**Decentralized Identity Management System for Public Sector using Blockchain**

A PROJECT REPORT

submitted

*in the partial fulfilment of the requirements for the award of the degree of*

**BACHELOR OF TECHNOLOGY**

in

**COMPUTER SCIENCE AND ENGINEERING**

by

**Devisetti Upendra (19B81A05P3)**

**Aluka Neeraj Reddy(19B81A05L5)**

**Giri Hruthik Reddy(19B81A05K4)**

Under the guidance of

**Dr. B. Ram Babu**

Professor, CSE Department

****

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**CVR COLLEGE OF ENGINEERING**

**(*An Autonomous institution, NBA, NAAC Accredited and Affiliated to JNTUH, Hyderabad*)**

Vastunagar, Mangalpalli (V), Ibrahimpatnam (M),  
Rangareddy (D), Telangana- 501 510

**Feburary 2023**

**ACKNOWLEDGEMENT**

The satisfaction that accomplishes the successful completion of any tasks would be incomplete without the mention of the people who made it possible and whose encouragement and guidance has been a source of inspiration throughout the course of the project.

It is great pleasure to convey our profound sense of gratitude to our principal **Dr. K Ramamohan Reddy Kasa**, Vice Principal **Prof. L.C. Siva Reddy**, Head of the CSE Department **Dr. A. Vani Vathsala**, CVR College of Engineering for having been kind enough for arranging the necessary facilities for executing the project in the college.

We would like to express my sincere gratitude to my guide, Dr. **B. Ram Babu**, Professor, CSE Dept., CVR College of Engineering, whose guidance and valuable suggestions have been indispensable to bring about the successful completion of our project.

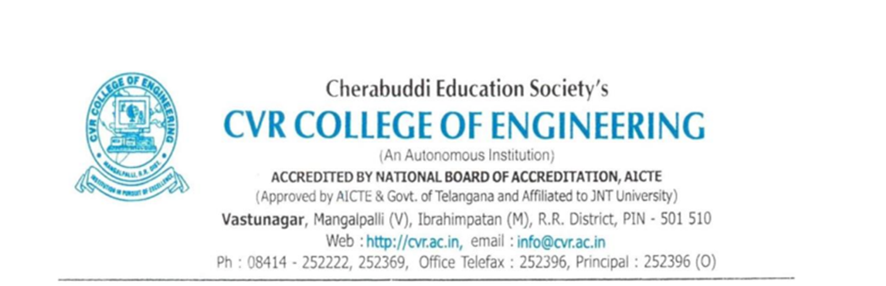
We wish a deep sense of gratitude and heartfelt thanks to management for providing excellent lab facilities and tools. Finally, I thank all those whose guidance helped us in this regard.

**Yours Sincerely,**

Devisetti Upendra (19B81A05P3)

Aluka Neeraj Reddy (19B81A05L5)

Giri Hruthik Reddy (19B81A05K4)

****

**CERTIFICATE**

This is to certify that the project entitled “**Decentralized Identity Management System for Public Sector using Blockchain**” being submitted by **Devisetti Upendra (19B81A05P3), Aluka Neeraj Reddy(19B81A05L5), Giri Hruthik Reddy(19B81A05K4)** in partial fulfilment for the award of Bachelor of Technology in Computer Science and Engineeringto the CVR College of Engineering, is a record of bona fide work carried out by them under my guidance and supervision during the year 2022-2023.

The results embodied in this project work have not been submitted to any other University or Institute for the award of any degree or diploma.

Signature of the project guide, Signature of the HOD

**Dr. B Ram Babu** **Dr. A. Vani Vathsala**

Professor Head of Department (CSE)

CSE Department CVR College of Engineering

External Examiner

**ABSTRACT**

Decentralized Identity Management System (DIMS) deals with the management of individual identities, their authentication, authorization, and privileges within or across systems and enterprise boundaries. If such identity is paper based, it is subject to loss, theft or fraud. A digital identity reduces the complexity of bureaucracy and speeds up the processes within an organization by allowing for greater interoperability between departments and other institutions. Current identity systems face the challenge of single point of failure, lack interoperability and transparency. Also, the systems have privacy issues such as enabling data collection and user tracking. In this project, we presented the blockchain based Decentralized Identity Management and Access Control system which overcomes these challenges. The proposed system allows the user to take control of their own identity (i.e., self-sovereign identity). The system enables everyone in the network to have a single source of truth that is independent of any central authority providing better security and transparency. With zero-knowledge proof and a built-in consent mechanism, an owner is able to convince the verifier that its claims are verified, without providing the credentials.

|  |  |  |  |
| --- | --- | --- | --- |
| **Table of Contents** | | | |
|  | | | Page No. |
|  |  | List of figures |  |
|  |  | Abbreviations |  |
| 1 |  | **Introduction** |  |
|  | 1.1 | Motivation |  |
|  | 1.2 | Problem Statement |  |
|  | 1.3 | Project Objectives |  |
|  | 1.4 | Project report Organization |  |
| 2 |  | **Literature Survey** |  |
|  | 2.1 | Existing work |  |
|  | 2.2 | Limitations of existing work |  |
| 3 |  | **Requirement Analysis** |  |
|  | 3.1 | Functional/Non-functional Requirements |  |
|  | 3.2 | Software requirements |  |
|  | 3.3 | Hardware requirements |  |
| 4 |  | **Proposed System Design** |  |
|  | 4.1 | Proposed methods |  |
|  | 4.2 | Class Diagram |  |
|  | 4.3 | Use case Diagram |  |
|  | 4.4 | Activity Diagram |  |
|  | 4.5 | Sequence Diagram |  |
|  | 4.6 | System Architecture |  |
| 5 |  | **Implementation & Testing** |  |
|  | 5.1 |  |  |
|  | 5.2 |  |  |
| 6 |  | **Conclusion & Future scope** |  |
|  |  | **References:** |  |
|  | |

**1.INTRODUCTION**

**1.1 MOTIVATION**

Over the years, the internet has become a driver of change that has brought about a fundamental shift in everyday life throughout society. The internet, which started as an open and decentralized communication network, has evolved into a backbone of countless applications that propel and bolster globalization and interconnectivity. The ripple effect of internet-driven disruption is evident in virtually any industry sector, including the public sector. We have witnessed the power of national authentication, authorization and privileges of utilizing an Aadhar card.

Moreover, the internet is a double-edged sword that offers easy data exchange and connectivity at the increased risk of compromising confidential data. However, in combination with technologies like blockchain, the internet allows for maintaining data integrity and data ownership across a network of stakeholders. Blockchain systems are known for high transparency, which is important when dealing with multiple stakeholders such as the different transportation authorities. However, the use of any service requires an account management system that allows users to access and manage their data.

**1.2 PROBLEM STATEMENT**

Usually, identity management systems are hosted in centralized databases that are controlled and managed by the service-providing authority. However, organizations such as the World Wide Web Consortium (W3C) have been working on new concepts and standards for decentralized identity solutions. The decentralized identifiers allow for linking users with their associated data without relying on third parties. Thus, users not only gain more control over their data but also gain overall sovereignty from the existing centralized systems, which inherently expose them to risks of data breaches and misuse. The ability to own and control one's private data is one of the core principles of self-sovereign identity, and these fundamentals are also rooted in the concept of blockchain technology.

Digital identity plays an increasingly important role in our interconnected, digitalized society. For example, most of us have several digital identities, associated with our workplace, our personal life, and other professional-related activities. This partly contributes to the growing reliance on identity information management (also referred to as identity management, identity management and access control, etc, in the literature), designed to manage and secure our identity information and to provide relevant services. Building on the success of blockchain, there have also been attempts to integrate blockchain in the design of the next generation of identity management solutions.

In a typical blockchain-based identity management system, there are many distributed nodes (Lim et al., 2018). Such nodes can be utilized to provide distributed storage, reliable access, and computation capabilities. The user in such a system acts as a node in the network; thus, allowing the storage of sensitive user data to shift from servers (in the conventional identity management solutions) to user devices/nodes (in the new blockchain-based paradigm). This facilitates self-sovereign identity (SSI), since the users will now have the capability to regain control of their own identity. Consequently, this minimizes various risks inherent of conventional identity management solutions (e.g., user identity abuse)

**1.3 PROJECT OBJECTIVES**

The objectives of a decentralized identity management system project for the public sector using blockchain technology could include:

1. Improved security: The primary objective of the project could be to improve the security of personal identity data by storing it on a decentralized network of computers, using cryptographic techniques and blockchain technology.
2. Increased control and ownership: Another objective could be to give individuals greater control and ownership of their personal identity data, by allowing them to hold the private keys that give them access to their information.
3. Improved efficiency: The project could aim to improve the efficiency of the identity management system by using a decentralized network of computers to manage data transactions, reducing processing times and wait times for individuals trying to access their information.
4. Cost savings: The project could aim to reduce the cost of identity management for public sector organizations by reducing the need for specialized hardware and software, as well as a large IT infrastructure.
5. Compliance with regulations: The project could aim to ensure that the decentralized identity management system complies with relevant data privacy and security regulations, such as the General Data Protection Regulation (GDPR) in Europe.
6. Increased trust and confidence: The project could aim to increase trust and confidence in the identity management system, by providing a secure, transparent, and decentralized solution for managing personal identity data.
7. Integration with existing systems: The project could aim to integrate the decentralized identity management system with existing systems and processes within the public sector, ensuring a seamless transition to the new system.

In summary, the objectives of a decentralized identity management system project for the public sector using blockchain technology could include improved security, increased control and ownership, improved efficiency, cost savings, compliance with regulations, increased trust and confidence, and integration with existing systems.

**1.4 PROJECT REPORT ORGANIZATION**

1. This report is divided into 6 chapters after this introductory chapter.
2. Chapter 2 deals with literature survey and limitations of existing system.
3. Chapter 3 summarizes functional, non-functional requirements and system requirements along with software and hardware specifications.
4. Chapter 4 deals with analysis and design of the proposed model which includes use case diagram etc.
5. Chapter 5 encloses Implementation and testing of the proposed model and testing with different scenarios.
6. Chapter 6 includes conclusion and future work.
7. Chapter 7 includes reference.

**2. LITERATURE SURVEY**

**2.1 EXISTING WORK**

Before the implementation of a decentralized identity management system for the public sector using blockchain technology, most organizations relied on centralized identity management systems. A centralized identity management system is controlled by a single entity, such as a government agency or a corporation, and all personal identity data is stored in a centralized database. This database is managed and maintained by the entity in control, who is responsible for ensuring the security and privacy of the data.

In centralized identity management systems, individuals had limited access to their personal identity information and were typically required to go through the centralized entity to make any changes or request information. This often involved filling out forms, submitting documentation, and waiting for a response, which could take several days or even weeks. In addition, the centralized entity had complete control over the personal identity information, which raised concerns about data privacy and security.

The centralized system also required specialized hardware and software to manage the centralized database, as well as a large IT infrastructure to support the system. This could be expensive and time-consuming to maintain, particularly for public sector organizations that have limited resources.

These limitations led to the development of decentralized identity management systems using blockchain technology. Decentralized systems store personal identity data on a decentralized network of computers, with no single entity in control. This eliminates the risk of a single point of failure and makes the system more secure and resistant to hacking and cyberattacks. In addition, decentralized systems use cryptographic techniques and blockchain technology to secure personal identity information, providing individuals with greater control and ownership over their data.

The decentralized identity management system for the public sector using blockchain technology offers a more secure, efficient, and cost-effective solution for managing personal identity data. By decentralizing the control of personal identity information and using blockchain technology, it provides individuals with greater control and ownership of their data, and reduces the risk of data breaches and other security threats.

**2.2 LIMITATIONS OF PREVIOUS SYSTEM**

Before the advent of decentralized identity management systems using blockchain technology, most public sector organizations relied on centralized identity management systems. These systems were controlled by a single entity, usually a government agency or a corporation, and stored identity information in a centralized database. The centralized system had several drawbacks:

1. Vulnerability to hacking and cyberattacks: Centralized systems are a single point of failure, making them vulnerable to hacking and cyberattacks. In the event of a successful attack, the attacker would have access to sensitive information, such as personal identity data, stored in the central database.
2. Lack of control and ownership of personal data: With a centralized system, individuals have limited control and ownership of their personal data, as it is controlled and managed by a single entity.
3. Inefficiency and slow processing times: Centralized systems are often slow and inefficient, as all requests for data must pass through a single point. This can result in long wait times for individuals trying to access their personal information.
4. High costs: Centralized systems can be expensive to implement and maintain, as they require specialized hardware and software and a large IT infrastructure to manage the centralized database.

The decentralized identity management system for the public sector using blockchain technology addresses these limitations by providing a secure, decentralized, and cost-effective solution for managing personal identity data. With a decentralized system, personal identity information is stored on a decentralized network of computers, making it more secure and resistant to hacking and cyberattacks. Additionally, individuals have greater control and ownership of their personal data, as they hold the private keys that give them access to their identity information. Finally, decentralized systems are typically faster and more efficient, as they rely on a distributed network of computers to manage data transactions.

**3.REQUIREMENT SPECIFICATION**

**3.1 FUNCTIONAL / NON-FUNCTIONAL REQUIREMENTS**

**FUNCTIONAL REQUIREMENTS**

Functional requirements for implementing a decentralized identity management system for the public sector using blockchain technology could include:

1. Decentralized data storage: The system should be able to store personal identity data on a decentralized network of computers, with no single entity in control.
2. Cryptographic security: The system should use cryptographic techniques and blockchain technology to secure personal identity information and protect it from unauthorized access.
3. User authentication: The system should provide a secure method for users to authenticate themselves and access their personal identity data.
4. Data privacy: The system should comply with relevant data privacy regulations, such as the General Data Protection Regulation (GDPR), and provide individuals with control over their personal identity information.
5. Integration with existing systems: The system should be able to integrate with existing systems and processes within the public sector, to ensure a seamless transition to the new system.
6. Access control: The system should have a robust access control mechanism to ensure that only authorized users can access personal identity information.
7. Scalability: The system should be scalable to accommodate a large number of users and handle the increasing volume of data transactions.
8. User-friendly interface: The system should have a user-friendly interface that is easy to use and understand for both technical and non-technical users.
9. Audibility: The system should provide an auditable trail of all data transactions to ensure transparency and accountability.
10. Performance: The system should have sufficient performance capabilities to handle the demands of a large number of users and provide fast and reliable access to personal identity data.

In summary, functional requirements for implementing a decentralized identity management system for the public sector using blockchain technology could include decentralized data storage, cryptographic security, user authentication, data privacy, integration with existing systems, access control, scalability, user-friendly interface, audibility, and performance.

**NON-FUNCTIONAL REQUIREMENTS**

Non-functional requirements for implementing a decentralized identity management system for the public sector using blockchain technology could include:

1. Security: The system should have strong security measures in place to protect personal identity information from unauthorized access, data breaches, and cyberattacks.
2. Privacy: The system should ensure the privacy of personal identity information by complying with relevant privacy regulations, such as the General Data Protection Regulation (GDPR).
3. Availability: The system should have a high level of availability to ensure that users can access their personal identity information when needed.
4. Reliability: The system should be reliable and consistent in its performance, with minimal downtime and errors.
5. Usability: The system should be user-friendly and easy to use, with a clear and intuitive interface.
6. Interoperability: The system should be interoperable with other systems and processes within the public sector, to ensure a seamless integration and reduce the risk of data duplication or loss.
7. Performance: The system should have adequate performance capabilities to handle a large number of users and data transactions.
8. Scalability: The system should be scalable to accommodate future growth and changing demands.
9. Compliance: The system should comply with relevant industry and government standards, such as ISO 27001 for information security management.
10. Maintainability: The system should be maintainable and easily updatable, with clear documentation and support resources.

In summary, non-functional requirements for implementing a decentralized identity management system for the public sector using blockchain technology could include security, privacy, availability, reliability, usability, interoperability, performance, scalability, compliance, and maintainability. These requirements are critical for ensuring the long-term success of the system and protecting the privacy and security of personal identity information.

**3.2 SOFTWARE REQUIREMENTS**

**3.2.1 V S Code**

Visual Studio Code (VS Code) is a free, open-source, and cross-platform code editor developed by Microsoft. It is widely used by developers for software development, web development, and data analysis.

One of the key features of VS Code is its support for a wide range of programming languages and file formats, including JavaScript, TypeScript, Python, HTML, CSS, and more. It also includes several built-in extensions, such as Git integration and debuggers, making it a versatile and flexible development environment.

Another key feature of VS Code is its lightweight design, which allows it to run smoothly on a wide range of hardware, including laptops and low-end computers. Despite its lightweight design, VS Code still offers several advanced features, such as code completion and linting, that help developers to write better code and catch errors before they become problems.

The user interface of VS Code is highly customizable, allowing developers to tailor the look and feel of the code editor to meet their individual needs. It also includes a number of helpful tools, such as the integrated terminal, which enables developers to run command-line tools and scripts directly within the code editor.

**3.2.2 NPM**

NPM, which stands for Node Package Manager, is a package manager for the JavaScript programming language. It is widely used by developers to manage the packages and dependencies needed for their projects.

One of the key features of NPM is its vast library of packages, which contains thousands of pre-written code modules that can be easily installed and used in projects. This library allows developers to save time and effort by reusing existing code instead of writing everything from scratch. Additionally, NPM automatically handles the installation of dependencies, making it easy for developers to manage their project's dependencies and ensure that everything works together correctly.

Another key feature of NPM is its ability to manage different versions of packages, enabling developers to use different versions of the same package in different projects. This allows developers to take advantage of new features and bug fixes in newer versions of packages while still maintaining compatibility with older versions.

NPM is also designed to be easy to use and integrate with other development tools. It includes a simple command-line interface that makes it easy to install and manage packages, as well as APIs that can be used by other tools and scripts to automate package management tasks.

**3.2.3 REACT**

React is a popular JavaScript library for building user interfaces. It was developed by Facebook and is now maintained by Facebook and a large community of individual developers and companies.

One of the key features of React is its ability to build complex and dynamic user interfaces using reusable components. React components are small, modular pieces of code that can be easily combined to build larger and more complex user interfaces. This makes it easier for developers to manage and maintain their code, and it also allows for greater reuse and consistency across different parts of the user interface.

Another key feature of React is its virtual DOM (Document Object Model), which is a lightweight in-memory representation of the actual DOM. The virtual DOM allows React to update the user interface more efficiently, by only changing the parts of the DOM that have actually changed, instead of having to update the entire DOM every time there is a change.

React is also highly modular and easy to use with other libraries and tools. It can be easily integrated with a wide range of other libraries, such as Redux for state management, and it can also be used in conjunction with server-side rendering technologies, such as Node.js, to build fast and scalable web applications.

**3.2.4 SOLIDITY**

Solidity is a contract-oriented, high-level programming language used to write smart contracts on the Ethereum blockchain. It was developed specifically for writing decentralized applications and is used to define the rules and conditions under which these applications will operate.

One of the key features of Solidity is its contract-oriented nature, which allows developers to define the terms and conditions of their applications in a clear and concise manner. This makes it easier for developers to reason about their code and to ensure that it will behave as intended in a decentralized environment.

Another key feature of Solidity is its support for inheritance and libraries, which enables developers to reuse code and build more complex and sophisticated smart contracts. This helps to reduce the amount of code that needs to be written and makes it easier for developers to manage and maintain their contracts over time.

Solidity is also designed to be secure, with built-in support for common security patterns, such as access control and error handling. It also has a growing ecosystem of tools and libraries, such as Remix and Truffle, that make it easier for developers to build and deploy their contracts to the Ethereum network.

**3.2.5 QUICKNODE**

QuickNode is a cloud-based platform that provides scalable and secure infrastructure for developers building decentralized applications (dapps) on the Ethereum blockchain. It is designed to make it easy for developers to access the resources they need to build, test, and deploy their dapps, without having to worry about the underlying infrastructure.

One of the key features of QuickNode is its scalability, which enables developers to easily add more resources to their dapps as they grow in popularity and usage. This helps to ensure that dapps continue to perform well and provide a seamless user experience, even as they become more popular and attract more users.

Another key feature of QuickNode is its security, which provides developers with a secure and reliable platform for building and deploying their dapps. QuickNode uses state-of-the-art security measures, such as SSL encryption and DDoS protection, to keep dapps and their data safe from malicious actors.

QuickNode also provides developers with a range of tools and resources to help them build and deploy their dapps, including a development sandbox, an API explorer, and integrations with popular development tools and frameworks, such as Remix, Truffle, and React.

**3.2.6 METAMASK**

MetaMask is a popular browser extension and digital wallet that allows users to securely interact with decentralized applications (dapps) built on the Ethereum blockchain. It provides users with a simple and intuitive interface for managing their digital assets and interacting with dapps, making it easier for people to participate in the growing world of decentralized finance (DeFi) and other blockchain-based applications.

One of the key features of MetaMask is its ease of use, which allows users to set up a digital wallet quickly and easily and start using dapps without having to navigate complex user interfaces or command-line tools. This makes it a valuable tool for people who are new to blockchain technology and want to participate in DeFi and other decentralized applications.

Another key feature of MetaMask is its security, which provides users with a secure and reliable way to manage their digital assets. MetaMask uses advanced security features, such as secure key storage and encrypted private key management, to keep users' assets safe from malicious actors.

MetaMask also provides users with a range of tools and resources to help them interact with dapps and manage their digital assets. This includes an intuitive interface for managing their wallet and digital assets, and a library of supported dapps and decentralized exchanges (DEXs).

**3.2.7 ETHEREUM**

Ethereum is a decentralized, open source blockchain platform that enables the creation and execution of smart contracts and decentralized applications (dapps). It was created in 2014 by Vitalik Buterin and has since become one of the most popular blockchain platforms in the world, with a thriving developer community and a wide range of decentralized applications built on top of its platform.

One of the key features of Ethereum is its support for smart contracts, which are self-executing contracts with the terms of the agreement directly written into code. This makes it possible to automate complex transactions and processes, such as financial transactions and supply chain management, in a transparent and secure way.

Another key feature of Ethereum is its support for decentralized applications, which are applications that run on a decentralized network of computers, rather than on a centralized server. This makes it possible to build a wide range of applications that are transparent, secure, and resistant to censorship and tampering.

Ethereum also provides developers with a range of tools and resources to help them build and deploy their decentralized applications, including the Solidity programming language, the Remix development environment, and a robust developer community.

**3.3 HARDWARE REQUIREMENTS**

A system with the following specifications can be used to implement this project:

* Processor: Intel core i5 or i7
* RAM: 8GB or above
* Storage: 100 GB or above
* Operating System: Windows 10 or above