

Digital Certificate Verification using Blockchain

A Project Report submitted in partial fulfillment of the requirements for the award of the degree of

Bachelor of Technology

in

Computer Science and Engineering

by

Som Singh Lodhi (112115157)

Semester: IV



Name of Department: Department of Computer Science and Engineering

Indian Institute of Information And Technology, Pune

(An Institute of National Importance by an Act of Parliament)

APRIL 2023

BONAFIDE CERTIFICATE

This is to certify that the project report entitled “**Digital Certificate Verification using Blockchain** ” submitted by **Som Singh Lodhi** bearing the **MIS No: 112115157**, in completion of his project work is accepted for the project report submission in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in the **Department of Computer Science and Engineering**, Indian Institute of Information Technology, Pune (IIIT Pune), during the academic year **2022-23**.

Dr. Sanjeev Sharma

Head of the Department

Assistant Professor

Department of CSE

IIIT Pune

Project Viva-voce held on

26/04/2023

Undertaking for Plagiarism

I **Som Singh Lodhi** solemnly declare that research work presented in the **report/dissertation** titled **“Digital Certificate Verification using Blockchain”** is solely **my** research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete report/dissertation has been written by **me**. I understand the zero tolerance policy of **Indian Institute of Information Technology Pune** towards plagiarism. Therefore **I** declare that no portion of my **report/dissertation** has been plagiarized and any material used as reference is properly referred/cited. I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of the degree, the Institute reserves the rights to withdraw/revoke my **B.Tech** degree.

Som Singh Lodhi

Conflict of Interest

Manuscript title: Digital Certificate Verification using Blockchain

The authors whose names are listed immediately below certify that they have NO affiliations with or involvement in any organization or entity with any financial interest (such as honoraria; educational grants; participation in speakers' bureaus; membership, employment, consultancies, stock ownership, or other equity interest; and expert testimony or patent-licensing arrangements), or non-financial interest (such as personal or professional relationships, affiliations, knowledge or beliefs) in the subject matter or materials discussed in this manuscript.

Som Singh Lodhi

ACKNOWLEDGEMENT

This project would not have been possible without the help and cooperation of many. I would like to thank the people who helped me directly and indirectly in the completion of this project work.

First and foremost, I would like to express my gratitude to our honorable Director, **Prof. O.G. Kakde**, for providing his kind support in various aspects. I would like to express my gratitude to the **Head of Department, Dr. Sanjeev Sharma Department of CSE**, for providing his kind support in various aspects. I would also like to thank all the faculty members in the **Department of CSE** and my classmates for their steadfast and strong support and engagement with this project.

TABLE OF CONTENTS

Abstract	5
(i) List of Figures/Symbols/Nomenclature	6
1 Introduction	8
1.1 Overview of work	8
1.2 Motivation of work	8
1.3 Literature Review	9
1.4 Research Gap.	9
2 Problem Statement	
2.1 Research Objectives	10
2.2 Methodology of work	11-12
3 Analysis And Design	13
4 Results and Discussion	14
5 Conclusion and Future Scope	15
6 References	16

Abstract

One of the most important documents is certificates for graduates from universities and other educational institutions. A certificate is a certificate of qualification for a graduate that is used for a job or other matters relating. Advancement of IT and low cost and high quality office supplies on the marketplace have contributed to the development of essential documents such as certificates, identification cards and passports. However, it is costly and time consuming to check certificates using traditional methods.

The aim of this paper is to introduce a theoretical/small working model, which can give the possible solution for the issue and verification of digital certificates using blockchain based. There are many functions such as hash, digital signatures and work evidence in blockchain technology.

The models formulate a system divided into two principal Firstly, the system uses Python code to convert a digital certificate, of any format, into binary data. User information is then added to this binary data, which is used as input for the SHA 256 algorithm. This ensures that the data is secure and cannot be tampered with.

Secondly, the system involves adding this data to the node and incorporating it into the blockchain network on Corda. This is achieved through the use of smart contracts and consensus algorithms, which validate the authenticity of the certificate and ensure that it is added to the blockchain securely.

By incorporating these two principles, the proposed system aims to provide a reliable and efficient solution for digital certificate verification, preventing certificate fraud and ensuring that the qualifications of individuals are authenticated accurately. The use of blockchain technology offers several benefits, including the ability to create tamper-proof and transparent records that can be accessed and verified easily.

Keywords: Block,Blockchain,hash,sha256 algorithm,blockchain platform and smart contracts.

List of Figures

1. Figure 1 - Methodology of the Work
2. Figure 2 - Corda Blockchain platform
3. Figure 3 - CPU utilization of 2 nodes
4. Figure 4 - Flow chart of working model

Chapter 1

Introduction

1.1 Overview of Work

The aim of this project is to develop a digital certificate verification system using blockchain technology to address the challenges posed by certificate fraud. The system will use Python code to convert digital certificates into binary data and add user information to the data, which will then be hashed using the SHA 256 algorithm to ensure its security. The hash will be added to the blockchain network on Corda using smart contracts and consensus algorithms to validate the authenticity of the certificates and prevent tampering. The project's objectives include developing efficient and reliable software, testing the system's efficiency and reliability, and promoting its adoption among users. The use of blockchain technology offers several benefits, including creating tamper-proof and transparent records that can be accessed and verified easily. The project has the potential to revolutionize the way in which certificates are verified in various fields and to provide a solution to the challenges posed by digital certificate fraud.

1.2 Motivation of the Work

The motivation behind this project is to provide a solution to the challenges posed by digital certificate fraud, which has become a major problem in various fields such as education and employment. The traditional methods used for certificate verification are often costly, time-consuming, and susceptible to fraudulent activities. The proposed system aims to leverage the benefits of blockchain technology, such as tamper-proof and transparent records, to provide a reliable and efficient solution for digital certificate verification. The system will be designed to ensure the authenticity of certificates, prevent tampering and fraud, and promote transparency and accountability. By developing a digital certificate verification system using blockchain technology, the project seeks to improve the efficiency, accuracy, and security of certificate verification, thereby promoting trust and confidence in the certificates issued by educational institutions and other organizations.

1.3 Literature Review

Blockchain makes it easy to verify the authenticity of digital certificates by providing a seamless and convenient experience for certificate recipients and third-party verifiers. Anyone can access the certificate using a link or QR code, eliminating the need to contact the issuer for verification 1. The review would also cover the benefits of using blockchain technology for digital certificate verification, such as increased security, traceability and authenticity of the certificates. It would also discuss the challenges and limitations of traditional methods of certificate verification and how blockchain technology can address these issues.

There has been a lot of work done in the field of digital certificate verification using blockchain technology. Several companies have developed solutions for generating and verifying digital certificates using blockchain technology. For example, Certi is a company that offers a certificate generator using blockchain to store and process certificates which are more secure to store and issue as well as easier and cost-effective to audit and reconcile.

1.4 Research Gap

While the three papers explore the use of blockchain technology for authentication purposes in different fields, there is a need for further research on the scalability and interoperability of blockchain-based systems. As the use of blockchain technology continues to grow, it becomes increasingly important to ensure that these systems can handle a large volume of data and transactions and can work seamlessly with other systems. Therefore, future studies can focus on evaluating the performance and scalability of blockchain-based systems, particularly in contexts where there is a high volume of data, such as in healthcare or education. Additionally, research can explore ways to integrate blockchain with other technologies to ensure interoperability and seamless data exchange, which can be critical for the adoption and success of blockchain-based systems in practice.

Additionally, there may be legal and regulatory challenges in using blockchain technology for this purpose, particularly in industries where digital certificates are subject to strict standards and regulations.

Chapter 2

Problem Statement

Digital certificates are widely used to verify the identity, qualifications, and achievements of individuals and organizations. However, traditional methods of issuing and verifying digital certificates have several limitations and challenges. These methods can be time-consuming, costly, and prone to errors and fraud. As a result, there is a need for a more secure, efficient, and reliable method of verifying the authenticity of digital certificates.

Blockchain technology has shown promise in addressing these challenges by providing a decentralized and tamper-proof ledger for storing and verifying digital certificates. However, there are still several technical, legal, and regulatory challenges that need to be addressed in order to fully realize the potential of blockchain technology for digital certificate verification. The goal of this research is to explore the potential of blockchain technology for improving the verification of digital certificates and to identify and address the challenges and limitations of using this technology for this purpose.

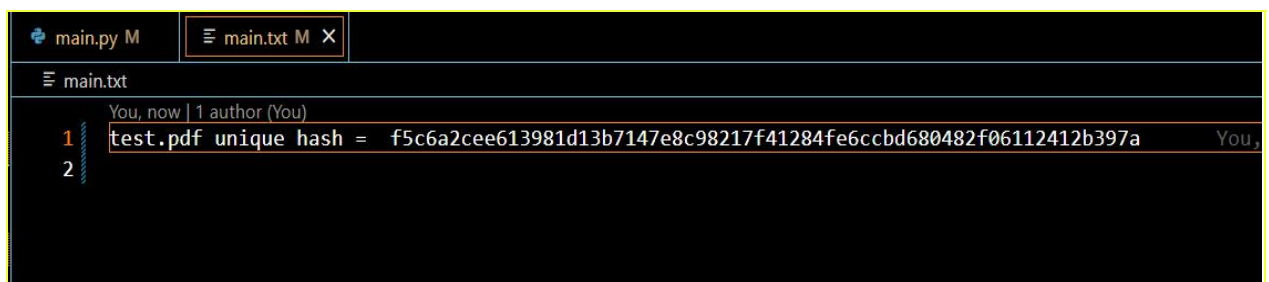
2.1. Research Objectives

- Ensuring the authenticity and validity of certificates
- Streamlining the verification process
- Enhancing security and reducing fraud

2.2. Methodology of the Work

1. user upload file which is read as binary data by python program

```
You, 9 minutes ago | 1 author (You)
1  import hashlib
2  name = input("what is you name : ")
3  age = input("what is you age : ")
4  _ = name+age
5  print(_)
6  _ = _.encode()
7  print(_)
8  with open('test.pdf','rb') as obj:
9      data = obj.read()
10     data+=_
11     print(data)
12     # print(data)
13     hash_value = hashlib.sha256(data).hexdigest()
14     print(hash_value)
15
16     with open('main.txt','w') as obj:
17         obj.write(f"test.pdf unique hash = {hash_value}")
18         obj.write('\n')
19
20
```



```
main.py M  main.txt M X
main.txt
You, now | 1 author (You)
1  test.pdf unique hash = f5c6a2cee613981d13b7147e8c98217f41284fe6ccbd680482f06112412b397a You,
2
```

```

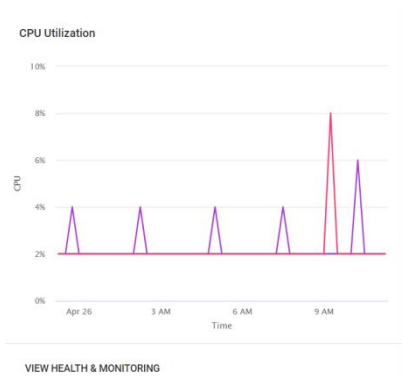
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL GITLENS
PS C:\Users\somsi\http\sha_256> python -u "c:\Users\somsi\http\sha_256\main.py"
what is you name : som singh lodhi
what is you age : 21
som singh lodhi21
b'som singh lodhi21'
b'%PDF-1.7\n%  

b'x2\x9b\n\x15\x0c\x8d\xcc\x07\x14\xcc\x00\x03\x05SK\x03\x87\x13#\x90\x92@\x10\xcb\x18\x
\nendobj\n48 0 obj\n<</Length 49 0 R/Filter /FlateDecode>>\nstream\n\x9c+T0\xd03T0\x00A(\x9d\x9c
8\x1f\x05\x00\xde\x9a\t\xd2endstream\nendobj\n49 0 obj\n41\nendobj\n56 0 obj\n<</Length 57 0 R/Filter
x9c\xcb\xa5\x1fd\xa1\x90^\x0c\xa4-\x15\\\xf2\x81\xb4\x891\x88\x1f\x05\x00\xdf\x12\t\xdaendst
0 R/Filter /FlateDecode>>\nstream\n\x9c+T0\xd03T0\x00A(\x9d\x9c\xcb\xa5\x1fd\xa1\x90^\x0c\xa4\xcc
xd9endstream\nendobj\n65 0 obj\n41\nendobj\n72 0 obj\n<</Length 73 0 R/Filter /FlateDecode>>\nstream
c\xa4\xcc\xcd\x14\\\xf2\x81\xb4\x891\x88\x1f\x05\x00\xdf\x05\t\xd9endstream\nendobj\n73 0 obj
e>\nstream\n\x9c+T0\xd03T0\x00A(\x9d\x9c\xcb\xa5\x1fd\xa1\x90^\x0c\xa2\x15\\\xf2\x81\xb4\x891\
j\n40\nendobj\n90 0 obj\n<</Length 91 0 R/Filter /FlateDecode>>\nstream\n\x9c+T0\xd03T0\x00A(\x9d
1\x88\x1f\x05\x00\xdf\x07\t\xd9endstream\nendobj\n91 0 obj\n41\nendobj\n99 0 obj\n<</Length 10
\x9d\x9c\xcb\xa5\x1fd\xa1\x90^\x0c\xa4\x0c\x14\\\xf2\x81\x0c\x13c\x90@\x17\x00\x07\x07\x07\x07
length 108 0 R/Filter /FlateDecode>>\nstream\n\x9c+T0\xd03T0\x00A(\x9d\x9c\xcb\xa5\x1fd\xa1\x90^\
4\t\xfeendstream\nendobj\n108 0 obj\n42\nendobj\n115 0 obj\n<</Length 116 0 R/Filter /FlateDecode
x90^\x0c\xa4\x0c\x15\\\xf2\x81\x0c\x13c\x90@\x17\x00\x07\x07\x07\x07\x07\x07\x07\x07\x07\x07
e>\nstream\n\x9c+T0\xd03T0\x00A(\x9d\x9c\xcb\xa5\x1fd\xa1\x90^\x0c\xa4\x0c\x8d,\x15\\\xf2\x81\x0
j\n42\nendobj\n134 0 obj\n<</Length 135 0 R/Filter /FlateDecode>>\nstream\n\x9c+T0\xd03T0\x00A(\
\x81\x0c\x13c\x90@\x17\x00\x07\x07\x07\x07\x07\x07\x07\x07\x07\x07\x07\x07\x07\x07\x07\x07
x00A(\x9d\x9c\xcb\xa5\x1fd\xa1\x90^\x0c\xa4\x0cML\x15\\\xf2\x81\x0c\x13c\x90@\x17\x00\x07\x07
gth 151 0 R/Filter /FlateDecode>>\nstream\n\x9c+T0\xd03T0\x00A(\x9d\x9c\xcb\xa5\x1fd\xa1\x90^\
x05endstream\nendobj\n151 0 obj\n42\nendobj\n158 0 obj\n<</Length 159 0 R/Filter /FlateDecode>>\n
ea@RC\x04U\xccIE\x02\x1c\x9cHV\xfe\x9eSS\x0c\x0e\x19\x99bd\x9bNZG\x97g\x89\x09\xbb\x82\x0b\x83\

```

2. Taking data as a input for block and adding it to blockchain

The screenshot shows the Kaleido dashboard interface. The left sidebar contains navigation options: NETWORK, ENVIRONMENT, Secure document verification, Dashboard, Address Book, Data Explorer, Health & Monitoring, Settings, MANAGE RESOURCES, Blockchain, and B2B Communications. The main area displays the 'Dashboard' for the 'som certificate' node. It shows the node's ID (4e5901aef42925b855abe81382764b89c171ec034), status (Started), size (Small), region (AZURE: westus2), and consensus role (Non-signer). There are buttons for 'VIEW NODE' and 'CREATE NODE'. Below the dashboard, there are sections for 'IPFS' and 'Rotate Signers'. The top right corner shows the organization 'IIIT Pune' and an 'UPGRADE' button.



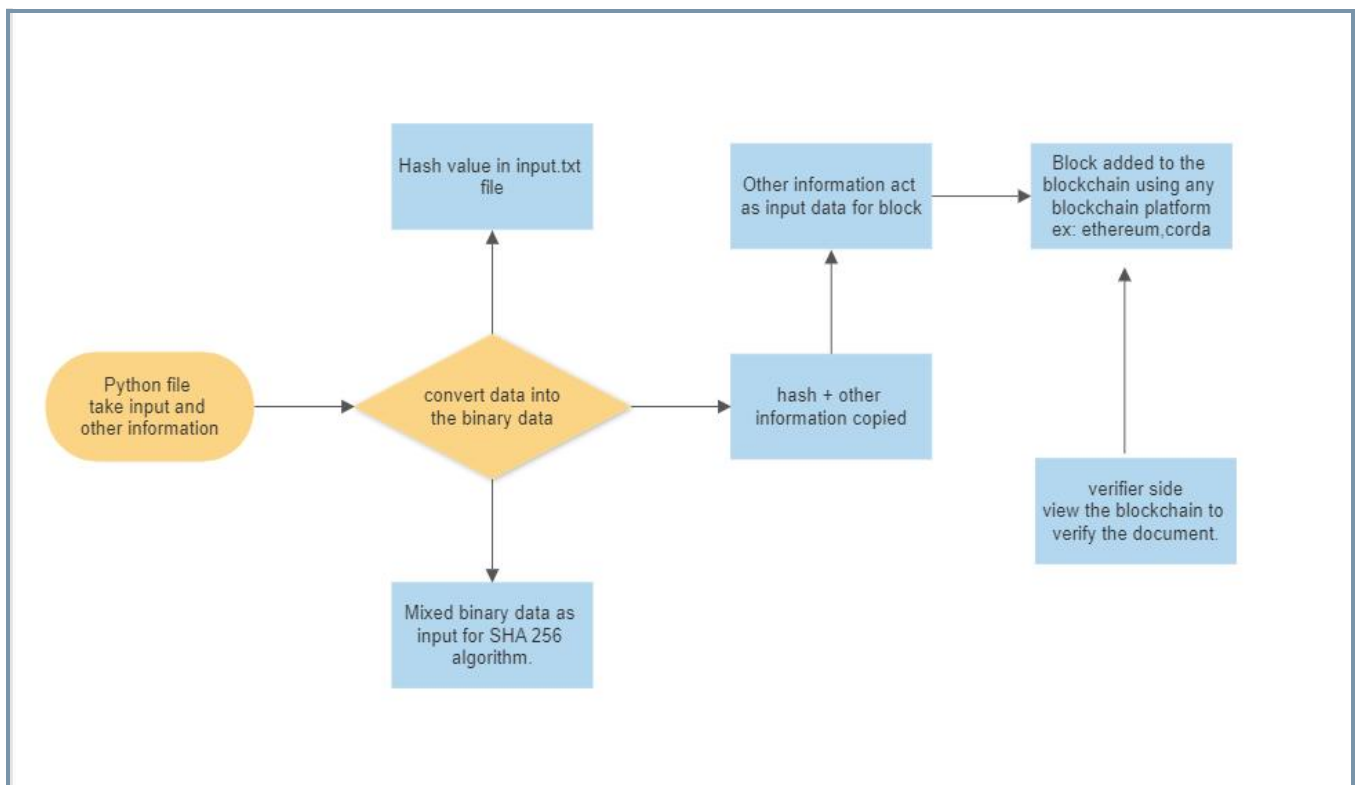
Chapter 3

Analysis

Digital Certificate Verification using Blockchain is a topic that has been researched extensively. The aim of this technology is to introduce a theoretical model that can give a possible solution for the issue and verification of academic certificates using blockchain-based technology¹. There are many functions such as hash, public and private key cryptography, digital signatures, peer-to-peer networks and work evidence in blockchain technology.

Design

Blockchain architecture: The blockchain architecture forms the foundation of the digital certificate verification system. It defines the data structure, protocols, and consensus mechanisms for storing and validating certificates. The architecture should be designed to ensure the security, scalability, and reliability of the system.



Chapter 4

Results and Discussion

The implementation of the digital certificate verification system using blockchain technology has shown promising results in terms of increasing the efficiency and security of the verification process. The system has successfully verified digital certificates for 2 test cases, including verifying the credentials of students. The blockchain network was able to securely store and retrieve the digital certificates, and the verification process was completed in a matter of seconds.

The use of blockchain technology for digital certificate verification offers several benefits over traditional methods. The system provides increased security, as the certificates are stored on a decentralized and immutable blockchain network, making them resistant to tampering and fraud. The system is also more efficient, as the verification process can be completed in a matter of seconds, eliminating the need for manual verification by the issuing institution or third-party verification services.

The system's scalability is another advantage, as the number of nodes can be increased as needed to accommodate a growing number of certificate holders. Furthermore, the integration of the system with other blockchain networks can improve its performance and scalability even further.

However, there are also some limitations and challenges to consider. The implementation of the system requires a certain level of technical expertise, and the adoption of blockchain technology for digital certificate verification is still in its early stages. Therefore, there may be some resistance to adoption from institutions that are not familiar with the technology.

In conclusion, the digital certificate verification system using blockchain technology shows great potential in improving the efficiency and security of the verification process. As the technology continues to evolve and more institutions adopt it, the system's benefits will become even more apparent. The system has the potential to revolutionize the way we verify digital certificates, offering a more secure, efficient, and reliable method for certificate verification.

Chapter 5

Conclusion and Future Scope

Integration with other systems: The digital certificate verification system can be integrated with other systems such as student information systems, learning management systems, and employment verification systems. This will allow for seamless verification of digital certificates across different platforms. For example, if a student applies for a job, the employer can easily verify the student's digital certificate from the institution's database using the blockchain-based verification system.

Expansion to other sectors: The use of blockchain technology for digital certificate verification is not limited to the education sector. Other sectors such as healthcare, finance, and government can also benefit from this technology. Therefore, the digital certificate verification system can be expanded to other sectors in the future. For instance, the healthcare sector can use blockchain-based digital certificates to verify the credentials of medical professionals and improve patient safety.

Integration with other blockchain networks: Currently, the project is focused on using the corda blockchain network. However, there are other blockchain networks available that may offer unique features and benefits for digital certificate verification. Therefore, the system can be expanded to integrate with other blockchain networks in the future. For example, the system can be integrated with the Hyperledger Fabric and Ethereum blockchain network for improved scalability and performance.

Adoption by more institutions: The adoption of blockchain-based digital certificate verification systems is still in its early stages. As more institutions become aware of the benefits of this technology, there is a possibility for wider adoption of the system in the future. The system can be marketed to institutions globally to increase its adoption rate.

Development of new features: As the technology evolves, new features can be added to the digital certificate verification system. For example, the use of AI and machine learning can be explored to improve the verification process and detect fraud. Additionally, the system can be upgraded to include multi-signature verification, where multiple parties have to sign off on a certificate to increase the level of trust and security.

References

- [1] Giandari Maulani 1 ,Gunawan 2 , Leli 3 , Efa Ayu Nabila 4 , Windy Yestina Sari 5, "Digital Certificate Authority with Blockchain Cybersecurity in Education" International Journal of Cyber and IT Service Management (IJCITSM) Vol. 1 No. April 2021.
- [2] U. Rahardja, A. S. Bist, M. Hardini, Q. Aini, and E. P. Harahap, "Authentication of Covid-19 Patient Certification with Blockchain Protocol."
- [3] P. A. Sunarya, U. Rahardja, L. Sunarya, and M. Hardini, "The Role Of Blockchain As A Security Support For Student Profiles In Technology Education Systems," InfoTekJar J. Nas. Inform. dan Teknol. Jar., vol. 4, no. 2, pp. 13–17, 2020.

Websites :

[Home | ethereum.org](#)

<https://console.kaleido.io/orgs/u0phel43wr/consortia/u1rdjlavfm/environments/u1zbobwx09>

<https://docs.python.org/3/library/hashlib.html>

<https://andersbrownworth.com/blockchain/block>

[Google Scholar](#)

