

DESIGN AND IMPLEMENTATION OF A DECENTRALIZED IDENTITY MANAGEMENT SYSTEM USING A BLOCKCHAIN TECHNOLOGY

¹Longinus. S. Ezema, ²G. N. Ezech, ³Olalomi, Suleman Alani, ⁴Ogbonna Alexander Chisom

⁵Agu Raymond Stephen

¹²³⁴⁵Department of Electrical and Electronic Engineering, School of Electrical Systems Engineering Technology,
Federal University of Technology, Owerri (FUTO)

Corresponding author Email: longinus.ezema@futo.edu.ng

ABSTRACT: In the rapidly evolving digital landscape, the significance of digital identities has grown immensely. These digital identities serve as virtual representations of individuals, enabling access to a myriad of online services and interactions. However, traditional identity systems, which rely on centralized authorities for authentication and management, present various challenges that impede the realization of a secure and user-centric identity ecosystem. Decentralized identity places the control of personal information back into the hands of the users themselves. By leveraging the principles of blockchain technology, SSI offers a more secure, transparent, and user-centric approach to identity management. At the heart of decentralized identity systems lies blockchain technology, a distributed and immutable ledger that ensures data integrity and eliminates the need for a central authority. Blockchain's decentralized consensus mechanism guarantees the tamperresistance and authenticity of user identity information. This paper proposes a school-based model of DecentralizedIdentity-Management system using the Federal University of Technology Owerri (FUTO), Electrical and Electronic Engineering department as case study to implement a functioning system. Furthermore, it proposes some suggestions on how this system can be further innovated and integrated into the university identity management systems.

keywords: Blockchain Technology, Decentralization, Distributed Ledger, Identity management systems, Smart Contracts

INTRODUCTION

Identity Management System (IDMS) refers to how users or individuals are identified and authorized to use organizational systems and services. The Identity Management System (IDMS) is a collection of policies and technologies that work together to ensure that the relevant users within an organization have access to technology resources such as applications systems, specific services, data, and cloud platforms. It guards against illegal access to systems and resources and generates alerts when unauthorized personnel or programs try to access information the management and authentication of digital identities. The purpose of a sophisticated IDMS is to improve the security of data and system productivity while lowering costs, and repetitive tasks. However, there exist several problems with the traditional IDMS, such as theft, fraud, lack of control, and loss of data. [1]Moreover, the

cumbersome and time-consuming verification processes in centralized systems can hinder user adoption and create barriers for individuals without easy access to official identification documents. The need to repeatedly verify identity information across various platforms also leads to redundancy and inefficiency. To address these challenges, a new paradigm called decentralized identity, or self-sovereign identity (SSI), has emerged. Decentralized identity places the control of personal information back into the hands of the users themselves. By leveraging the principles of blockchain technology, SSI offers a more secure, transparent, and user-centric approach to identity management.

Blockchain-based decentralized identity management provides a promising solution to improve the security and privacy of healthcare systems and make them scalable. In contrast, decentralized identity management based on the blockchain can ensure secure and transparent access to student's data while preserving privacy. This approach enables students to control their personal academic records while granting permission for authorized personnel to access specific information as needed. Blockchain technology and distributed ledger (DL) are generating a lot of buzz and spurring many initiatives in various industrial sectors. Nonetheless, the financial sector is seen as the primary user of blockchain technology. Blockchain technologies' emergence enables self-governing identities to practice decentralization where each node that participates is separate from the others. Instead of adopting a centralized authority's guidelines, distributed entities use common standards to connect yet preserve their independence and maintain internal confidentiality. An identity authentication system is required to keep the environments secure because of this decentralization of the network. Though blockchain is a relatively new technology, it possesses properties of transparency, immutability, credibility, tamper resistance, traceability, and decentralization necessary for various applications. [2] Using blockchain for identity management can give individuals ownership of their identities by providing a global ID that can be used for diverse purposes. The verification of digital identity confirms that individuals on digital platforms are who they appear to be. Identity verification and the security of confidential information are core components of trust in identity management. Personal information used to authenticate someone's identity, such as a name or unique identity number, is recorded on the block's hash using the blockchain authentication scheme. SelfSovereign Identity (SSI) is a form of digital identity management that empowers individuals with control over their digital identities. [3] The vision of decentralized identity extends beyond individual empowerment. It has the potential to revolutionize various industries, including finance, healthcare, and e-government services.

I. LITERATURE REVIEW

A framework known as an identity management system (IDM) assists organizations in managing and controlling user identities, authentication, and authorization across various applications and systems. While protecting data privacy, it makes sure that resources are accessible securely and effectively. The nature of Identity Management (IDM) systems can vary, and they can be both centralized and decentralized, depending on the architecture and design.

Centralized IDM: In a centralized IDM system, user identities, authentication, and authorization policies are managed and controlled from a single point of administration. This approach offers unified control over access and

security, making it easier to manage user accounts, permissions, and compliance. Traditional on-premises IDM systems often follow this centralized model.

Decentralized IDM: Some modern IDM systems adopt a decentralized approach, where identity information is distributed across various interconnected systems. Decentralized systems may use technologies like blockchain to enable secure and verifiable identity management without relying on a central authority.

Hybrid IDM: Many organizations adopt a hybrid approach, combining elements of both centralized and decentralized IDM. For instance, they might use a central identity provider for authentication and access control while allowing decentralized management of user attributes.

In order to accommodate various use cases and requirements within an organization, Identity Management (IDM) systems may need to incorporate more than one specific management style. A more complete and flexible solution may be offered by the ability to support various management styles. The modularity, extensibility, and compatibility of the IDM system should be taken into consideration when creating it in order to successfully integrate various management styles. This enables the organization to maintain a unified and manageable IDM ecosystem while selecting and configuring the appropriate style for various use cases.

The challenges faced by Centralized Identity Management Systems include; Single Point of Failure, Scalability, Performance Bottlenecks, Data Privacy Concerns, Compliance Challenges, Vendor Lock-In, Limited Flexibility, Complex Migration, Costs and Resources, and Resistance to Change

The fundamental principles and architecture of decentralized identity systems include; Self-Sovereign Identity (SSI), Verifiable Credentials, and Decentralized Identifiers (DIDs) while some blockchain technology concepts and principles includes; Distributed Ledger, Cryptographic Hashing, Consensus Mechanisms, Decentralization, Transparency and Auditability, Smart Contracts and Privacy and Security.

Blockchain creates an SSI or DTI across distributed systems by ensuring trust, and privacy. Several companies and information technology organizations are concentrating their efforts on creating BC-based digital IDMS. Below, we discuss some major BCbased IDMS offered in the market

U.PORT: uPort is an open-source decentralized identity framework that seeks to give everyone a decentralized identity. It uses a public permissionless Ethereum blockchain and multiple smart contracts to maintain SSI. It consists of a mobile application, multiple Ethereum smart contracts, and a public registry for uPort identities. Using this framework, users can safely disclose their identity, including the transfer of credentials for accessing different services, signing transactions, and managing keys and data securely. However, the original uPort project has been divided into two new projects, Veramo and Serto, both aiming to give users control over their identity data. Veramo is a JavaScriptbased framework that facilitates the usage of cryptographically verified data in applications utilized by anyone. Serto offers organizations to get started with DIDs and VCs. It is built on W3C open standards. In addition, uPort mobile applications, libraries, and services are deprecated now [4]

SOVRIN: Sovrin is a public blockchain that anyone can use without obtaining prior authorization. It is based on a permissioned blockchain Hyperledger Indy, which means that only verified nodes can participate in the consensus procedure. Sovrin employs a voting ledger to grant permissions to nodes. The nodes are divided into two types, validators and observers. Validator nodes are permitted to commit new blocks in the blockchain, which contains

transactions. Observer nodes, in contrast, only read the blockchain data. Nodes, particularly validators, need unique privileges to join the network. A quorum of the board of trustees determines which privileges are granted. According to the rules, this board's trustees can elect new members and choose stewards. Stewards are entities (trusted organizations within the ecosystem) responsible for performing consensus and managing validator nodes. Sovrin employs ZKP for all valid identity claims to keep data disclosure to a minimum. [5]

SHOCARD: ShoCard provides business users with a service for authentication and permission for information. It is a public Bitcoin blockchain-based digital identity and authentication platform. It enables individuals and companies to identify each other in a safe and verifiable manner to enable any transaction to be performed swiftly, effortlessly, and with peace of mind. ShoCard identities are kept in the bitcoin blockchain. Users have their private keys on their phones or PCs, and they also have a public key that services can use to authenticate their identity with ShoCard. Though is built on top of a public blockchain, its architecture is engineered to be very scalable. However, Shocard does not provide minimization of data. [6]

SELFKEY: SelfKey is a decentralized, BC platform for the SSI environment. It is an Ethereum-based platform that allows individuals to exchange their identification traits with certifiers and service providers such as notaries and banks. Individual users' data is stored on the user's device, which is within the user's control. Other entities can only access specific data if they have been granted permission. [7]

CIVIC: Civic resembles and functions similarly to a digital wallet, except instead of storing money, it safeguards personal information while enabling users to share it selectively. Here, identification information is maintained on the user's device so it is constantly available. The Civic application provides several identity-aware features, ranging from password-free online logins to secure storage of sensitive data such as healthcare information, and bank statements. It authenticates users with the use of a smartphone fingerprint scanner. The data may then be shared directly with businesses and people, who can verify it using Bitcoin's blockchain. After a user submits identity data, Civic checks it against the phone, credit card, social media, and other public records using several identity validation service providers. In order to establish a secure digital identity, civic users rely on authentication authorities, resulting in a lack of portability. Civic achieves a high pass rate for genuine users. It limits the dangers of fraudulent conduct by integrating various reliable sources with fraud detection algorithms, and manual auditing. It distributes verified identification data to the user's Civic App and blockchain attestations.[8]

To solve the issue of identity management and enable smooth running of digital system in FUTO, a Decentralized Identity Management System (DIM) using the polygon blockchain and Solidity smart contracts is proposed in this work. The DIM system provides a secure and efficient way to manage and verify identities in a decentralized manner. Through the use of smart contracts, access control mechanisms, and cryptographic techniques, we have established a reliable platform for creating, updating, and storing student profiles, documents, and approvals. The system ensures transparency, immutability, and user autonomy in managing identity-related data

II. SYSTEM DESIGN

The system requirements of the implementation of the DIDMS using the polygon blockchain is provided by the solidity smart contract to ensure smooth operation of the system. These requirements include:

Roles and Permissions: The contract implements an access control system with roles like "Admin" and "regular". The owner of the contract can manage roles and permissions. Admins can mint student identities and create profiles, while regular users(students) can update their own profiles.

Student Management: Admins can mint student identities with details like name, registration number, and department. Students can update their own profile information.

Profile Management: Users can create profiles associated with their identities. Profiles contain document information, such as document name and hash, stored in a nested mapping structure. Users can list and remove profiles associated with their identity.

Approval System: Admins can approve students and grant them access to the system. Admins can approve students to delete their profiles.

Events: The contract emits events for actions like minting, updating, setting, and removing profiles. Events serve as a way to track and log activities on the blockchain. Overall, the contract aims to provide a decentralized identity management system where students can create and manage their profiles while adhering to specified roles and permissions. The smart contract ensures data integrity and security by utilizing the Ethereum blockchain's decentralized nature and cryptographic functions.

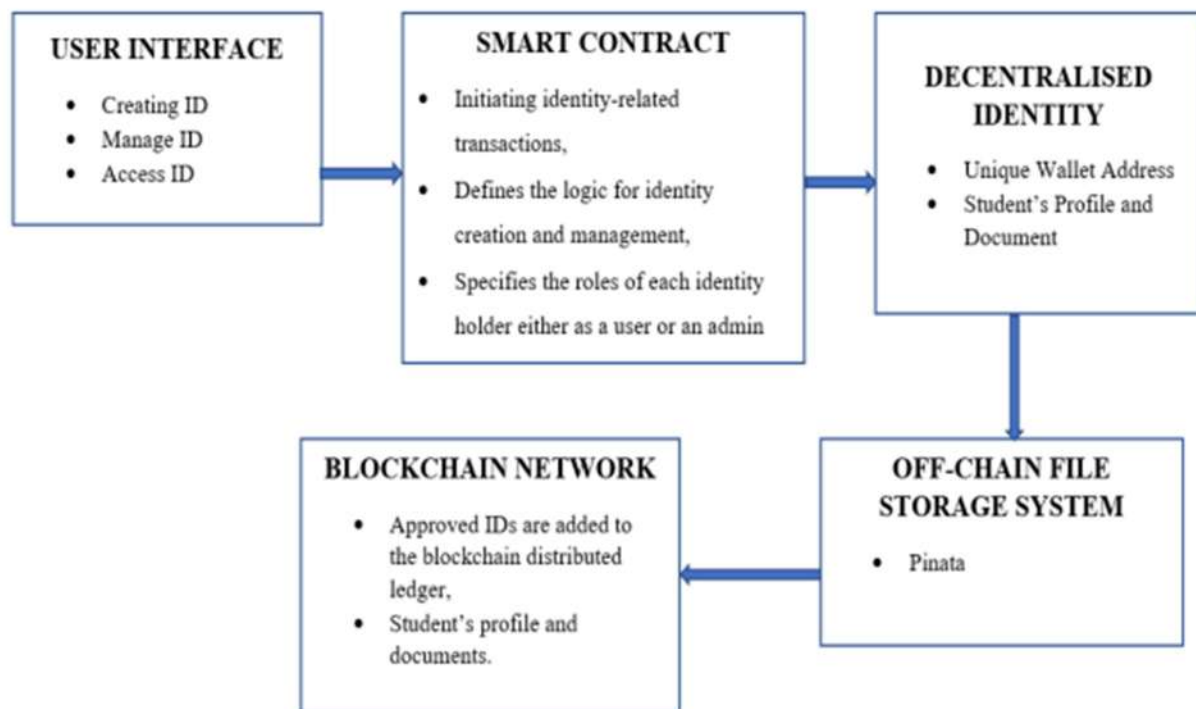


Figure 1: Block diagram of the Decentralised Identity Management System

This research explores the extensive system architecture that supports the DID Management System. It describes the structure, elements, and interactions that make up this creative solution's framework. Each component of the

system design, from DID creation and registration to authentication, authorization, and interoperability, has been painstakingly constructed to guarantee not just technological brilliance but also adherence to privacy laws and industry best practices. The system architecture provides an overview of the components and their interactions within the blockchain-based voting system. It typically consists of the following key components;

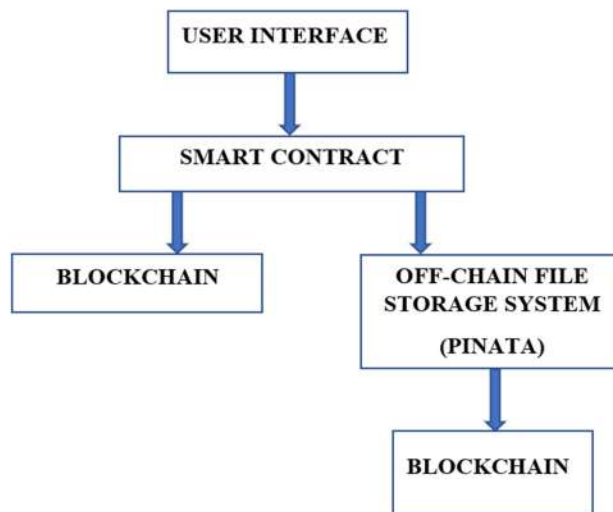


Figure 2: System Architecture Diagram

User Interface Layer

The user interface (UI) of the DIDMS is crucial for user interaction. It was designed to be user-friendly, intuitive, and visually appealing. Users should be able to create, manage, and update their identities easily. The UI facilitates the issuance and verification of digital credentials, as well as access control and permissions. It interacts with blockchain smart contracts for seamless actions and guides users in secure authentication and key management. Real-time updates and multi-platform support enhance user experience. Overall, a well-designed front end is vital for user engagement and effective utilization of your blockchain-based identity management solution.

Smart Contract Layer

The smart contract layer is a crucial part of this decentralized identity management system, governing interactions and processes on the blockchain. Smart contracts automate actions, enforce rules, and ensure data integrity. This layer provides transparency, immutability, and accountability through verifiable transactions. The Smart contracts support decentralized governance, secure identity transactions, and interoperability with other systems. They enable conditional execution and reduce the need for intermediaries. Ultimately, smart contracts empower users with self-sovereign identity, revolutionizing identity management by combining automation, security, and decentralization for a user-centric and efficient system.

Blockchain Layer

The blockchain layer is essential for your decentralized identity management system using blockchain technology. It ensures trust and security by decentralizing data across nodes, preventing unauthorized changes through consensus mechanisms like PoW or PoS. Immutability guarantees tamper resistance, critical for reliable identity data. Transparency and auditability come from recording all changes on the blockchain, enhancing accountability. Interoperability lets the blockchain integrate with external systems. This layer establishes a strong foundation for secure, user-controlled identity management.

The Off-Chain Layer

The off-chain layer is a vital part of your decentralized identity management system, working alongside the blockchain layer to improve scalability and handle certain types of data more efficiently. It stores large files using IPFS(pinata), manages frequently changing data, and handles sensitive information with encryption. This layer also boosts interoperability with external systems, enhancing overall system performance. By combining blockchain and off-chain approaches, your system achieves optimal efficiency in storing critical data while managing other data types effectively. This creates a comprehensive identity management solution with improved scalability and privacy features.

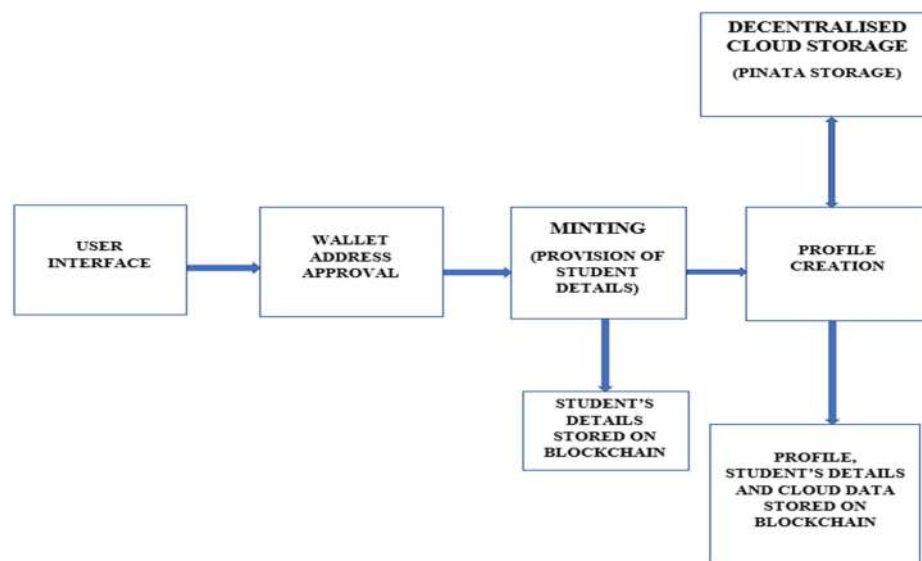


Figure 3: The Flow Diagram of the Implementation of the DIDMS

Application Of the Smart Contract to the Project:

Identity Management: The contract facilitates the creation and management of student identities. Students can be "minted" into the system, creating a new identity record that includes their name, registration number, department, and timestamp. The "Admin" role allows approved users to perform identity-related operations, such as minting, updating, and deleting student identities.

Access Control: The "Access Control" contract provides role-based access control. The contract owner is the primary administrator with the highest privileges ("Admin" role). They can approve students, revoke approvals, and grant access rights to perform specific functions within the system

Student Approval: The contract allows the contract owner to approve or revoke approval for students. Approved students gain the "Admin" role, enabling them to perform identity-related functions. This functionality ensures that only authorized individuals can participate in the identity management process.

Identity Data Modification: The "mint" and "update" functions enable students and the contract owner to modify identity information. This ensures that students can update their records if needed while maintaining data integrity and transparency.

Profile Creation and Management: The contract allows students to create profiles and store associated documents securely on the blockchain. Third parties and individual users can interact with these profiles to access verified information. The "approvedToDelete" functionality ensures that students can also delete their profiles, providing control over their personal data.

Event Logging: The contract emits events, such as "Mint," "Burn," "Update," "SetProfile," and "RemoveProfile," to provide transparency and allow external systems to react to state changes. Some of the Applications used for the implementation of this work are Nodejs, VsCode, Remix Ethereum, Pinata cloud, Polygon Mumbai and Reactjs.

III. RESULTS AND DISCUSSIONS

Role Management

Admin Role: The contract owner is initially set as an Admin. Admins have the highest level of access and control over the contract. They can perform administrative tasks such as approving students and managing roles.

Regular Role: Users who are not Admins fall into the "regular" category. They have limited access and can perform actions related to their own profiles, such as creating, updating, and deleting their data.

Student Management

Minting a Student Profile: Authorized users (Admins or the contract owner) can authorize the mint of a new student profile. To mint a student profile, the user(student) submits their wallet address to the admin for approval. After being approved, the user provides the student's name, registration number, and department. A timestamp is recorded for when the student profile is created and the student profile count is incremented. The student's information is stored in the students mapping with their address as the key.

Burning a Student Profile: Students or the contract owner can burn (delete) a student profile. When burning a profile, the student's data is deleted, including associated profiles and documents. Users are only allowed to delete their own profiles unless they have Admin privileges.

Updating a Student Profile: Students or the contract owner can update their own profile information. The updated information includes the name, registration number, and department. An event is emitted to indicate that the profile has been updated.

Profile Management

Creating a Profile: Authorized users can create a profile for an existing student. Profiles are associated with a specific student and can store documents. Users can attach documents to a profile by providing a document name and its hash. The profile count for the associated student is incremented. Figures 4 and 5 show student profile creation page and all the individual documents that the students uploaded in the creation of student's profiles.

Removing a Profile: Students can request the removal of their own profile data. Admin approval is required for profile deletion, which can be granted using the “approveDeleteforStudentProfile” function. Once approved, students can use the “removeProfile” function to delete their profiles and associated documents.

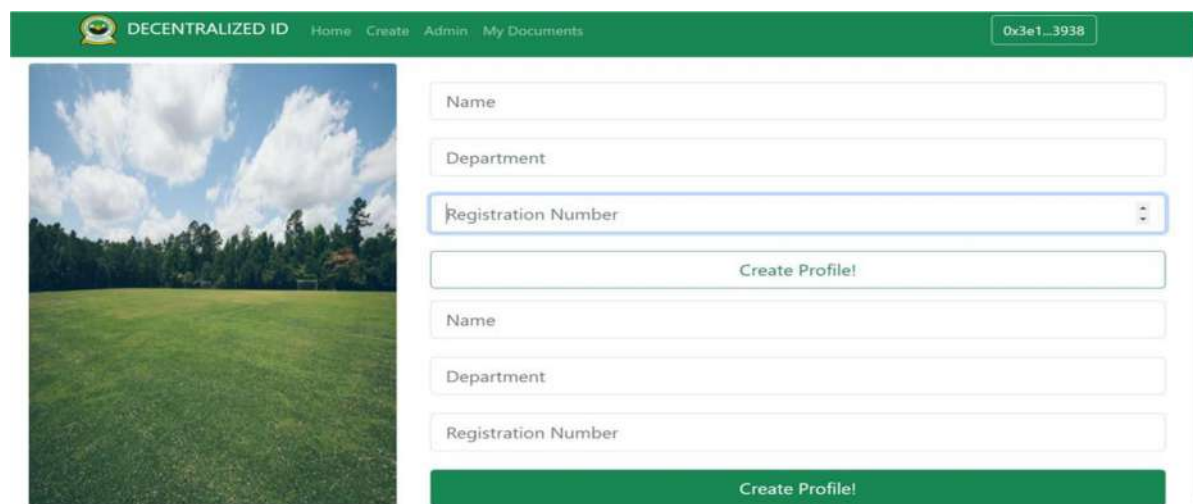


Figure 4: Student Profile Management Page

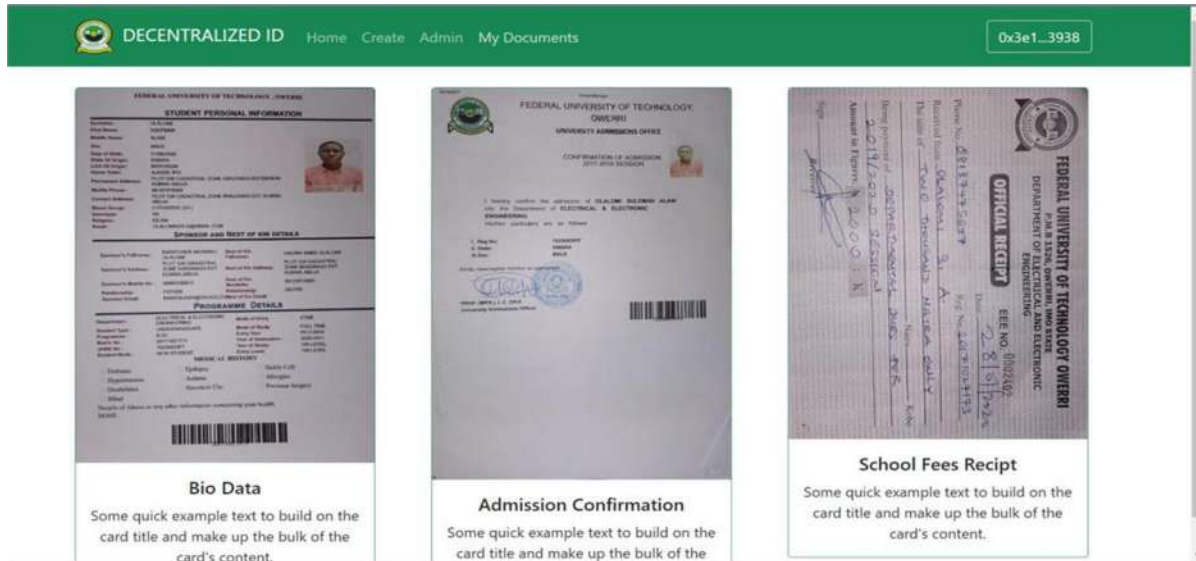


Figure 5: Student Document Page

Approval Management

Approving and Revoking Student Status: The contract owner (Admin) can approve or revoke a student's status. Approved students have certain privileges within the contract. Revoking approval limits the student's access to contract functions. Events are emitted when student approval status changes.

Approving Profile Deletion: The contract owner can approve or revoke a student's ability to delete their profile data. Admin approval is required for profile deletion, which can be granted using the "approveDeleteforStudentProfile" function.

Batch Operations

Batch Approving Students: The contract owner can use the batchApprove function to approve multiple students in a single transaction.

Querying

Checking Student Existence: Users can check whether a student profile exists using the "hasStudent" function. **Retrieving Student and Profile Information:** Users can retrieve student information (name, registration number, department) using the "getStudent" function. Users can retrieve specific profile information (name, registration number, department, document details) using the "getProfile" function. Users can list all profiles associated with a student using the "listProfiles" function.

System Testing and Evaluation

To validate the functionality and performance of the DIDMS the different functions specified in the smart contract were tested by multiple users on different device to ensure the proper operation of the system. A user-friendly and

intuitive interface is crucial to ensure smooth user interactions with the voting system. This has to do with the design principles, usability testing, and accessibility considerations for the user interface. It covers aspects such as clear instructions, visual design, support for multiple languages, and compatibility with assertive technologies.

IV. CONCLUSION

The Decentralized Identity Management System offers a promising solution to the challenges associated with centralized identity management. By leveraging blockchain technology, we have created a tamper-proof and auditable record of student identities and associated documents. This system enhances data security, minimizes the risk of identity fraud, and provides individuals with greater control over their personal information. Through the implementation of access control and role-based permissions, we have established a robust framework for managing user interactions and data sharing. We have addressed key challenges in traditional identity management systems, such as data privacy, security, and user autonomy. The use of cryptographic techniques, immutability, and decentralized storage ensures that identity information remains tamper-proof and resistant to unauthorized access. The system's architecture, including access control mechanisms and role-based permissions, provides a fine-tuned level of control over data sharing and interactions. The DIMS System underscores the transformative potential of blockchain technology in reshaping traditional identity management paradigms. By empowering individuals with control over their identity data and providing a secure, transparent, and efficient verification process, the project opens doors to a new era of decentralized identity management that prioritizes privacy, security, and user empowerment.

REFERENES

- [1] Md. Rayhan Ahmed , A. K. M. Muzahidul Islam, Swakkhar Shatabda, and Salekul Islam, "Blockchain-based Identity Management System and Self Sovereign Identity," IEEE Access, vol. 10, 2022. <https://ieeexplore.ieee.org/document/9927415>
- [2] H. Wang and Y. Jiang, "A novel blockchain identity authentication scheme implemented in fog computing," Wireless Communications and Mobile Computing, Vol. 2020, pp. 1–7, Aug. 2020. <https://www.hindawi.com/journals/wcmc/2020/8849363/>
- [3] M. S. Ferdous, F. Chowdhury, and M. O. Alasaifi, "In search of self sovereign identity leveraging blockchain technology," IEEE Access, Vol. 7, pp. 103059–103079, 2019. <https://ieeexplore.ieee.org/document/8776589>
- [4] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena, "Uport: A Platform for Self Sovereign Identity", 2016 [Accessed Online on 23 September, 2023]. Available: https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf
- [5] A. Tobin and D. Reed, "The inevitable rise of self sovereign identity," Sovrin Found., Vol. 29, no. 2016, p. 18, 2017. <https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf>
- [6] A. Satybaldy, M. Nowostawski, and J. Ellingsen, "Self-sovereign identity systems: valuation framework," IFIP Adv. Inf. Commun. Technol., Vol.576, pp. 447–461, Apr. 2021. <https://inria.hal.science/hal-03378970/document>

- [7] A. E. Panait, R. F. Olimid, and A. Stefanescu, “Identity management on blockchain—privacy and security aspects,” in Proc. Romanian Acad. A, Math. Phys. Tech. Sci. Inf. Sci., 2020, Vol. 21, No. 1, pp. 45–52. <https://arxiv.org/abs/2004.13107>
- [8] M. Shuaib, N. H. Hassan, S. Usman, S. Alam, S. Bhatia, A. Mashat, A. Kumar, and M. Kumar, “Selfsovereign identity solution for blockchain-based land registry system: A comparison,” Mobile Inf. Syst., vol. 2022, pp. 1–17, Apr. 2022. <https://www.hindawi.com/journals/misy/2022/8930472/>