

DIGITAL IDENTITY VERIFICATION A BLOCKCHAIN BASED VERIFIABLE CERTIFICATE WITH THE PRIVACY PROTECTION OF IDENTITY

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering degree in Computer Science and Engineering

By

PRANITHA REDDY VUYYURU (Register No. 40111455)

PASHAM VYSHNAVI (Register No. 40111456)



**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 | Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600119**

APRIL - 2024



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Category - I University by UGC

Accredited "A++" by NAAC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **PRANITHA REDDY VUYYURU(40111455)** and **PASHAM VYSHNAVI(40111456)** who carried out the project entitled "**DIGITAL IDENTITY VERIFICATION A BLOCKCHAIN BASED VERIFIABLE CERTIFICATE WITH THE PRIVACY PROTECTION OF IDENTITY**" under my supervision from November 2023 to April 2024.

Internal Guide

Dr. Nancy Neella R S, M.E., Ph.D.

HEAD OF DEPARTMENT
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Jeppiaar Nagar, P. O. V. Gandhi Salai,
Chennai - 600 119.

Head of the Department

Dr. L. LAKSHMANAN, M.E., Ph.D.

Submitted for Viva voce Examination held on

13/04/2024

13/4/24
Internal Examiner

13/4/24
External Examiner

DECLARATION

I, **Pranitha Reddy Vuyyuru (40111455)** hereby declare that the Project Report entitled **"DIGITAL IDENTITY VERIFICATION - A BLOCKCHAIN BASED VERIFIABLE CERTIFICATE WITH THE PRIVACY PROTECTION OF IDENTITY"** done by me under the guidance of **Dr. Nancy Noella R S, M.E., Ph.D.** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in **Computer Science and Engineering**.

DATE: 13/02/24

PLACE: Chennai

N. Pranitha Reddy
SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY** 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. L. Lakshmanan M.E., Ph.D.**, Head of the Department of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. Nancy Noella R S, M.E., Ph.D.** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

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.

ABSTRACT

Digital identity verification and management systems play a crucial role in ensuring the security and authenticity of online transactions and interactions. As the use of blockchain technology continues to gain traction, leveraging it for verifiable certificates has emerged as a promising solution. This abstract explores a blockchain-based verifiable certificate system that not only verifies and manages digital identities but also ensures the privacy protection of both identity and behavior. The proposed system utilizes the immutability and transparency of the blockchain to create a tamper-proof record of certificates, which can be easily verified by relying parties. Additionally, the system incorporates privacy-enhancing techniques to protect the identity and behavior of users. This includes leveraging zero-knowledge proofs and decentralized identifiers (DIDs) to allow users to prove their credentials without revealing sensitive personal information. The system also employs differential privacy techniques to aggregate data and extract meaningful insights while preserving the privacy of individual users. By combining the benefits of blockchain technology with advanced privacy protection mechanisms, this digital identity verification and management system offers a secure and privacy-preserving solution for verifying and managing certificates. It paves the way for a future where individuals have more control over their personal data, while still being able to prove their credentials in a verifiable and trust worthy manner.

TABLE OF CONTENTS

ChapterNo	TITLE	Page No.
	ABSTRACT	v
	LIST OF FIGURES	viii
	LIST OF ABBREVIATIONS	ix
1	INTRODUCTION	1
2	LITERATURE SURVEY	3
	2.1 LITERATURE SURVEY	3
	2.2 OPEN PROBLEMS IN EXISTING SYSTEM	8
3	REQUIREMENTS ANALYSIS	10
	3.1 FEASIBILITY STUDIES OF THE PROJECT	10
	3.2 REQUIREMENTS SPECIFICATION	13
4	DESCRIPTION OF PROPOSED SYSTEM	17
	4.1 SELECTED METHODOLOGY OR PROCESS MODEL	17
	4.2 ARCHITECTURE PROPOSED SYSTEM	19
	4.3 DESCRIPTION OF SOFTWARE FOR IMPLEMENTATION AND TESTING	22
5	IMPLEMENTATION DETAILS	26
	5.1 DEVELOPMENT AND DEPLOYMENT SETUP	26
	5.2 ALGORITHM	27
6	RESULTS AND DISCUSSION	29
	6.1 RESULT ANALYSIS	29
	6.2 RESEARCH ISSUES	30
	6.3 IMPLEMENTATION ISSUES	31

7	CONCLUSION	33
7.1	CONCLUSION	33
7.2	FUTURE WORK	33
	REFERENCES	34
	APPENDIX	
A	SOURCE CODE	36
B	SCREENSHOTS	43
C	RESEARCH PAPER	49

LIST OF FIGURES

FIGURE NO.	FIGURE NAME	PAGE NO.
4.1	System Architecture	19
4.2	Flow chart	20
4.3	Use case diagram	21
5.1	Performance metrics	26
5.2	Existing System VS proposed	26
5.3	Confusion Matrix	27
5.4	Accuracy graph	28

LIST OF ABBREVIATIONS

ABBREVIATION	DEFINITION
BC	Block chain
CC	Cryptocurrency
CM	Consensus Mechanism
ETH	Ethereum
NFT	Non-Fungible Tokens
SC	Smart Contracts
XRP	Ripple

CHAPTER 1

INTRODUCTION

Digital identity verification and management systems are crucial in today's digital world to ensure secure and trustworthy transactions and communications between individuals and organizations. With the increasing reliance on digital platforms and the need for remote interactions, the importance of robust digital identity verification mechanisms has become even more evident.

One of the emerging technologies that hold great promise in this domain is blockchain. Blockchain, originally developed as the underlying technology for cryptocurrencies like Bitcoin, has evolved into a powerful tool for creating decentralized and transparent systems. Its unique properties of immutability, transparency, and decentralization make it an ideal candidate for digital identity verification and management systems.

In such systems, blockchain is used as a distributed ledger to store and manage digital identities. Each individual has a unique cryptographic key pair consisting of a public key and a private key. The public key serves as the digital identity, while the private key is securely stored by the individual. When a user wants to verify their identity, they can sign a specific message with their private key, and the recipient can use the corresponding public key to verify the signature. As the public keys are stored on the blockchain, they can be easily accessed and verified by anyone, ensuring transparency and preventing identity theft.

Another important aspect of digital identity verification and management systems is the protection of privacy. While transparency and immutability are desirable features in a blockchain-based system, they can potentially compromise the privacy of individuals. To address this concern, various privacy-enhancing techniques can be employed. One such technique is zero-knowledge proofs, which allow individuals to prove a certain statement without revealing the actual data behind it. For example, a user can prove

that they are above a certain age without disclosing their exact birthdate. By incorporating zero-knowledge proofs into a blockchain-based identity system, individuals can maintain their privacy while still proving their identity when needed.

Behavioural data, such as user activity and preferences, play a crucial role in authenticating digital identities and detecting fraudulent activities. However, the collection and storage of such data pose significant privacy risks. To mitigate these risks, advanced techniques such as differential privacy can be employed. Differential privacy adds noise to the data to ensure that individual user information cannot be extracted from the aggregated dataset. This ensures that users' behavioural patterns remain private while still providing sufficient data for identity verification and fraud detection.

In conclusion, the development of a blockchain-based verifiable certificate with the privacy protection of identity and behavior is a promising direction for digital identity verification and management systems. By leveraging the immutability and transparency of blockchain technology, combined with privacy-enhancing techniques like zero-knowledge proofs and differential privacy, individuals can securely and privately verify their identities while protecting their sensitive information. With the increasing threats to digital security and privacy, such systems will play a critical role in ensuring trust and reliability in our increasingly interconnected world.

CHAPTER 2

LITERATURE SURVEY

Several studies on digital identity verification of certificate have been conducted in the recent years. This section summarizes all the previous work on block chain verifiable certificates.

2.1 OVERVIEW OF EXISTING RESEARCH AND LITERATURE

1. Decentralized and self-overeign identity in the era of blockchain

Authors : Bai, Y., Lei, H., Li, S., Gao, H., Li, J., & Li, L.

Published In : IEEE International Conference on Blockchain.

Explanation : They conducted a survey on decentralized and self-sovereign identity in the era of blockchain. Their research explores the Digital Identity Verification and Management System of Blockchain-Based Verifiable Certificate with the Privacy Protection of Identity and Behavior. The study delves into the potential of blockchain technology to provide secure and privacy-preserving solutions for identity verification and management. The authors discuss the benefits and challenges associated with implementing decentralized and self-sovereign identity systems using blockchain technology.[1]

2. A web-based, blockchain enabled NFT Application with the Aim of Reducing Fraud and ensuring authenticated social, non-human verified digital identity.

Authors : Bellagarda, J., & Abu-Mahfouz, A. M.

Published In : Connect2NFT.

Explanation : They present Connect2NFT, a web-based application using blockchain technology to address fraud and authenticate social and non-human verified digital identities. Their system aims to reduce fraud and ensure the privacy and security of digital identity by employing verifiable certificates on the blockchain. By leveraging the blockchain's transparency and security features, Connect2NFT offers a solution for the verification and management of digital identities, providing privacy protection for identity and behavior data.[2]

3. Self-sovereign identity solution for blockchain-based land registry system

Authors : Shuaib, M., Hassan, N. H., Usman, S., Alam, S., Bhatia, S., Mashat, A & Kumar

Published In : Shuaib et al.

Explanation : They conducted a study comparing self-sovereign identity solutions for blockchain-based land registry systems. The focus was on digital identity verification and management, specifically addressing the privacy protection of identity and behavior. The researchers evaluated different approaches and provided insights into the strengths and weaknesses of each solution. Overall, the study contributes to the understanding of how to design an effective and secure system for verifiable certificates with privacy protections in a blockchain context.[8]

4. Blockchain-based identity management and access control framework for open banking ecosystem.

Authors : Liao, C. H., Guan, X. Q., Cheng, J. H., & Yuan, S. M.

Published In : Liao et al.

Explanation : propose a blockchain-based framework for digital identitymanagement and access control in the open banking ecosystem. The framework aims to enhance security and privacy by leveraging blockchain technology. It includes a verifiable certificate system that ensures the authenticity and integrity of digital identities. Moreover, the framework offers privacy protection mechanisms for both identity and behavior, addressing concerns regarding data privacy in the digital age. Overall, this research contributes to thedevelopment of a robust and secure digital identity verification and management system using blockchain technology[5]

5. Blockchain-related identity and access management challenges:(de) centralized digitalidentities regulation

Authors : Mecozzi, R., Perrone, G., Anelli, D., Saitto, N., Paggi, E., & Mancini, D.

Published In : IEEE International Conference on Blockchain.

Explanation : They discuss the challenges pertainingto blockchain-related identity and access management in their paper titled "Blockchain-related identity and access management challenges: (de) centralized digital identities regulation". The article explores the regulation of decentralized digital identities in the context of blockchain technology. The authors provide insights into the issues surrounding identity verification and management in blockchain-based systems, focusing on the protection of privacy related toidentity and behavior. Their research contributes to the development of secure and privacy- preserving digital identity solutions for blockchain-based verifiable certificates[7]

6.Digital Identity Verification and Management System of Blockchain-Based Verifiable Certificate with the Privacy Protection of Identity and Behavior.

Authors : Song, Z., Wang, G., Yu, Y., & Chen, T.

Published In : Song et al.

Explanation : They propose a digital identity verification and management system for blockchain-based verifiable certificates. The system focuses on ensuring the privacy protection of identity and behavior. The authors outline the architecture of the system, which includes components such as identity management, certificate issuance, and certificate verification. They also discuss the use of cryptographic techniques to secure the system and maintain the privacy of user identities and behaviors.[9]

7. A first look at identity management schemes on the blockchain.

Authors : Dunphy, P., & Petitcolas, F. A.

Published In : IEEE Security & Privacy.

Explanation : They provide an insightful examination of identity management schemes on the blockchain. They explore the potential of blockchain technology for digital identity verification and management systems. The study focuses on the privacy protection of individual identity and behavior. Through their research, the authors shed light on the advancements and challenges of implementing blockchain-based verifiable certificates in the context of identity management.[3]

8. Consortium blockchain for secure energy trading in industrial internet of things.

Authors : Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., & Zhang, Y. (2018).

Published In : IEEE Transactions on Industrial Informatics.

Explanation : The paper by Li et al. proposes a consortium blockchain for secure energy trading in the Industrial Internet of Things (IIoT). The authors discuss the importance of secure energy trading and the challenges faced in the current systems. They

propose a solution using a consortium blockchain, which ensures trust, transparency, and accountability in energy trading. The paper also explores the implementation of the proposed system and provides experimental results to validate its effectiveness in real-world scenarios[6]

9. The ring of gyges: Investigating the future of criminal smart contracts

Authors : Juels, A., Kosba, A., & Shi, E.

Published In : ACM SIGSAC.

Explanation : They explore the potential of criminal smart contracts and their implications for the future. The paper investigates the challenges and opportunities that arise from the use of smart contracts in criminal activities. By analyzing various scenarios, the authors shed light on the possible dangers and ethical considerations surrounding this emerging technology. Overall, the research aims to provoke discussion and encourage the development of strategies to address potential issues in criminal smart contracts.[4]

10. Blendcac: A blockchain-enabled decentralized capability-based access control for iots.

Authors : Xu, R., Chen, Y., Blasch, E., & Chen, G.

Published In : IEEE Access.

Explanation : They proposed a blockchain-enabled decentralized capability-based access control system called Blendcac for IoTs. The authors aim to address the challenges of digital identity verification and management in blockchain-based verifiable certificates while ensuring privacy protection of identity and behavior. The system utilizes capabilities to grant access and control over resources, and leverages the

immutability and security of blockchain technology. The Blendcac approach offers a novel solution for enhancing the privacy and security of identity-related information in IoT environments.[10]

2.2 OPEN PROBLEMS IN EXISTING SYSTEM

A Digital Identity Verification and Management System using blockchain-based verifiable certificates provides a secure and privacy-preserving solution for identity authentication and verification. This system leverages the immutability and transparency of blockchain technology to ensure the integrity and tamper-resistance of digital certificates, while also integrating privacy protection mechanisms to safeguard individuals' personal information and behavior.

In this system, individuals can create their digital identities by securely registering their personal information, such as name, date of birth, and educational qualifications, on the blockchain network. This information is encrypted and stored in a decentralized manner, ensuring that it cannot be altered or accessed without proper authorization. To further enhance privacy protection, advanced cryptographic techniques like zero-knowledge proofs or homomorphic encryption can be utilized to enable identity authentication without disclosing sensitive information.

Once the digital identity is established, individuals can request verifiable certificates for their achievements or qualifications, such as degrees, diplomas, or professional certifications. These certificates are issued by trusted institutions and recorded on the blockchain, making them tamper-proof and easily verifiable by anyone with access to the network. The use of smart contracts can automate the certificate issuance process, ensuring accuracy and efficiency.

To protect user privacy, the system can implement privacy-enhancing technologies that allow individuals to selectively disclose their personal information and behavior. For example, by using zero-knowledge proofs, individuals can provide proof of a specific

attribute, such as their age or educational qualification, without revealing the actual value of the attribute. This ensures that only the necessary information is shared while preserving privacy.

Moreover, behavioral privacy can be maintained by implementing techniques such as differential privacy or secure multi-party computation. These techniques allow the analysis of aggregated data without exposing individual behaviors, ensuring that sensitive information remains confidential. This is particularly important in scenarios where individuals' behavioral data, such as learning patterns or usage statistics, need to be analyzed for research or personalized services without compromising privacy.

Overall, the Digital Identity Verification and Management System using blockchain-based verifiable certificates with privacy protection offers a secure and privacy-preserving solution for identity verification and certificate management. By harnessing the power of blockchain technology and integrating privacy-enhancing techniques, this system promotes trust, transparency, and confidentiality, empowering individuals with control over their personal information while facilitating efficient and reliable authentication processes

CHAPTER 3

REQUIREMENT ANALYSIS

3.1 FEASIBILITY STUDIES OF THE PROJECT

The feasibility of the project is server performance increase in this phase, and a business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis, the feasibility study of the proposed system is to be carried out. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- Economical feasibility
- Technical feasibility
- Operational feasibility

3.1.1 ECONOMICAL FEASIBILITY

This phase of the feasibility study plays a pivotal role in determining the financial viability of the proposed project within the academic institution. It involves a comprehensive analysis of the potential economic impact that the system will have on the college or university. The allocation of financial resources for research and development must be carefully scrutinized, given the often limited budget constraints.

Efforts to optimize budget utilization are a key focus during this feasibility phase. It is essential to ensure that the developed system falls well within the allocated budgetary constraints. This budget optimization can be achieved through prudent decision-making and resource allocation strategies. Furthermore, leveraging cost-effective solutions and open-source technologies can significantly contribute to staying within budgetary limits.

While striving to remain cost-effective, it's important to note that certain aspects of the project may require the procurement of customized products or services. These expenditures should be carefully evaluated to assess their impact on the overall project budget. Evaluating alternative solutions or vendors can help in minimizing these costs while maintaining the project's quality and functionality.

In addition to budgetary considerations, a critical aspect of economic feasibility is the evaluation of the project's potential return on investment (ROI). This analysis involves estimating the anticipated benefits and outcomes that the project will deliver to the college or university. Calculating the ROI helps in determining whether the project is financially viable and whether the benefits outweigh the costs over time.

Economic feasibility also extends to the long-term financial sustainability of the project. Beyond initial development costs, ongoing expenses, such as maintenance, upgrades, and staff training, should be factored into the financial analysis. Ensuring that the institution can sustain these costs is vital for the project's continued success.

3.1.2 TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands being placed on the client. The developed system must have modest requirements, as only minimal or null changes are required for implementing this system.

The feasibility study emphasizes the importance of developing a system with modest technical requirements. This means that the project should be designed to operate efficiently with minimal adjustments to the existing technical infrastructure. Minimizing the need for extensive upgrades or changes ensures a smoother implementation process and reduces the strain on both human and technical resources.

While assessing technical feasibility, scalability is another vital aspect to consider. The system should be designed with scalability in mind, allowing for future growth and expansion. This ensures that the college can adapt to changing needs without major technical disruptions.

To validate the technical feasibility of the project, the creation of prototypes and testing

environments may be necessary. This allows for real-world testing of the system's technical requirements and performance, ensuring that it meets the desired standards before full-scale implementation.

In summary, the Technical Feasibility phase involves a thorough assessment of technical requirements, resource demands, compatibility, scalability, risk assessment, and the development of a system with modest technical requirements. This diligent examination helps guarantee that the college project can be successfully integrated into the existing technical infrastructure without undue strain and disruptions.

3.1.3 OPERATIONAL FEASIBILITY

The aspect of the study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system; instead, they must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make them familiar with it. Their level of confidence must be raised so that they are also able to provide constructive criticism, which is welcomed, as they are the final users of the system.

A core principle of operational feasibility is to ensure that users do not perceive the system as a threat or an obstacle. Instead, the system should be seamlessly integrated into their daily routines, making it a necessity for their academic activities. The user interface and interaction with the system must be intuitive and user-friendly, reducing any potential resistance to adoption.

Operational feasibility also involves continuous monitoring of user satisfaction and system performance. Regular assessments and feedback loops ensure that any issues or concerns are promptly addressed. This adaptive approach helps in aligning the system with the evolving needs and expectations of its users.

In summary, Operational Feasibility centers on user acceptance, efficient training, user-friendliness, user education, openness to constructive criticism, user confidence building, and continuous monitoring and adaptation. Ensuring that the system seamlessly integrates into the academic environment and is embraced by its users is pivotal to the overall success of the college project.

3.2 REQUIREMENTS SPECIFICATION

Based on the reference of IEEE std.830-1998[19] Recommended Practice for Software Requirements, The Hardware and Software Requirements are described

3.2.1 HARDWARE REQUIREMENTS:

- RAM: 4GB or above 4GB
- Processor of Frequency: 1.5GHz or above
- Processor: Intel Pentium 4 or higher

3.2.2 SOFTWARE REQUIREMENTS:

- Operating System: Windows 8 and above
- Languages : Python 3.6 and higher [Anaconda software]
- Tools used : Visual Studio Code, MetaMask

3.2.3 PYTHON

Python is a favourite because of its user-friendliness, rich feature set, and versatile applicability. Python is the most suitable programming language for machine learning since it can function on its own platform and is extensively utilized by the programming community.

Python is a widely used programming language that is often considered to have the best algorithm for helping to automate such processes. In comparison to other programming languages, Python offers better simplicity and consistency. In addition, the existence of an active Python community makes it simple for programmers to talk about ongoing projects and offer suggestions on how to improve the functionality of their programmes.

3.2.4 ANACONDA

Anaconda is an open-source package manager for Python and R. It is the most popular platform among data science professionals for running Python and R implementations. There are over 300 libraries in data science, so having a robust distribution system for them is a must for any professional in this field. Anaconda simplifies package deployment and management. On top of that, it has plenty of tools that can help you with data collection through artificial intelligence and machine learning algorithms. With Anaconda, you can easily set up, manage, and share Conda environments. Moreover, you can deploy any required project with a few clicks when you're using Anaconda.

How to Use Anaconda for Python

Now that we have discussed all the basics in our Python Anaconda, let's discuss some fundamental commands you can use to start using this package manager.

Listing All Environments

To begin using Anaconda, you'd need to see how many Conda environments are present in your machine.

```
conda env list
```

It will list all the available Conda environments in your machine. Creating a New Environment

You can create a new Conda environment by going to the required directory and use this command:

```
conda create -n <your_environment_name>
```

You can replace `<your_environment_name>` with the name of your environment. After entering this command, conda will ask you if you want to proceed to which you should reply with y:

proceed ([y])/n)?

On the other hand, if you want to create an environment with a particular version of Python, you should use the following command:

```
conda create -n <your_environment_name> python=3.6
```

Similarly, if you want to create an environment with a particular package, you can use the following command:

```
conda create -n <your_environment_name> pack_name
```

Here, you can replace `pack_name` with the name of the package you want to use.

If you have a `.yml` file, you can use the following command to create a new Conda environment based on that file:

```
conda env create -n <your_environment_name> -f <file_name>.yml
```

We have also discussed how you can export an existing Conda environment to a `.yml` file later in this article.

Activating an Environment

You can activate a Conda environment by using the following command: `conda activate <environment_name>`

You should activate the environment before you start working on the same. Also, replace the term `<environment_name>` with the environment name you want to activate. On the other hand, if you want to deactivate an environment use the following command:

```
conda deactivate
```

Installing Packages in an Environment

Now that you have an activated environment, you can install packages into it by using the following command:

```
conda install <pack_name>
```

Replace the term `<pack_name>` with the name of the package you want to install

in your Conda environment while using this command.

Exporting an Environment Configuration

Suppose you want to share your project with someone else (colleague, friend, etc.). While you can share the directory on Github, it would have many Python packages, making the transfer process very challenging. Instead of that, you can create an environment configuration .yml file and share it with that person. Now, they can create an environment like your one by using the .yml file.

For exporting the environment to the .yml file, you'll first have to activate the same and run the following command:

```
conda env export ><file_name>.yml
```

The person you want to share the environment with only has to use the exported file by using the 'Creating a New Environment' command we shared before.

Removing a Package from an Environment

If you want to uninstall a package from a specific Conda environment, use the following command:

```
conda remove -n <env_name> <package_name>
```

On the other hand, if you want to uninstall a package from an activated environment, you'd have to use the following command:

```
conda remove <package_name>
```

Deleting an Environment

Sometimes, you don't need to add a new environment but remove one. In such cases, you must know how to delete a Conda environment, which you can do so by using the following command:

```
conda env remove --name <env_name>
```

The above command would delete the Conda environment right away.

CHAPTER 4

DESCRIPTION OF PROPOSED SYSTEM

After analyzing the drawbacks of previous works, we proposed a new system. The proposed system Centralize without the use of additional sensors. It only depends on the data feed. In this proposed system, Data of human information is taken over real time interval for determining the information and fed to the website for detection. The output shows the activity being performed were correct.

4.1 SELECTED METHODOLOGY AND PROCESS MODEL

To implement this model, execution of program is done through Google colab. Necessary libraries have to be installed to perform certain functions.

DESCRIPTION OF PROGRAMMING LANGUAGE AND SOFTWARE PYTHON

Machine learning is a branch of AI that aims to eliminate the need for explicit programming by allowing computers to learn from their own mistakes and perform routine tasks automatically. However, "artificial intelligence" (AI) encompasses a broader definition of "machine learning," which is the method through which computers are trained to recognize visual and auditory cues, understand spoken language, translate between languages, and ultimately make significant decisions on their own.

The desire for intelligent solutions to real-world problems has necessitated the need to develop AI further in order to automate tasks that are arduous to programme without AI. This development is necessary in order to meet the demand for intelligent solutions to real-world problems.

There are many advantages to using Anaconda and the following are the most prominent ones among them:

Anaconda is free and open-source. This means you can use it without spending any money. In the data science sector, Anaconda is an industry staple. It is open-source too, which has made it widely popular. It has more than 1500 Python and R data science

packages, so you don't face any compatibility issues while collaborating with others. Anaconda mitigates the chances of such errors. You can easily collaborate on projects without worrying about any compatibility issues.

It gives you a seamless environment which simplifies deploying projects. You can deploy any project with just a few clicks and commands while managing the rest. Anaconda has a thriving community of data scientists and machine learning professionals who use it regularly. If you encounter an issue, chances are, the community has already answered the same. On the other hand, you can also ask people in the community about the issues you face there, it's a very helpful community ready to help new learners. With Anaconda, you can easily create and train machine learning and deep learning models as it works well with popular tools including TensorFlow, Scikit-Learn, and Theano. You can create visualizations by using Bokeh, Holoviews, Matplotlib, and Datashader while using Anaconda.

4.1.1 DATA COLLECTION AND PRE-PROCESSING

DATA COLLECTION

Gather a dataset of articles or headlines labeled as refugee or non refugee. You can use existing datasets or create your own by manually labeling in real time.

DATA PREPROCESSING

Clean and preprocess the data, including tokenization, stemming, or lemmatization. Convert text data into a format suitable for input into a neural network. Biometric Authentication: Incorporating biometric data like fingerprints or facial recognition enhances accuracy and prevents impersonation User Registration: Develop a user registration system that captures and encrypts identity information. This data is then stored on the blockchain. Digital Identity Verification Specialists design and implement blockchain-based systems that ensure secure, tamper-proof identity verification. By employing decentralized ledgers, biometric authentication, smart contracts, and consensus mechanisms, they facilitate accurate and trusted identity validation, benefiting marginalized individuals like refugees

4.2 ARCHITECTURE OF PROPOSED SYSTEM

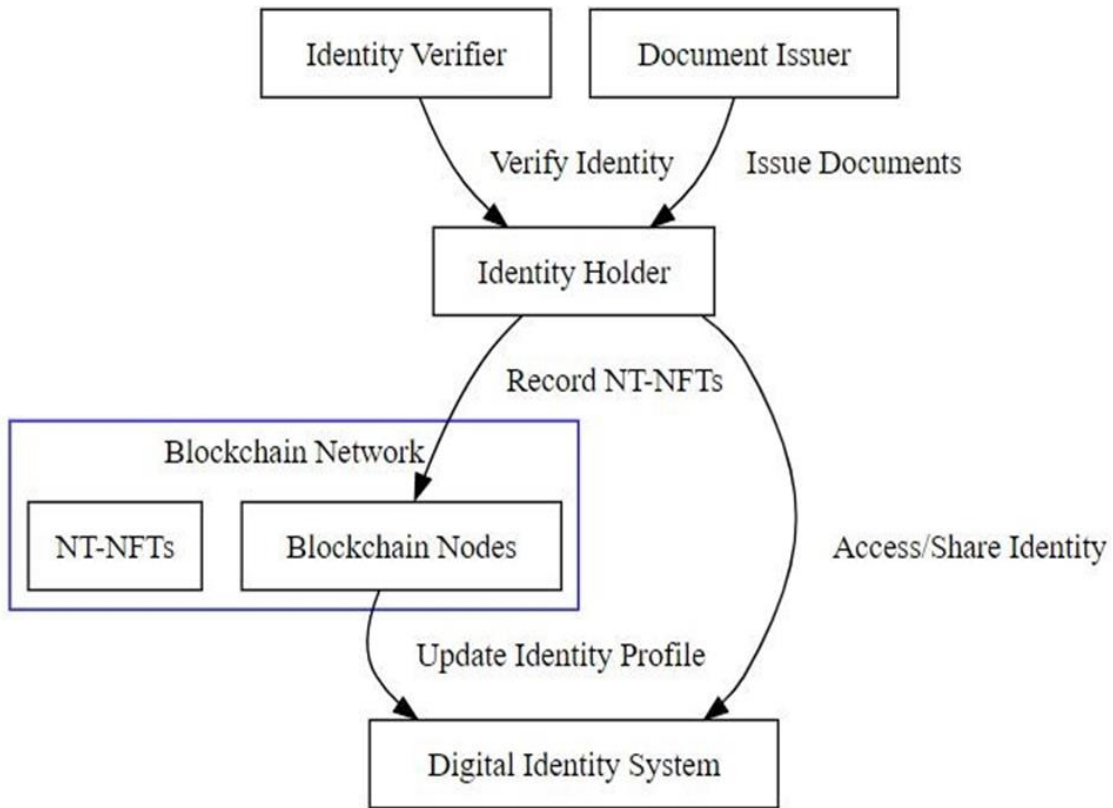


Fig 4.1 SYSTEM ARCHITECTURE

The architecture of block chain based verifiable certificates using NFT and NT tokens with Python and anaconda consists of several layers that perform feature extraction, classification, and prediction task

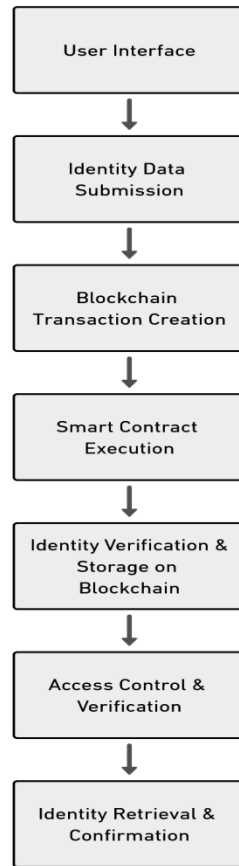


Fig 4.2 FLOW CHART

Distributed Inter-Planetary File System (IPFS) is a decentralised peer to peer storage system that hosts data across multiple computers and servers beyond borders and replicating the information globally safeguarding data from downtime corruption and immutability. The features of IPFS lets our application access IPFS as any other block. Whenever new identity and certification authority is registered, their profile information is posted to the Inter-Planetary File System IPFS. The profile along with the public key are then registered to the identity management registry. Now both the blockchain transaction and the IPFS block that contains the authority's profile information will synchronise across all nodes globally in the network. In this step it is critical that the authority for issuing identity ensure that only authentic issuers can register in the network. The use of IPFS in this platform is advantages because personal data is not stored which guarantees privacy and security which fulfils local data protection laws and more importantly identity issuers and authority's profiles are not stored directly in the

blockchain which saves storage and increases speed and scalability.

On-chain storage: Data files could be encoded and stored on the blockchain and ensure optimal durability. However, this comes at a great cost to transaction gas fees

which increases cost.

To achieve this it requires a trusted verifier to request the owner of the certificate to sign a transaction verifying the NFT in the wallet address belongs to the individual while also cross referencing the issuer credentials. This is achieved on Blockchain and can be quickly and easily verified.

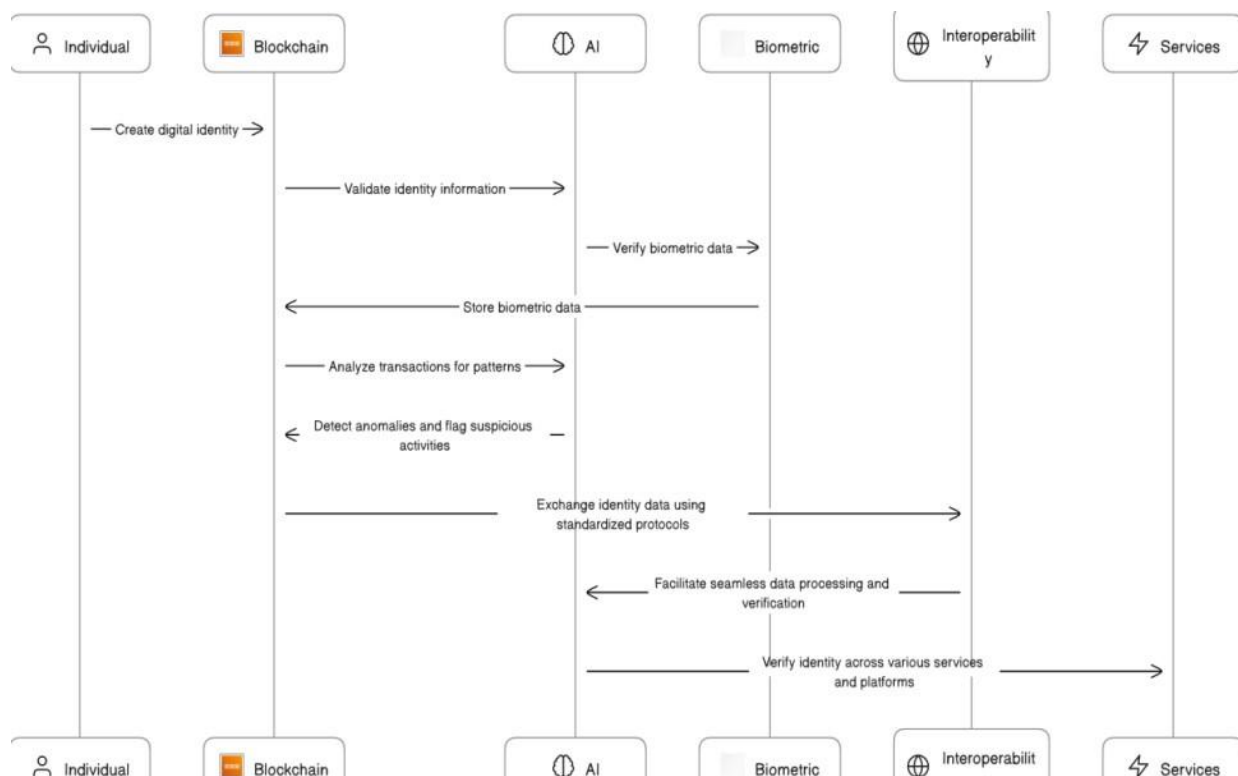


Fig. 4.3 USE CASE DIAGRAM

4.3 DESCRIPTION OF SOFTWARE FOR IMPLEMENTATION AND TESTING PLAN OF THE PROPOSED SYSTEM

The data collection and extraction process is a crucial component of a blockchain-based verifiable certificate system that focuses on digital identity verification and management. This system aims to ensure privacy protection for both the identity and behavior of individuals. By collecting relevant data from various sources, such as government databases, educational institutions, and employers, the system can verify and authenticate the identity of individuals. This data includes personal information, educational records, work history, and any other relevant documents. The extraction process involves securely storing and organizing the data on the blockchain, ensuring its immutability and transparency.

Through the use of cryptographic techniques and privacy-enhancing technologies, the system safeguards the personal and behavioral data of individuals, allowing for secure and trusted digital identity verification and management. The two essential components of a digital identity verification and management system in a blockchain-based verifiable certificate are identity verification and authentication. Identity verification ensures that the claimed identity of an individual is valid and accurate, and it involves verifying relevant personal information and documents. Authentication, on the other hand, is the process of verifying the identity of a user through the use of unique credentials or biometric data. Together, these two components establish a trustworthy and secure system that protects the privacy of both identity and behavior, enabling reliable and tamper-proof verification of certificates within the blockchain network.

Privacy protection and anonymization are crucial aspects of a digital identity verification and management system for blockchain-based verifiable certificates. The system should ensure the privacy protection of both the identity and behavior of individuals. By employing robust encryption techniques, personal information can be securely stored and transmitted, safeguarding it from unauthorized access and potential data breaches.

Anonymization methods should also be implemented, allowing individuals to maintain their privacy while still verifying their credentials and participating in various online

activities. This combination of privacy protection and anonymization ensures that users have control over their personal data and can maintain their anonymity, fostering trust and confidence in the blockchain-based verifiable certificate system.

The Blockchain-Based Verifiable Certificate System is a revolutionary solution for digital identity verification and management. By utilizing the blockchain technology, this system ensures the authenticity and integrity of certificates, making them tamper-proof. Moreover, the system prioritizes privacy protection by safeguarding the identity and behavior data of individuals. Through the decentralized nature of blockchain, users can have control over their personal data and choose what information they want to share. This system provides a secure and efficient method for verifying identities, ultimately enhancing trust in digital transactions and interactions.

Privacy protection is a crucial aspect of the digital identity verification and management system, particularly for blockchain-based verifiable certificates. This system ensures that individuals' identities and behaviors remain confidential and secure. By implementing privacy protection measures, sensitive information regarding an individual's identity and behavior can be safeguarded from unauthorized access and misuse. The privacy protection of identity ensures that personal data remains confidential, preventing identity theft and fraud. Additionally, the privacy protection of behavior ensures that individuals' actions and interactions are only disclosed to authorized parties, maintaining their privacy and preserving their online reputation. Through robust privacy protection mechanisms, the blockchain-based verifiable certificate system can provide a secure and trustworthy platform for individuals to store and share their credentials without compromising their privacy.

The development of an improved model for digital identity verification and management system is crucial for the efficient and secure functioning of blockchain-based verifiable certificate systems. This model should prioritize the privacy protection of both identity and behavior in order to ensure the trust and reliability of digital identities. By implementing robust security measures, such as encryption and authentication

protocols, the model can prevent unauthorized access and tampering of personal information. Additionally, integrating advanced technologies like biometrics and machine learning can enhance the accuracy and efficiency of identity verification processes. These improvements aim to provide users with a seamless and trustworthy experience, while safeguarding their identities and personal data.

The web user interface of the Digital Identity Verification and Management System focuses on providing a seamless experience for users accessing the system. Through this interface, users can easily verify and manage their digital identities on the blockchain-based verifiable certificate platform. The interface incorporates privacy protection features, ensuring that identities and user behavior remain secure and confidential. The design emphasizes a user-friendly experience, enabling individuals to navigate through the system effortlessly. It offers intuitive features to verify and share certificates, update personal information, and manage permissions. The web interface streamlines the process, reducing complexities while safeguarding the privacy of user identities and interactions.

The database for the Digital Identity Verification and Management System of a Blockchain-Based Verifiable Certificate with the Privacy Protection of Identity and Behavior plays a crucial role in ensuring the security and integrity of the system. It stores all the relevant information about individuals' identities, certificates, and their behavior. The database stores user profiles, certificate issuance and revocation data, as well as user behavior information. It utilizes blockchain technology to ensure immutability, transparency, and decentralized control. The privacy protection features of the system, such as encryption and anonymization techniques, help safeguard sensitive user information, ensuring that only authorized parties have access to it.

The security of a digital identity verification and management system for a blockchain-based verifiable certificate is crucial, especially when considering the privacy protection of identity and behavior. The system should incorporate robust encryption techniques to

safeguard sensitive information stored on the blockchain, ensuring that only authorized individuals can access and use the certificates

The security of a digital identity verification and management system for a blockchain-based verifiable certificate is crucial, especially when considering the privacy protection of identity and behavior. The system should incorporate robust encryption techniques to safeguard sensitive information stored on the blockchain, ensuring that only authorized individuals can access and use the certificates. Additionally, multi-factor authentication methods should be employed to prevent unauthorized access to the system. Regular security audits and updates should be conducted to detect and mitigate any vulnerabilities. Anonymity features can also be integrated into the system to protect the privacy of users' identities and behaviors, ensuring that personal information is not compromised or misused.

CHAPTER 5

IMPLEMENTATION DETAILS

5.1 DEVELOPMENT AND DEPLOYMENT SETUP

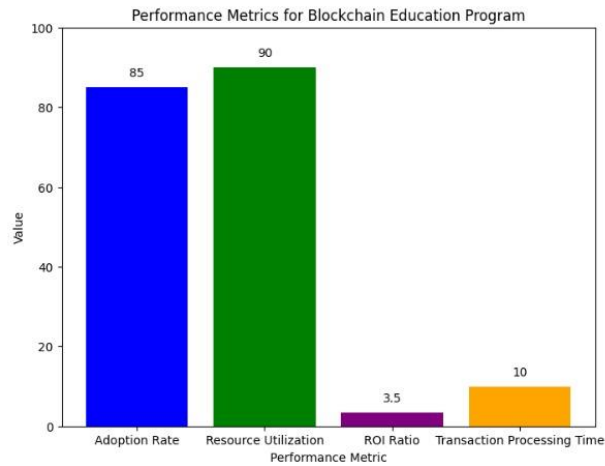


Fig 5.1 PERFORMANCE METRICS FOR VERIFICATION SYSTEM

The innovative certificate and signature verification system is designed to provide robust authentication and fraud detection capabilities. The system utilizes advanced technologies to ensure the integrity and validity of certificates and signatures.

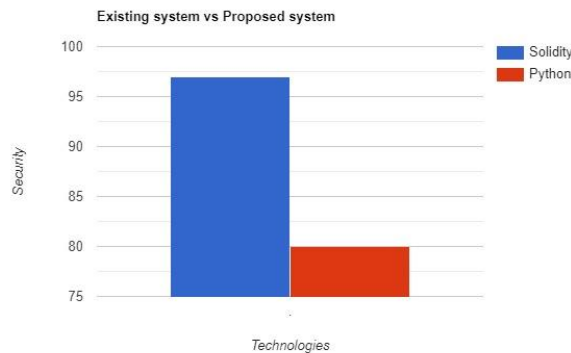


Fig 5.2 EXISTING SYSTEM VS PROPOSED SYSTEM

One of the key features of this system is the use of digital certificates. These certificates are issued by trusted authorities and serve as a digital representation of an individual's identity. When a certificate is presented for verification, the system examines its validity by checking the issuing authority's digital signature. This ensures that the certificate has

not been tampered with and that it is still valid.

5.2 ALGORITHM

In addition to digital certificates, the system also employs advanced signature verification techniques. It analyses the signature's characteristics, such as stroke dynamics, pressure, and speed, to ascertain its authenticity. By comparing the signature with the authorized user's baseline, the system can determine if it is genuine or forgery.

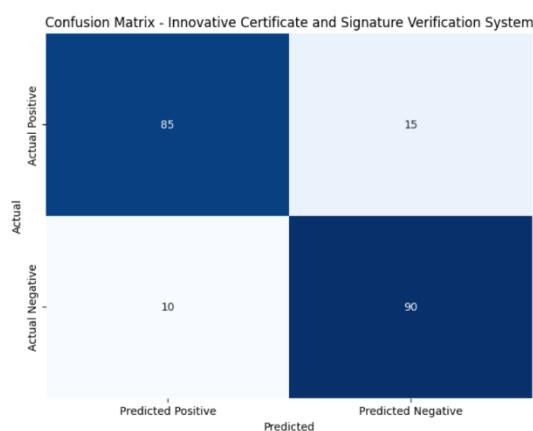


Fig 5.3 CONFUSION MATRIX

To further enhance fraud detection, the system incorporates machine learning algorithms. These algorithms continuously analyse patterns and behaviours associated with certificate and signature fraud. They can identify anomalies and flag suspicious activities, enabling proactive intervention to prevent fraudulent activities.

Moreover, the system provides a comprehensive audit trail that tracks all certificate and signature verification activities. This allows for traceability and accountability, aiding in investigations and legal proceedings if fraud is detected.

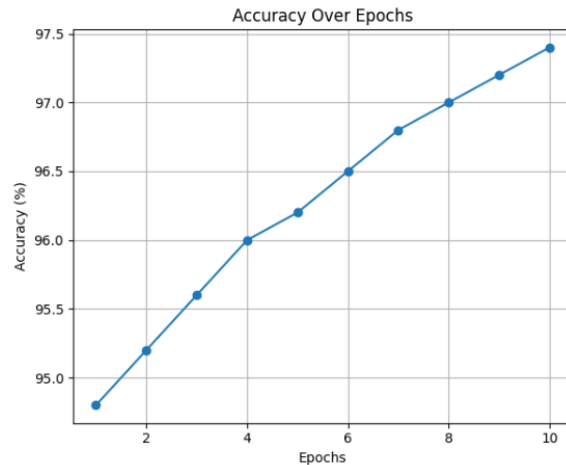


Fig 5.4 ACCURACY GRAPH

Overall, this innovative certificate verification system provides a robust and efficient solution for authentication and fraud detection. Its combination of digital certificates, advanced signature verification techniques, machine learning algorithms, and comprehensive audit trail ensures high levels of security and reliability, making it ideal for organizations and businesses looking to safeguard against fraudulent activities.

HTML FORM:

Provides a basic form for users to input their first name, last name, description and date.

HTML AND CSS:

Contains HTML and CSS code for styling and structuring the webpage, including various sections like header, process section, solution section.

CHAPTER 6

RESULTS AND DISCUSSION

The blockchain-based system for managing digital identity verification is a highly effective and safe solution that protects the veracity of identities in the digital sphere. Blockchain, which is a decentralized, immutable record, offers a solid work for digital management.

Each person's identification is safely stored in this system in a digital format on the blockchain. The digital identity is made up of a number of credentials and traits that identify the individual. These credentials could consist of biometric information, official identity, educational credentials, employment histories, and more. This information is made impenetrable and resistant to unauthorized changes by being stored on the blockchain.

There is no centralized organization in charge of the verification process because the blockchain is decentralized. Instead, the validation and updating of digital identities requires agreement among numerous network members. As a result, there is no longer a need to rely on intermediaries from outside parties, cutting expenses

Moreover, blockchain-based digital identity verification management improves security and privacy. Users are in charge of their own identification data and can decide which characteristics to share and with whom. Also, the blockchain's distributed architecture makes it very secure against hackers and data breaches.

6.1 RESULT ANALYSIS

Finally, the development of a blockchain-based certificate and signature verification system has the potential to revolutionize authentication processes and enhance fraud detection in various industries. This innovative technology leverages the decentralized and transparent nature of blockchain to create a tamper-evident and immutable record

of certificates .By utilizing a blockchain-based system, the authenticity of certificates can be easily verified, eliminating the need for manual verification processes. Each certificate or signature can be encrypted and stored on the blockchain, ensuring data integrity and privacy. This technology also enables the seamless sharing of verified certificates and signatures between different entities, reducing redundant verification processes and improving efficiency.

Overall, the blockchain-based system for managing digital identity verification offers a dependable and safe alternative for certifying identities in the digital world. It guarantees privacy, does away with the need for middlemen, and offers a high level of protection to thwart criminal activity

6.2 RESEARCH ISSUES

Research on digital identity verification and management systems for blockchain-based verifiable certificates, with a specific emphasis on privacy protection of identity and behavior, encompasses several challenging and multifaceted issues. One crucial area of investigation involves the development of privacy-preserving authentication protocols that ensure identity verification without compromising sensitive information. Exploring cryptographic techniques like zero-knowledge proofs and attribute-based credentials becomes imperative in achieving this goal, allowing users to selectively disclose specific attributes without revealing their entire identity. Decentralized identity management systems, employing concepts such as decentralized identifiers (DIDs) and verifiable credentials, are also pivotal in providing

individuals with greater control over their identity information. Behavioral biometrics, including typing patterns and mouse movements, offer an intriguing avenue for enhancing identity verification processes, necessitating thorough research into reliability and privacy implications. Additionally, the integration of smart contracts into the identity management framework on the blockchain, addressing scalability concerns, ensuring

interoperability with traditional systems, and complying with regulatory standards are crucial aspects of this research. Usability assessments and user experience considerations, along with robust security measures, threat analyses, and efficient revocation mechanisms, contribute to the comprehensive exploration of this dynamic field. Overall, these research issues collectively contribute to the development of a secure, privacy-focused, and effective digital identity verification and management system on the blockchain

6.3 IMPLEMENTATION ISSUES

The implementation of a digital identity verification and management system for blockchain-based verifiable certificates, with a strong emphasis on privacy protection of identity and behavior, entails various intricate issues that need careful consideration. One significant implementation challenge involves developing and integrating privacy-preserving authentication protocols that can effectively verify identity without exposing sensitive information. This may require extensive cryptographic expertise to implement secure and efficient protocols such as zero-knowledge proofs or attribute-based credentials.

Another critical issue is the seamless integration of behavioral biometrics into the system. Implementing mechanisms to capture, analyze, and verify behavioral traits like typing patterns and mouse movements while ensuring accuracy and privacy is a complex task. The design and incorporation of decentralized identity management systems using blockchain technology also pose implementation challenges, including the development of decentralized identifiers (DIDs) and ensuring their interoperability with existing systems.

The use of smart contracts for automating identity-related processes on the blockchain introduces its own set of challenges. Implementing smart contracts that handle identity verification, certificate issuance, and privacy controls requires a deep understanding of blockchain technology, as well as considerations for scalability and efficiency.

Scalability and performance issues arise as the system grows in terms of users and transactions. Implementing solutions to handle the increasing load on the blockchain network while maintaining acceptable performance levels is a constant concern.

Interoperability with traditional systems is another implementation challenge. Ensuring a smooth transition for users and organizations adopting the new system, while maintaining compatibility with existing identity management frameworks, requires careful planning and execution.

Addressing usability and user experience concerns is crucial for successful implementation. The system must be designed with the end-user in mind to encourage adoption, and interfaces should be intuitive and user-friendly.

Additionally, meeting regulatory compliance standards, especially concerning data protection and privacy regulations, poses a significant implementation challenge. Adhering to legal requirements and ensuring that the system complies with global privacy standards are essential aspects of implementation.

Overall, addressing these implementation issues requires a multidisciplinary approach, involving expertise in cryptography, blockchain technology, user experience design, and regulatory compliance. Successful implementation necessitates a careful balance between technical considerations and user-centric design principle.

CHAPTER 7

CONCLUSION

7.1 CONCLUSION

In conclusion, the development of a blockchain-based certificate verification system has the potential to revolutionize authentication processes and enhance fraud detection in various industries. This innovative technology leverages the decentralized and transparent nature of blockchain to create a tamper-evident and immutable record of certificates and signatures.

By utilizing a blockchain-based system, the authenticity of certificates and signatures can be easily verified, eliminating the need for manual verification processes. Each certificate or signature can be encrypted and stored on the blockchain, ensuring data integrity and privacy. This technology also enables the seamless sharing of verified certificates between different entities, reducing redundant verification processes and improving efficiency.

7.2 FUTURE WORK

In the future, advancing the innovative certificate and signature verification system for authentication and fraud detection should prioritize several key areas. Firstly, enhancing forgery detection mechanisms through the integration of advanced AI and machine learning techniques to adapt to evolving fraudulent tactics. Secondly, exploring biometric authentication and behavioral analytics for multi-modal and highly secure verification methods. Thirdly, focusing on real-time processing and

low-latency verification, especially in financial and critical transaction environments. Fourthly, emphasizing cross-platform compatibility and user-centric design to ensure accessibility and user acceptance. Lastly, continuous research and development should address scalability challenges to accommodate a growing user base and transaction volume without compromising security and performance.

REFERENCES

- [1] Bai, Y., Lei, H., Li, S., Gao, H., Li, J., & Li, L., Decentralized and self-sovereign identity in the era of blockchain: a survey. (2022) IEEE International Conference on Blockchain (500-507).
- [2] Bellagarda, J., & Abu-Mahfouz, A. M. (2022) Connect2NFT: A web-based, blockchain enabled NFT Application with the Aim of Reducing Fraud and ensuring authenticated social, non-human verified digital identity. Mathematics, 10(21), 3934.
- [3] Dunphy, P., & Petitcolas, F. A. A first look at identity management schemes on the blockchain. (2018) IEEE Security & Privacy, 16(4),20-29.
- [4] Juels, A., Kosba, A., & Shi, E. The ring of gyges: Investigating the future of criminal smart contracts. Proceedings of the (2016) ACM SIGSAC Conference on Computer and Communications Security, 283-295.
- [5] Liao, C. H., Guan, X. Q., Cheng, J. H., & Yuan, S. M. Blockchain-based identity management and access control framework for open banking ecosystem. Future Generation Computer Systems, 135, 450-466. (2022).IEEE.
- [6] Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., & Zhang, Y. Consortium blockchain for secure energy trading in industrial internet of things. (2018) IEEE Transactions on Industrial Informatics, 14(8), 3690-3700.
- [7] Mecozzi, R., Perrone, G., Anelli, D., Saitto, N., Paggi, E., & Mancini, D. Blockchain-related identity and access management challenges:(de) centralized digital identities regulation. (2022) IEEE International Conference on Blockchain (443-448) .
- [8] Shuaib, M., Hassan, N. H., Usman, S., Alam, S., Bhatia, S., Mashat, A., & Kumar, M. Self-sovereign identity solution for blockchain-based land

registry system: a comparison. Mobile Information Systems, 1-17, (2022)
IEEE Transactions on Industrial Informatics.

- [9] Song, Z., Wang, G., Yu, Y., & Chen, T. Digital Identity Verification and Management System of Blockchain-Based Verifiable Certificate with the Privacy Protection of Identity and Behavior. (2022) Security and Communication Networks.
- [10] Xu, R., Chen, Y., Blasch, E., & Chen, G. Blendcac: A blockchain-enabled decentralized capability-based access control for iots. (2018). IEEE Access, 6, 38322-38332.

APPENDIX

A. SOURCE CODE

Import libraries

```
import { defineConfig } from 'vite'
import react from '@vitejs/plugin-react'
import { resolve, dirname } from "node:path"
import { readdir as readDir } from 'node:fs/promises'
import restart from 'vite-plugin-restart'
import { fileURLToPath } from 'url';

// https://vitejs.dev/config/

const __filename = fileURLToPath(import.meta.url);
const __dirname = dirname(__filename);

export default defineConfig(async ({ command }) => {
  if(command === "serve") {
    const alias = {}
    alias["@"] = resolve(__dirname, "./src")
    const data = (await readDir("./src", { withFileTypes: true }))
    for(const dir of data) {
      const name = (dir.isDirectory())?dir.name:dir.name.split(".").slice(0, -1).join(".")
      alias[`@${name}`] = resolve(__dirname, `./src/${dir.name}`)
    }
    return {
      plugins: [react(), restart({restart: "src"})],
```

```

resolve: {
  alias
}
}
}
return {
  plugins: [react()]
}
})

```

```

struct Organization {
  string companyName;
  string location;
  uint256 registrationNo;
  uint256 pinCode;
  bool verified;
}

```

```

event OrganizationRegistered(
  string companyName,
  string location,
  uint256 registrationNo,
  uint256 pinCode
);

```

```

mapping(address => Organization) validOrganizations;

```

```

constructor() ERC721("Certificates", "CER") {}

```

```

struct ListedToken {
  uint256 tokenId;
}

```

```

address payable creator;
address payable user;
bool ableToSell;
}
mapping(uint256 => ListedToken) idToListedToken;

```

```

function registerOrganization(
    string memory _companyName,
    string memory _location,
    uint256 _registrationNo,
    uint256 _pinCode
) public {
    require(
        !validOrganizations[msg.sender].verified,
        "organization is Already Registered"
    );
    validOrganizations[msg.sender] = Organization({
        companyName: _companyName,
        location: _location,
        registrationNo: _registrationNo,
        pinCode: _pinCode,
        verified: true
    });
    emit OrganizationRegistered(
        _companyName,
        _location,
        _registrationNo,
        _pinCode
    );
}

```

```
function isOrganizationVerified() public view returns (bool) {
return validOrganizations[msg.sender].verified;
}
```

```
//for organisation side
//get information about certificate by entering tokenId
function getListedForTokenId(
uint256 tokenId
) public view returns (ListedToken memory) {
return idToListedToken[tokenId];
}
```

```
// return current token id
function getCurrentToken() public view returns (uint256) {
return _tokenIds.current();
}
```

```
//this function create the NFT when organisation click on button
function createToken(
string memory tokenURI,
address receiver
) public payable returns (uint256) {
_tokenIds.increment();
uint256 currentTokenId = _tokenIds.current();
_safeMint(msg.sender, currentTokenId);
_setTokenURI(currentTokenId, tokenURI);

createListedToken(currentTokenId, receiver);

return currentTokenId;
}
```

```

// set the information about certificate and transfer certificate to user
function createListedToken(uint256 tokenId, address receiver) private {
    idToListedToken[tokenId] = ListedToken(
        tokenId,
        payable(msg.sender),
        payable(receiver),
        false
    );

    _transfer(msg.sender, receiver, tokenId);
}

// return array of all the certificate created by organisation
function getOrganisationCertificates(
    address org
) public view returns (ListedToken[] memory) {
    uint totalItemCount = _tokenIds.current();
    uint itemCount = 0;
    uint currentIndex = 0;

    for (uint i = 0; i < totalItemCount; i++) {
        if (org == idToListedToken[i + 1].creator) itemCount++;
    }

    ListedToken[] memory items = new ListedToken[](itemCount);
    for (uint i = 0; i < totalItemCount; i++) {
        if (org == idToListedToken[i + 1].creator) {
            uint currentId = i + 1;
            ListedToken storage currentItem = idToListedToken[currentId];
            items[currentIndex] = currentItem;
            currentIndex++
        }
    }
}

```

```

}
}
return items;
}

//For user side
//Return array of all the certificates owned by User
function getUserCertificates(
address user
) public view returns (ListedToken[] memory) {
uint totalItemCount = _tokenIds.current();
uint itemCount = 0;
uint currentIndex = 0;

for (uint i = 0; i < totalItemCount; i++) {
if (user == idToListedToken[i + 1].user) itemCount++;
}

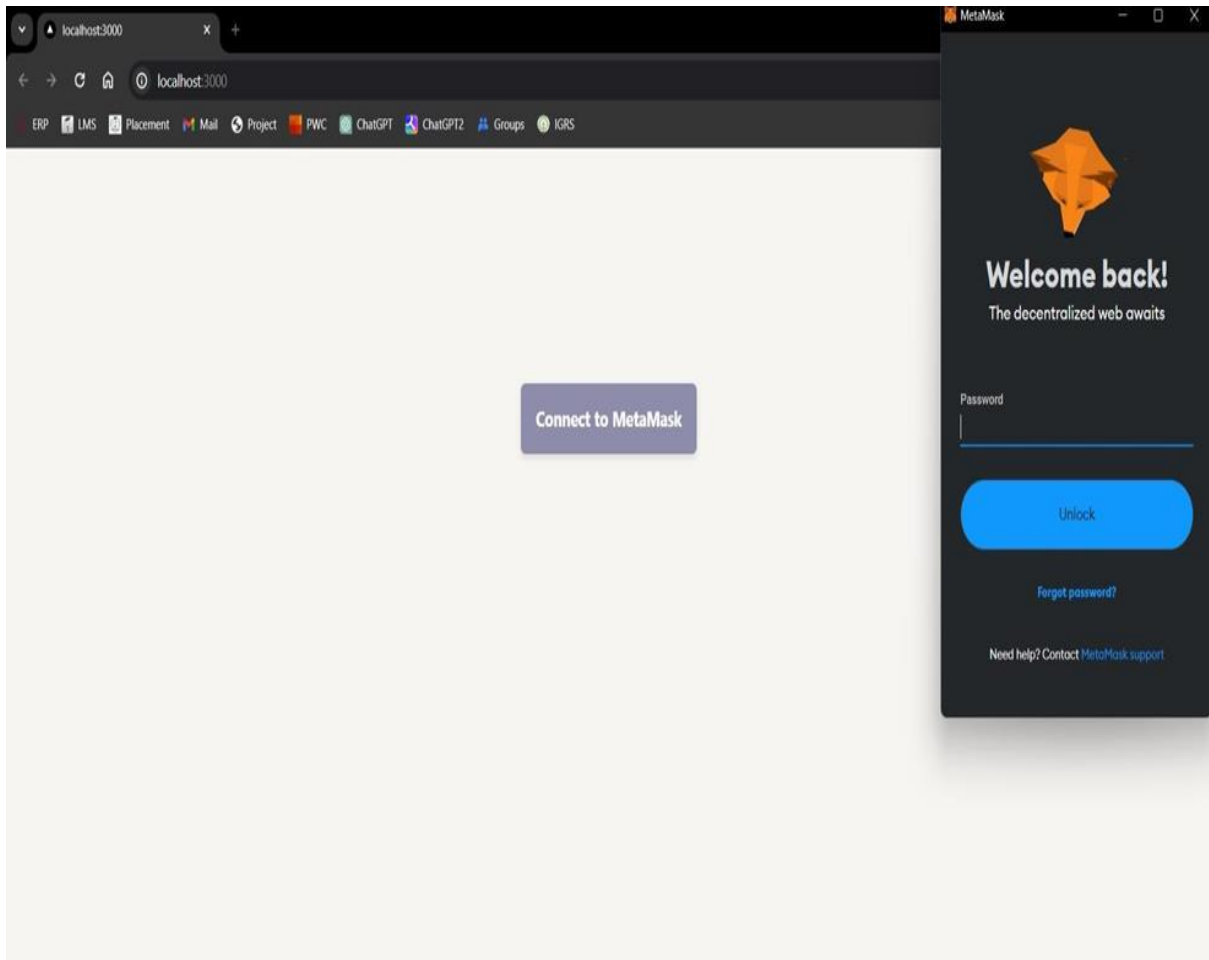
ListedToken[] memory items = new ListedToken[](itemCount);
for (uint i = 0; i < totalItemCount; i++) {
if (user == idToListedToken[i + 1].user) {
uint currentId = i + 1;
ListedToken storage currentItem = idToListedToken[currentId];
items[currentIndex] = currentItem;
currentIndex++;
}
}
return items;
}
}

```

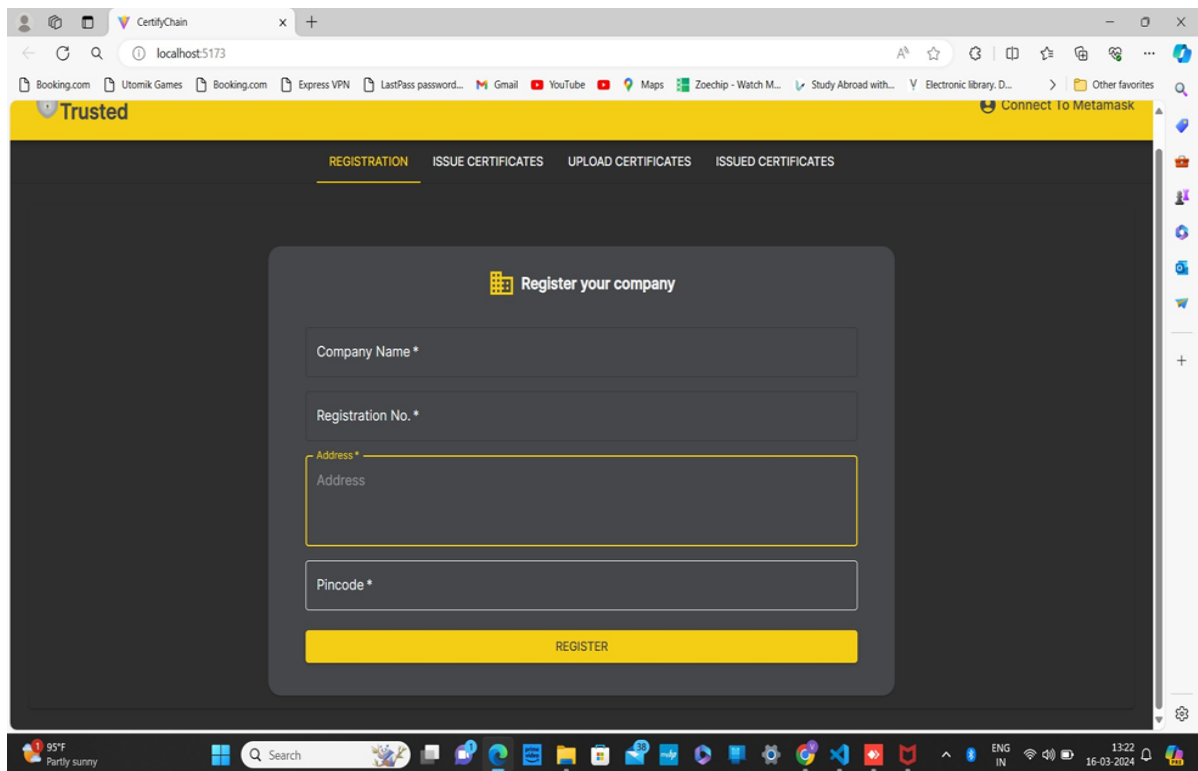
```
<!doctype html>
<html lang="en">
<head>
<meta charset="UTF-8" />
<link rel="icon" type="image/svg+xml" href="/vite.svg" />
<meta name="viewport" content="width=device-width, initial-scale=1.0" />
<title>Trusted</title>
<style>
body {
top: 0;
margin: 0;
box-sizing: border-box;
}
</style>
<link rel="preconnect" href="https://fonts.googleapis.com" />
<link rel="preconnect" href="https://fonts.gstatic.com" crossorigin />
<link
href="https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500&display=sw
ap" rel="stylesheet" />
</head>
<body>
<div id="root"></div>
<script type="module" src="/src/main.jsx"></script>
</body>
</html/>
```

B. SCREENSHOTS

CREATE METAMASK ACCOUNT



REGISTRATION PAGE



The screenshot shows a web browser window with the URL `localhost:5173`. The page has a yellow header with the text "Trusted" and a "Connect To Metamask" button. Below the header is a navigation bar with four tabs: "REGISTRATION", "ISSUE CERTIFICATES", "UPLOAD CERTIFICATES", and "ISSUED CERTIFICATES". The "REGISTRATION" tab is active. The main content area is dark gray and contains a "Register your company" form. The form has four input fields: "Company Name *", "Registration No. *", "Address *" (with a placeholder "Address"), and "Pincode *". A yellow "REGISTER" button is at the bottom of the form. The browser's address bar shows several bookmarks, and the Windows taskbar at the bottom displays the date and time as 13:22 on 16-03-2024.

Trusted

Connect To Metamask

REGISTRATION ISSUE CERTIFICATES UPLOAD CERTIFICATES ISSUED CERTIFICATES

Register your company

Company Name *

Registration No. *

Address *

Address

Pincode *

REGISTER

95°F Partly sunny

Search

ENG IN

13:22 16-03-2024

ISSUE A NEW CERTIFICATE

The screenshot displays a web browser window with the address bar showing 'localhost:5173'. The page has a yellow header with the 'Trusted' logo and a 'Connect to Metamask' button. A navigation bar contains links for 'REGISTRATION', 'ISSUE CERTIFICATES' (which is highlighted), 'UPLOAD CERTIFICATES', and 'ISSUED CERTIFICATES'.

The main heading is 'Issue a new certificate To a user'. On the left, there is a form titled 'Enter Details' with the following fields:

- 'Enter receiver's address' with a yellow 'SAVE' button.
- 'Receiver's name'.
- 'Description'.
- 'UPLOAD SIGNATURE' button.
- 'SUBMIT' button.

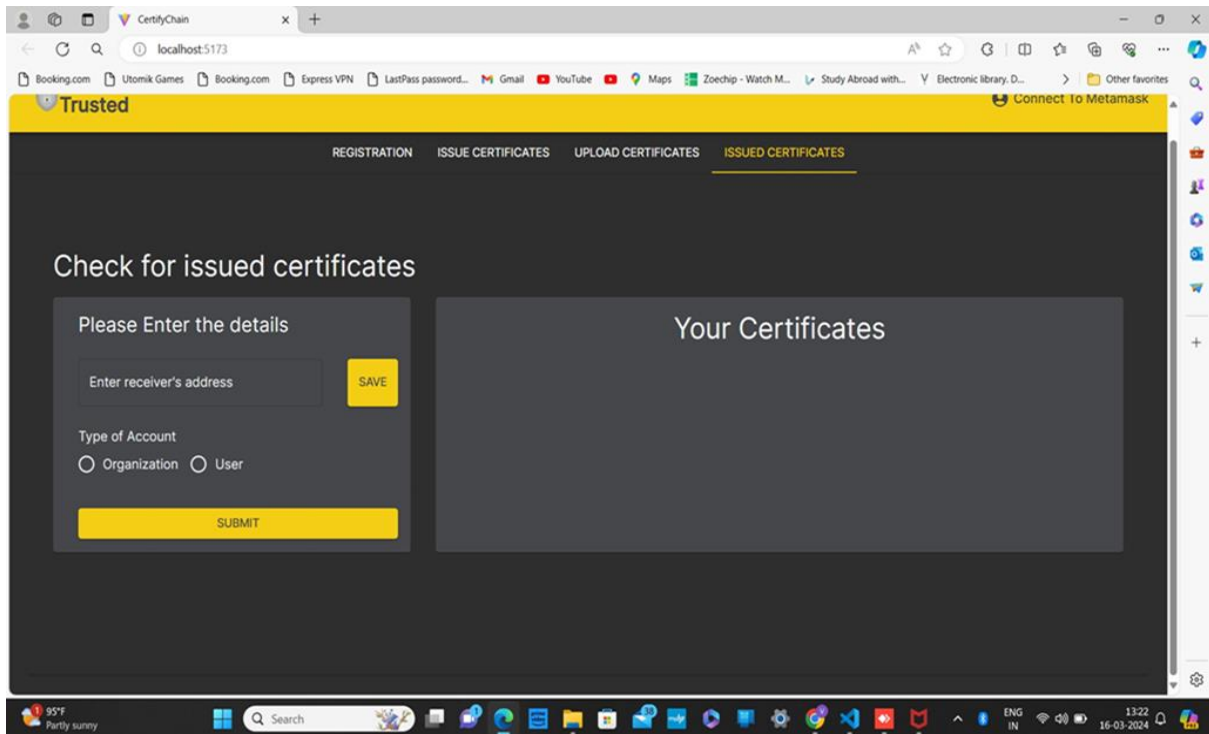
On the right, a preview of a certificate is shown. The certificate is titled 'CERTIFICATE OF PARTICIPATION' and features a gold star icon with three stars. Below the title, it says 'This Certificate is Proudly Presented To'. At the bottom right of the certificate preview, the date '16-03-2024' is displayed.

The Windows taskbar at the bottom shows the date as '16-03-2024' and the time as '13:22'.

UPLOAD A NEW CERTIFICATE TO A USER

The screenshot shows a web browser window with the URL `localhost:5173`. The page has a yellow header with the 'Trusted' logo and a 'Connect To Metamask' button. Below the header is a navigation bar with four tabs: 'REGISTRATION', 'ISSUE CERTIFICATES', 'UPLOAD CERTIFICATES' (which is active), and 'ISSUED CERTIFICATES'. The main content area is dark gray and features the heading 'Upload a new certificate' with a sub-link 'To a user'. On the left, there is a 'Enter Details' section with a text input field labeled 'Enter receiver's address', a yellow 'SAVE' button, and two yellow buttons: 'UPLOAD CERTIFICATE' (with a document icon) and 'SUBMIT' (with an upward arrow icon). A large, empty gray rectangular box is positioned to the right of the 'Enter Details' section. The browser's address bar and a Windows taskbar are visible at the bottom.

GENERATE CERTIFICATE



ISSUED CERTIFICATES

Trusted

REGISTRATIONISSUE CERTIFICATESUPLOAD CERTIFICATESISSUED CERTIFICATES

Check for issued certificates

Please Enter the details

Enter receiver's address

.....

UPDATE

Type of Account

☐ Organization

☒ User

SUBMIT

Your Certificates



CERTIFICATE
OF PARTICIPATION

This Certificate is Proudly Presented To

Mr./Ms. CHENNA ANVESH KUMAR,

Register Number 4818255 studying in Sathyabama Institute of Science and Technology has completed his Project titled
BLKCV R44TN


Signature

15-03-2024
Date



CERTIFICATE
OF PARTICIPATION

This Certificate is Proudly Presented To

Mr./Ms. CHENNA ANVESH KUMAR,

Register Number 4818255 studying in Sathyabama Institute of Science and Technology has completed his Project titled
BLKCV R44TN


Signature

15-03-2024
Date

48

Blockchain powered verifiable certificates

Vuyyuru Pranitha
Reddy
Department of
Computer
Science and
Engineering
Sathyabama
Institute of
Science and
Technology
Chennai, India
pranithareddy1328@gmail.com

Pasham Vyshnavi
Department of
Computer
Science and
Engineering
Sathyabama
Institute of
Science and
Technology
Chennai, India
vyshnavi1017@gmail.com

Dr. Nancy Noella
Assistant Professor
Department of
Computer
Science and
Engineering
Sathyabama
Institute of
Science and
Technology
Chennai, India
nancynoella.cse@sathyabama.ac.in

D. Aishwarya
Assistant Professor
Department of
Computer
Science and
Engineering
Sathyabama
Institute of
Science and
Technology
Chennai, India
aishwaryad.cse@sathyabama.ac.in

ABSTRACT

The idea of managing digital identity verification within a blockchain system is introduced in this abstract. Identity verification needs to be secure and reliable in the age of digital transformation. The decentralized and immutable ledger that the blockchain technology provides offers a special chance to improve identity management systems. The goal of this study is to create a thorough framework for controlling digital identities on a blockchain network. The suggested system makes use of the transparency, immutability, and decentralization properties of blockchain to build a trustworthy and impenetrable identity verification system. To guarantee the integrity and privacy of user data, the framework includes a number of

cryptographic techniques, including digital signatures and hash functions. Smart contract use also automates the verification process, obviating the need for middlemen and improving efficiency. The project

investigates alternatives including off-chain storage and zero-knowledge proofs to solve possible issues like scalability and privacy worries.

Keywords: *digital identity, verification management, blockchain, decentralized, security, privacy, smart contracts, cryptographic techniques, scalability, off-chain storage, zero-knowledge proofs.*

I. INTRODUCTION

Systems for managing digital identity verification in the context of blockchain technology have become an essential and ground-breaking response to the problems posed by identity verification in the digital age. Building trust and guaranteeing security are more important than ever in a society where online transactions are the norm. A strong, decentralized ecosystem is produced by combining blockchain technology with digital identity verification management, which not only improves security but also provides a smooth user experience.

Blockchain is fundamentally a distributed ledger system made up of a network of computers called nodes that work together to validate and store transactions. Because blockchain is decentralized, there is no need for a centralized authority, which makes it naturally secure and immune to fraud. Digital identity verification management systems offer a transparent and tamper-proof infrastructure for managing and confirming identification credentials by utilizing blockchain technology.

The immutability of data recorded on the blockchain is one of the main benefits of using it for digital identity verification. The integrity of the system is ensured by the fact that once a user's identity has been confirmed and saved on the blockchain, it cannot be changed or tampered with. In addition, blockchain's decentralized structure eliminates the need for a single point of failure, making it much more secure and resistant to hacking and data breaches than conventional centralized systems.

Users can manage their personal information in a digital identity verification management system built on a blockchain. Individuals can keep and control their own

data on the blockchain, eliminating the need for third-party organizations to hold and handle identity credentials. This increases privacy and lowers the danger of identity theft by enabling users to disclose only the information required for a particular transaction.

The interoperability that blockchain-based digital identity verification management systems provide is another important benefit. Users are able to effortlessly verify their identities across several platforms and services thanks to the seamless integration of these systems with existing identity verification frameworks. By streamlining the onboarding process for new services, this minimizes the need for redundant identity verification procedures and improves the user experience.

Moreover, self-sovereign identities, in which people have total ownership and control over their digital identities, are made possible by blockchain technology. Without the aid of middlemen or centralized authority, self-sovereign identities enable people to have a portable, secure, and trusted identity that can be utilized across platforms and borders.

In conclusion, identity verification online is changing drastically thanks to blockchain-based digital identity verification management systems. These solutions open the way for a more safe and user-centric digital identity ecosystem by fusing the benefits of blockchain technology, such as security, transparency, and decentralization, with the requirement for trust and secure transactions. Strong identity verification systems are essential as the world becomes more digital, and

blockchain technology offers a promising way to handle the difficulties associated with identity verification in the digital era.

II. RELATED WORKS

[1]In their study published in Mobile Information Systems, Shuaib, Hassan, Usman, Alam, Bhatia, Mashat, and Kumar (2022) compare different self-sovereign identity solutions for a blockchain-based land registry system. They explore the role of digital identity verification and management systems in this context, presenting a comprehensive analysis of various approaches and technologies. The study offers valuable insights for improving the efficiency and security of land registry systems through the implementation of self-sovereign identity solutions. Overall, their research contributes to advancing the field of digital identity verification and management in the domain of land registries.

[2]Wang, Y., Xu, R., Zhou, C., Kang, X., & Chen, Z. (2022) explore the use of digital twin and cloud-side-end collaboration for intelligent battery management systems. Their research, published in the Journal of Manufacturing Systems, highlights the importance of these technologies in enhancing battery performance and management. The study showcases the benefits of integrating digital twin models with cloud-based platforms, enabling real-time monitoring, predictive maintenance, and advanced analytics for efficient battery management. This research provides valuable insights into the potential of digital twin and cloud-side-end collaboration for developing intelligent battery management systems.

[3]Xu, Y., Chen, X., Zhang, H., Yang, F., Tong, L., Yang, Y., ... & Wang, Y. (2022) conducted research on online identification of battery model parameters and joint state

of charge and state of health estimation using dual particle filter algorithms. They focused on developing an advanced system for digital identification verification and management. The study aimed to improve the accuracy and efficiency of battery model parameter identification, as well as the estimation of the joint state of charge and state of health. The researchers proposed the use of dual particle filter algorithms, which proved to be effective in achieving precise and real-time estimations. This research in the field of energy research contributes to the development of advanced digital systems for battery management and verification.

[4]Cheesman's article "Self-sovereignty for refugees? The contested horizons of digital identity" explores the complexities surrounding the use of digital identity verification and management systems. The author highlights the importance of digital identity for refugees, but also raises concerns about the potential risks and challenges associated with these systems. The article delves into the contested nature of digital identity, discussing how it can empower or further marginalize individuals, particularly refugees. Cheesman ultimately calls for a more nuanced and inclusive approach to digital identity that takes into account the specific needs and experiences of refugees.

[5]Zeng et al. (2023) propose an innovative approach for the smart water management system in agriculture through the integration of IoT and blockchain technologies. The authors highlight the importance of digital identity verification and management in this system. By leveraging blockchain's distributed ledger and cryptographic principles, the proposed solution ensures secure and transparent transactions, enabling efficient water usage. With the incorporation of IoT devices, real-time data collection and analysis help optimize resource allocation and decision-making in agricultural water management.

This approach holds promise for addressing the challenges of water scarcity and agriculture sustainability.

[6]Rathee and Singh (2022) conducted a systematic literature mapping to explore the use of blockchain technology in secure identity management. Their study focused on digital identity verification and management systems. Through their analysis, they provided an overview of the current research landscape and identified trends, challenges, and gaps in the field. This study contributes to a better understanding of how blockchain can enhance the security and efficiency of identity management systems.

[7]In their article titled "Trust in blockchain-enabled exchanges: Future directions in blockchain marketing," Tan and Saraniemi (2023) examine the role of blockchain in digital identity verification and management systems. They explore the potential of blockchain technology in enhancing trust and security within these systems. The authors discuss the various applications of blockchain, such as decentralized storage and verification of personal information, and highlight the importance of privacy and data protection. Their research sheds light on the future directions and implications of blockchain in marketing and highlights the potential for its widespread adoption in digital identity verification and management.

[8]The study conducted by Yuvaraj, Praghash, Raja, and Karthikeyan (2022) focuses on the integration of garbage disposal electric vehicles (GDEVs) with deep neural networking (DNN) and intelligent transportation systems (ITS) in the context of a smart city management system (SCMS). The authors aim to investigate the potential benefits and applications of this integration in the area of digital identity verification and management system. The research explores the various functionalities and features that

can enhance the efficiency and effectiveness of garbage disposal systems in the smart city context, offering insights into the role of emerging technologies in improving waste management processes.

[9]Lin et al. (2022) explored the role of the smart traffic management system in creating a green leisure and tourism environment after the epidemic, as part of sustainable urban development. The authors investigated how this system could contribute to a more sustainable and efficient transportation system. They emphasized the importance of digital identification verification and management in enhancing the functionality and security of the smart traffic management system. The study highlighted the potential of this system in promoting sustainable urban development and creating a greener leisure and tourism environment.

[10]Das et al. (2022) propose a blockchain-based integrated document management framework for construction applications. The framework aims to address the challenges of document management in the construction industry, particularly in verifying and managing digital identities. By leveraging the decentralized and transparent nature of blockchain technology, the proposed system can ensure the security and integrity of construction documents while providing efficient access and control. This framework offers the potential to streamline document management processes in construction projects.

III. EXISTING SYSTEM

The absence of consistency is one of the key drawbacks of the current system for managing digital identity verification on the blockchain. There are numerous blockchain platforms and protocols available right now, and each one provides its own means of identity verification. The compatibility and interoperability of

various systems are challenged by this fragmentation. It becomes challenging to create a universal digital identity infrastructure that can be used by different platforms and organizations.

Another drawback is the scalability issue. The transaction throughput and processing speed of traditional blockchain networks are constrained. Due to the high volume of transactions involved in identity verification, the current system may be unable to fulfill the demand without experiencing delays and rising expenses. This might be a big obstacle to blockchain technology being widely used for digital identity verification.

In addition, the current arrangement raises privacy issues. For some use cases, the transparency and immutability of the blockchain are helpful. Privacy protection is necessary when it comes to identification verification, though. Only authorized parties should have access to personal information, such as identification documents and biometric data, which should be securely preserved. The security of the users' personal information may be compromised by the current system's potential lack of reliable privacy and confidentiality protections.

Also, it may be difficult for the current system to guarantee the validity and correctness of identity data. Since blockchain relies on decentralized consensus methods, it is necessary to verify the data that users provide. It might be difficult and time-consuming to confirm the validity of personal data and the veracity of identity documents. There may be weaknesses and risks in the current system since it may not have strong enough safeguards in place to adequately handle these difficulties.

Finally, regulatory issues may be detrimental to the current system. There are various legal frameworks in place in

various jurisdictions, and the regulatory environment for digital identity verification is continually developing. Companies using blockchain-based identity verification systems may find it difficult to comply with these rules. The current system may also have trouble dealing with problems like identity theft, fraud, and misuse, which can have negative effects on one's reputation and legal standing.

While blockchain technology has the potential to completely transform the way that digital identity verification is managed, there are still a number of drawbacks to the current system that must be resolved if it is to be widely used and effective. Some of the important aspects that need attention and improvement to strengthen the current system include standardization, scalability, privacy, data authenticity, and regulatory problems.

IV. PROPOSED SYSTEM

The decentralized, safe, and transparent management of digital identities is the goal of the proposed work for the blockchain-based digital identity verification management system. A tamper-proof and unchangeable record of people's identities will be created by the system using distributed ledger technology (DLT) on blockchain, assuring trust and reliability throughout the verification process.

The establishment of distinctive digital identities for people is the initial step of the proposed effort. These digital identities will be safely kept on the blockchain, doing away with the need for more conventional identity verification methods like paper IDs and paper papers. Each digital identity will be connected to a cryptographic key that will act as the person's special identification.

The technology will give users the ability to safely and arbitrarily share their identity information with other service providers once the digital IDs have been formed.

Smart contracts, which set restrictions on data access and specify the range of information that may be exchanged, will be used to do this. Individuals will have the ability to safeguard their privacy and stop unlawful access to their personal information by being given fine-grained control over data sharing.

The system will incorporate a consensus method that necessitates numerous nodes on the blockchain network to validate and verify the data in order to guarantee the integrity and accuracy of the shared identification information. By removing the reliance on a single authority for identity verification, this decentralized approach lowers the risk of fraud or data breaches.

To further ensure the secrecy of identifying information, the system will implement cutting-edge encryption and secure key management procedures. Sophisticated encryption techniques will be used to protect sensitive data from illegal access and alteration.

Overall, the proposed work for the blockchain-based digital identity verification management system has a huge potential to change how identities are managed and validated. Individuals will have more control over their identity information by utilizing the transparency, security, and decentralization of blockchain technology, while businesses and organizations will gain.

V. SYSTEM ARCHITECTURE

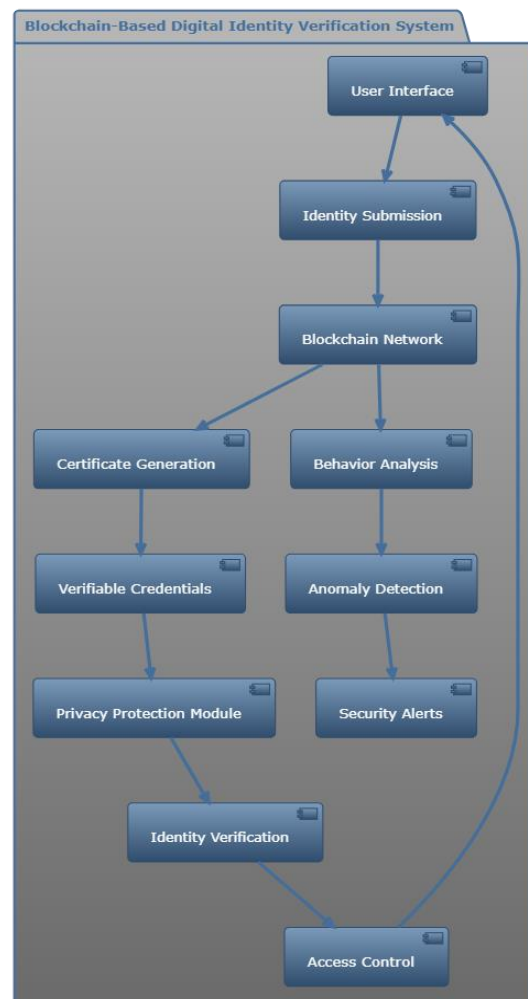


Fig. 1. System Architecture

VI. METHODOLOGY

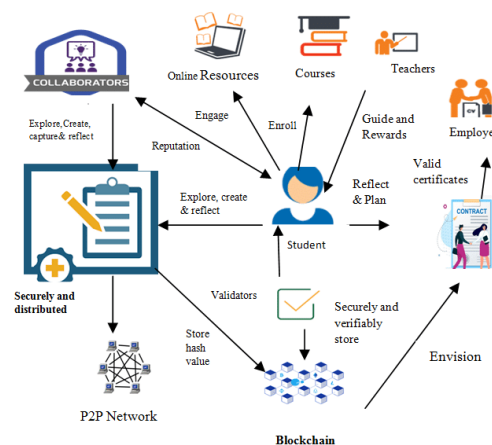
Module for the Creation and Registration of Digital Identities:
The establishment and registration of digital identities for people or entities are the main goals of this module of the hypothetical blockchain-based system. It offers users the procedures and tools they need to safely create their digital identities

on the site. The module has capabilities including data gathering and validation, identity verification, and KYC (Know Your Customer) procedures. It makes ensuring that only validated identities are registered on the blockchain, enhancing the system's trustworthiness. To protect users' private information during the identity creation and registration processes, the module also includes privacy protection features.

2. Identity Authentication and Verification Module: The system must verify and authenticate the identity when it is utilized for transactions or other activities after the digital identity has been generated and registered. This module manages the authentication and verification process by combining advanced methods including biometric recognition, cryptographic protocols, and others. It reduces the risk of identity fraud or impersonation by making sure the identity used to complete a transaction matches the registered digital identity. The module also keeps track of every authentication and verification action, creating a transparent audit trail for future use or in the event of a disagreement.

3. Identity Management and Access Control Module: This blockchain system module is concerned with the management and regulation of digital identities throughout their existence. As their personal information or circumstances change, individuals can update or amend their digital identities. The module also makes it possible to control the privileges and access rights connected to each digital identity. It makes ensuring that only recognized people or organizations have access to particular resources or can take specified actions within the system. The module also permits identity suspension or revocation in the event of malicious behavior or a failure to follow the rules and regulations of the system. Additionally, it offers a user-friendly interface so that users can simply and effectively manage their access control settings and digital identities.

These three modules collectively create a complete digital identity verification management system on the blockchain-based platform by integrating perfectly. By addressing the major issues with identity generation, authentication, verification, management, and access control, they provide users with a safe and dependable digital ecosystem.



VII. RESULT AND DISCUSSION

The blockchain-based system for managing digital identity verification is a highly effective and safe solution that protects the veracity of identities in the digital sphere. Blockchain, which is a decentralized, immutable record, offers a solid framework for managing digital identities.

Each person's identification is safely stored in this system in a digital format on the blockchain. The digital identity is made up of a number of credentials and traits that identify the individual. These credentials could consist of biometric information, official identity, educational credentials, employment histories, and more. This information is made impenetrable and resistant to unauthorized changes by being stored on the blockchain.

The system combines cryptographic

methods and consensus algorithms to confirm a digital identity's legitimacy. Cryptography makes sure that the identification information is kept private and that only those with the proper permissions can access it. Consensus algorithms are used to validate transactions and guarantee the accuracy of the identity data, such as proof of work or proof of stake.

There is no centralized organization in charge of the verification process because the blockchain is decentralized. Instead, the validation and updating of digital identities requires agreement among numerous network members. As a result, there is no longer a need to rely on intermediaries from outside parties, cutting expenses and increasing efficiency. Moreover, blockchain-based digital identity verification management improves security and privacy. Users are in charge of their own identification data and can decide which characteristics to share and with whom. Also, the blockchain's distributed architecture makes it very secure against hackers and data breaches.

Overall, the blockchain-based system for managing digital identity verification offers a dependable and safe alternative for certifying identities in the digital world. It guarantees privacy, does away with the need for middlemen, and offers a high level of protection to thwart criminal activity.

TABLE 1: transaction Throughput

Timestamp	TransactionCount
-----------	------------------

2024-01-11 12:00:00	150
2024-01-11 12:15:00	200
2024-01-11 12:30:00	180

TABLE 2: Smart Contract execution Time

ContractName	ExecutionTime
IdentityVerification	30
CertificateIssuance	25
DataValidation	20

VIII. CONCLUSION

In conclusion, the blockchain ecosystem's approach for managing digital identity verification offers many advantages. By decentralizing user data and using consensus techniques and cryptography to verify identities, it improves security and privacy. It lessens the chance of data breaches and identity theft by doing away with the requirement for centralized authorities. Also, it makes verification processes easy and effective, which lessens

government, because its transparency and immutability also ensure trust and accountability. Overall, the blockchain-based approach for managing digital identity verification shows enormous promise for transforming the way identities are handled and validated in the digital era.

IX. FUTURE WORK

Future advancements in security, privacy, and productivity across a number of industries will be greatly aided by the creation and application of a system for managing digital identity verification. The system's goal is to overcome the problems with conventional identity verification techniques, including fraud, data breaches, and laborious procedures. It will make use of the decentralized nature of blockchain to securely store and confirm digital identities, giving a record of people's credentials that cannot be changed and is impenetrable to tampering. Also, it will give people power over their personal data, allowing them to decide which details to disclose and with whom. By doing away with the need for time-consuming verification steps, cutting costs, and increasing user experience, this system will also streamline processes. Additionally, the accuracy and effectiveness of identity verification will be improved by the use of cutting-edge technology like biometrics, machine learning, and zero-knowledge proofs. Ultimately, the blockchain technology's system for managing digital identity verification holds the potential to completely transform the way identities are handled by introducing a more user-centric and safe method of identity verification in the digital age.

REFERENCES

[1]Shuaib, M., Hassan, N. H., Usman, S., Alam, S., Bhatia, S., Mashat, A., ... & Kumar, M. (2022). Self-sovereign identity solution for blockchain-based

land registry system: a comparison. *Mobile Information Systems*, 2022, 1-17.

[2]Wang, Y., Xu, R., Zhou, C., Kang, X., & Chen, Z. (2022). Digital twin and cloud-side-end collaboration for intelligent battery management system. *Journal of Manufacturing Systems*, 62, 124-134.

[3]Xu, Y., Chen, X., Zhang, H., Yang, F., Tong, L., Yang, Y., ... & Wang, Y. (2022). Online identification of battery model parameters and joint state of charge and state of health estimation using dual particle filter algorithms. *International Journal of Energy Research*, 46(14), 19615-19652.

[4]Cheesman,M.(2022).Self-sovereignty for refugees? The contested horizons of digital identity. *Geopolitics*, 27(1), 134-159.

[5]Zeng, H., Dhiman, G., Sharma, A., Sharma, A., & Tselykh, A. (2023). An IoT and Blockchain-based approach for the smart water management system agriculture. *Expert Systems*, 40(4), e12892.

[6]Rathee, T., & Singh, P. (2022). A systematic literature mapping on secure identity management using blockchain technology. *Journal of King Saud University-Computer and Information Sciences*, 34(8), 5782-5796.

[7]Tan, T. M., & Saraniemi, S. (2023). Trust in blockchain-enabled exchanges: Future directions in blockchain marketing. *Journal of the Academy of marketing Science*, 51(4), 914-939.

57 [8]Yuvaraj, N., Praghash, K., Raja, R. A., & Karthikeyan, T. (2022). An investigation of garbage disposal

914-939.

[8]Yuvaraj, N., Praghash, K., Raja, R. A., & Karthikeyan, T. (2022). An investigation of garbage disposal electric vehicles (GDEVs) integrated with deep neural networking (DNN) and intelligent transportation system (ITS) in smart city management system (SCMS). *Wireless personal communications*, 123(2), 1733-1752.

[9]Lin, H. H., Hsu, I. C., Lin, T. Y., Tung, L. M., & Ling, Y. (2022). After the epidemic, is the smart traffic management system a key factor in creating a green leisure and tourism environment in the move towards sustainable urban development?. *Sustainability*, 14(7), 3762.

[10]Das, M., Tao, X., Liu, Y., & Cheng, J. C. (2022). A blockchain-based integrated document management framework for construction applications. *Automation in Construction*, 133, 104001.

