Malnad College of Engineering

(An Autonomous Institution under Visvesvaraya Technological University, Belgavi)

Department of Information Science & Engineering

Hassan - 573 202

Seminar Report on

"Certificate Authentication using Blockchain"

Submitted to fulfill the requirement of Seminar on Advanced Topics **(20IS801)** of VIII Semester for the academic year 2023-2024.

Submitted by

Thejaswini B S - 4MC20IS057

Malnad College of Engineering Hassan – 573 202
2023-2024

URL: www.mcehassan.ac.in

Malnad College of Engineering

(An Autonomous Institution under Visvesvaraya Technological University, Belgavi)

Department of Information Science & Engineering

Hassan - 573 202

CERTIFICATE

Thejaswini B S – 4MC20IS057

This is to certify that the above student has satisfactorily presented a **Seminar on Advanced Topics (20IS801**) on the topic "Certificate Authentication using Blockchain", in VIII Semester as per the requirement of autonomous program for the academic year 2023-2024.

Guide	Examiners (Signature and Name)
Dr. Nanditha B R ***Assistant Professor***	1. Dr. Vinutha M R Assistant Professor 2. Mr. Krishna Swaroop A Assistant Professor

(Dr. Chandrika J)
Professor & Head

ABSTRACT

In the current digital landscape, educational institutions are digitizing certificates like the Secondary School Leaving Certificate (SSLC), Higher Secondary Leaving Certificate (HSLC), and academic certificates. However, the increasing number of security breaches poses a threat to the privacy of users' academic digital certificates. The process of validating and verifying these digital certificates becomes challenging for both educational institutions and businesses.

To address these challenges, the proposed system suggests implementing a certificate administration and verification system using blockchain technology. Blockchain offers various capabilities, including hash functions, public-private key cryptography, mining, peer-to-peer networks, and proof of work. These features contribute to creating a secure and efficient environment for digital certificate validation.

In essence, the proposed system aims to leverage blockchain technology to provide a practical solution for the issuance and verification of academic credentials. This approach enhances the safety and efficiency of the validation process, safeguarding users' privacy in the face of security threats.

CONTENTS

LIST OF FIGURES

CHAPTER 1

1.1 INTRODUCTION

In the realm of digital certification, the need for secure and transparent exchange of data is paramount. To address this, we've developed an Android application aimed at providing foolproof verification of certificates. In today's landscape, where diplomas and transcripts are susceptible to forgery or alteration, ensuring the authenticity of such documents is crucial. Blockchain technology, coupled with various hashing algorithms, emerges as a potent solution in preserving data integrity. By leveraging blockchain, we not only mitigate the risk of counterfeit certificates but also streamline the verification process, eliminating the need for constant validation.

Digital signatures stand out as a vital security measure, ensuring verification, integrity, and non-repudiation of digital documents. The advent of blockchain further enhances the safety of storing certificates, bolstering their authenticity and confidentiality. Through the application of these technologies, we've devised a secure authentication system for digital certificates. Hashing data plays a pivotal role in modern cryptography, transforming data into irreversible hash codes, thus ensuring data integrity and security.

In today's evolving educational landscape, characterized by decentralization and diversity, maintaining the integrity of certifications remains paramount. With increasing demands for document verification across various domains like land registration, PAN cards, and Aadhar cards, blockchain technology offers a promising avenue for enhancing transparency and trust. By utilizing blockchain, we aim to address concerns surrounding certificate authentication, potentially revolutionizing how educational credentials are verified.

The application of blockchain technology and its broader implications extend to creating immutable and transparent distributed environments. A blockchain operates as a decentralized database, storing transaction records in incorruptible blocks. Through consensus among stakeholders, entries are validated and added to the blockchain, ensuring data permanence and security. This approach holds the promise of fostering open and secure systems across diverse domains.

Traditional methods of verifying diplomas or certificates often entail significant time and resource investments. Blockchain technology offers a disruptive solution by eliminating the need for centralized authorities in certificate verification. Through blockchain-based educational credentials, students can obtain tamper-proof digital certificates recorded on platforms like Blockchain. These certificates, cryptographically signed and accessible online, bypass the need for third-party validation, ushering in a new era of trust and accessibility in education.

1.2 OBJECTIVE

- Addressing Certificate Forgery Concerns:

  To address the prevalent issues of certificate forgery and alteration in modern-day certifications, emphasizing the need for a more secure authentication method.
- Developing a Secure Authentication System:

  To propose the development of a blockchain-based authentication system designed to ensure the integrity and authenticity of digital certificates issued by educational institutions.
- Utilizing Blockchain and Hashing Algorithms:

  It focuses on leveraging blockchain technology in conjunction with various hashing algorithms to create a robust and tamper-proof system for preserving certificate data integrity.
- Enhancing Certificate Verification Processes:

  To enhance the efficiency and reliability of certificate verification processes by implementing blockchain technology, thereby reducing the need for continuous manual validation.
- Contributing to Academic Research and Practice:

  To contribute to academic research and practice by presenting a novel approach to certificate authentication that harnesses the capabilities of blockchain technology, potentially offering a more secure and reliable solution for verifying educational credentials.

CHAPTER 2

LITERATURE REVIEW

[1] G. Balamurugan and K. K. A. Sahayaraj

Volume: pp. 1-7 Issue: 24 | May-2023

Title - A Blockchain Based Certificate Authentication System

In this paper the suggest a new way to authenticate certificates using blockchain technology. Their idea aims to solve the problems with traditional methods by using blockchain's decentralized and unchangeable features. With their system, they want to make certificate authentication more secure, dependable, and transparent. By sharing their research at the conference, they add to the ongoing efforts to use blockchain in different areas, highlighting how it could change certificate authentication worldwide.

[2] Shivani Pathak, Vimal Gupta, Nitima Malsa, Ankush Ghosh & R. N. Shaw

Volume: 914 Issue: 31 | August 2022

Title - Blockchain-Based Academic Certificate Verification System—A Review

They offer a detailed look at how blockchain can be used to verify academic certificates. They carefully study different ways blockchain is used for this purpose, looking at what works well and what doesn't. Their goal is to find ways to make the process better. By sharing their findings at the conference, they add important information to the conversation about using blockchain in education. They show both the good things and the problems that come with using blockchain for certificate verification.

[3] Md. Mijanur Rahman, Md. Tanzinul Kabir Tonmoy, Saifur Rahman Shihab, Riya Farhana

Volume: 11Issue: 03 | March 2023

Title - Blockchain-Based Certificate Authentication System with Enabling Correction", Journal of Computer and Communications

In their paper titled "Blockchain-Based Certificate Authentication System with Enabling Correction," published in the Journal of Computer and Communications in March 2023, Md. Mijanur Rahman, Md. Tanzinul Kabir Tonmoy, Saifur Rahman Shihab, and Riya

Farhana present a system that utilizes blockchain technology for authenticating certificates while allowing for corrections when needed. Their research addresses the limitations of traditional certificate authentication methods by leveraging blockchain's immutable nature and incorporating mechanisms for error correction. By publishing their work in a reputable journal, Rahman et al. contribute to the advancement of blockchain applications in certificate authentication, offering a solution that balances security with flexibility.

[4] C.Rashmi, G. Archana, K. Rashmika, K. Spandana, Ch. Manasa

Volume: 14(03), 939–946Issue: 2023

Title-A Blockchain Based Secure And Efficient Validation System For Digital Certificates

In this paper, they introduce a system that uses blockchain technology to securely and efficiently validate digital certificates. Their research aims to address the challenges associated with traditional certificate validation methods by leveraging the inherent security and transparency of blockchain. By presenting their findings, Rashmi et al. contribute to the advancement of blockchain applications in certificate validation, offering insights into how this technology can enhance the trustworthiness and reliability of digital certificates.

CHAPTER 3

3.1 CHALLENGES IN TRADITIONAL CERTIFICATE AUTHENTICATION SYSTEMS

Traditional certificate authentication systems, characterized by paper-based records and manual verification processes, face significant challenges in today's digital age. These challenges hinder the effectiveness, efficiency, and security of certificate authentication, impacting individuals, organizations, and institutions relying on traditional methods. In this paper, we explore the key challenges encountered by traditional certificate authentication systems, including security vulnerabilities, scalability issues, authenticity concerns, regulatory compliance, and technological obsolescence. By identifying and understanding these challenges, we can better appreciate the limitations of traditional approaches and explore potential strategies for addressing them.

- **Security Vulnerabilities:**
  One of the foremost challenges in traditional certificate authentication systems is security vulnerabilities. Traditional methods often rely on centralized databases or paper-based records, which are susceptible to various security threats such as hacking, data breaches, and identity theft. Centralized databases are attractive targets for malicious actors seeking to exploit vulnerabilities and gain unauthorized access to sensitive information. Moreover, paper-based records are prone to loss, theft, or tampering, compromising the integrity and confidentiality of certificates. These security vulnerabilities pose significant risks to individuals, organizations, and institutions relying on traditional certificate authentication systems, necessitating robust security measures to mitigate potential threats.
- **Scalability Issues:**
  Scalability represents a significant challenge for traditional certificate authentication systems, particularly as the volume of certificates and transactions continues to grow. Traditional methods often struggle to accommodate the increasing demand for certificate authentication, leading to processing delays, inefficiencies, and resource constraints. Centralized databases may experience performance bottlenecks and scalability limitations as the number of users and transactions escalates. Additionally, manual verification processes can become overwhelmed by the sheer volume of requests, resulting in processing delays and backlogs. These scalability issues hinder

the ability of traditional systems to effectively manage and authenticate certificates at scale, necessitating scalable and efficient authentication solutions to meet growing demands.

- **Authenticity Concerns:**

  Ensuring the authenticity of certificates represents a critical challenge in traditional certificate authentication systems. Traditional methods often rely on manual verification processes, which are prone to errors, inconsistencies, and fraudulent activities. Verifying the authenticity of paper-based certificates can be time-consuming and labor-intensive, requiring extensive manual effort and document inspection. Furthermore, centralized databases may contain inaccurate or outdated information, leading to discrepancies and doubts regarding the validity of certificates. These authenticity concerns undermine the trust and reliability of traditional certificate authentication systems, casting doubt on the integrity of authenticated credentials and necessitating robust mechanisms for verifying authenticity.

- **Regulatory Compliance:**

  Compliance with regulatory requirements poses a significant challenge for traditional certificate authentication systems, particularly in highly regulated industries such as finance, healthcare, and education. Traditional methods may struggle to meet stringent regulatory standards and requirements, leading to compliance gaps and legal liabilities. Regulatory frameworks such as GDPR, HIPAA, and FERPA impose strict guidelines for data privacy, security, and confidentiality, which traditional systems must adhere to. Failure to comply with regulatory mandates can result in hefty fines, legal penalties, and reputational damage for organizations and institutions. Therefore, ensuring regulatory compliance represents a critical challenge for traditional certificate authentication systems, requiring robust governance and compliance mechanisms to mitigate risks and ensure adherence to regulatory standards.

- **Technological Obsolescence:**

  Technological obsolescence is a pervasive challenge faced by traditional certificate authentication systems, particularly in the rapidly evolving landscape of information technology. Traditional methods often rely on outdated technologies, legacy systems, and manual processes that struggle to keep pace with advancements in digital authentication and cybersecurity. As new technologies such as blockchain, biometrics, and digital signatures emerge, traditional systems risk becoming obsolete, inefficient, and incompatible with modern authentication requirements. Additionally, technological obsolescence may hinder interoperability, data sharing, and integration with emerging platforms and ecosystems. Therefore, addressing technological obsolescence represents a critical challenge for traditional certificate authentication systems, necessitating ongoing innovation, modernization, and adaptation to evolving technological landscapes.

Thus, the traditional certificate authentication systems face numerous challenges that impact their effectiveness, efficiency, and security. These challenges include security vulnerabilities, scalability issues, authenticity concerns, regulatory compliance, and technological obsolescence. Addressing these challenges requires a comprehensive approach that leverages innovative technologies, robust security measures, and compliance frameworks. Embracing emerging technologies such as blockchain, biometrics, and digital signatures offers promising solutions for enhancing the security, efficiency, and reliability of certificate authentication in the digital age. By recognizing and addressing these challenges, stakeholders can ensure the continued relevance and effectiveness of certificate authentication systems in an increasingly digital and interconnected world.

3.2 WHY BLOCKCHAIN IN AUTHENTICATION

Blockchain technology has emerged as a revolutionary force in the realm of authentication, promising to reshape traditional methods and address longstanding challenges. The rationale behind integrating blockchain into authentication processes lies in its unique properties and capabilities, which offer unparalleled security, transparency, and decentralization. By harnessing these attributes, blockchain not only enhances the security of authentication systems but also streamlines processes, fosters trust, and promotes interoperability across diverse platforms.

At its core, blockchain serves as a decentralized and immutable ledger, recording transactions in a transparent and tamper-resistant manner across a network of computers. Each transaction is cryptographically linked to the preceding one, forming a chain of blocks that cannot be altered retroactively. This decentralized architecture eliminates the need for a central authority or intermediary, mitigating the risk of single points of failure and unauthorized access. In authentication, this distributed nature of blockchain ensures that authentication records remain secure and verifiable, safeguarding sensitive information from cyber threats and fraudulent activities.

One of the primary advantages of blockchain in authentication is its ability to enhance security and prevent unauthorized access. Traditional authentication methods often rely on centralized databases or third-party intermediaries, which are vulnerable to hacking and data breaches. Blockchain, however, employs cryptographic algorithms and consensus mechanisms to verify transactions, making it virtually impossible for malicious actors to tamper with or manipulate authentication data. By decentralizing authentication processes, blockchain minimizes the risk of unauthorized access and ensures the integrity of authentication records, thereby bolstering security and trust in digital interactions.

Blockchain-based authentication systems streamline and automate authentication processes, reducing the need for manual intervention and accelerating authentication times. Traditional authentication methods often involve complex and time-consuming procedures, such as manual verification and validation. Blockchain-based authentication systems, on the other hand, leverage smart contracts to automate authentication processes, enabling seamless and efficient authentication for users and organizations alike. By digitizing and automating authentication processes, blockchain enhances efficiency and reduces operational costs associated with manual authentication methods.

Moreover, blockchain offers unprecedented transparency and traceability, which are essential for effective authentication. Every transaction recorded on the blockchain is transparent and visible to all participants in the network, ensuring accountability and preventing fraud. In authentication systems, this transparency allows users to track the entire authentication process, from the initial request to the final verification, enabling them to verify the authenticity of transactions in real-time. Additionally, blockchain's immutable nature ensures that once a transaction is recorded on the blockchain, it cannot be altered or deleted, providing a reliable audit trail for authentication activities.

Another compelling reason for integrating blockchain into authentication is its potential to streamline and simplify authentication processes. Traditional authentication methods often involve complex and time-consuming procedures, such as manual verification and validation. Blockchain-based authentication systems, on the other hand, automate and digitize these processes, reducing the need for manual intervention and accelerating authentication times. By leveraging smart contracts, blockchain can automate authentication processes, enabling seamless and efficient authentication for users and organizations alike. This automation not only improves user experience but also enhances the overall efficiency and scalability of authentication systems and ensuring that users can securely access sensitive information without fear of unauthorized access or manipulation. By leveraging blockchain's decentralized architecture and cryptographic security, organizations can provide users with a secure and reliable authentication experience, enhancing trust and confidence in their services.

Furthermore, blockchain promotes interoperability and collaboration among different authentication systems and platforms. In today's interconnected digital landscape, users often interact with multiple authentication systems across various platforms and applications. Blockchain's decentralized architecture allows different authentication systems to communicate and share authentication data securely, facilitating seamless authentication experiences for users across different platforms. This interoperability not only enhances user convenience but also strengthens the overall security and reliability of authentication systems, fostering trust and collaboration in the digital ecosystem.

The blockchain technology represents a paradigm shift in authentication, offering a secure, transparent, and decentralized alternative to traditional methods. By leveraging its unique properties, such as cryptographic security, transparency, and automation, blockchain has the potential to revolutionize authentication processes, making them more secure, efficient, and user-friendly. As organizations continue to embrace digital transformation and the adoption of blockchain accelerates, blockchain-based authentication systems are poised to play a pivotal role in safeguarding sensitive information, fostering trust, and enabling seamless digital interactions in the modern age.

CHAPTER 4

RELATED WORKS

A. Blockchain Technology

In 2008, an individual or group using the pseudonym Satoshi Nakamoto introduced the revolutionary concept of blockchain technology. Essentially, a blockchain is a digital ledger distributed across multiple nodes or computers that allows for transparent and decentralized data exchange. Each transaction stored within this ledger is compressed and added to separate blocks, ensuring that verifications can occur without the need for intermediaries. Once added, the data becomes immutable and is time stamped, creating a secure and transparent record accessible to the public while maintaining its integrity and safety.

The introduction of Ethereum Smart Contracts around 2013 marked a significant advancement in blockchain technology, leading to what is often referred to as blockchain 2.0. While blockchain 1.0, exemplified by Bitcoin, primarily addressed issues related to cryptocurrencies and decentralized payments, blockchain 2.0 expanded the scope to decentralize entire markets. Smart contracts, a key feature of blockchain 2.0, enable the conversion of assets and facilitate the creation of alternative cryptocurrencies beyond Bitcoin, thereby adding value and fostering innovation in the blockchain ecosystem.

B. Ethereum

Ethereum is a decentralized platform that enables developers to build and deploy smart contracts and decentralized applications (DApps). Unlike traditional centralized systems, where data and control are held by a single authority, Ethereum operates on a blockchain, which is a distributed ledger shared across multiple computers. At the core of Ethereum is its cryptocurrency called Ether (ETH), which is used to facilitate transactions and compensate participants who contribute computing power to the network. However, Ethereum's significance goes beyond just being a digital currency. Its main feature is the ability to execute smart contracts, which are self-executing agreements with the terms of the contract directly written into code.

These smart contracts run on the Ethereum Virtual Machine (EVM), a decentralized runtime environment. This means that once deployed, smart contracts operate autonomously, executing their programmed instructions without the need for intermediaries. Ethereum has opened up a world of possibilities for developers, businesses, and individuals. DApp developers can leverage Ethereum's platform to create decentralized applications for various purposes, such as finance, gaming, supply chain management, and more. These DApps can operate transparently and securely, thanks to Ethereum's blockchain technology.

Ethereum functions as a decentralized and transparent platform supporting a wide array of applications that derive from it. One of its distinctive features lies in its Turing completeness, allowing for versatile and adaptable programming capabilities. Ethereum serves as the primary platform for generating smart contracts and facilitating decentralized autonomous organizations (DAOs). While Bitcoin's blockchains serve as a global payment network, Ethereum can be likened to a universal computing system, offering broader utility beyond financial transactions.

In essence, Ethereum operates as an open-source platform akin to Android, providing developers with the necessary tools and infrastructure to create various applications. Both Ethereum itself and the developers utilizing its resources share responsibility for the ongoing development and upkeep of the underlying infrastructure. The following is an outline of some of Ethereum's primary attributes:

- Ethereum Virtual Machine (EVM)
  The Ethereum Virtual Machine (EVM) functions as a flexible blockchain platform. Unlike Bitcoin's limited set of instructions, the EVM grants developers the liberty to execute programs as they desire. Developers utilize Solidity, a high-level programming language, to provide instructions to the EVM on how applications should run.
- Solidity
  Solidity serves as a programming language specifically designed for building smart contracts. It shares similarities with JavaScript in terms of its structure and functionality. Once a smart contract is written using Solidity, it needs to be compiled into contract bytecode using a compiler. The Ethereum Virtual Machine (EVM) is then responsible for interpreting this bytecode. Subsequently, the constructed instructions are added to the Ethereum blockchain, completing the entire process.

C. Smart Contracts

In the early 1990s, Nick Szabo introduced the concept of smart contracts, defining them as digital contracts executed by computers based on predefined terms. With the rise of blockchain technology, smart contracts have gained significant attention, particularly on platforms like Ethereum, launched in 2015, which are notable for their support of smart contracts.

Smart contracts essentially automate transactions and processes, reducing human error and potential conflicts by executing actions according to predefined rules. They can be utilized for various applications, including voting systems and cryptocurrencies, offering benefits such as transparency and immutability of data.

Smart contracts are typically written in high-level scripting languages like Solidity and LLL. Solidity is commonly used by developers to build smart contracts, which are then compiled into opcode for execution on the Ethereum Virtual Machine (EVM). However, developing smart contracts may incur certain charges.

These smart contracts run on the Ethereum Virtual Machine (EVM), a decentralized runtime environment. This means that once deployed, smart contracts operate autonomously, executing their programmed instructions without the need for intermediaries.

Despite challenges like scalability and privacy concerns, blockchain technology, along with cryptocurrencies like Bitcoin and Ethereum, offers numerous benefits, potentially transforming existing business operations. For instance, one application discussed involves creating electronic certificates, generating their hash values, and storing them on a blockchain. A QR code linked to the original certificate's hash value allows for easy verification using mobile devices.

While public blockchains like Ethereum are widely used for their transparency and decentralization, Hyperledger, chosen primarily for B2B transactions, faces limitations such as privacy concerns and scalability issues.

CHAPTER 5

PROPOSED METHODOLOGY

To enable semantic search on data transactions within blockchain systems, it's essential to develop an efficient data method tailored to the proposed system's requirements. By integrating Blockchain technology with the capabilities of Hyperledger Fabric, we can ensure the authenticity and verification of educational and commercial certifications. The goal is to design an application that leverages blockchain technology to identify counterfeit diplomas within educational institutions.

The process begins with educational institutions inputting student information, including names and email addresses, into our application interface. This data is then securely stored in a database. Subsequently, the program records the certificates issued by the registrar, and collectively, these certificates form a blockchain. Employers and verifiers can verify the authenticity of a certificate by inputting the student's details into the application, as depicted in Figure 1.

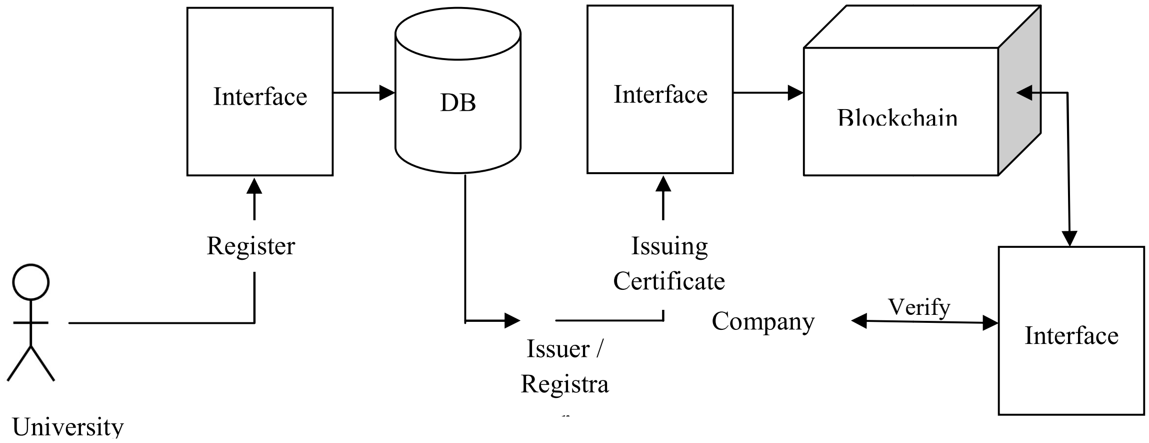

Figure 5.1: Proposed Model for Digital Certificate

In essence, the application serves as a platform for educational institutions to securely store and verify certificates, thereby safeguarding against fraudulent credentials. Through the utilization of blockchain technology, we aim to enhance the integrity and trustworthiness of certification processes, ultimately benefiting both employers and students alike.

A. System Design and Working

The solution combines decentralized technologies like IPFS and Ethereum smart contracts to easily check if a document is real and confirm its integrity and authenticity. The process of how users interact with smart contracts is illustrated in Figure 2.

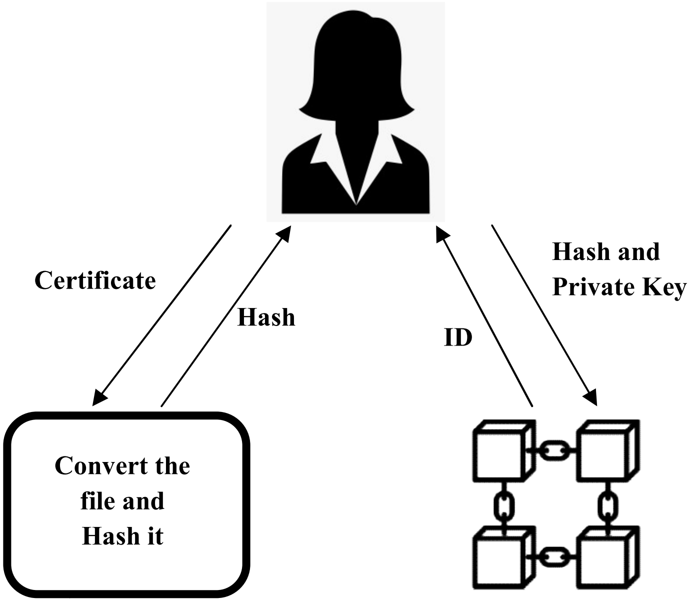

Figure 5.2 : Flow Diagram

There are three main users: the user, the organization, and the corporation that verifies information. The certificates legally belong to the user, who has the authority to share them with businesses. The institutions are responsible for granting certifications. Only authorized firms, including organizations and verifiers, can access the system. Organizations can upload certifications and other relevant information, while verifiers can validate the user's certifications on the chain. Once the user receives the certificates and evidence from the organization, they can share them with any verifier they choose.

Here's how the process works: The college, as the certificate issuer, enters information into a Certificate Template. Then, the issuer fills in the required details to generate the document. Once all necessary information is collected, it's added to a predefined certificate template, and a copy of the document is generated for review. If the issuer is satisfied, they click "Approve." After data storage and approval, the document'sinformation is compiled and added to a bit array. This data is then sent to IPFS, which applies its hashing method and saves the hash alongside the original document.

Next, the information is sent to the Blockchain via IPFS. The issuer validates the generation charges using Metamask. The hash is then saved on the Blockchain, where it remains immutable. If there's any attempt to alter the data, other blockchain servers will alert each other. Now, the student can provide this hash or their digital certificate to multiple companies. The issuer can upload the document, or the hash can be entered manually. The system will then respond, indicating whether the document is legitimate or not.

B. Digital Certificate Creation

When a student earns certificates from their university, those certificates are usually in paper form. But nowadays, universities are moving towards digitizing these certificates. This means turning the paper certificates into digital ones, which are stored on computers or online databases. Let's take a look at how this process works and why it's important.

Firstly, when a student receives certificates for their academic achievements or sports activities, the university takes these paper certificates and makes digital copies of them. This process involves using technology to convert the images on the paper certificates into digital images. This is done using special techniques that can change pictures from the old-fashioned analog format to the modern digital format. These digital certificates are then stored in a database. A database is like a digital filing cabinet where information can be organized and kept safe. So, instead of keeping the paper certificates in a physical filing cabinet, the university keeps digital copies in a virtual filing cabinet on a computer or server.

Now, you might wonder why it's important to digitize these certificates. Well, there are several reasons. Firstly, digital certificates are much easier to store and manage. Instead of having piles of paper certificates that can get lost or damaged, universities can keep all the certificates neatly organized on a computer. Secondly, digital certificates can be accessed from anywhere at any time, as long as there's an internet connection. This means that students don't have to worry about carrying around paper certificates or making sure they don't lose them. They can simply log in to their university's website and access their digital certificates whenever they need them.

Another important reason for digitizing certificates is security. Paper certificates can be easily forged or tampered with. But digital certificates are much harder to fake because they have special security features built into them. For example, each digital certificate has its own unique set of codes made up of 0s and 1s, which represent its authenticity. Furthermore, digitizing certificates makes it easier for employers or other institutions to verify their authenticity. Instead of having to send physical copies of certificates back and forth, they can simply check the digital database to make sure that the certificates are genuine.

Thus, converting paper certificates into digital ones is an important step towards modernizing the education system. It makes certificates easier to manage, more accessible, and more secure. So, the next time you receive a certificate from your university, remember that it's not just a piece of paper – it's a digital record of your achievements that will last a lifetime. It is possible to transform an analogue picture of the certificate into a digital one by using the technique of conversing between analogue and digital images and the proposed architecture as shown in fig 3 and where ECS stands for Electronic Certificate System.

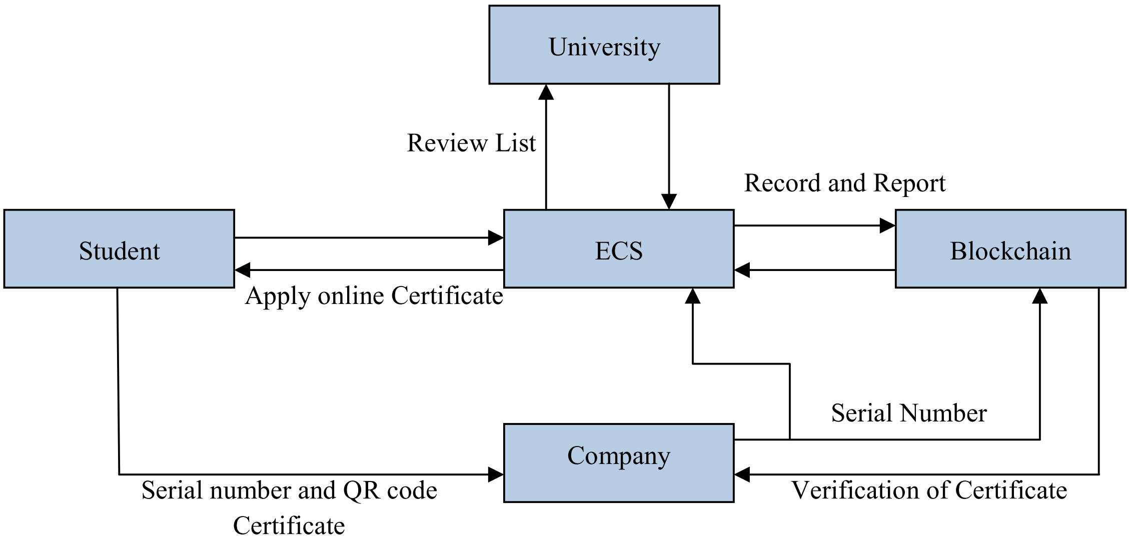

Figure 5.3: Proposed Architecture

In a digital picture, every point on a two-dimensional function has specific coordinates and values, each of which corresponds to a pixel. These pixels collectively form the image we see on our screens. When an administrator accesses our program using their admin login credentials, they gain the ability to upload a student's certificate directly into the application. Once uploaded, the application performs a process called sampling and quantization on the picture. This process is necessary to convert the certificate from its original analog format into a digital format that the application can work with.

Within the application, administrators have two main options: they can either add a new student or upload a certificate for an existing student. These options are typically available on the same page for convenience. If an administrative staff member chooses to add a new student, they will initiate the registration process for that student within the application. Then, whenever an administrator selects the option to add a certificate, the uploaded certificate will be linked to the corresponding student's profile.

This process ensures that each student's certificates are securely stored within the application and associated with the correct student record. By digitizing these certificates, the application enables easy access and management for administrators. They no longer need to keep physical copies of certificates or deal with the hassle of manual record-keeping.

Furthermore, the conversion of analog certificates to digital format through sampling and quantization ensures that the integrity of the certificate is preserved. While the original analog image may have infinite points and values, the digital version is represented by a finite set of pixels with discrete values. This transformation allows the application to accurately display and manipulate the certificate within its digital environment.

Overall, the process of uploading and managing student certificates within the application simplifies administrative tasks and enhances the efficiency of certificate management. It provides a centralized and organized platform for storing and accessing important student records, contributing to the overall effectiveness of educational administration.

C. Hash Code Generation

In a certificate authentication system using blockchain technology, generating a hash code plays a crucial role in ensuring the security and integrity of certificates. Let's break down how this process works in simple terms. When a certificate is created or uploaded onto the Blockchain -based authentication system, it undergoes a process where a unique identifier, known as a hash code, is generated. Think of a hash code as a digital fingerprint of the certificate. This hash code is created using a cryptographic hash function, which takes the content of the certificate as input and produces a fixed-length string of characters as output.

The beauty of a hash code lies in its uniqueness and unpredictability. Even the slightest change in the content of the certificate will result in a completely different hash code. This property ensures that each certificate has its own distinct identifier, making it tamper-proof and easily verifiable.

Once the hash code is generated, it is securely stored on the blockchain along with other relevant information about the certificate, such as the issuing authority, the date of issuance, and the recipient's details. The blockchain serves as a decentralized and immutable ledger, meaning that once information is recorded on it, it cannot be altered or deleted.

Now, when someone needs to verify the authenticity of a certificate, they can simply access the blockchain and retrieve the corresponding hash code. By recalculating the hash code of the certificate using the same cryptographic hash function, they can compare it with the hash code stored on the blockchain. If the two hash codes match, it provides irrefutable proof that the certificate has not been altered since it was issued.

This process of hash code generation and verification adds an extra layer of security and trust to the certificate authentication system. It ensures that certificates remain tamper-proof and verifiable, even in a digital environment. Moreover, by leveraging blockchain technology, the authentication system becomes decentralized and transparent, reducing the risk of fraud or manipulation.

The verification process begins by using the same initial conditions and parameter settings employed during the hash code generation. This ensures consistency, allowing for the recreation of the same result each time. Whenever a digital certificate is submitted, the system generates its hash value using the process depicted in figure 4.

One notable advantage of this approach is its collision resistance, which surpasses that of the SHA-1 algorithm. Collision resistance refers to the ability of a hash function to avoid generating the same hash value for different inputs. The chaotic hashing algorithm demonstrates superior collision resistance, making it more reliable in ensuring the uniqueness and integrity of digital certificates compared to traditional methods like SHA-1. The cryptographic hash functions like SHA-1 (Secure Hash Algorithm 1) have historically played a significant role. However, it's important to note that SHA-1 has vulnerabilities that make it less suitable for security-critical applications in modern times.

SHA-1 is a widely-used cryptographic hash function that produces a fixed-size output (160 bits) regardless of the input size. It has been widely adopted for various security applications, including digital signatures and certificate authentication.

In the context of certificate authentication using blockchain, SHA-1 is used to generate unique hash values for digital certificates. These hash values serve as digital fingerprints, providing a secure and efficient way to verify the integrity and authenticity of certificates stored on the blockchain.

When a certificate is created or updated, its content is hashed using SHA-1, and the resulting hash value is stored on the blockchain along with other relevant information about the certificate. This hash value acts as a tamper-proof seal, as any alteration to the certificate's content would result in a different hash value.

However, SHA-1 is not without its flaws. Over the years, vulnerabilities have been discovered that undermine its security. In particular, collision attacks have been demonstrated, where different inputs produce the same hash value. This poses a significant risk in scenarios where security and integrity are paramount, such as certificate authentication.

As a result, many organizations and standards bodies have deprecated the use of SHA-1 in favor of more secure hash functions like SHA-256. In the context of blockchain-based certificate authentication systems, the transition to stronger hash functions is essential to maintain the security and trustworthiness of the system.

By leveraging the chaotic algorithm, the certificate authentication system enhances security and reliability in verifying the authenticity of digital certificates. This innovative approach not only maintains consistency in hash code generation but also mitigates the risk of unauthorized alterations or tampering with certificate data.

In essence, the integration of the chaotic algorithm into the hash function reinforces the robustness of the certificate authentication system, contributing to its effectiveness in safeguarding digital credentials and maintaining trust in the authenticity of certificates.

Pseudo code for Hashing Algorithm

```
getSHAEncryptedString (String encTarget) {
    MessageDigest SHAEnc = null;
    try {
        SHAEnc = MessageDigest.getInstance("SHA5");
    } catch (NoSuchAlgorithmException e) {
        System.out.println("Exception while encrypting to SHA");
        e.printStackTrace();
    }// Hashing algorithm
SHAEnc.update(encTarget.getBytes(), 0, encTarget.length());
String SHA = new BigInteger(1, SHAEnc.digest()).toString(16);
while (SHA length() < 32){
    SHA = "0"+ SHA;
  }
return SHA;
}
```

D. Digital certificate Verification

The users are entrusted with the responsibility of uploading various credentials through a dedicated module. These credentials encompass a wide array, including high school mark lists (for both 10th and 12th grades), college certificates, and government-issued documents. The essence of this module lies in its ability to convert uploaded files into assets within the Hyperledger framework. Moreover, users have the option to leverage IPFS, an acronym for the Internet Protocol File System. IPFS serves as a peer-to-peer decentralized file system with the noble aim of unifying all computer devices under one cohesive file system.

Before the certificates are uploaded, a crucial step ensues: they undergo thorough validation by pertinent industry authorities. For instance, in the case of a school certificate upload, the certificate number is meticulously cross-referenced against the school's database server. Only if the certificate is deemed valid does it earn the privilege of being securely stored on the server; otherwise, it is swiftly discarded. This stringent validation process is instrumental in upholding the integrity of the system and ensuring that only authentic certificates are processed and stored.

One of the system's most notable features is its seamless verification process, which poses no obstacles for verifiers. When a verifier seeks to authenticate a certificate, the student provides a unique code associated with the certificate in question. Upon inputting this code into the designated field, the verifier gains immediate access to the relevant certificate. Furthermore, the system meticulously documents the entire academic journey of each student, leaving no room for ambiguity or doubt. This comprehensive documentation not only furnishes verifiers with invaluable context but also instills unwavering confidence in the authenticity of the certificates presented.

In essence, this system represents a paradigm shift in the realm of certificate authentication, offering a seamless and efficient solution while safeguarding the integrity and authenticity of certificates. Through rigorous industry validation and meticulous documentation, it stands as a testament to innovation in digital credential verification. By embracing cutting-edge technologies like blockchain and IPFS, this system paves the way for a future where certificate authentication is streamlined, reliable, and devoid of any ambiguity.

CHAPTER 6

CASE STUDY ON SUPPLY CHAIN MANAGEMENT

Sony Global Education partnered with IBM Japan to create the "Blockchain-based Student Records Platform," aiming to improve academic credential verification.

The collaboration stemmed from Sony's desire to tackle issues like inefficiencies, fraud, and lack of transparency in credential verification. In 2017, they joined forces to develop a blockchain-based platform specifically for managing student records. Their objectives were clear: improve the efficiency and reliability of academic credential verification, ensure the integrity and authenticity of digital certificates, and enhance trust and transparency in the verification process.

The development of the blockchain platform involved close collaboration between Sony Global Education and IBM Japan. They utilized Hyperledger Fabric, an open-source blockchain framework, to create a secure and scalable solution for managing student records.

Educational institutions participating in the platform issued digital certificates to students upon graduation or completion of courses. Each digital certificate contained crucial information such as the student's name, degree or course completed, date of issuance, and a unique identifier. Before issuing digital certificates, participating institutions hashed the certificate data using cryptographic algorithms like SHA-256. These hashed values were then recorded on a blockchain, creating an immutable and transparent ledger of certificate transactions.

Certificate verification became streamlined with the blockchain-based platform. Employers, academic institutions, or other parties seeking to verify a student's credentials could access the blockchain to retrieve the hashed values of the digital certificates. By independently computing the hash of the received certificate using the same cryptographic algorithm, they could confirm its authenticity.

The implementation of the blockchain-based platform yielded several benefits. It increased efficiency by streamlining the verification process, reduced the time and resources required for credential authentication, and enhanced security by ensuring the integrity and authenticity of digital certificates. Moreover, it improved trust and transparency in the credentialing process, as employers and academic institutions had confidence in the validity of verified credentials.

In conclusion, the partnership between Sony Global Education and IBM Japan exemplifies the transformative potential of blockchain technology in revolutionizing academic credential verification. By offering a secure, transparent, and efficient solution, blockchain technology has the capacity to reshape the education sector and enhance trust in academic credentials.

CHAPTER 7

CONCLUSION

The implementation of a Certificate Authentication System using blockchain technology marks a significant advancement in the realm of digital credential verification. By leveraging the inherent security and transparency of blockchain, coupled with innovative features such as IPFS integration, the system offers a robust solution for ensuring the integrity and authenticity of certificates.

Through a user-friendly interface, users can effortlessly upload various credentials, including high school mark lists, college certificates, and government-issued documents. These files are transformed into assets within the Hyperledger framework, ensuring secure storage and tamper-proofing through cryptographic hashing. Additionally, the option to utilize IPFS provides a decentralized file storage solution, further enhancing the system's resilience and accessibility.

Prior to upload, certificates undergo stringent validation by relevant industry authorities, guaranteeing their authenticity. This validation process, coupled with meticulous documentation of each student's academic journey, instills confidence in the verifiers. Verifying the authenticity of certificates becomes seamless, with verifiers granted access through unique codes associated with each certificate.

Overall, the Certificate Authentication System using blockchain offers a streamlined, secure, and transparent solution for digital credential verification. By embracing emerging technologies and industry best practices, it sets a new standard for certificate authentication, benefiting students, institutions, and verifiers alike. As we continue to navigate the digital landscape, such innovative systems pave the way for a future where trust and integrity in digital credentials are paramount.

REFERENCES

1. G. Balamurugan and K. K. A. Sahayaraj, "A Blockchain Based Certificate Authentication System," 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023
2. Shivani Pathak, Vimal Gupta, Nitima Malsa, Ankush Ghosh & R. N. Shaw, "Blockchain-Based Academic Certificate Verification System—A Review", International Conference paper August 2022
3. Md. Mijanur Rahman, Md. Tanzinul Kabir Tonmoy, Saifur Rahman Shihab, Riya Farhana, "Blockchain-Based Certificate Authentication System with Enabling Correction", Journal of Computer and Communications, Volume 11, Issue 3 (March 2023)
4. C.Rashmi, G. Archana, K. Rashmika, K. Spandana, Ch. Manasa., "A Blockchain Based Secure And Efficient Validation System For Digital Certificates", 2023, v14i03.14172
5. Lyndon Lyons and Andreas Bachmann Jan Seffinga, "The Blockchain (R)evolution – The Swiss Perspective," Switgerland, 2017
6. Engin Zeydanand Suayb SbArslan Gültekin Berahan Mermer, "An overview of blockchain technologies: Principles, opportunities and challenges, "in IEEE, Turkey, 2018
7. Narn - Yih Lee, Chien Chi and Yi-Hua Chen Jiin-Chiou Cheng, "Blockchain and smart contract for digital certificate, "in IEEE, Japan, 2018