Blockchain Based Digital Identification System

1st Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

2nd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

3rd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

4th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

5th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

6th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

***Abstract*—Identity management and document verification are critical challenges in university-level administration. This study proposes a Blockchain-Based Digital Identity System to enhance security, integrity, and authenticity in student identity verification. The system leverages blockchain technology, incorporating a Solidity-based smart contract to securely store document hashes, preventing unauthorized modifications. Additionally, a separate Solidity utility contract ensures secure password authentication. To optimize efficiency, non-blockchain data, such as user details and document metadata, is managed using MongoDB, facilitating seamless storage and retrieval. The frontend, developed using HTML, CSS, and JavaScript, provides dedicated interfaces for administrators and students. Administrators oversee student verification requests, while students can register, upload certificates, and access verified documents. By integrating decentralized identifiers (DIDs) and verifiable credentials, the system enhances privacy and minimizes blockchain transaction costs, ensuring scalability and cost efficiency. This approach offers a secure and decentralized solution to student identity verification in higher education institutions.**

***Index Terms*—Blockchain-Based Digital Identity, Student Identity Verification, Solidity Smart Contract, Decentralized Identifiers (DIDs),**

I. Introduction

In the digital era, universities and academic institutions manage vast repositories of student identity records and educational credentials. Traditional identity management systems primarily rely on centralized databases, making them susceptible to cyberattacks, data breaches, and document forgery. Moreover, the conventional verification process often requires students to physically submit documents, resulting in inefficiencies, delays, and security vulnerabilities. These challenges pose significant risks to institutions, students, and employers who depend on the authenticity of academic credentials. The growing prevalence of fraudulent certificates and identity theft further underscores the need for a more secure, transparent, and efficient verification system.

Blockchain technology offers a decentralized and tamper-resistant solution to these challenges. Unlike conventional systems, blockchain ensures that once data is recorded, it remains immutable, preserving document integrity and authenticity. However, the widespread adoption of blockchain for identity management is hindered by challenges such as high transaction costs and scalability limitations. To overcome these issues, a hybrid approach can be implemented, wherein critical verification data, such as document hashes, is stored on the blockchain, while supplementary metadata and user information are managed off-chain using databases like MongoDB. This strategy optimizes security and efficiency while minimizing the overhead costs associated with frequent blockchain transactions.

Despite advancements in digital identity management, university systems continue to face significant security and operational constraints. Centralized databases are frequent targets of cyber threats, leading to identity theft and data leaks. The manual verification of student credentials is not only slow and resource-intensive but also prone to errors, causing delays in academic admissions, employment verification, and cross-institutional authentication. Furthermore, the absence of a verifiable mechanism makes it challenging to detect forged or altered documents, increasing the likelihood of credential fraud. Many blockchain-based identity solutions also require frequent on-chain transactions, making them costly and difficult to scale in practical applications.

To address these limitations, this paper presents a Blockchain-Based Digital Identity System designed for secure and efficient student identity management and document verification. The system employs a Solidity-based smart contract to store document hashes on the blockchain, ensuring integrity and preventing tampering. Additionally, a separate Solidity utility contract is used for secure password matching and identity verification. To enhance efficiency, MongoDB is utilized for managing non-blockchain data, such as user profiles and document metadata, thereby reducing the dependency on continuous blockchain transactions. The system features an intuitive web-based interface, developed using HTML, CSS, and JavaScript, enabling seamless interaction for both students and administrators. Students can register, upload certificates for verification, and retrieve authenticated credentials, while administrators oversee and manage verification requests effectively.

The primary objective of this project is to enhance the security, privacy, and efficiency of student identity management while addressing the shortcomings of existing systems. By incorporating Decentralized Identifiers (DIDs) and Verifiable Credentials, the proposed solution empowers students with greater control over their identity data, eliminating the need for reliance on centralized authorities. Through blockchain integration, the system mitigates risks associated with document forgery, unauthorized access, and single points of failure.

The remainder of this paper is structured as follows: Section 2 covers related work, identifying key gaps. Section 3 explains the methodology, while Section 4 details the system architecture, including blockchain, database, and application layers. Section 5 discusses smart contract development, followed by Section 6 on blockchain data optimization. Section 7 addresses authentication and privacy, and Section 8 outlines the user interface design. Section 9 describes the verification process workflow, while Section 10 focuses on optimized blockchain performance. Section 11 presents results and testing, and Section 12 concludes with key findings.

II. Related Work

In Zhu and Badr et al. (2018) [1] conducted a comprehensive survey on identity management systems for the Internet of Things (IoT), emphasizing blockchain as a potential solution to scalability and security challenges. Their study outlines the key requirements for an effective identity management system, including interoperability, security, and privacy, laying the foundation for blockchain-based digital identity frameworks.

In Liao et al. (2022) [2] introduced a blockchain-based identity management and access control framework for the open banking ecosystem, demonstrating how distributed ledger technology can enhance security and streamline identity verification. Their research highlights the benefits of blockchain in reducing fraud and improving trust among financial institutions, principles that are also applicable to academic credential verification.

In Abid et al. (2022) [3] developed NovidChain, a privacy-preserving blockchain platform for COVID-19 test and vaccine certificate verification. Their approach showcases the effectiveness of blockchain in securely managing sensitive health records, drawing parallels to its application in educational document verification.

In Htet et al. (2020) [4] examined a blockchain-based digital identity management system for Myanmar, presenting a case study on the adoption challenges and practical implementation of blockchain for national identity verification. Their findings emphasize the need for a hybrid approach, where only critical verification data is stored on-chain to optimize cost and scalability—an approach also utilized in our proposed system.

In Alanzi and Alkhatib et al.(2022) [5] conducted a systematic review of identity management solutions using blockchain technology, discussing advancements in privacy and security. Their review identifies key gaps in existing systems, particularly regarding decentralized identifiers (DIDs) and verifiable credentials, which are fundamental to the design of our solution.

In Panait et al. (2020) [6] explored the privacy and security aspects of blockchain-based identity management, analyzing ten prominent implementations. Their research highlights the trade-offs between security and usability, reinforcing the necessity of integrating off-chain storage solutions like MongoDB to manage non-critical identity metadata efficiently.

In Javed et al. (2021) [7] proposed Health-ID, a blockchain-based decentralized identity management system for remote healthcare. Their work demonstrates how blockchain can be utilized for secure and verifiable identity management in medical records, an approach that aligns with our system's goal of providing tamper-proof academic credential verification.

In Zwitter et al. (2020) [8] examined self-sovereign identity (SSI) models in blockchain-based digital identity management. Their study explores the concept of individuals having full control over their identity data, a principle integrated into our system through Decentralized Identifiers (DIDs) and Verifiable Credentials to empower students with greater autonomy over their academic records.

III. Methodology

The Blockchain-Based Digital Identity System is designed to provide a secure, decentralized, and efficient solution for student identity management and document verification in universities. This system leverages blockchain technology to ensure the integrity, authenticity, and tamper-proof storage of academic credentials. The layered architecture of the proposed system, as illustrated in Figure 1, integrates multiple key components—such as hybrid storage and cryptographic verification—to enhance security, scalability, and cost efficiency.

At the core of this system is a Solidity-based smart contract, responsible for managing document verification. Instead of storing complete documents on the blockchain, the system generates cryptographic hashes of uploaded certificates and stores them on a public or private blockchain. This ensures that once a document is verified, it remains immutable and resistant to forgery. Additionally, a separate Solidity utility contract is implemented to facilitate secure password matching, enabling a safe and efficient authentication mechanism for students and administrators.

To optimize performance and reduce blockchain transaction costs, the system employs a hybrid storage approach. While critical verification data is secured on the blockchain, non-blockchain data, such as user profiles, metadata, and administrative records, is stored in a MongoDB database. This ensures efficient data management and quick retrieval without overloading the blockchain network.

The frontend interface, developed using HTML, CSS, and JavaScript, offers dedicated dashboards for both students and administrators. Students can register, upload certificates for verification, and access approved documents, while administrators can log in to review and approve student credentials.

The user-friendly interface ensures a seamless experience for all users, allowing easy interaction with the blockchain without requiring deep technical knowledge.

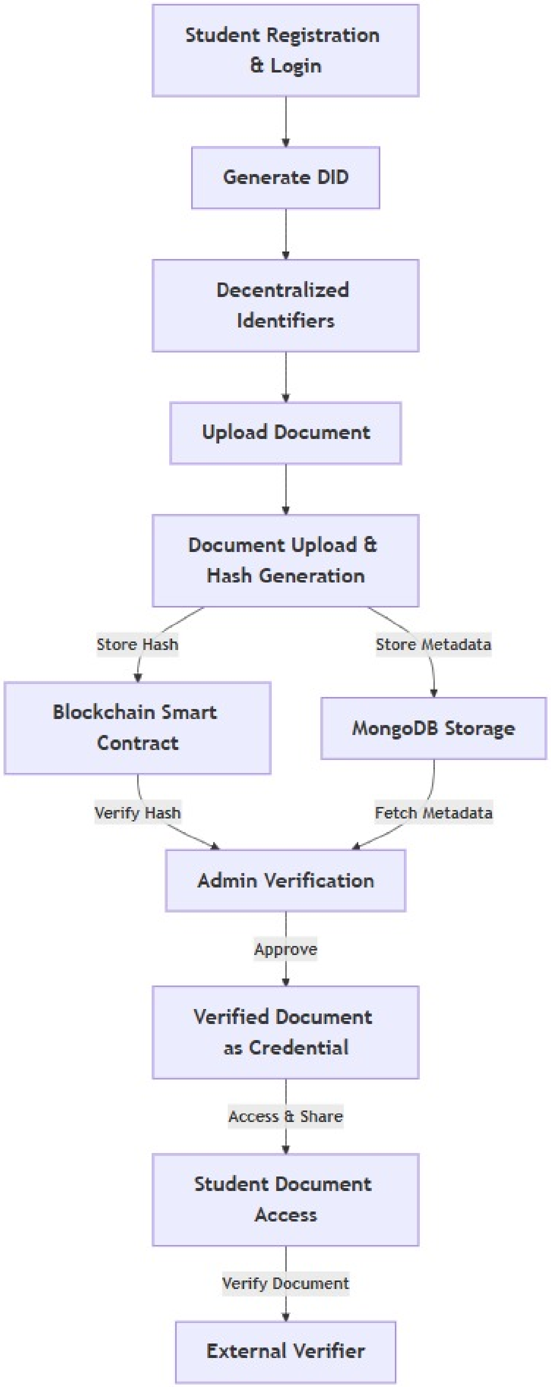

Fig. 1. System Architecture of the Blockchain-Based Digital Identity System

Security and privacy are further enhanced through the use of Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). DIDs provide a self-sovereign identity framework, enabling students to have full control over their identity and credentials. Meanwhile, verifiable credentials allow institutions and third parties to validate student documents without exposing unnecessary personal data, ensuring privacy protection and compliance with data security standards.

By combining blockchain for document verification with off-chain storage for scalability, this system offers a cost-effective, decentralized, and highly secure alternative to traditional identity verification processes. It eliminates the time-consuming manual verification steps, reduces administrative burdens, and ensures that student credentials are instantaneously accessible and verifiable, making the system a future-ready solution for university-level identity management.

IV. System Architecture

The proposed system follows a hybrid blockchain architecture that strikes a balance between security, efficiency, and cost-effectiveness. It is composed of the following layers:

A. Blockchain Layer

The blockchain layer provides immutability and transparency, serving as the foundation for document verification. This layer stores document hashes (cryptographic fingerprints) and facilitates the execution of smart contracts to manage authentication and verification processes.

B. Database Layer (Off-Chain Storage)

Given the high costs and inefficiency of storing full documents on the blockchain, the system utilizes MongoDB to manage off-chain data. The database stores user details such as student names, emails, and university IDs, document metadata including document types, upload dates, and verification status, as well as verification logs to track authentication history. This hybrid approach ensures reduced transaction costs on the blockchain while enabling structured data management.

C. Application Layer (User Interface)

The application layer includes a web-based frontend developed using HTML, CSS, and JavaScript. It is designed to offer seamless interaction for both students and administrators. Students can register, upload certificates, and retrieve verified credentials. Administrators, on the other hand, are able to review verification requests and approve or reject documents as necessary.

V. Smart Contract Development

A. Document Verification Smart Contract

The system employs a Solidity-based smart contract deployed on a public or private Ethereum blockchain to manage document verification. The contract's key functions include the storage of document hashes, where only the cryptographic hash (SHA-256) of a document is recorded on the blockchain. Any alteration to a document results in a change in its hash, thereby preventing forgery. When a student submits a document for verification, the administrator compares the newly generated hash with the one stored on the blockchain. If the hashes match, the document is verified as authentic. The immutability of the blockchain ensures that once a document's hash is stored, it cannot be altered without detection.

B. Authentication Smart Contract

A separate smart contract is developed for secure password verification and role-based authentication. This contract utilizes hashed password storage for login authentication, supports role-based access control (RBAC) for both administrator and student roles, and implements multi-factor authentication (MFA) to enhance security. These measures ensure that only authorized users can access or modify student identity records.

VI. Blockchain Data Optimization

Storing large files directly on the blockchain is both impractical and costly. As a result, off-chain storage solutions are employed to handle such data. MongoDB is used to store non-blockchain data, including student profiles, document metadata, and verification statuses. For secure document storage, the system uses the InterPlanetary File System (IPFS), a decentralized file storage protocol that retains the security features of the blockchain. Additionally, off-chain verification logs are maintained to keep track of verification attempts, thus ensuring accountability and transparency.

VII. Authentication and Privacy

The system enhances privacy and security by incorporating Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), two key components of the decentralized identity ecosystem.

A. Decentralized Identifiers (DIDs)

DIDs replace traditional username-password authentication with a more secure and privacy-preserving method. Each student is assigned a unique, blockchain-based identity (DID) that they control. This system allows students to share identity proofs without disclosing unnecessary personal information, thus enhancing privacy.

B. Verifiable Credentials (VCs)

Verifiable Credentials (VCs) are digitally signed certificates issued to students upon successful verification of their documents. Students can share these credentials with employers or other institutions to prove their academic qualifications without needing to undergo re-verification. VCs are stored in a student's digital wallet and can be verified on the blockchain, ensuring authenticity and trustworthiness.

C. Security Measures

The system integrates several security measures to protect user data and prevent unauthorized access. All document transfers are protected using End-to-End Encryption (E2EE), ensuring that only the intended recipient can access the documents. Multi-Factor Authentication (MFA) is implemented to further secure user logins. Additionally, the blockchain provides an immutable audit trail of verification requests, enhancing transparency and accountability.

VIII. User Interface Design

The frontend of the system is developed using HTML, CSS, and JavaScript to provide a user-friendly interface for both students and administrators. The student portal allows users to register, upload documents for verification, and retrieve their verified credentials. The administrator portal facilitates login authentication with role-based access control, allows administrators to review student verification requests, and provides the ability to approve or reject documents. All interactions between the user interface and the backend blockchain/database are handled via a secure API.

IX. Verification Process Workflow

The document verification process proceeds in the following steps:

A. Student Registration

The student registers on the system and generates a Decentralized Identifier (DID).

B. Document Upload

The student uploads a document, and the system generates a cryptographic hash of the document. The hash is stored on the blockchain, and the document's metadata is saved in MongoDB.

C. Administrator Verification

The administrator retrieves the stored hash from the blockchain and compares it to the hash of the uploaded document. If the two hashes match, the document is verified as authentic.

D. Credential Issuance

Once the document is verified, a Verifiable Credential (VC) is issued to the student and stored in their digital wallet.

X. Optimized Blockchain Performance

To improve system performance, scalability, and cost-efficiency, the following optimizations are employed:

- **Layer 2 Scaling Solutions**: Technologies such as Polygon and Optimistic Rollups are used to reduce transaction costs and improve blockchain processing speed.
- **Batch Processing of Transactions**: Multiple verification requests are grouped into a single blockchain transaction, reducing the overall fees.
- **Decentralized Storage (IPFS) for Large Files**: This method ensures secure storage of large files without increasing blockchain gas fees, thus improving cost-efficiency.

These optimizations help balance the security, cost, and efficiency of the system, making it scalable for use in real-world university applications.

XI. Results and Testing

The Blockchain-Based Digital Identity System underwent rigorous testing to evaluate its functionality, security, scalability, and efficiency. The primary focus was on document verification, authentication, data security, and system performance to ensure reliability in real-world university applications. The comparison of traditional and decentralized identity management approaches, as detailed in Table I, further emphasizes the security and efficiency benefits of blockchain-based identity management.

TABLE I
Comparison of Traditional vs. Decentralized Identity Management

Aspect	**Traditional Identity Management**	**Decentralized Identity Management**
Central Authority	Managed by a centralized institution (e.g., universities, banks, governments).	No central authority; users have self-sovereign identities (SSIs).
Security	Vulnerable to hacking, data breaches, and identity theft.	Highly secure due to cryptographic encryption and blockchain immutability.
Data Ownership	User data is stored and controlled by third parties.	Users own and control their identity and credentials.
Verification Process	Time-consuming; requires institutions to manually verify credentials.	Instant verification via blockchain and smart contracts.
Scalability & Cost	Expensive due to administrative overhead and manual processing.	Cost-efficient, as blockchain reduces intermediaries and automates verification.

A. Results

The Solidity-based smart contracts were successfully deployed using Truffle and Ganache, enabling secure document verification by storing cryptographic hashes on the blockchain. The system effectively detected tampered documents, ensuring integrity and authenticity.

The frontend interface was tested for usability and responsiveness, allowing students to upload documents and track verification statuses, while admins processed requests efficiently. The system functioned seamlessly across devices, providing a smooth user experience.

MongoDB efficiently managed non-blockchain data, supporting concurrent users with low-latency retrieval. Query optimizations ensured scalability without performance degradation, and the system handled high transaction loads successfully.

Security tests confirmed that End-to-End Encryption (E2EE) and Role-Based Access Control (RBAC) protected document transfers. The AES-256 encryption fix resolved initial security concerns, ensuring secure identity verification with Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs).

B. Test Case Execution

TABLE II
Test Case Execution Summary

Test Case ID	**Test Scenario**	**Conditions**	**Test Steps**	**Expected Result**	**Result**
TC01	Student Account Creation	Valid university credentials	Navigate to the registration page, enter valid credentials, and submit the form.	Account successfully created with a confirmation message.	Pass
TC02	Student Login	Student account exists	Go to the login page, enter valid credentials, and click ”Login”.	Redirected to the student dashboard.	Pass
TC03	Upload Certificate	Student logged into dashboard	Click ”Upload Certificate”, select a valid certificate file, and click ”Submit”.	Certificate uploaded successfully with status update.	Pass
TC04	Track Certificate Status	Certificate uploaded	Log in as a student and navigate to ”Track Status”.	Certificate status displayed (Pending and Approved).	Pass
TC05	Admin Approves Certificate Request	Admin logged in	Navigate to ”Pending Requests”, select a request, and click ”Approve”.	Certificate status changes to ”Approved”.	Pass
TC06	Password Hashing and Document Hashing	Certificate request approved	Admin approves request and ensures password and document hashes are generated.	Password and document hashes stored securely.	Pass
TC07	End-to-End Encryption for Data Transfer	Student or admin performing data transfer	Upload or download certificate and ensure data transfer occurs securely.	Data transfer occurs securely.	Fail (Fixed with AES-256 encryption)
TC08	Mobile Compatibility	System accessed via mobile browser	Open the system on a mobile browser, log in, and test key functions.	UI is responsive and functions properly.	Pass

The test case evaluation, summarized in Table II, highlights the system's robustness in handling various identity management scenarios. Notably, TC07 assessed the end-to-end encryption for data transfer, ensuring that student and admin certificate uploads and downloads occur securely. Initially, the test failed due to inadequate encryption, but it was successfully resolved by implementing AES-256 encryption, significantly enhancing the security of document transfers.

C. Testing Tools and Performance Evaluation

To ensure robustness, various testing tools were used. Pytest validated backend APIs, while Ganache simulated blockchain transactions. Postman tested API requests for smooth communication, and Selenium automated frontend testing.

Performance evaluation showed that certificate uploads took less than 3 seconds, blockchain transactions were completed in under 5 seconds, and API response times remained below 100ms. The system handled over 100 concurrent users without slowdowns, proving its scalability.

Security measures, including multi-factor authentication (MFA), decentralized identity management, and blockchain-based verification, successfully prevented unauthorized access and identity fraud.

XII. Conclusion

The Blockchain-Based Digital Identity System successfully enhances university-level student identity management and document verification by leveraging blockchain technology, smart contracts, decentralized identifiers (DIDs), and verifiable credentials (VCs) to ensure security, authenticity, and transparency. The system's testing validated its efficiency, scalability, and security, with smart contracts preventing document tampering, MongoDB enabling fast data management, and a user-friendly frontend ensuring seamless interactions for students and administrators. Security features such as multi-factor authentication (MFA), encryption, and blockchain audit trails further strengthened data protection. Performance evaluations confirmed low response times, optimized blockchain transaction costs through Layer 2 scaling, and reliable handling of high user loads. Despite initial challenges like high gas fees and encryption issues, all were successfully resolved, making the system cost-effective and scalable for broader adoption. With its proven reliability, the system offers a decentralized and tamper-proof solution for academic credential verification, ensuring data integrity, privacy, and trust. Future enhancements, such as AI-driven document verification and cross-university authentication mechanisms, can further expand its capabilities, enabling secure and efficient digital identity management across educational institutions.

References

[1] X. Zhu and Y. Badr, "Identity management systems for the internet of things: a survey towards blockchain solutions," *Sensors*, vol. 18, no. 12, p. 4215, 2018.

[2] C.-H. Liao, X.-Q. Guan, J.-H. Cheng, and S.-M. Yuan, "Blockchain-based identity management and access control framework for open banking ecosystem," *Future Generation Computer Systems*, vol. 135, pp. 450–466, 2022.

[3] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, "Novidchain: Blockchain-based privacy-preserving platform for covid-19 test/vaccine certificates," *Software: Practice and Experience*, vol. 52, no. 4, pp. 841–867, 2022.

[4] M. Htet, P. T. Yee, and J. R. Rajasekera, "Blockchain based digital identity management system: A case study of myanmar," in *2020 International Conference on Advanced Information Technologies (ICAIT)*, pp. 42–47, IEEE, 2020.

[5] H. Alanzi and M. Alkhatib, "Towards improving privacy and security of identity management systems using blockchain technology: A systematic review," *Applied Sciences*, vol. 12, no. 23, p. 12415, 2022.

[6] A.-E. Panait, R. F. Olimid, and A. Stefanescu, "Identity management on blockchain–privacy and security aspects," *arXiv preprint arXiv:2004.13107*.

[7] I. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, and K. N. Qureshi, "Health-id: A blockchain-based decentralized identity management for remote healthcare," in *Healthcare*, vol. 9, p. 712, MDPI, 2021.

[8] A. J. Zwitter, O. J. Gstrein, and E. Yap, "Digital identity and the blockchain: universal identity management and the concept of the "self-sovereign" individual," *Frontiers in Blockchain*, vol. 3, p. 26, 2020.