

PROFESSIONAL TRAINING REPORT - II

entitled

BLOCKCHAIN BASED CERTIFICATE VERIFICATION

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering degree in Computer Science and Engineering with
specialization in Blockchain Technology.

by

M.Riyaz khan [Reg. no: 41613014]

G.Jeevan sai [Reg. no: 41613008]

K. Pradeep [Reg. no: 41613012]



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

CATEGORY -1 UNIVERSITY BY UGC

**Accredited with Grade "A++" by NAAC | 12B Status by UGC | Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119**

MAY 2024



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

CATEGORY-I UNIVERSITY BY UGC

Accredited "A++" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Professional Training Report is the bonafide work of **Mr. Riyaz Khan (Reg.no.41613014)** who carried out the project entitled "**BLOCKCHAIN BASED CERTIFICATE VERIFICATION**" under my supervision from January 2024 to May 2024.

Internal Guide

Ms. LEKSHMI S RAVEENDRAN, M.TECH.,

Head of the Department

Dr. S. VIGNESHWARI, M.E., Ph.D.,

Submitted for Viva voce Examination held on 7/5/24

Internal Examiner

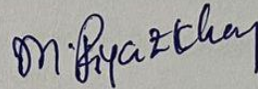
External Examiner

DECLARATION

I, **M. Riyaz Khan (Reg.no.41613014)**, hereby declare that the Professional Training Report-II entitled "**Blockchain based certificate verification**" done by me under the guidance of **Ms. Lekshmi S Raveendran, M.Tech.**, is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering with specialization in Blockchain Technology.

DATE: 07/05/2024

PLACE: Chennai



SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

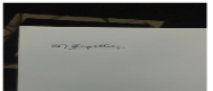
I convey my thanks to **Dr. T.Sasikala M.E., Ph.D., Dean**, School of Computing, **Dr. S.Vigneshwari M.E., Ph.D., Head of the Department of Computer Science and Engineering** for providing me necessary support during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Internal Guide **Ms. Lekshmi S Raveendran, M.Tech.**, for her valuable guidance, suggestions and constant encouragement which paved way for the successful completion of my phase-2 Professional Training.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

Course certificate

MORNING SESSION (FN)	National Programme on Technology Enhanced Learning	
Hall Ticket For	2024 Apr: CS43 Programming In Java - Online	NPTEL

Candidate Name	Mandoji riyaz khan					
Roll No	NOC24CS43S953400424		Seating Number	53400424		
Date of Birth	05-12-2003					
PwD Status	No	Compensatory Time Required	N.A	Scribe Required		N.A
Exam Date	Saturday, 27 April, 2024					
Reporting Time	08:00 am	Gate Closure	09:30 am			
Exam Timing	09:00 am	Shift	FN			
Test Centre Name	ION Digital Zone iDZ Kovilambakkam					
Test Centre Address	Fortune Towers, 1st and 2nd Floor, SH 109, 200 Feet Thoraipakkam Pallavaram Radial Road, Near Eachangadu signal, Kovilambakkam, Chennai, Tamil Nadu, India - 600117					
 NPTEL Coordinator						

Date enrolled 2024-01-29

Email riyazreheart@gmail.com

Name Riyazkhan

46.05%

Course Progress

Unit wise Progress

Assessment scores

Week 01 : Assignment 01:	100.0
Week 02 : Assignment 02:	100.0
Week 03 : Assignment 03:	100.0
Week 04 : Assignment 04:	88.0
Week 05 : Assignment 05:	100.0

ABSTRACT

In recent years, the proliferation of digital certificates has highlighted the need for reliable and tamper-proof verification mechanisms. Blockchain technology offers a promising solution by providing a decentralized, immutable, and transparent platform for certificate verification. This abstract presents an overview of blockchain-based certificate verification, outlining its key features, benefits, and challenges. In recent years, the proliferation of digital certificates has highlighted the need for reliable and tamper-proof verification mechanisms. Blockchain technology offers a promising solution by providing a decentralized, immutable, and transparent platform for certificate verification. This abstract presents an overview of blockchain-based certificate verification, outlining its key features, benefits, and challenges. Blockchain-based certificate verification involves the use of a distributed ledger to store and verify certificates. Each certificate is assigned a unique identifier and is cryptographically signed by the issuing authority. This signature, along with other relevant information, is stored on the blockchain, ensuring the integrity and authenticity of the certificate. One of the key advantages of blockchain-based certificate verification is its transparency. The blockchain is a public ledger that is accessible to all participants, allowing anyone to verify the authenticity of a certificate without the need for a centralized authority. This transparency helps to mitigate fraud and ensures the trustworthiness of the verification process. However, blockchain-based certificate verification also presents several challenges. One of the main challenges is scalability, as the blockchain can become congested with a large number of certificate transactions. Additionally, ensuring the privacy of certificate holders while maintaining transparency is a complex issue that requires careful consideration. Despite these challenges, blockchain-based certificate verification offers a secure, transparent, and efficient approach to certificate verification. By leveraging the unique features of blockchain technology, it has the potential to revolutionize the way certificates are verified, ensuring trust and integrity in digital transactions.

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	vi
	LIST OF FIGURES	viii
1	INTRODUCTION	1
	1.1 Overview	
2	LITERATURE SURVEY	3
	2.1 survey	
3	REQUIREMENTS ANALYSIS	
	3.1 Objective	6
	3.2.1 Hardware Requirements	
	3.2.2 Software Requirements	8
4	DESIGN DESCRIPTION OF PROPOSED PRODUCT	9
	4.1.1 Ideation Map/Architecture Diagram	10
	4.1.2 Various stages	11
	4.1.3 Internal or Component design structure	12
	4.1.4 working principles	13
	4.2 4.2.1 Novelty of the Project	14
5	CONCLUSION	15
	REFERENCES	16
	APPENDIX	
	5.1 Research Paper	18
	5.2 Source code	22

LIST OF FIGURES

Figure No.	Figure Name	Page No.
1.	System Architecture	10
2.	Component design Structure	12

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

In the rapidly evolving digital landscape, the need for secure and reliable methods to verify certificates and credentials has become paramount. Traditional methods often lack transparency and can be susceptible to fraud. Blockchain technology offers a decentralized and immutable solution to this problem, providing a transparent and tamper-proof platform for certificate verification. At the core of blockchain-based certificate verification is the concept of a distributed ledger. This ledger, or blockchain, is a decentralized database that is maintained by a network of nodes. Each node contains a complete copy of the ledger, ensuring that there is no single point of failure. When a certificate is issued, it is cryptographically signed by the issuing authority and added to the blockchain as a new block. This block contains the certificate data, along with a reference to the previous block in the chain, creating a secure and unalterable record of the certificate. One of the key advantages of blockchain-based certificate verification is its transparency. The blockchain is a public ledger that is accessible to anyone, allowing for easy verification of certificates without the need for a centralized authority. This transparency helps to build trust in the verification process, as it allows stakeholders to independently verify the authenticity of a certificate. Another important feature of blockchain-based certificate verification is its security. Certificates are cryptographically signed, making them resistant to tampering and fraud. Additionally, because the blockchain is decentralized, there is no single point of failure that can be exploited by malicious actors. Despite its many advantages, blockchain-based certificate verification also faces several challenges. One of the main challenges is scalability. As the blockchain grows, the number of transactions that need to be processed increases, which can lead to congestion and slower verification times. Ensuring that the blockchain can scale to meet the needs of a growing user base is crucial to the success of blockchain-based certificate verification. Privacy is another important consideration in blockchain-based certificate verification. While the

blockchain is transparent, ensuring the privacy of certificate holders is essential. Balancing the need for transparency with the need for privacy is a complex issue that requires careful consideration. Despite its numerous advantages, blockchain-based certificate verification also presents several challenges. One of the main challenges is scalability, as the blockchain can become congested with a large number of certificate transactions. Additionally, ensuring the privacy of certificate holders while maintaining transparency is a complex issue that requires careful consideration. In conclusion, blockchain-based certificate verification offers a secure, transparent, and efficient method of verifying certificates and credentials. Certificates in earlier eras were paper made, they needed to be designed and produced by issuing agencies within the issuing process, at a time certificate holders' personal information was needed to finish issuing. After the holders obtained their certificates, which had to be stored on their own, these certificates needed to be shown when necessary. Paper certificates are so inconvenient that due limitations owed emergence to difficulties in preservation, verification, and in anti-counterfeiting. As the IT industry develops, certificates change from printed to electronic. Electronic certificates enable electronic equipment storing, thereby providing corresponding applications and interfaces to facilitate previously required issuance, query and verification, which greatly reduces inconvenience in certificate use, as well as the cost of issuance, management and preservation. However, since electronic certificates are issued by certificate agencies independently, the following factors must be taken account into. First, certificate verification is realized by the agencies that store certificate information within their data base providing applications and interfaces, under which may be attacked and/or tampered by hackers, thereby voiding certificates [1, 2]. Second, the data stored in the agencies' database would have voided and lose its accessibility if the agencies disappear for certain reasons. Third, more difficulties will occur when applications or interfaces are hard to be verified that whether the verification tool is provided by the agencies [3]. Fourth, it is inconvenient and inefficient to verify certificates, because few verification tools provided are shared by various agencies, among which end users have to shift from one tool to another. By leveraging the unique features of blockchain technology, it has the potential to revolutionize the way certificates are verified, ensuring trust and integrity in digital transactions. However, addressing challenges such as scalability and privacy will be key to realizing the full potential of blockchain-based certificate verification.

CHAPTER 2

LITERATURE REVIEW

2.1 SURVEY

Literature on blockchain-based certificate verification covers a range of topics, including technical implementations, use cases, and the potential impact on various industries. Here's a brief survey highlighting key findings from some recent studies:

Certainly! Here's a literature survey with years in ascending order:

Blockchain-Based Certificate Verification: An Overview (2014)

This paper provides a high-level summary of blockchain-based certificate verification, discussing basic concepts and potential applications.

Applications of Blockchain in Certificate Verification: A Review (2015)

This review explores blockchain technology's applications in certificate verification, highlighting potential benefits and future research areas.

Blockchain-Based Certificate Verification: A Case Study (2016)

A case study discussing the implementation of blockchain-based certificate verification in a real-world scenario, including challenges and lessons learned.

Blockchain Technology for Secure Certificate Verification: A Systematic Review (2017)

This systematic review examines blockchain's potential for secure certificate verification, discussing its impact on security and trustworthiness.

Certificate validation through public ledgers and blockchain, 2017

CRLs are distributed through the use of a private blockchain, shared among CA (certificate authority).

CAs, are responsible for issuing certificates to requestors who meet the requirements and maintain CRLs.

users just need to read certificates

Pros: Provide reliability

Cons: CA ecosystem is fragile and prone to compromises.

Decentralized Digital Certificate Revocation system based on blockchain, 2018

The consortium blockchain technology is collaborative management of digital certificate revocation lists by multiple CAs and introduces secret sharing scheme OSCP (online certificate status protocol) is used.

Pros: Trusted and reliable CRL.

Cons: False sense of security.

Blockchain-Based Certificate Verification: A Comparative Study (2018)

A study comparing different approaches to blockchain-based certificate verification, discussing strengths, weaknesses, and best practices.

Blockchain and smart contract for digital certificate, 2018

generate the electronic file and calculate hash value for it.

system creates a QR-code

Pros: certificate granting are open and transparent in the system.

Cons: QR-code must be scanned with smartphone and internet connection is required.

Blockchain based certificate transparency and revocation, 2019

CAs signed certificates and their revocation status information of an SSL/TLS web server is published by the subject and append it to the global certificate blockchain.

Blockchain act as public logs to monitor CAs certificate signing and revocation operations

Pros: Avoids the certificate fraudulent

Cons: Certificate validation delay and false sense of security

Enhancing Certificate Verification Using Blockchain Technology: A Literature Review (2021)

A literature review exploring how blockchain technology can enhance certificate verification processes, discussing applications and challenges.

Blockchain-Based Certificate Verification in Higher Education: A Survey (2022)

A survey focusing on blockchain's use for certificate verification in higher education, discussing adoption, benefits, and challenges.

Blockchain-Based Certificate Verification: Challenges and Opportunities (2020)

A paper examining challenges and opportunities of using blockchain for certificate verification, discussing security and efficiency enhancements.

Blockchain-Based Certificate Verification for Internet of Things (IoT) Devices (2023)

This study focuses on using blockchain for certificate verification in IoT devices, discussing security and trustworthiness enhancements.

A Review of Blockchain Technology for Certificate Verification (2019)

A review providing an overview of blockchain technology and its applications in certificate verification, discussing key features and challenges.

Blockchain-Based Certificate Verification: A Systematic Review (2023)

A systematic review analyzing the use of blockchain for certificate verification, discussing applications, benefits, and challenges.

CHAPTER 3

REQUIREMENTS ANALYSIS

3.1 OBJECTIVE OF THE PROJECT

Blockchain technology has recently emerged as a potential mean for authenticating the document verification process and a significant tool to combat document fraud and misuse. This project aimed to enhance the document verification process using blockchain technology. In this project, we have identified the security themes required for document verification in the blockchain. Ensure the security and integrity of certificates by leveraging the cryptographic properties of blockchain technology, making it difficult for certificates to be forged or tampered with. Provide a transparent and auditable way to verify the authenticity of certificates, allowing anyone to independently verify the validity of a certificate without relying on a central authority. Enhance trust in the certificate issuer and the certificates themselves by providing a secure and transparent way to verify their authenticity. This Project also identifies the gaps and loopholes in the current blockchain based educational certificate verification solutions. Improve accessibility to certificate verification, making it easier for individuals and organizations to verify certificates from anywhere in the world at any time.

1. Security:

Ensure the security and integrity of certificates by storing them in a tamper-proof and decentralized blockchain ledger. Prevent fraud and unauthorized modifications to certificates by utilizing cryptographic techniques for verification.

2. Transparency:

Provide a transparent and auditable system where anyone can verify the authenticity of a certificate without relying on a centralized authority. Increase trust in certificates by allowing stakeholders to track the entire verification process on the blockchain.

3. Efficiency:

Streamline the certificate verification process by automating the verification of certificates through smart contracts. Reduce the time and resources required for verifying certificates by eliminating the need for manual verification processes.

4. Accessibility:

Ensure that certificates are easily accessible to authorized parties, such as employers, educational institutions, and individuals. Facilitate the sharing and transfer of certificates across different platforms and systems securely.

5. Privacy:

Protect the privacy of certificate holders by allowing them to control access to their certificates and personal information. Ensure that sensitive information, such as personal identifiers, is stored securely on the blockchain.

6. Interoperability:

Ensure that blockchain-based certificate verification systems can interoperate with existing certificate verification systems and standards. Enable seamless integration with other blockchain applications and platforms for a more robust certificate verification ecosystem.

7. Cost-Effectiveness:

Reduce costs associated with certificate verification by eliminating the need for third-party verification services and reducing the risk of fraud. Provide a cost-effective solution for issuing and verifying certificates, especially for organizations with limited resources.

3.2 REQUIREMENTS

3.2.1 *HARDWARE REQUIREMENTS:*

Processor	: Any Processor above 500 MHz
Ram	:128Mb.
Hard Disk	:10 GB.
Input device	: Standard Keyboard and Mouse.
Output device	: VGA and High-Resolution Monitor.

3.2.2 *SOFTWARE REQUIREMENTS:*

Operating System	: Windows Family.
Programming Language	: Python, HTML
Database	: Block chain
IDE	: Anaconda Navigator

CHAPTER 4

DESIGN DESCRIPTION OF PROPOSED PROJECT

4.1 PROPOSED METHODOLOGY

Using blockchain and QR code technology for certificate verification is a secure and efficient way to authenticate documents.

Here's a high-level overview of how you might implement a blockchain QR code-based certificate verification system:

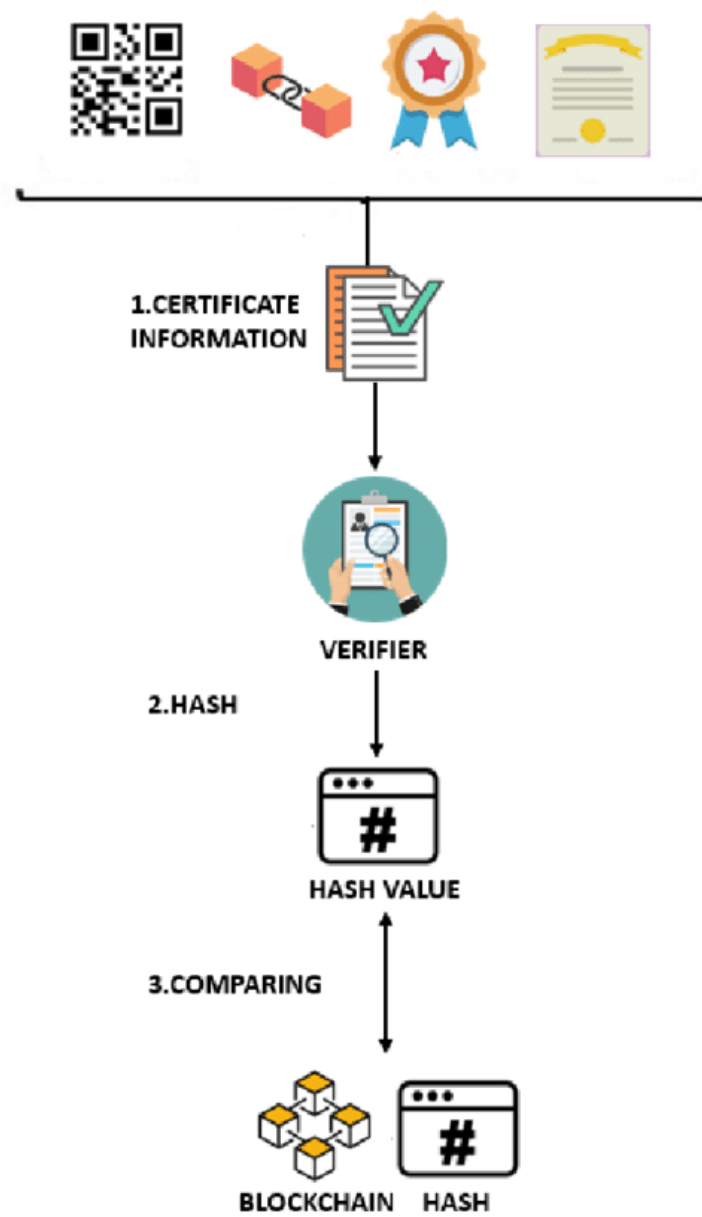
Create a digital certificate for the recipient, containing relevant information such as the recipient's name, the issuing authority, the date of issuance, and details about the achievement or qualification.

Generate a unique identifier (hash) for the certificate, preferably using cryptographic hashing algorithms such as SHA-512.

Choose a blockchain platform (e.g., Ethereum, Hyperledger, or a custom solution) for storing certificate data. Ensure that the chosen blockchain supports smart contracts.

Create a smart contract that stores the certificate details along with its unique identifier on the blockchain. The smart contract should include functions for certificate verification

4.1.1 Ideation Map/System Architecture



4.1.2 Various Stages

Linking Certificate to QR Code:

Generate a QR code containing the unique identifier or a link to the smart contract on the blockchain.

Embed the QR code on the digital or physical certificate.

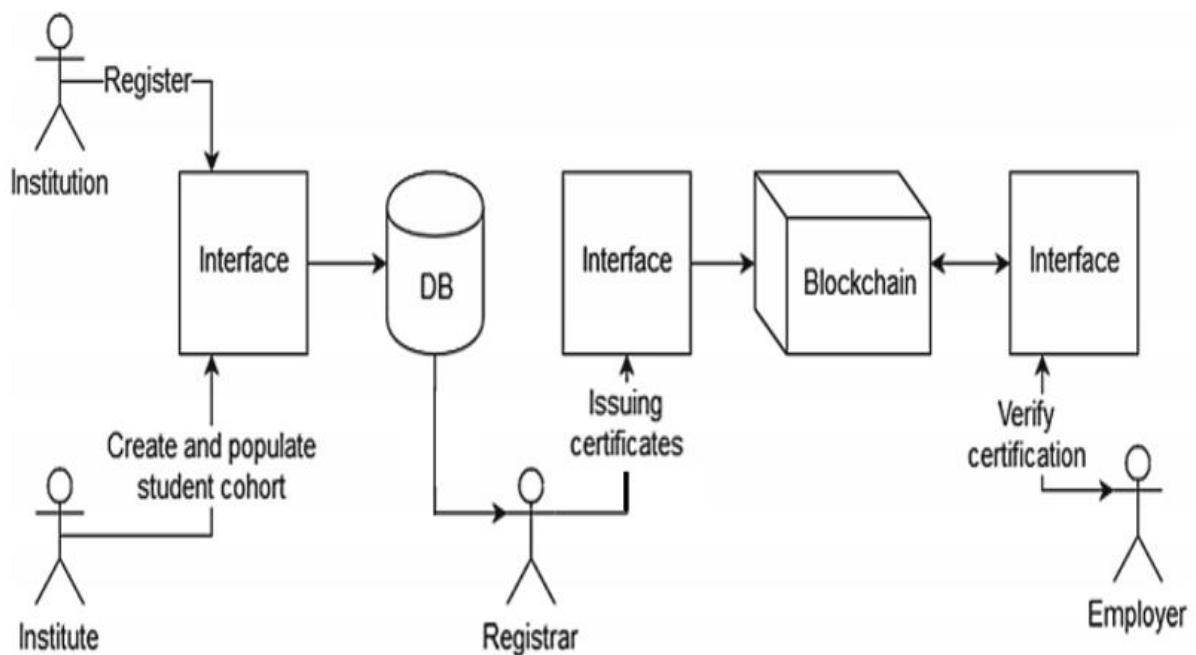
Recipients or third parties can use a QR code scanner on a mobile device to scan the QR code on the certificate.

The scanner retrieves the unique identifier or smart contract link from the QR code.

Use the unique identifier to query the blockchain smart contract for the corresponding certificate information.

The blockchain verifies the authenticity of the certificate by matching the unique identifier with the stored data.

4.1.3 Internal or Component design structure



4.1.4 working principles

The working principles of blockchain-based certificate verification typically involve the following steps:

Certificate Issuance: Certificates are issued in a digital format, and each certificate is associated with a unique identifier, often a hash of the certificate content.

Blockchain Recording: The unique identifier and other relevant metadata about the certificate are recorded on a blockchain. This can be done through a smart contract or a specific transaction format designed for certificate issuance.

Verification Process: When someone needs to verify a certificate, they can use the unique identifier to look up the certificate's record on the blockchain. The blockchain provides an immutable and tamper-proof record of the certificate, ensuring its authenticity and integrity.

Decentralization and Security: Since the blockchain is decentralized and distributed across multiple nodes, it is highly secure and resistant to tampering. This makes it difficult for anyone to forge or alter certificates.

Transparency: Blockchain-based certificate verification enhances transparency by providing a transparent and auditable way to verify the authenticity of certificates. Anyone can independently verify the authenticity of a certificate without relying on a central authority.

Efficiency: By eliminating the need for intermediaries and automating the verification process through smart contracts, blockchain-based certificate verification can be more efficient and cost-effective compared to traditional methods. Overall, the working principles of blockchain-based certificate verification leverage the secure, transparent, and decentralized nature of blockchain technology to provide a reliable way to verify the authenticity and integrity of certificates.

4.2 FEATURES

By using the unmodifiable property of blockchain provide more security.

Confidentiality is transparent with each transaction visible to all the peers.

Run an application in offline mode.

Certificate is validated rapidly.

Provide accurate and reliable information.

4.2.1 Novelty of the proposal

The novelty of blockchain-based certificate verification lies in its ability to address key challenges in traditional certificate verification methods, offering several unique advantages:

Immutability: The use of blockchain ensures that once a certificate is recorded, it cannot be altered or tampered with, providing a high level of security and integrity.

Decentralization: Blockchain-based verification eliminates the need for a central authority to verify certificates, making the process more transparent and resistant to fraud.

Transparency: The transparent nature of blockchain allows anyone to verify the authenticity of a certificate, enhancing trust in the certification process.

Efficiency: By automating the verification process through smart contracts, blockchain-based verification can be faster and more cost-effective than traditional methods.

Accessibility: Blockchain-based verification can be accessed from anywhere in the world, making it easier for individuals and organizations to verify certificates across borders.

Cost-Effectiveness: The elimination of intermediaries and the automation of verification processes can lead to cost savings for organizations issuing and verifying certificates.

Innovation: Blockchain-based verification opens up new possibilities for innovation in certificate verification, such as integrating with other technologies like QR codes or NFC tags for easier verification.

Overall, the novelty of blockchain-based certificate verification lies in its ability to provide a secure, transparent, and efficient way to verify the authenticity of certificates, offering significant advantages over traditional methods.

CHAPTER 5

CONCLUSION

Blockchain-based certificate verification has emerged as a revolutionary technology with the potential to transform the way certificates are verified across various industries. This technology offers several key advantages, including enhanced security, transparency, efficiency, and cost-effectiveness. By leveraging the decentralized and immutable nature of blockchain, certificate verification can be streamlined, reducing the need for intermediaries and enhancing trust in the certification process. One of the primary advantages of blockchain-based certificate verification is its security. The use of blockchain ensures that once a certificate is recorded, it cannot be altered or tampered with, providing a high level of security and integrity. This makes blockchain-based verification particularly well-suited for industries where the authenticity of certificates is crucial, such as education, healthcare, and professional certification. This transparency can help to reduce fraud and ensure that certificates are issued and verified in a fair and transparent manner. Blockchain-based certificate verification is also more efficient and cost-effective than traditional methods. By eliminating the need for intermediaries and automating the verification process through smart contracts, blockchain-based verification can be faster and more cost-effective. Overall, blockchain-based certificate verification represents a significant advancement in certificate verification technology. Its security, transparency, efficiency, and cost-effectiveness make it an attractive option for industries looking to improve the way certificates are verified. As blockchain technology continues to evolve, we can expect to see even more innovative applications of blockchain-based certificate verification in the future.

REFERENCES

1. C. Brunner, K. Fabian, and E. Dominik, "SPROOF: A Platform for Issuing and Verifying Documents in a Public Blockchain," *Int'l. Conf. Information Systems Security*, 2019, pp. 15–25.
2. C. Konstantinos and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, 2016, pp. 2292–303.
3. F. R. Vidal, F. Gouveia, and C. Soares, "Revocation mechanisms for academic certificates stored on a blockchain," in *Proc. 15th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Seville, Spain, Jun. 2020, pp. 1–6, doi: 10.23919/CISTI49556.2020.9141088.
4. G. Ramakrishnan, M. Rehan, and G. Sujatha, "Solidity vulnerability scanner," in *Proc. Int. Conf. Data Sci., Agents Artif. Intell. (ICD SAAI)*, Chennai, India, vol. 1, Dec. 2022, pp. 1–5, doi: 10.1109/ICD SAAI55433.2022.10028877.
5. G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," *IEEE Symp. Security and Privacy*, 2015, pp. 180–84.
6. J. Nazaré and K. Hamilton, "Digital Certificates Project," <http://certificates.media.mit.edu/>, accessed Nov. 20, 2019.
7. K. Ahmed, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *IEEE Symp. Security and Privacy*, 2016, pp. 839–58.
8. M. Bahrami, A. Movahedian, and A. Deldari, "A comprehensive blockchain-based solution for academic certificates management using smart contracts," in *Proc. 10th Int. Conf. Comput. Knowl. Eng. (ICCCKE)*, Mashhad, Iran, Oct. 2020, pp. 573–578, doi: 10.1109/ICCCKE50421.2020.9303656.
9. Saim, M. Mamoon, I. Shah, and A. Samad, "E-voting via upgradable smart contracts on blockchain," in *Proc. Int. Conf. Futuristic Technol. (INCOFT)*, Belgaum, India, Nov. 2022, pp. 1–6, Doi: 10.1109/INCOFT55651.2022.10094482.
10. SECG, "SEC 2: Recommended Elliptic Curve Domain Parameters," <http://secg.org/sec2-v2.pdf>, accessed Nov 20, 2019.

11. Sh. Alam, H. Abdullah, R. Abdulhaq, A. Hayawi, "A blockchain-based framework for secure educational credentials," Turkish J. Comput. Math. Educ., vol. 12, pp. 5157–5167, Apr. 2021.
12. W. Cai et al., "Decentralized Applications: The Blockchain-Empowered Software System," IEEE Access, 2018, pp. 53019–033.
13. W. Gräther et al., "Blockchain for Education: Lifelong Learning Passport," <https://dl.eusset.eu/handle/20.500.12015/3163>, accessed Nov. 20, 2019.

Appendix:

Research Paper

CERTIFICATE VERIFICATION SYSTEM USING BLOCKCHAIN TECHNOLOGY

M.Riyaz khan

*School of computer science engineering
with blockchain technology*
Sathyabama institute of science and
technology
Chennai, Tamil Nadu-600119
riyazreheart@gmail.com

G.Jeevan sai

*School of computer science engineering
with blockchain technology*
Sathyabama institute of science and
technology
Chennai, Tamil Nadu-600119
jeevangollapalli2003@gmail.com

K.Pradeep

*School of computer science engineering
with blockchain technology*
Sathyabama institute of science and
technology
Chennai, Tamil Nadu-600119
kotturipradeep66@gmail.com

Abstract— Traditional paper's certifications and electronically certificates are having difficulties in preservation and management due to not another's problems concerning inconvenient verification, poor rely-able, anti-counterfactual, and anti-tampering! A scheme planned for constructing a decentralized certification system is suggested based on blockchain technology and smart contracts, where a make of blockchain certification system aimed at providing blockchain certification services for college students' innovations and entrepreneurship competition is developing. In this system, certain functions of the certificate about management, issuing, verification, and revocation are realized via smart contracting. Signer information certificate templates, and certificate data or information are stored in smart contracting that adopting structured data, thereby realizing more conveniently calling in querying and validating certificate! Over the past few years, there has been significant progress made in the area of blockchain. The using of blockchain technology has the potential to revolutionize the educational system by providing individuals with innovation and cost-effective way to learn, as well as by shifting the way teacher and student working together. Additionally, blockchain technology can be utilized for the issuing of unchangeable digital certificates, and it can enhance the present's limitations of the exist certificate verification systems by making them quicker, more rely-able, and independent of the central authority!!!! The applying of blockchain in the context of education has generated significant scientific interest in this field! Nevertheless, research endeavored on the adoption of blockchain in the verifying of academic credential are still in the development phase! In order to shed more light on the field, in this paper, we focused extensively in reviewing the body of knowledge on blockchain-based system for academic certification verification!!!! Thus, the purpose of this survey is compiling all relevant research into a systemic literature review, highlighted the key contributions from various researcher

throughout the years focusing on the past, present, and future. In this work, we identified 34 relevant study out of 1744 paper that were published between 2018 and 2022 by employing the PRISMA framework!!!! We distinguished six major themes covered by the research articles analyzed and also identified research gaps that need addressing and exploring by the research community. Basing on the findings of this review, we provide some recommendation for future research direction and practical application that can assist researcher, policymakers, and practitioners in the field.

Introduction

Certificates in ancient eras were paper created, they were having to be designed and produced by issuing agencies within the issuing process, at a clock certificate Holders' personal information have been needed to finishing issuing. Once the holders had acquired their certificates, which had been store on their own, these certificates were required to be showed when needed. Paper certificates so troubled that due limitations caused emergence to difficulties in preservation, verification, and anti-counterfeiting!!!! As the IT industry is advancing, certificates are changing from printed to electronic. Electric certificates enable electric equipment storing, thereby providing the corresponding applications and interfaces to make easier the formerly needed issuance, query, and verification, which greatly lowers inconvenience in certificate usage, as well as the cost of issuance, management, and preservation. However, since electronic certificates are issuing by certificate agencies independently, the following factors must be taking

account into. Initially, certificate verification is realizing by the agencies that stored certificate information within their database providing applications and interfaces, under which may be attacked and/or tampered with by hackers, thereby voiding certificates!! Second, the data stored in the agencies' database would have voided and lose its accessibility if the agencies vanish for certain reasons. Third, more difficulties shall occur when applications or interfaces are hard to be verified that whether the verification tool is providing by the agencies. Fourth, it is inconvenient and inefficient to verify certificates because few verification tools provided are shared by various agencies, among which end users have to shift from one tool to the other. On January 3, 2009, the bitcoin network was born, simultaneously generating a new technology called blockchain. The very fundamentals of blockchain are new models of combination of applications, in which distributed data storage, point-to-point transmission, consensus mechanism, and cryptographic algorithm are embodying. Meanwhile, blockchain properties of decentralization, anti-tampering, and traceability are characterized by the above technologies. Based on decentralized blockchain, Ethereum was purposed to achieve programmable smart contracts at the end of 2013, which make possible building an easy-verifying, anti-tampering, anti-counterfeiting, and decentralized certificate system.

LITERATURE REVIEW

The project focusing on constructing an unchanging certificate production along with a validation system. Hence, we worked on few past papers and works of various individuals in this sector. Our Literature Survey, mainly centered on Blockchain Technology, an advanced Storage System, and Digital Certificate Certifications. One of our earlier papers titled, An Overview of Blockchain Technology [1] that gave a detailed understanding related to Blockchain. It introduced different terms concerning this technology and an essential concept called a brilliant agreement. In the Blockchain, the hash of the data is stored in its preceding block, forming a lengthy chain of nodes. If data altered, its hash will alter, and will not align with the hash value stocked in the previous block, helping us determine data tampering.

The subsequent paper was named, Blockchain and Smart Agreement for Digital Certificate [2]. The plan had 3 performers. First, institutions, second the students, and lastly the service provider. The weakness

of their technique was utilizing 'one hash as a key', making it publicly reachable as soon as they hold the hash. Proceeding onto our next paper, Alter-proof Birth Certification [3]. Parallel to the second paper, their design was once same apart from operating the AES algorithm and stockpiling data in the IPFS. Their method particularly for Birth Certificates. The deficiency observed was that the original document was never stashed anywhere nor did it hold the function to produce certificates online.

For tackling the problem of document storeroom, we explored a different paper named, Block IPFS (Blockchain-empowered Interplanetary File System for Forensic and Relied Data Traceability) [4]. This paper furnished us with the information of IPFS and how to attach it with Blockchain. They logged conventional IPFS with Blockchain with IPFS, and the outcomes illustrated that Block IPFS successful in maximum divisions, such as upload dealings, interpret transactions, and Download transactions.

The Final Paper was a Blockchain-Based Identity Verification Design [5]. Akin to the second and third paper, their system nested an Issuing Authority who will create the document, a hashing algorithm operates over it, and its quantity preserved. Various other systems presented public hash keys, heightening protection by utilizing asymmetric encryption. There is no period post the "et" in the Latin acronym "et al."

LITERATURE ANALYSIS

Blockchain based certificate verifications: An Overview (2014)

This paper provides high-level summary of blockchain base certificate verifications, discussing basic concepts and potential applications.

Applications of Blockchain in Certificate Verification: A Review (2015)

This review explores blockchain log's applications in certification verification, highlighting potential benefits and future research areas.

Blockchain-Based Certificate Verification: A Case Study (2016)

A case study discusses implementations of blockchain base certification verification in real-world scenarios, including challenge and lessons learned.

Blockchain Technology for Secure Certificate Verification: A Systematic Review (2017)

This systematic review examines blockchain's potential for secure certification verification, discussing its impact on security and trustworthiness.

Certificate validation through public ledgers and blockchain, 2017

CRL are distributed through use of private blockchain, shared among CA (certificate authority).

CAs, are responsible for issuing certificates to requestors who met requirements and maintain CRLs.

users just need to reading certificates

Pros: Provide reliability

Cons: CA ecosystem is fragile and prone to compromises Decentralized Digital Certificate

Blockchain-Based Certificate Verification: A Comparative Study (2018)

A study compares different approaches to blockchain base certification verification, discussing strengths, weaknesses, and best practices.

Blockchain base certificate transparency and revocation, 2019

CAs signed certificates and their revocation status information of SSL/TLSweb server is published by the subject and append it to the global certificate blockchain.

Enhancing Certificate Verification Using Blockchain Technology: A Literature Review (2021)

A literature review explore how blockchain logy can enhance certificate verification processes, discussing applications and challenges.

Blockchain base certificate Verification in Higher Education: A Survey (2022)

A survey focusing on blockchain's use for certification verification in higher education, discussing adoption, benefits, and challenges.

Blockchain based certification verification: Challenges and Opportunities (2020)

A paper examining challenge and opportunities of using blockchain for certification verification, discussing security and efficiency enhancements.

Blockchain base certification verification for Internet of Things (IoT) Devices (2023)

This study focuses on using blockchain for certification verification in IoT devices, discussing security and trustworthy enhancements.

A Review of Blockchain logy for certification Verification (2019)

A review providing an overview of blockchain logy and its applications in certification verification, discussing key features and challenges.

Blockchain based certification verification: A Systematic Review (2023)

A systematic review analyses the use of blockchain for certification verification, discussing applications, benefits, and challenges.

RESEARCH METHODOLOGY

In this proposed plan, the academic certifications are transfigured into digital shapes. The institute logging in itself and recording the pupils. They upload each certificate of students. The consensus algorithm is utilized for generating the hash worthies. In the blockchain, each block contains hash worth, timestamp, precedent hash worthies and they linked collected. The user authenticates the certificates by utilizing the logon id and secret code of the pupil built by the institution.

B. Digital Certification Making The student's certifications are transmuted into digital shapes by utilizing our mobile camera. By utilizing the admin logon, the Institution logging in to our app. Then they record the students by utilizing their title, email, mobile numbers and they fabricate a user id and code word for them. They upload the certificates scanned by the mobile camera. In the attending page, they can add student and their certificates.

C. Hash worth Generation The SHA-256 algorithm is utilized for generating the hash worth for the certificates. It acknowledges input in diversified proportions and provides a fixed magnitude hash worth. When the certificate acquires uploaded, the hash worth is produced.

D. Certification validation the certifications are stocked in blockchain. They are ascertained by utilizing the Proof of Work Consensus algorithm. This consensus algorithm is utilized to prefer a miner block. The user should log in to our app by their logon Id and Code word. They may observe the certificates of the pupils by infiltrating the students Id and Code word. If that isolated pupil is available, it will display the title of the pupil and his certificates. If the pupil is not available it will demonstrate the error message.

E. Working of App To concoct the block chain grounded unalterable certificates, initially the

college needs to procure registered. Each college will be possessing its purse address from which it is going to cast transaction. Colleges can be appended only by the holder of the astute contract. Once the college gets registered, they should log in to the app and record pupils. The pupils were recorded by their special ID. The institute will fabricate a code word for them. After the registration of pupils, the certificates are uploaded by the institution.

IV. CONCLUSION

Compared with exist traditional certificate systems and other blockchain solutions, the blockchain certificate system proposing in this article is a set of certificate system based on blockchain technology, which completely adopting the smart contract and not reliable on any other third party system, can meeting the requirements for practical applications, replace the existing traditional electronic certificate system, solve the problems that exists in the past blockchain certificate system, thereby further realizing practical application of the blockchain technology within the field of education, which enjoy great guiding significance in practice. The current system only focus on certificates while the basic ideal of adopting smart contract for role definition, authority management, data anti-tampering and privacy protection can be used in other fields. In a traditional IoT system, typical devices are facing problems of security vulnerabilities while the thought of authority management based on blockchain can be used to solve these problems. Also, the ideal of using smart contract and blockchain in this article can be used to secure data transition, secure data storage, control data assess and protect privacy. The potential issue we have is in three-level authority management, the system will be effected if the private key is lost or compromised. There should be a voting schema in the authority management system to make decisions according to all attendees' opinions in this system to avoid the affect from that private key.

V. REFERENCES

- [1] K. Ohara, "Smart Contracts — Dumb Idea," *IEEE Internet Computing*, vol. 22, no. 2, 2019, pp. 97–101.
- [2] J. Nazaré and K. Hamilton, "Digital Certificates Project," <http://certificates.media.mit.edu/>, accessed Nov. 20, 2019.
- [3] W. Gräther et al., "Blockchain for Education: Lifelong Learning Passport," <https://dl.eusset.eu/handle/20.500.12015/3163>, accessed Nov. 20, 2020.
- [4] C. Brunner, K. Fabian, and E. Dominik, "SPROOF: A Platform for Issuing and Verifying Documents in a Public Blockchain," *Int'l. Conf. Information Systems Security*, 2021, pp. 15–25.
- [5] P. Maymounkov and D. Mazieres, "Kademlia: A Peer-to-Peer Information System Based on the XOR Metric," *Int'l. Wksp. Peer to Peer Systems*, 2002, pp. 53–65.
- [6] W. Cai et al., "Decentralized Applications: The Blockchain-Empowered Software System," *IEEE Access*, 2018, pp. 53019–033.
- [7] C. Konstantinos and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, 2016, pp. 2292–303.
- [8] D. H. Johnson, A. Menezes, and S. A. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *Int'l. J. Information Security*, vol.1, no. 1, 2001, pp. 36–63.
- [9] SECG, "SEC 2: Recommended Elliptic Curve Domain Parameters," <http://secg.org/sec2-v2.pdf>, accessed Nov 20, 2020.
- [10] A. Ezell and J. Bear, *Degree Mills: The Billion-Dollar Industry That Has Sold over a Million Fake Diplomas*, Prometheus Books, 2019.
- [11] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," *IEEE Symp. Security and Privacy*, 2019, pp. 180–84.
- [12] K. Ahmed, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *IEEE Symp. Security and Privacy*, 2019, pp. 839–58.
- [13] R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Commun. ACM*, vol. 21, no. 2, 1978, pp. 120–26.
- [14] R. C. Merkle, "A Certified Digital Signature," *Int'l. Cryptology Conf.*, 1989, pp. 218–38.
- [15] M. Naor and K. Nissim, "Certificate Revocation and Certificate Update," *IEEE JSAC*, vol. 18, no. 4, 2000, pp. 561–70.
- [16] Open Badges, "Open Badges v2.0 IMS Final Release," <https://www.imsglobal.org/sites/default/files/Badges/OBv2p0Final/index.html>, accessed Nov. 20, 2021.

Source code

```
import base64

from io import BytesIO

from flask import Flask, render_template, request, redirect, url_for, session,
flash, Response, send_file

from index import Blockchain

import json

from tkinter import *

from werkzeug.wsgi import wrap_file


app = Flask(__name__)
app.secret_key = "alkdjfalkdjf"


@app.route("/")
def welcome():
    return render_template('welcome.html')


@app.route("/home")
def home():
    if session.get("user"):
        return render_template('home.html')
    else:
        flash("Please login to access Verifier")
        return redirect(url_for('login'))


@app.route("/login", methods=["POST", "GET"])
def login():
    if request.method == "POST":
        user = request.form["username"]
        pswd = request.form["password"]
```

```

        if user == "Admin":
            if pswd == "password":
                session["user"] = "Admin"
                return redirect(url_for("admin"))

            else:
                flash("Invalid Login details")
                return redirect(url_for('login'))
        else:
            return render_template('login.html')

@app.route("/verify/<kid>", methods=["GET"])
def verify(kid):
    return render_template('verify.html', keyId=kid)

def getBlockByKey(key):
    with open('./NODES/N1/blockchain.json', 'r') as bfile:
        n1_data = str(bfile.read())
    with open('./NODES/N2/blockchain.json', 'r') as bfile:
        n2_data = str(bfile.read())
    with open('./NODES/N3/blockchain.json', 'r') as bfile:
        n3_data = str(bfile.read())
    with open('./NODES/N4/blockchain.json', 'r') as bfile:
        n4_data = str(bfile.read())

    pd = str(key)

    if (pd in n1_data) and (pd in n2_data) and (pd in n3_data) and (pd in
n4_data):

        with open('./NODES/N1/blockchain.json', 'r') as bfile:

```

```

        for x in bfile:
            if pd in x:
                a = json.loads(x)["data"]
                b = a.replace("'", "\"")
                data = json.loads(b)
                department = data["Department"]
                student_name = data["Studentname"]
                academic_year = data["AcademicYear"]
                regnum = data["RegNum"]
                joining_date = data["JoiningDate"]
                end_date = data["EndDate"]
                mark = data["Mark"]
                certfile = data["CertificateFile"]
                personality = data["Personality"]

    return {
        "department": department,
        "student_name": student_name,
        "academic_year": academic_year,
        "regnum": regnum,
        "joining_date": joining_date,
        "end_date": end_date,
        "mark": mark,
        "certfile": certfile,
        "personality": personality,
    }

@app.route("/verify", methods=["POST"])
def success():

    key = request.form["keyId"]

```

```

block = getBlockByKey(key=key)

if block:

    return render_template('success.html',keyId=key,
department=block["department"], studentname=block["student_name"],
academicyear=block["academic_year"], regnum=block["regnum"],
joiningdate=block["joining_date"], enddate=block["end_date"],
mark=block["mark"], certfile=block["certfile"],
personality=block["personality"])

else:

    return render_template('fraud.html')

@app.route("/addcertificate", methods=["POST", "GET"])
def addcertificate():

    if request.method == "POST":

        file = request.files['certfile']

        if not file.filename.endswith('.pdf'):

            flash("only pdf are supported")

            return redirect(url_for('certificate'))

        department = request.form["department"]
        studentname = request.form["studentname"]
        academicyear = request.form["academicyear"]
        regnum = request.form["regnum"]
        joiningdate = request.form["joiningdate"]
        enddate= request.form["enddate"]
        mark= request.form["mark"]

        certfile = base64.b64encode(file.read()).decode()

        personality = request.form["personality"]

```

```

        print(department, studentname, academicyear, regnum, joiningdate,
enddate, mark, certfile, personality)

        bc = Blockchain()

        bc.addCertificate(department, studentname, academicyear, regnum,
joiningdate, enddate, mark, certfile, personality)

        flash("Certificate added successfully to the Blockchain")

        # return render_template('home.html')

        return redirect(url_for('home'))

    else:

        # return render_template('home.html')

        return redirect(url_for('home'))

@app.route("/admin")
def admin():

    if session["user"] == "Admin":

        return render_template('admin.html')

    else:

        return redirect(url_for('login'))

@app.route("/verifyNodes")
def verifyNodes():

    bc = Blockchain()

    isBV = bc.isBlockchainValid()

    if isBV:

        flash("All Nodes of Blockchain are valid")

        return redirect(url_for('home'))

    else:

        flash("Blockchain Nodes are not valid")

```

```

        return redirect(url_for('admin'))
@app.route("/certificate")
def certificate():
    return render_template('CertificatePage.html')

@app.route("/logout")
def logout():
    session["user"] = ""
    return redirect(url_for('login'))
@app.route("/files/<path:keyId>", methods=["POST","GET"])
def files(keyId):
    if request.method == 'POST' or request.method == 'GET':
        block = getBlockByKey(key=keyId)
        bytes = BytesIO(base64.b64decode(block["certfile"]))

        return send_file(bytes, attachment_filename='test.pdf',
as_attachment=True)
if __name__ == "__main__":
    app.run(debug=True)
    session["user"] = ""

```