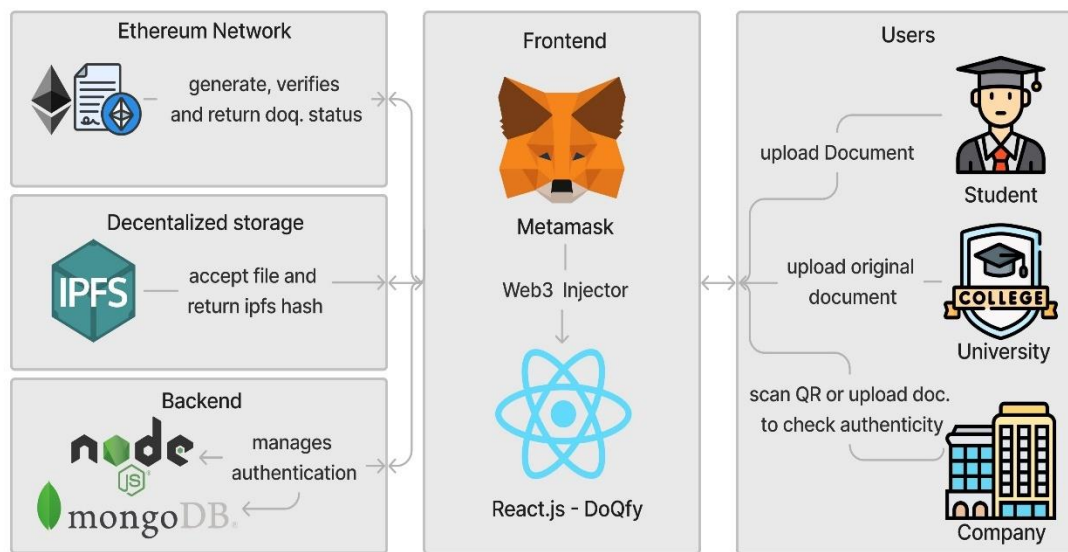


Figure 3.1 Proposed System Model

3.4 MODULES

1 The Ethereum network

stands as a pioneering force in the realm of blockchain technology, renowned for its versatility and expansive capabilities beyond simple value transfer. Serving as a decentralized platform for building and deploying smart contracts and decentralized applications (DApps), Ethereum has transformed the landscape of digital innovation. Launched in 2015 by Vitalik Buterin, Ethereum introduced the concept of programmable blockchain, enabling developers to create complex, self-executing contracts and applications that run exactly as programmed without the need for intermediaries. Its native cryptocurrency, Ether (ETH)

2 Ganache:

Ganache is a personal blockchain software that allows users to create their own Ethereum blockchain network for development and testing purposes. It provides a local blockchain environment that runs on the user's machine, allowing for faster and more efficient development without the need for interaction with the public Ethereum network.

Ganache serves as a valuable tool for blockchain developers, providing a personal blockchain environment tailored specifically for Ethereum development and testing. With Ganache, users can effortlessly create their own private Ethereum blockchain networks directly on their local machine. This localized environment offers a range of benefits, notably speed and efficiency, as developers can iterate and test their smart contracts and decentralized applications (DApps) without the delays and costs associated with interacting with the public Ethereum network.

One of Ganache's key features is its user-friendly interface, which simplifies the process of setting up and configuring a local blockchain network. Developers can customize various parameters, such as the number of simulated accounts, gas limits, and block times, to closely mimic real-world conditions or specific testing scenarios.

Ganache also provides a suite of powerful development tools and features to aid developers in their workflow. For example, it offers built-in blockchain explorer functionality, allowing users to inspect transactions, account balances, and contract state changes in real-time. Additionally, Ganache seamlessly integrates with popular development frameworks like Truffle, enabling smooth integration into existing development workflows.

3 Truffle Suite

Truffle Suite is a development framework for building decentralized applications (DApp) and smart contracts on various blockchain platforms, including Ethereum. It offers a suite of tools that simplify the development, testing, deployment, and management of blockchain-based applications.

The Truffle Suite stands out as a comprehensive development framework tailored for the creation of decentralized applications (DApps) and smart contracts, particularly on blockchain platforms like Ethereum. Its multifaceted toolkit encompasses a range of

tools and functionalities aimed at streamlining every stage of the development lifecycle. Truffle's arsenal includes features for development, testing, deployment, and management of blockchain-based applications, making it a go-to solution for developers seeking efficiency and productivity.

Firstly, Truffle simplifies the development process by providing a suite of development tools and boilerplate templates that expedite project setup and coding. This includes scaffolding for smart contracts, enabling developers to focus on application logic rather than boilerplate code.

Secondly, Truffle offers robust testing capabilities, allowing developers to write and execute automated tests for smart contracts and DApps. This ensures the reliability and security of the codebase by identifying potential bugs and vulnerabilities early in the development process.

Furthermore, Truffle facilitates the deployment of smart contracts and DApps to blockchain networks, offering seamless integration with popular platforms like Ethereum. Its deployment tools automate many of the manual tasks involved in deploying contracts, reducing the risk of errors and streamlining the deployment process.

Lastly, Truffle provides management tools that simplify the maintenance and upgrade of deployed contracts and applications. This includes features for contract migration, versioning, and interaction with deployed contracts, enabling developers to manage their applications with ease.

4 Metamask

Metamask is a web browser extension that serves as a bridge between the browser and the Ethereum blockchain. It provides a user-friendly interface for interacting with blockchain networks and managing Ethereum accounts.

MetaMask is a versatile web browser extension designed to bridge the gap between traditional web browsers and the Ethereum blockchain. By integrating seamlessly into popular browsers like Chrome, Firefox, and Brave, MetaMask empowers users to access and interact with decentralized applications (DApps) directly from their web browser. One of MetaMask's primary functions is to serve as a user-friendly interface for managing Ethereum accounts and interacting with blockchain networks. Users can

effortlessly create, import, and manage their Ethereum wallets through MetaMask, allowing them to securely store and transact with Ether (ETH) and other Ethereum-based tokens. Moreover, MetaMask facilitates the seamless execution of blockchain transactions, providing users with intuitive prompts and notifications to confirm and approve transactions directly from their browser window. Additionally, MetaMask enhances privacy and security by safeguarding users' private keys and sensitive information within the extension's encrypted storage, ensuring a secure browsing experience. Overall, MetaMask plays a pivotal role in democratizing access to the Ethereum ecosystem by providing a user-friendly gateway for individuals to explore and engage with decentralized applications and blockchain technology.

5 IPFS

InterPlanetary File System (IPFS) is a decentralized protocol designed to create a peer-to-peer network for storing and sharing hypermedia content across a distributed system of nodes. Unlike traditional web servers that rely on centralized infrastructure, IPFS leverages a distributed network of nodes to store and retrieve content, making it resistant to censorship and single points of failure.

6 MongoDB

MongoDB is a popular NoSQL database that excels in handling unstructured data and offers robust scalability and flexibility. Its distinguishing feature is its document-oriented model, storing data in flexible JSON-like documents. MongoDB's text search capabilities enable efficient querying and indexing of textual data, empowering users to perform complex searches across large datasets. With support for full-text search, MongoDB facilitates the retrieval of relevant information by analysing text fields within documents.

7 Decentralised Storage

Decentralized storage refers to a method of storing data across a network of nodes, rather than relying on a central server. In this approach, files are broken down into smaller chunks and distributed across multiple nodes, enhancing data resilience and accessibility. Each file is referenced using content-based addressing, reducing dependence on specific servers. One prominent example of decentralized storage is the InterPlanetary File System (IPFS), which allows users to store and retrieve files in a

peer-to-peer manner. Decentralized storage systems offer several advantages, including increased security, reduced risk of data loss due to single points of failure, and improved scalability. Additionally, they can contribute to the decentralization of the internet by providing alternatives to traditional, centralized storage solutions.

8 Ethers.js:

It is a JavaScript library for Ethereum development, facilitating smart contract interactions and wallet management. It simplifies blockchain transactions, making it popular among developers for building decentralized applications (DApps) with ease and efficiency. Ethers.js is a powerful JavaScript library tailored for Ethereum development, specifically designed to streamline interactions with smart contracts and facilitate wallet management. Its primary aim is to simplify the complexities of blockchain transactions, making it an invaluable tool for developers seeking to build decentralized applications (DApps) efficiently. By abstracting away many of the intricacies associated with Ethereum's protocol, Ethers.js empowers developers to focus more on application logic and user experience rather than grappling with low-level blockchain operations. Its popularity stems from its intuitive interface and comprehensive functionality, enabling seamless integration of Ethereum-based features into web and mobile applications. With Ethers.js, developers can harness the potential of Ethereum's decentralized network without the steep learning curve traditionally associated with blockchain development, thereby accelerating the adoption of DApps across various industries

9 React

React is employed for building the frontend, offering users a seamless experience with features like smooth page switches, fast loading and added features for extra security, compiling and storing HTML pages in the backend without revealing details to users.

React is a widely-used JavaScript library employed for frontend development, particularly favored for its ability to create dynamic and interactive user interfaces. It enhances user experience by providing features such as smooth page transitions, fast loading times, and additional security measures. One of React's key advantages lies in its virtual DOM (Document Object Model), which enables efficient rendering of UI components and ensures rapid updates without requiring a full page reload. This contributes to the seamless user experience mentioned, as React optimizes the rendering

process for improved performance. Moreover, React allows for the creation of reusable UI components, promoting code reusability and maintainability. Additionally, React can be integrated with backend systems to compile and store HTML pages without exposing sensitive details to end-users, thus enhancing security. This combination of features makes React a popular choice for frontend development, empowering developers to craft engaging and secure user interfaces for web applications.

10 Node.js

Node.js is a server-side JavaScript runtime environment that facilitates the execution of JavaScript code outside the browser, enabling efficient and scalable web application development. It is recognized for its non-blocking, event-driven architecture, enhancing the responsiveness of applications.

Node.js is a server-side JavaScript runtime environment renowned for its ability to execute JavaScript code outside of the browser, thus enabling the development of efficient and scalable web applications. One of Node.js's standout features is its non-blocking, event-driven architecture, which significantly enhances application responsiveness. Unlike traditional server-side technologies that utilize a synchronous, blocking approach, Node.js employs an asynchronous model, allowing multiple operations to be executed concurrently without waiting for each one to complete. This non-blocking nature ensures that Node.js applications can handle large numbers of simultaneous connections without becoming sluggish or unresponsive. Additionally, Node.js boasts a rich ecosystem of libraries and frameworks, further simplifying the development process and empowering developers to build robust, high-performance web applications. Overall, Node.js has revolutionized server-side development by offering a lightweight, scalable solution that leverages JavaScript's versatility and popularity.

3.5 ENTITIES IN THE SYSTEM

This approach streamlines the verification of document authenticity, guaranteeing both integrity and originality through the utilization of technologies like blockchain and IPFS. The Fig illustrates how users engage with smart contracts, involving the following participants:

a) *Student*: The student initiates the process by selecting their university from a list and uploading the document they wish to verify. Upon completion, the student receives a documentId for reference.

b) *University*: The university acts as a Certificate Verifying Authority

- For former students who are not part of the new system: University officials handle the verification process by selecting the document submitted by the student and uploading the original digital copy they possess. The system verifies the data by matching both documents, ensuring authenticity, and updates the status to verified if data matches.
- For new students: the university simplifies the process by directly generating verified documents before handing them to students. This eliminates the need for students to undergo additional verification steps. After verification, an email is sent to the student, including the documentId, hash, and a QR code embedded in the document for easy reference and validation.

c) *Company*: Companies, as end-users, play a crucial role in the system. They can access only those documents for which students or universities have granted permission for viewing.

- They can scan the QR code of the document to obtain details about the document's originality, integrity, and authenticity.
- During the hiring process, companies can also upload documents provided by the student to verify their authenticity and check the verification status

d) *Owner*: The owner manages the registration of universities and companies to prevent the inclusion of fake entities by verifying their legal government documents

Process: Users start by signing up and logging into the website “Doqfy”. Ethers.js seamlessly connects the site with Metamask and the smart contract, ensuring a smooth integration between the user's account, their Metamask wallet, and the underlying blockchain-based smart contract functionality.

- First student selects the university and upload the document that document is send to ipfs through node.js and ipfs return the ipfs hash or cid which is unique for each document then this hash, student address, selected university address and

documentId generated by system is send to Ethereum smart contract function upload Document which creates a mapping of document with documentId and stores this information in blockchain.

- Second university get request for verification of document then they select the document which they want to verify then upload the original copy of document that they have and click on verify, then again document is send to ipfs, it returns the ipfs hash, then this hash and documentId is send to smart contract function verify document which checks the hash of student uploaded document and original university document hash if they both match then verification status is updated to true.
- Third Company can upload the document uploaded by student and check its authenticity by using the same above process or give unique documentId to check verification status of document, then this id is sent to smart contract function check status which returns the document verification status true or false depending upon verified or not.

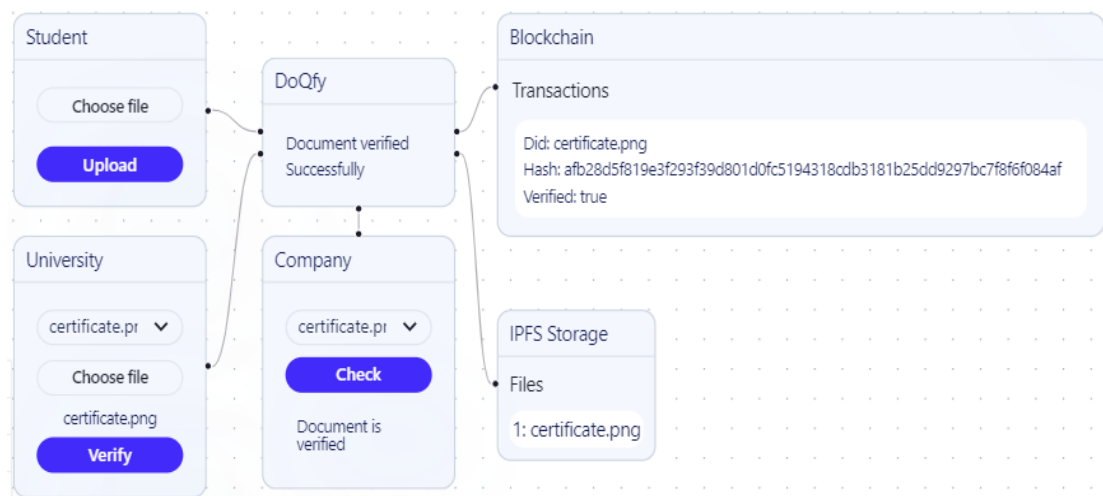


Figure 3.2 System Work Flow

CHAPTER 4

IMPLEMENTATION

IMPLEMENTATION

The Implementation involves key components such as the Ethereum blockchain, IPFS for document storage, smart contract development using Solidity, and interaction with the Ethereum network using tools like Truffle and ethers.js.

4.1 SMART CONTRACT: A smart contract named DoQfy is deployed on the Ethereum blockchain. The contract contains a struct named Document to represent document details, including owner address, university address, IPFS hash, and verification status. Documents are stored in a mapping named documents By Id with

```
//SPDX-License-Identifier: MIT
pragma solidity ^0.8.1;
contract DoQfy {
    struct Document {
        address owner;
        address universityAddress;
        string ipfsHash;
        bool verified;
    }
    mapping(string => Document) private
    documentsById;
    event LogPrint(string message);

    function uploadDocument(string memory
    uniqueId, string memory ipfsHash,
    address universityAddress) public {
        Document memory document =
        Document({
            owner: msg.sender,
            universityAddress:
            universityAddress,
            ipfsHash: ipfsHash,
            verified: false
        });
        documentsById[uniqueId]=document;
        emit LogPrint("Document uploaded
        successfully");
    }

    function verifyDocument(string memory
    uniqueId, string memory ipfsHash)
    public{
        Document storage document =
        documentsById[uniqueId];
        require(keccak256(abi.encodePacked
        (document.ipfsHash)) == keccak256
        (abi.encodePacked(ipfsHash)),
        "Fake document");
        document.verified = true;
        emit LogPrint("Document verified
        successfully");
    }
}
```

unique documentId. Events, such as Log Print, are emitted to signify successful transactions.

4.2 IPFS INTEGRATION: The IPFS client is utilized to pin documents on the IPFS network. Files are added to IPFS, and the resulting CID (Content Identifier) or hash is returned.

```
const ipfs = create({
  host: "localhost",
  protocol: "http",
  port: 5001,
});

const result = await ipfs.add(file, {
  pin: true,
});
return result.cid.toString();
```

4.3 ETHERS.JS AND CONTRACT INTERACTION: Leveraging the Ethers.js library enables communication with the Ethereum blockchain. A signer is acquired through MetaMask or equivalent providers. The instantiation of the DoQfy smart contract involves supplying the contract address and Application Binary Interface (ABI).

```
const userSigner = new ethers.providers.Web3Provider(window.ethereum).
  getSigner();
const smartContract = new ethers.Contract(contractAddress, contractAbi,
  userSigner);
const userAccounts = await window.ethereum.request({ method: '
  eth_requestAccounts' });
const transaction1 = await contract.uploadDocument(uniqueId, ipfsHash,
  universityAddress, { from: userAccounts[0] }); await transaction.wait
  ();
const transaction2 = await contract.verifyDocument(uniqueId, ipfsHash, {
  from: userAccounts[0] }); await transaction.wait();
const transaction3 = await contract.checkStatus(uniqueId, { from:
  userAccounts[0] }); return transaction3;
```

4.4 USER AUTHENTICATION: User registration and login are securely managed using MongoDB and Node.js, providing a robust backend for the DoQfy platform. This implementation guarantees a secure and scalable document verification system by integrating blockchain and IPFS technologies effectively.

CHAPTER 5
RESULT
AND
DISCUSSION

RESULT AND DISCUSSION

5.1 AUTHENTICATION: Users begin by selecting their role and registering using their email and password. Additionally, the Metamask account address is automatically fetched and set during registration

Pages / Authentication

Login

2

Email

yash@gmail.com

Password

...

Wallet Address

0x3992d518a61c16f37765a8aae1f96f1e3700a567

Otp

Otp

Send OTP Login

Screenshot 5.1 Authentication page

5.2 OWNER: The owner is responsible for verifying university and company registrations. After successful verification, universities or companies can commence their respective operations.

Pages / Owner

Owner

0xccbfcc2ea11f018328072a447bd9e66711283b73

26.78 ETH

Verify or Un-Verify University

0x3992d518A61c16F37765A8aaE1f96f1E3700A567

Verify Un-Verify

Universities

Search university

S.N	Universities	Verified
1	0x3992d518A61c16F37765...	✓

Google Chrome

Confirmed transaction
Transaction 59 confirmed!

Screenshot 5.2 Owner Page

5.3 STUDENT: Students choose their university, upload the document, and confirm the Meta mask transaction from their account. The document is then sent to the university for verification.

The screenshot shows the 'Student' page. At the top, there's a header with 'Pages / Student' and a balance of '19.76 ETH'. Below the header, the 'Student' title is prominent. The main content area is divided into two columns. The left column contains an 'Account' section with the address '0x4c351602b9a2d34122b3cfb09fe3e62c7e74f26c' and an 'Upload Document' section. The 'Upload Document' section has a dropdown menu showing '0x3992d518A61c16F37765A8aaE1f96f1E3700A567', a large blue arrow icon with the text 'Upload Files', and a note 'Only PDF file is allowed. Selected file: file.pdf'. Below this is a blue 'Upload' button. The right column contains a 'Total Documents' section showing '1' and a 'Transaction Details' section. The 'Transaction Details' section lists the following information: DOCUMENT: ee6da520-517a-4964-b821-1eebc9b95f79, TX: 0x4d12f700d080448d769e9a32835a29630bd215033913b4c170f57c99d3b1e4fd, FROM: 0x4C351602B9a2d34122b3CFb09Fe3e62C7E74f26C, TO: 0x5534FC747a528B4b136234B2733823629171D471, NONCE: 68, IPFS CID: QmRwDEkWaQINqN9nftk99jwXHugNXLchCoouomFi1pAHh4, and IPFS LINK: http://localhost:8080/ipfs/ipfs_cid.

Screenshot 5.3 Student Page

5.4 UNIVERSITY: Universities select the document for verification, upload the original copy, and click "verify." If both documents match, the verification status is set to true.

The screenshot shows the 'University' page. At the top, there's a header with 'Pages / University' and a balance of '19.79 ETH'. Below the header, the 'University' title is prominent. The main content area is divided into two columns. The left column contains an 'Account' section with the address '0x3992d518a61c16f37765a8aaE1f96f1E3700a567' and a 'Verify Document' section. The 'Verify Document' section has a dropdown menu showing 'ee6da520-517a-4964-b821-1eebc9b95f79', a large blue arrow icon with the text 'Upload Files', and a note 'Only PDF file is allowed. Selected file: file.pdf'. Below this are two buttons: 'Verify' and 'Un-Verify'. The right column contains a 'University Status' section. A MetaMask transaction confirmation overlay is visible in the foreground. The overlay shows the 'Estimated gas fee' as '\$3.16 0.001402 ETH' (Site suggested) and 'Max fee: 0.00140164 ETH'. The 'Total' is '\$3.16 0.00140164 ETH' (Amount + gas fee) and 'Max amount: 0.00140164 ETH'. The 'CUSTOM NONCE' is '79'. At the bottom of the overlay are 'Reject' and 'Confirm' buttons.

Screenshot 5.4 University Page

5.5 COMPANY: Companies have two options: they can either scan the QR code or upload the document submitted by the student to check the authenticity and verification status of the document.

Pages / Company

Company

Account: 0xea5ae9e788c8a0101af469841d387c54b512768b

Company Status

19.92 ETH

Check & Verify Document

ee6da520-517a-4964-b821-1eebc9b95f79

Upload Files

Only PDF file is allowed
Selected file: download (1).pdf

Check & Verify **checkStatus**

Document Status

Document is Valid & Verified

DOCUMENT: ee6da520-517a-4964-b821-1eebc9b95f79

STUDENT: 0x4C351602B9a2d34122b3CFb09Fe3e62C7E74f26C

UNIVERSITY: 0x3992d518A61c16F37765A8aaE1f96f1E3700A567

IPFS CID: QmfDYdieuQGKKCDY4DiHadjDTTf92e1ogoRTHY7DH4GF

IPFS LINK: <http://localhost:8080/ipfs/QmfDYdieuQGKKCDY4DiHadjDTTf92e1ogoRTHY7DH4GF>

VERIFIED:

Screenshot 5.5 Company Page

5.6 RESULT: The result is a verified document with a QR code embedded on it.

Results - Winter 2020
FOUR YEAR B.E SEMESTER : FIRST(CGS)

Name : YASH KUMAR SUGANDHI

College & Code : [0]312-Shri Sant Gajanan Maharaj Engineering College,SHEGAON

Subject	Paper	Max Marks	Marks Scored	Grade Point	Grade	Remarks
ENGINEERING MATHEMATICS-I	THEORY	80	80	10	AA	
	I.A.	20	19			
ENGINEERING PHYSICS	THEORY	80	80	10	AA	
	I.A.	20	20			
ENGINEERING MECHANICS	THEORY	80	53	9	AB	
	I.A.	20	20			
COMPUTER PROGRAMMING	THEORY	80	80	10	AA	
	I.A.	20	20			
WORKSHOP PRACTICE	PRACTICAL	25	20	9	AB	
	I.A.(PRAC)	25	21			
ENGINEERING PHYSICS-Lab	PRACTICAL	25	23	10	AA	
	I.A.(PRAC)	25	23			
ENGINEERING MECHANICS-Lab	PRACTICAL	25	22	9	AB	
	I.A.(PRAC)	25	20			
COMPUTER PROGRAMMING-LABORATORY	PRACTICAL	25	23	10	AA	
	I.A.(PRAC)	25	22			

Max Marks : 600 Result : PASS SGPA : 9.69

Abbreviation: 11945- ENGINEERING MATHEMATICS-I, 11946- ENGINEERING PHYSICS, 11947- ENGINEERING MECHANICS, 11948- COMPUTER PROGRAMMING, 11953- WORKSHOP PRACTICE, 11954- ENGINEERING PHYSICS- Lab, 11955- ENGINEERING MECHANICS- Lab, 11956- COMPUTER PROGRAMMING-LABORATORY

Date of declaration: 16-07-2021

@= Passes by incentive marks vide ordinance no. 1 of 1985
 *a Passes by Grace Marks vide Ordinance no. 18 of 2001
 **a Passes by condonation marks vide ordinance no. 18 of 2001
 *Sant Gadge Baba Amravati University, Amravati is not responsible for any inadvertent error that may have incept due to internet error and bugs in the result being published on net.
 The Result/Marks statement published on net are for immediate information to the Student. Original mark sheets have been issued by the University via respective colleges and only these Marks statement is considered as Authentic for any purpose.

ee6da520-517a-4964-b821-1eebc9b95f79

Screenshot 5.6 Verified Document

5.7 GAS USAGE METRICS: In the Ethereum ecosystem, gas fees are a critical aspect of executing transactions and interacting with smart contracts. Computational effort on the Ethereum network is measured in units referred to as Gas.

In the Ethereum smart contracts context, gas functions as a unit representing the computational resources essential for executing operations. For the 'upload Document' function, the gas used is 270,035 units, reflecting the computational effort involved in executing this particular smart contract function. The gas price, set at 20 Gwei (20,000,000,000 Wei, a smaller denomination of Ether), determines the cost per unit of gas. The gas limit, also set at 270,035 units, represents the Doqfy: Digital Document Verification using Blockchain and IPFS.

Table I: Upload Document Gas Cost

Gas Used	Gas Cost	Gas Fee
270035	20Gwei	0.005401 Eth

maximum amount of gas allowed for the function. In this case, the gas fee for executing 'upload Document' is calculated by multiplying the gas used (270,035) by the gas price (20 Gwei), resulting in a fee of 0.005401 ETH.

Table II: Verify Document Gas Cost

Gas Used	Gas Cost	Gas Fee
70082	20Gwei	0.00 Eth

Similarly, for the 'verify Document' function, the gas used is 70,082 units, reflecting the computational resources expended during execution. The gas price remains at 20 Gwei, and the gas limit is 70,082 units. Consequently, the gas fee for 'verify Document' is calculated as the multiplication of the gas (70,082) and the price of gas (20 Gwei), resulting in a fee of 0.001402 ETH. These gas parameters, including gas used, gas price, and gas limit, collectively determine the cost and resource allocation associated with executing specific functions on the Ethereum blockchain.

CHAPTER 6
CONCLUSION

CONCLUSION

6.1 CONCLUSION

The primary advantage of Blockchain lies in its capability to generate immutable records. This feature ensures a transparent and secure system. The system automates certificate generation, reducing manual work for verification. This not only minimizes the risk of students losing certificates but also enhances data security. Hash values of certificates find their storage in the blockchain, while the primary documents are maintained within the InterPlanetary File System (IPFS), ensuring data preservation and transparency. Traditional document verification for employment is both costly and time consuming, often relying on third parties. The paper illustrates how blockchain technology eliminates these challenges. Implementing such a system can significantly reduce fraud related to work history, offering a more reliable solution for companies.

6.2 FUTURE SCOPE

In the future, blockchain-based document verification is poised to revolutionize various industries with advancements in interoperability, privacy, and AI integration. Expect streamlined exchange of verified documents across platforms, bolstered by zero-knowledge proofs and advanced encryption for heightened security. AI algorithms will enhance fraud detection, while decentralized identity management systems will empower individuals to control their digital identities securely. This technology will expand beyond education and employment verification, reaching into healthcare, supply chain management, and legal documentation. Governments will increasingly adopt blockchain for public services, supported by regulatory frameworks ensuring compliance and consumer protection. User-centric design will prioritize intuitive interfaces, making document verification processes accessible and efficient. With sustainability initiatives and ongoing innovation, blockchain-based document verification will continue to shape a trusted and transparent digital future.

REFERENCES

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), Honolulu, HI, USA, 2017, pp. 557-564, doi: 10.1109/BigData Congress.2017.85.
- [2] 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), Chiba, Japan, 2018, pp. 1046-1051, doi: 10.1109/ICASI.2018.8394455.
- [3] A. Singh, S. Chauhan and A. K. Goel, "Blockchain Based Verification of Educational and Professional Certificates," 2023 2nd International Conference on Computational Systems and Communication (ICCSC), Thiruvananthapuram, India, 2023, pp. 1-7, doi: 10.1109/ICCSC56913.2023.10143008.
- [4] J. Gupta and S. Nath, "SkillCheck: An Incentive-based Certification System using Blockchains," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2020, pp. 1-3, doi: 10.1109/ICBC48266.2020.9169457.
- [5] E. Nyaletyey, R. M. Parizi, Q. Zhang and K.-K. R. Choo, "Block IPFS- Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 18-25, doi: 10.1109/Blockchain.2019.00012.
- [6] G. Malik, K. Parasrampur, S. P. Reddy and S. Shah, "Blockchain Based Identity Verification Model," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, 2019, pp. 1-6, doi: 10.1109/ViTE CoN.2019.8899569.
- [7]. Hunhevicz, Jens J., and Daniel M. Hall. "Do you need a blockchain in construction? Use case categories and decision framework for DLT design options." *Advanced Engineering Informatics* 45 (2020): 101094.
- [8]. Ali, Omar, et al. "A comparative study: Blockchain technology utilization benefits, challenges, and functionalities." *IEEE Access* 9 (2021): 12730-12749.

- [9]. Bhutta, Muhammad Nasir Mumtaz, et al. "A survey on blockchain technology: evolution, architecture, and security." *IEEE Access* 9 (2021): 61048-61073.
- [10]. Jambhulkar, Swaroop, et al. "Blockchain-based fake product identification system." *International Research Journal of Modernization in Engineering Technology and Science*(2021): 2582-5208.
- [11]. Dursun, Taner, et al. "Blockchain Technology for Supply Chain Management." *Global Joint Conference on Industrial Engineering and Its Application Areas*. Springer, Cham, 2020.
- [12]. Al-Farsi, Sana, Muhammad Mazhar Rathore, and Spiros Bakiras. "Security of blockchain-based supply chain management systems: challenges and opportunities." *Applied Sciences* 11.12 (2021): 5585.
- [13]. Aini, Qurotul, et al. "Embedding a blockchain technology pattern into the QR code for an authentication certificate." *Journal Online Informatika* 5.2 (2020): 239-244.
- [14]. Xie, Shundao, et al. "Two-stage textured-patterns embedded QR codes for printed matter authentication.", *Research Square* (2021).
- [15]. Turjo, Manoshi Das, et al. "Smart supply chain management using the blockchain and smart contract." *Scientific programming* 2021.
- [16]. Shreekumar, T., et al. "Fake Product Detection Using Blockchain Technology." *JOURNAL OF ALGEBRAIC STATISTICS* 13.3 (2022): 2815-2821
- [17]. Muhammad Nasir Mumtaz Bhutta, Amir A. Khwaja, Adnan Nadeem, Hafiz Farooq Ahmad , Muhammad Khurram Khan, Moataz A. Hanif, Houbing Song, Majed Alshamari , and Yue Cao , "A Survey on Blockchain Technology: Evolution, Architecture and Security", *IEEE special section on intelligent big data analytics for internet of things, services and people*, 2021, pp. 61048 – 61073.
- [18]. Rishabh Sushil Bhatnagar, Sneha Manoj Jha , Shrey Surendra Singh, Rajkumar Shende "Product Traceability using Blockchain", 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN).
- [19]. Si Chen , Rui Shi , Zhuangyu Ren , Jiaqi Yan , Yani shi , Jinyu Zhang, "A Blockchain-based Supply Chain Quality Management Framework", 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)

DISSEMINATION OF WORK

SN Computer Science

Doqfy: Digital Document Verification using Blockchain and IPFS

--Manuscript Draft--

Manuscript Number:	SNCS-D-24-00512
Full Title:	Doqfy: Digital Document Verification using Blockchain and IPFS
Article Type:	Original Research
Section/Category:	Innovation in Block chain and Distributed Ledgers
Funding Information:	
Abstract:	<p>Every year, millions of students enroll in Indian higher education institutions, generating numerous certificates such as marksheets, certificates, appreciation cards, and diplomas throughout their academic journey. For admissions or job applications, students are required to submit these documents to institutes or companies. However, manually tracking and validating the authenticity of these certificates becomes a tedious task. In the era of AI tools and smart editing technologies, the risk of modifying scores on scorecards or forging someone else's documents has increased. Manual document verification is not only time-consuming but also incurs paper costs and poses challenges to managing old records. There is a pressing need to address this issue and streamline the document verification process, ensuring confidentiality, reliability, and data availability. This paper suggests creating a verification system based on blockchain and Ipfs technology aimed at preserving data integrity. The system involves three key entities: the student, the university, and the company. The student initiates the verification process by uploading the document, and the university validates it by uploading the original document they possess. If the hash values match, the document is considered verified, and a QR code is embedded for easy sharing and verification status checks by companies. The advantages of such a system include reduced risk for students of losing or damaging certificates and simplified certificate validation procedures. This blockchain-based approach enhances the security, efficiency, and integrity of the document verification process.</p>
Corresponding Author:	Yash Kumar Sugandhi Shri Sant Gajanan Maharaj College of Engineering INDIA
Corresponding Author Secondary Information:	
Corresponding Author's Institution:	Shri Sant Gajanan Maharaj College of Engineering
Corresponding Author's Secondary Institution:	
First Author:	Yash Kumar Sugandhi
First Author Secondary Information:	
Order of Authors:	Yash Kumar Sugandhi Pratik Ganesh Ekhande Jaikumar M Patil Smita Bansod
Order of Authors Secondary Information:	
Author Comments:	
Suggested Reviewers:	

Doqfy: Digital Document Verification using Blockchain and IPFS

Yash Kumar Sugandhi

*Computer Science and Engineering Department
Shri Sant Gajanan Maharaj College of Engineering
Shegaon, India
yashsugandhi96442@gmail.com*

Dr. Jaikumar M. Patil

*Computer Science and Engineering Department
Shri Sant Gajanan Maharaj College of Engineering
Shegaon, India
jmpatil@sngmce.ac.in*

Pratik Ganesh Ekhande

*Computer Science and Engineering Department
Shri Sant Gajanan Maharaj College of Engineering
Shegaon, India
ekhandepratik123@gmail.com*

Smita Bansod

*Information Technology Department
Shah And Anchor Kutchhi Engineering College
Mumbai, India
smita.bansod@sakec.ac.in*

Abstract—Every year, millions of students enroll in Indian higher education institutions, generating numerous certificates such as marksheets, certificates, appreciation cards, and diplomas throughout their academic journey. For admissions or job applications, students are required to submit these documents to institutes or companies. However, manually tracking and validating the authenticity of these certificates becomes a tedious task. In the era of AI tools and smart editing technologies, the risk of modifying scores on scorecards or forging someone else's documents has increased. Manual document verification is not only time-consuming but also incurs paper costs and poses challenges to managing old records. There is a pressing need to address this issue and streamline the document verification process, ensuring confidentiality, reliability, and data availability. This paper suggests creating a verification system based on blockchain technology aimed at preserving data integrity. The system involves three key entities: the student, the university, and the company. The student initiates the verification process by uploading the document, and the university validates it by uploading the original document they possess. If the hash values match, the document is considered verified, and a QR code is embedded for easy sharing and verification status checks by companies. The advantages of such a system include reduced risk for students of losing or damaging certificates and simplified certificate validation procedures. This blockchain-based approach enhances the security, efficiency, and integrity of the document verification process.

Index Terms—blockchain, manual verification, QR code, confidentiality, reliability, data availability

I. INTRODUCTION

In India, the basic cycle of education involves students being promoted to higher classes each year. After completing higher secondary education, students seek admission to junior college. For undergraduate education, there is yet another transition to a different college, and some may pursue postgraduate studies or opt for job placements.

However, a significant challenge arises as students need to present all their certificates at each stage for validation. This manual verification process becomes tedious for validators,

requiring them to meticulously check each document detail against the original copies they maintain. Moreover, this process involves record-keeping and incurs paper costs. Another concern is the counterfeiting of documents, which is prevalent at a mass level. In India, obtaining a white-collar job without academic credentials is nearly impossible, leading some students with lower scores to resort to illegal means. Various methods are employed, including:

- 1) Degree Mills: Where fake degrees are generated and sold to clients.
- 2) Modified Documents: Involving alterations to original documents, such as changes in name or scores.
- 3) In-House Produced: Involving the creation of fake documents with the assistance of corrupt officials within institutions.

Even if the documents are genuine, the traditional verification process demands the submission of documents to the company, leading to a waste of time for the student, the university, and the company.

To address these challenges and mitigate the issues, blockchain technology emerges as a viable solution. Blockchain ensures data integrity since the information stored in it cannot be altered. With this technology, data validation occurs only when a consensus is reached. Every transaction within the blockchain is interconnected within a chain, guaranteeing that all participants possess the most recent ledger version. The concept of a distributed ledger involves duplicating and storing transactional data across multiple nodes. Because blockchain operates as a peer-to-peer network, there's no reliance on third-party providers for transaction validation.

This approach to record-keeping ensures resistance to tampering, with each peer retaining a complete ledger copy. The incorporation of new transactions necessitates consensus from the majority of peers or compliance with predetermined rules. This transformative approach not only addresses document

verification challenges but also revolutionizes the process. By implementing blockchain in the education system, the need for physical document submission is eliminated. Instead of conventional approaches, academic certificates and accomplishments find secure storage on the blockchain, presenting a decentralized and transparent method for institutions and businesses to authenticate their validity. This not only amplifies security and operational efficiency but also mitigates the hazards associated with manual document management, ensuring a dependable and efficient verification process for all stakeholders engaged.

II. LITERATURE SURVEY

To address issues in the current document verification process, the paper proposes a system that automatically generates and verifies certificates, leveraging decentralized document storage and record-keeping in an immutable distributed ledger such as the Ethereum blockchain given in [1]. This also enhances understanding of blockchain, transactions, and data storage in interconnected blocks. If data in any block changes, its hash is altered, indicating tampering.

Broadly, the system involves three primary stakeholders: students, universities, and companies as found in [2]. This paper introduces a significant role, the owner, responsible for verifying and granting permissions to universities and companies to eliminate fake registrations.

The encryption algorithm used for data is AES, as proposed in [3], which also eliminates reliance on centralized systems for file storage by incorporating decentralized storage, IPFS. However, a drawback is identified: using the 'document hash' as a key, publicly available on the chain, poses challenges in future larger implementations.

The platform SkillCheck, outlined in [4], awards crypto tokens to evaluators, relying entirely on blockchain and employing technologies like Ganache, Truffle, and the Metamask wallet for transactions, simplifying testing. The system efficiently manages a large number of students with minimal teaching staff.

A potential cost concern arises if documents are converted into binary and stored on the blockchain compared to the current centralized system. Paper [5] proposes an alternative, suggesting storing documents in a decentralized manner using IPFS, enhancing data resilience and accessibility by breaking files into smaller chunks distributed across a node network. Each file is referenced using content-based addressing, reducing dependence on servers compared to traditional storage systems.

By combining the insights from all these references, a system can be built that utilizes decentralized storage (IPFS) and the Ethereum blockchain for the verification of document

identity, as detailed in [6].

This paper addresses the problems and drawbacks identified in the previously proposed methodologies

III. PROPOSED METHODOLOGY

A. Modules

- 1) Blockchain: is like a steady digital ledger, forming the heart of the project. It creates a reliable space where all actions are visible and impossible to change.
- 2) Ethereum: is a decentralized blockchain platform enabling smart contracts and decentralized applications (DApps). Smart contracts are self-executing contracts with encoded terms, facilitating trustless and automated transactions on the Ethereum network. Solidity is Ethereum's programming language for creating smart contracts, defining their logic and behavior.
- 3) IPFS: (InterPlanetary File System) is a peer-to-peer protocol designed for decentralized file storage and sharing. It operates on a distributed network, utilizing content-based addressing to locate files efficiently.
- 4) Ganache: is a local blockchain development environment that allows developers to test and deploy Ethereum smart contracts on a personal blockchain. It provides a user-friendly interface for simulating various blockchain scenarios and interactions.
- 5) Truffle: streamlines the compilation, linking, deployment, and binary management of Solidity smart contracts.
- 6) MetaMask: is a popular cryptocurrency wallet and browser extension that enables users to interact with decentralized applications (DApps) on the Ethereum blockchain.
- 7) Ethers.js: is a JavaScript library for Ethereum development, facilitating smart contract interactions and wallet management. It simplifies blockchain transactions, making it popular among developers for building decentralized applications (DApps) with ease and efficiency.
- 8) React: is employed for building the frontend, offering users a seamless experience with features like smooth page switches, fast loading and added features for extra security, compiling and storing HTML pages in the backend without revealing details to users.
- 9) Node.js: is a server-side JavaScript runtime environment that facilitates the execution of JavaScript code outside the browser, enabling efficient and scalable web application development. It is recognized for its non-blocking, event-driven architecture, enhancing the responsiveness of applications.
- 10) MongoDB: is a versatile NoSQL database, storing data in a flexible, document-oriented format. It is favored for its scalability and efficiency in handling diverse data types.

B. Project Description

To address existing flaws in current verification methods, this system introduces an automatic certificate verification

process, complemented by QR codes for seamless sharing and validation. This ensures authenticated, reliable, and unalterable data. The following sections provide an in-depth explanation of the system design and functionality

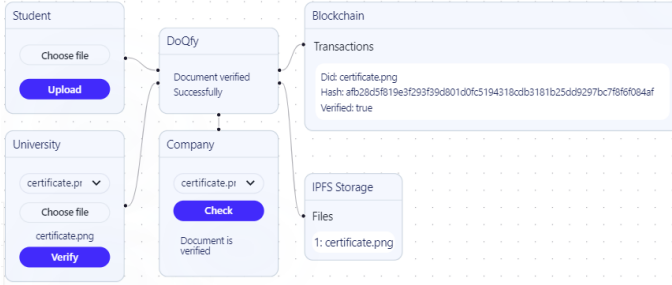


Fig. 1. User Interaction

1) *Working:* This approach streamlines the verification of document authenticity, guaranteeing both integrity and originality through the utilization of technologies like blockchain and IPFS. The Fig. 1 illustrates how users engage with smart contracts, involving the following participants:

- Student:** The student initiates the process by selecting their university from a list and uploading the document they wish to verify. Upon completion, the student receives a documentId for reference.
- University:** The university acts as a Certificate Verifying Authority
 - For former students who are not part of the new system: University officials handle the verification process by selecting the document submitted by the student and uploading the original digital copy they possess. The system verifies the data by matching both documents, ensuring authenticity, and updates the status to verified if data matches.
 - For new students: the university simplifies the process by directly generating verified documents before handing them to students. This eliminates the need for students to undergo additional verification steps.

After verification, an email is sent to the student, including the documentId, hash, and a QR code embedded in the document for easy reference and validation.

- Company:** Companies, as end-users, play a crucial role in the system. They can access only those documents for which students or universities have granted permission for viewing.
 - They can scan the QR code of the document to obtain details about the document's originality, integrity, and authenticity.
 - During the hiring process, companies can also upload documents provided by the student to verify their authenticity and check the verification status
- Owner:** The owner manages the registration of universities and companies to prevent the inclusion of fake entities by verifying their legal government documents.

C. System Design

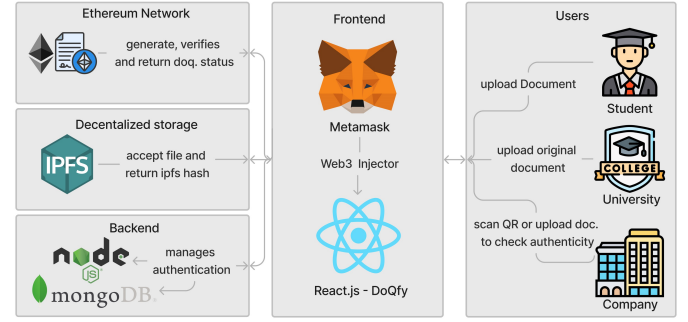


Fig. 2. System Design

Users start by signing up and logging into the website "Do-qfy.". Ethers.js seamlessly connects the site with Metamask and the smart contract, ensuring a smooth integration between the user's account, their Metamask wallet, and the underlying blockchain-based smart contract functionality.

First student select the university and upload the document that document is send to ipfs through node.js and ipfs return the ipfs hash or cid which is unique for each document then this hash ,student address ,selected university address and documentId generated by system is send to ethereum smart contract function uploadDocument which creates a mapping of document with documentId and stores this information in blockchain.

Second university get request for verification of document then they select the document which they want to verify then upload the original copy of document that they have and click on verify , then again document is send to ipfs, it return the ipfs hash , then this hash and documentId is send to smart contract function verifydocument which checks the hash of student uploaded document and original university document hash if they both match then verification status is updated to true.

Third Company can upload the document uploaded by student and check its authenticity by using the same above process or give unique documentId to check verification status of document, then this id is send to smart contract function checkstatus which returns the document verification status true or false depending upon verified or not.

IV. IMPLEMENTATION DETAILS

The implementation involves key components such as the Ethereum blockchain, IPFS for document storage, smart contract development using Solidity, and interaction with the Ethereum network using tools like Truffle and ethers.js.

A. Smart Contract

A smart contract named DoQfy is deployed on the Ethereum blockchain. The contract contains a struct named Document to represent document details, including owner address, university address, IPFS hash, and verification status. Documents are stored in a mapping named documentsById with unique

document IDs. Events, such as LogPrint, are emitted to signify successful transactions.

```
//SPDX-License-Identifier: MIT
pragma solidity ^0.8.1;
contract DoQfy {
    struct Document {
        address owner;
        address universityAddress;
        string ipfsHash;
        bool verified;
    }
    mapping(string => Document) private
    documentsById;
    event LogPrint(string message);

    function uploadDocument(string memory
    uniqueId, string memory ipfsHash,
    address universityAddress) public {
        Document memory document =
        Document({
            owner: msg.sender,
            universityAddress:
            universityAddress,
            ipfsHash: ipfsHash,
            verified: false
        });
        documentsById[uniqueId]=document;
        emit LogPrint("Document uploaded
        successfully");
    }

    function verifyDocument(string memory
    uniqueId, string memory ipfsHash)
    public{
        Document storage document =
        documentsById[uniqueId];
        require(keccak256(abi.encodePacked
        (document.ipfsHash)) == keccak256
        (abi.encodePacked(ipfsHash)),
        "Fake document");
        document.verified = true;
        emit LogPrint("Document verified
        successfully");
    }

    function checkStatus(string memory
    uniqueId)
    public view returns (bool) {
        Document storage document =
        documentsById[uniqueId];
        return document.verified;
    }
}
```

B. IPFS Integration

The IPFS client is utilized to pin documents on the IPFS network. Files are added to IPFS, and the resulting CID (Content Identifier) or hash is returned.

```
const ipfs = create({
    host: "localhost",
    protocol: "http",
    port: 5001,
});

const result = await ipfs.add(file, {
    pin: true,
});
return result.cid.toString();
```

C. Ethers.js and Contract Interaction

Leveraging the Ethers.js library enables communication with the Ethereum blockchain. A signer is acquired through MetaMask or equivalent providers. The instantiation of the DoQfy smart contract involves supplying the contract address and Application Binary Interface (ABI).

```
const userSigner = new ethers.providers.Web3Provider
(window.ethereum).getSigner();
const smartContract = new ethers.Contract(
    contractAddress, contractAbi, userSigner);
const userAccounts = await window.ethereum.request({
    method: 'eth_requestAccounts' });
const transaction1 = await contract.uploadDocument(
    uniqueId, ipfsHash, universityAddress, { from:
    userAccounts[0] }); await transaction.wait();
const transaction2 = await contract.verifyDocument(
    uniqueId, ipfsHash, { from: userAccounts[0] });
await transaction.wait();
const transaction3 = await contract.checkStatus(
    uniqueId, { from: userAccounts[0] }); return
transaction3;
```

D. User Authentication

User registration and login are securely managed using MongoDB and Node.js, providing a robust backend for the DoQfy platform.

This implementation guarantees a secure and scalable document verification system by integrating blockchain and IPFS technologies effectively.

V. RESULTS AND DISCUSSIONS

Following are some of the implementation results:

A. Registration

Users begin by selecting their role and registering using their email and password. Additionally, the Metamask account address is automatically fetched and set during registration

The registration page features a progress bar at the top with two steps. The first step is marked with a checkmark, and the second step is marked with the number '2'. Below the progress bar, there are three input fields: 'Email' with the value 'student@gmail.com', 'Password' with masked characters '.....', and 'Wallet Address' with the value '0x4c351602b9a2d34122b3cfb09fe3e62c7e74f26c'. At the bottom of the form is a blue button labeled 'Login'.

Fig. 3. Registration Page

B. Owner

The owner is responsible for verifying university and company registrations. After successful verification, universities or companies can commence their respective operations.

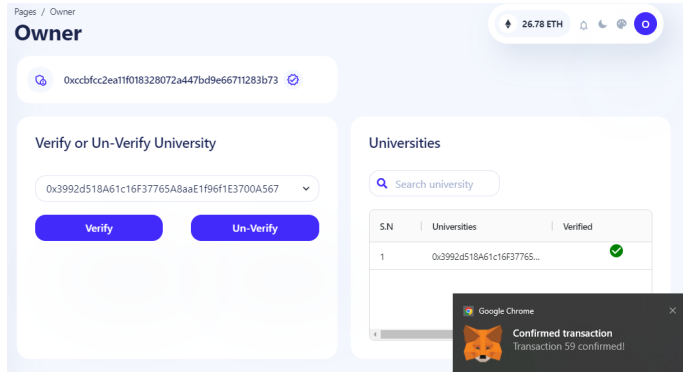


Fig. 4. Owner Page

E. Company

Companies have two options: they can either scan the QR code or upload the document submitted by the student to check the authenticity and verification status of the document.

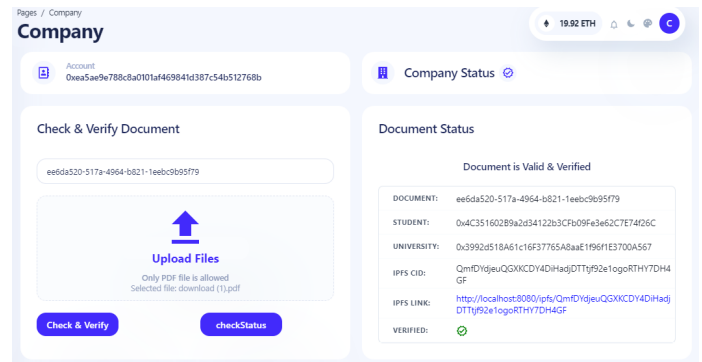


Fig. 7. Company Page

C. Student

Students choose their university, upload the document, and confirm the Metamask transaction from their account. The document is then sent to the university for verification.

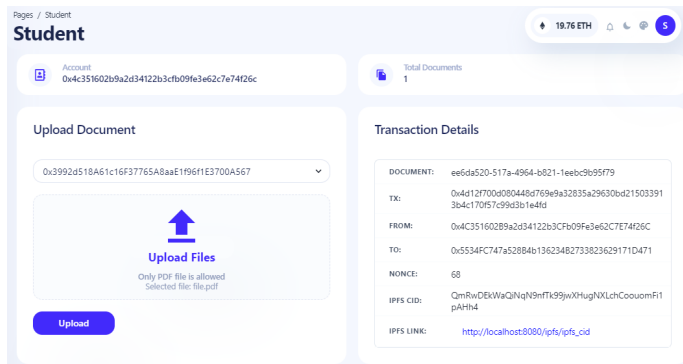


Fig. 5. Student Page

D. University

Universities select the document for verification, upload the original copy, and click "verify." If both documents match, the verification status is set to true.

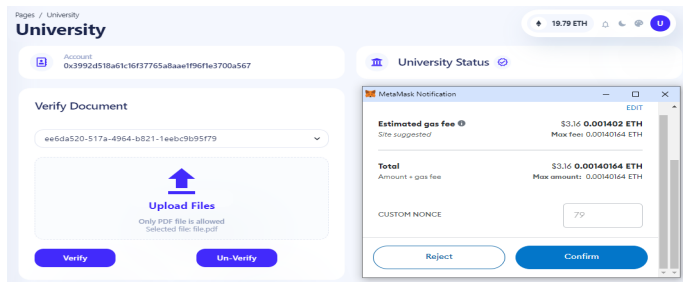


Fig. 6. University Page

F. Result

The result is a verified document with a QR code embedded on it.

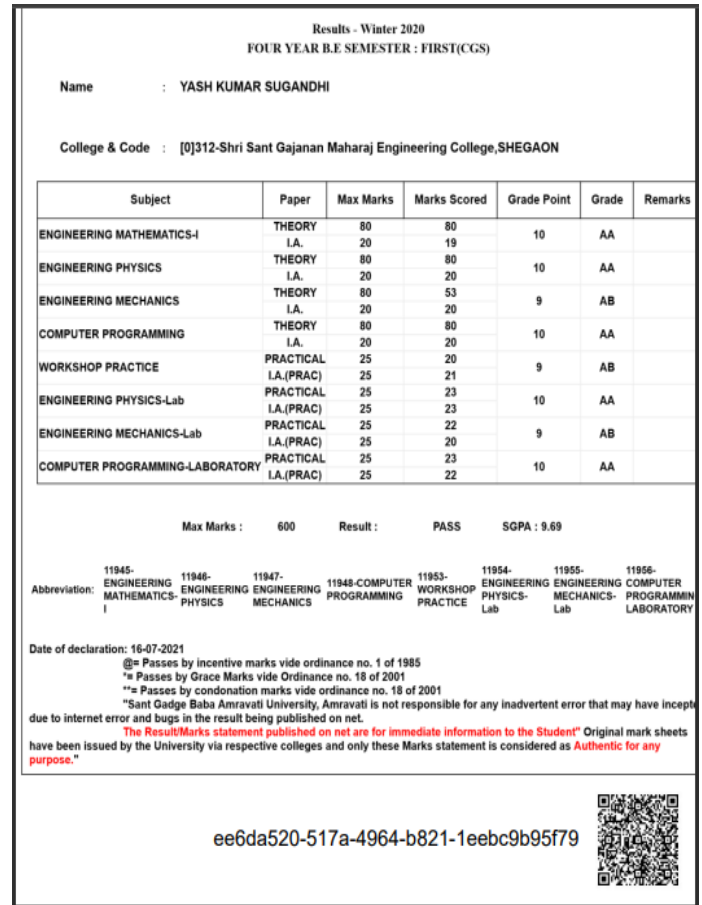


Fig. 8. Result Page

G. Gas Usage Metrics

In the Ethereum ecosystem, gas fees are a critical aspect of executing transactions and interacting with smart contracts. Computational effort on the Ethereum network is measured in units referred to as Gas. When users initiate transactions or engage with smart contracts, they must pay a corresponding gas fee, denominated in Ether (ETH), to compensate network miners. This fee varies based on the complexity of the operation and network demand.

TABLE I
UPLOADDOCUMENT GAS COST

Gas Used	Gas Cost	Gas Fee
270035	20 Gwei	0.005401 Eth

In the Ethereum smart contracts context, gas functions as a unit representing the computational resources essential for executing operations. For the 'uploadDocument' function, the gas used is 270,035 units, reflecting the computational effort involved in executing this particular smart contract function. The gas price, set at 20 Gwei (20,000,000,000 wei, a smaller denomination of Ether), determines the cost per unit of gas. The gas limit, also set at 270,035 units, represents the maximum amount of gas allowed for the function. In this case, the gas fee for executing 'uploadDocument' is calculated by multiplying the gas used (270,035) by the gas price (20 Gwei), resulting in a fee of 0.005401 ETH.

TABLE II
VERIFYDOCUMENT GAS COST

Gas Used	Gas Cost	Gas Fee
70082	20 Gwei	0.001402 Eth

Similarly, for the 'verifyDocument' function, the gas used is 70,082 units, reflecting the computational resources expended during execution. The gas price remains at 20 Gwei, and the gas limit is 70,082 units. Consequently, the gas fee for 'verifyDocument' is calculated as the multiplication of the gas (70,082) and the price of gas (20 Gwei), resulting in a fee of 0.001402 ETH. These gas parameters, including gas used, gas price, and gas limit, collectively determine the cost and resource allocation associated with executing specific functions on the Ethereum blockchain.

VI. CONCLUSION

The primary advantage of Blockchain lies in its capability to generate immutable records. This feature ensures a transparent and secure system. The system automates certificate generation, reducing manual work for verification. This not only minimizes the risk of students losing certificates but also enhances data security. Hash values of certificates find their storage in the blockchain, while the primary documents are maintained within the InterPlanetary File System (IPFS), ensuring data preservation and transparency.

Traditional document verification for employment is both costly and time-consuming, often relying on third parties. The paper illustrates how blockchain technology eliminates these challenges. Implementing such a system can significantly reduce fraud related to work history, offering a more reliable solution for companies.

ACKNOWLEDGMENT

Academic knowledge is translated into practical solutions with the system "Doqfy: Digital Document Verification Using Blockchain and IPFS." Grateful for the opportunity, we extend our heartfelt thanks to our guide, Dr. JaiKumar Patil, whose unwavering motivation and guidance propelled us. Special thanks to Prof. Smita Bansod for her crucial support in making this paper a reality. Lastly, the paper acknowledges and appreciates the authors of the references and literature that contributed to the project.

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), Honolulu, HI, USA, 2017, pp. 557-564, doi: 10.1109/BigData-Congress.2017.85.
- [2] 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), Chiba, Japan, 2018, pp. 1046-1051, doi: 10.1109/ICASI.2018.8394455.
- [3] A. Singh, S. Chauhan and A. K. Goel, "Blockchain Based Verification of Educational and Professional Certificates," 2023 2nd International Conference on Computational Systems and Communication (ICCCS), Thiruvananthapuram, India, 2023, pp. 1-7, doi: 10.1109/ICCCS56913.2023.10143008.
- [4] J. Gupta and S. Nath, "SkillCheck: An Incentive-based Certification System using Blockchains," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2020, pp. 1-3, doi: 10.1109/ICBC48266.2020.9169457.
- [5] E. Nyaletey, R. M. Parizi, Q. Zhang and K. -K. R. Choo, "Block-IPFS - Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 18-25, doi: 10.1109/Blockchain.2019.00012.
- [6] G. Malik, K. Parasrampur, S. P. Reddy and S. Shah, "Blockchain Based Identity Verification Model," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, 2019, pp. 1-6, doi: 10.1109/ViTE-CoN.2019.8899569.
- [7] A. K. Shrivastava, C. Vashisth, A. Rajak and A. K. Tripathi, "A Decentralized Way to Store and Authenticate Educational Documents on Private Blockchain," 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Ghaziabad, India, 2019, pp. 1-6, doi: 10.1109/ICICT46931.2019.8977633.
- [8] M. Z. Chowdhury and Asaduzzaman, "A Blockchain-Based Decentralized Document Authentication System for Multiple Organizations," 2022 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE), Naya Raipur, India, 2022, pp. 269-274, doi: 10.1109/WIECON-ECE57977.2022.10151411.
- [9] S. Halder, H. A. Kumar, S. Lavu and R. S. R., "Digital Degree Issuing and Verification Using Blockchain," 2022 Fourth International Conference on Cognitive Computing and Information Processing (CCIP), Bengaluru, India, 2022, pp. 1-4, doi: 10.1109/CCIP57447.2022.10058644.
- [10] P. Haveri, U. B. Rashmi, D. G. Narayan, K. Nagarathna and K. Shivaraj, "EduBlock: Securing Educational Documents using Blockchain Technology," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-7, doi: 10.1109/ICCCNT49239.2020.9225265.

Splitted group5 final report-test (1).docx

ORIGINALITY REPORT

8%

SIMILARITY INDEX

5%

INTERNET SOURCES

2%

PUBLICATIONS

3%

STUDENT PAPERS

PRIMARY SOURCES

1

vesit.ves.ac.in

Internet Source

4%

2

Submitted to PES University

Student Paper

2%

3

Atik Zakirhusen Mujawar, Akash Lalitkumar Makwana, Lalit Shailesh Jain, Dev Vikesh Doshi, Smita Bansod, Nivedeeta Mukherjee. "Blockchain qualified: Verification system", 2023 International Conference on Advanced Computing Technologies and Applications (ICACTA), 2023

Publication

1%

4

ebin.pub

Internet Source

1%

Exclude quotes Off

Exclude matches Off

Exclude bibliography On

AUTHORS

<p>Name: Pratik Ganesh Ekhande</p> <p>Address: Bhusawal, 425201(M.H)</p> <p>Email: ekhandepratik123@gmail.com</p> <p>Phone: 9112875663</p>	
<p>Name: Yash Kumar Sugandhi</p> <p>Address: Burhanpur 450331 (M.P)</p> <p>Email: yashsugandhi96442@gmail.com</p> <p>Phone: 7999801303</p>	

Youtube:<https://youtu.be/xJZIwHtlueA?si=vbq dofQl-8pf79Dk>