Journal of Computer Science, Information Technology and Telecommunication Engineering (JCoSITTE)
Vol. 7, No. 1, March 2026, pp. 1068~1078
ISSN: 2721-3838, DOI: 10.30596/jcositte.v7i1.29044

Development of a Blockchain-Based Digital Data Identity Management System

Ardi Birawinata[1], Muhammad Nasir[-2],
[1,2]Informatics Engineering Study Program, Faculty of Science and Technology

ABSTRACT

The management of student identity data requires a system that ensures data security, integrity, and transparency. Conventional data management methods are vulnerable to data redundancy and manipulation, particularly in educational institutions. This study aims to develop a blockchain-based digital identity data management system for SMK Bina Sriwijaya Palembang using the Prototyping development method. The Prototyping approach was selected to allow iterative system evaluation and validation, especially for complex Smart Contract logic. The system was implemented as a web-based application using React JS for the front-end and Node.js for the back-end, with Ethereum Smart Contracts developed in Solidity. Ganache was used as a local blockchain network for testing, while IPFS was integrated for decentralized storage of digital assets. The results show that the proposed system successfully secures student identity data, prevents unauthorized data manipulation, and improves the efficiency of data verification processes. This study demonstrates that blockchain technology combined with a prototyping approach can provide a reliable solution for digital identity management in educational environments.

Keyword : Blockchain; Digital Identity; Prototyping Method; Smart Contract; Data Security.

Corresponding Author:
Ardi Birawinata
Department Informatics Engineering
Universitas Bina Darma,
Jl. Ahmad Yani No. 12, Kota Palembang.
Email : : natagskt97@gmail.com

Article history:
Received Feb 5, 2026
Revised Mar 5, 2026
Accepted Mar 24, 2026

1. INTRODUCTION

The rapid development of digital technology has made digital identity a fundamental component across various sectors, including education, government, and public services. Digital identity plays a crucial role in authentication, authorization, and individual data validation processes. However, conventional digital identity management systems are predominantly centralized and face significant challenges such as data breaches, identity forgery, data manipulation, and a lack of transparency and user trust. These challenges are further intensified in the VUCA era, which demands secure, adaptive, and sustainable information systems (Suminar & Nugroho, 2023).

Blockchain technology has emerged as a promising solution to address these issues. Its core characteristics decentralization, transparency, immutability, and cryptographic security enable blockchain to ensure data integrity and authenticity (Fitrian et al., 2025). According to Simanungkalit (2024), blockchain is highly effective in securing digital data transactions because all data changes are permanently recorded and cannot be altered unilaterally. These characteristics make blockchain highly suitable for digital identity data management systems .

In the education sector, the management of identity and academic data is a critical issue. Cases of diploma forgery, grade manipulation, and unauthorized document modification remain prevalent. Vaher, Simanjuntak, and Vaher et al. (2025) demonstrated that the implementation of blockchain significantly enhances the security and reliability of academic record management in higher education institutions. Similarly, Fitriani (2021) found that blockchain adoption in educational management improves administrative efficiency and data transparency.

At the primary and secondary education levels, blockchain-based digital identity systems have also shown positive outcomes. Slam et al. (2025) through black-box testing, confirmed that blockchain-based student digital identity systems provide high levels of security and transparency. Tanadi et al. (2025) Additionally, the application of blockchain for digital signatures and academic document management has proven effective in ensuring document authenticity and reducing reliance on manual processes (Rakhmansyah et al., 2021).

Furthermore, blockchain supports the concept of self-sovereign identity (SSI), which allows individuals to maintain full control over their personal identity data. (Putra & Setiadi, 2025) emphasized that the successful implementation of blockchain-based SSI depends on regulatory readiness, technological infrastructure, and user awareness, while also contributing to the achievement of sustainable development goals. Identity protection can be further strengthened by integrating blockchain with zero-trust architecture, which enhances digital identity security and data privacy (Hose et al., 2025).

The integration of blockchain with complementary technologies has expanded its potential applications in digital identity management. (Fadhilah et al., 2023) developed a blockchain-based system utilizing smart contracts and NFTs to ensure data authenticity and process automation. Meanwhile, (Famuji et al., 2025), demonstrated that decentralized systems combining blockchain and IPFS effectively secure sensitive data. Despite its advantages, blockchain implementation still faces challenges related to scalability, regulatory compliance, and infrastructure readiness (Chic & Bilqisthi, 2024).

In conclusion, blockchain-based digital identity data management systems offer significant potential as a strategic solution to enhance security, transparency, and trust in digital identity management. Therefore, a comprehensive and well-integrated system design is essential to ensure that blockchain implementation delivers optimal benefits for both users and institutions.

2. RESEARCH METHOD

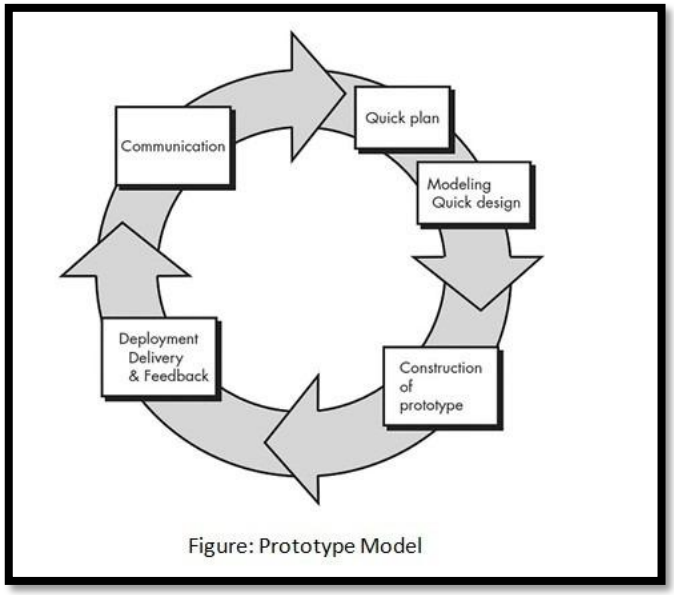

Figure 1. Research Method Prototype

Cahya Pramuditya (2023) The software development method used in this study is the Prototyping method. This method was chosen because Blockchain-based systems have logical complexity that requires repeated validation, particularly in the Smart Contract mechanism. Kuswayati & Rusdan (2023) The Prototyping approach allows developers and users to evaluate the system prototype incrementally before full implementation.

The stages of system development using the Prototyping method in this research are as follows:

1. Requirements Gathering (Communication)
   This stage begins with identifying the problems and fundamental needs of the partner institution, namely SMK Bina Sriwijaya Palembang. The primary focus at this stage is mapping the security requirements for student identity data.
2. Quick Planning (Quick Plan)
   At this stage, a preliminary architectural design is developed, including the local Blockchain network topology, data flow, and the structure of Hybrid storage (On-chain and Off-chain).
3. Design Modeling (Modeling Quick Design)

This stage involves designing the User Interface (UI) and developing the Smart Contract logic scheme to be implemented in the system.

4. Prototype Construction (Construction of Prototype)
   The design is translated into programming code. The author performs the coding process using React JS for the user interface and Solidity for the Smart Contract.
5. Deployment and Feedback (Deployment & Feedback)
   The developed prototype is tested on a local network using Ganache. The test results are evaluated to ensure the validity of the logic and data security before the system is considered final.

3. RESULTS AND DISCUSSION

The system implementation was developed using Ganache as a local blockchain network environment, selected for rapid simulation and testing during development. The network was configured with an RPC Server at 127.0.0.1:7545 and Chain ID 1337. Ganache automatically provides ten pre-funded accounts for transaction testing, of which the first three accounts are assigned as system administrators.

The process of adding student data to the blockchain follows a structured workflow to ensure data validity. A Technical Administrator inputs student data through a React-based user interface, while student photos are uploaded to IPFS, generating a unique hash value. The backend submits a data addition proposal to the Smart Contract, which is then reviewed and approved by a Legal Administrator. Once the multi-signature requirement is met, the Smart Contract permanently records the student data on the blockchain. All transactions are logged to support audit tracking.

Graduate data verification can be performed by external parties by comparing the document hash with the hash stored on the blockchain. Any data modification results in a different hash value, enabling automatic detection of data manipulation.

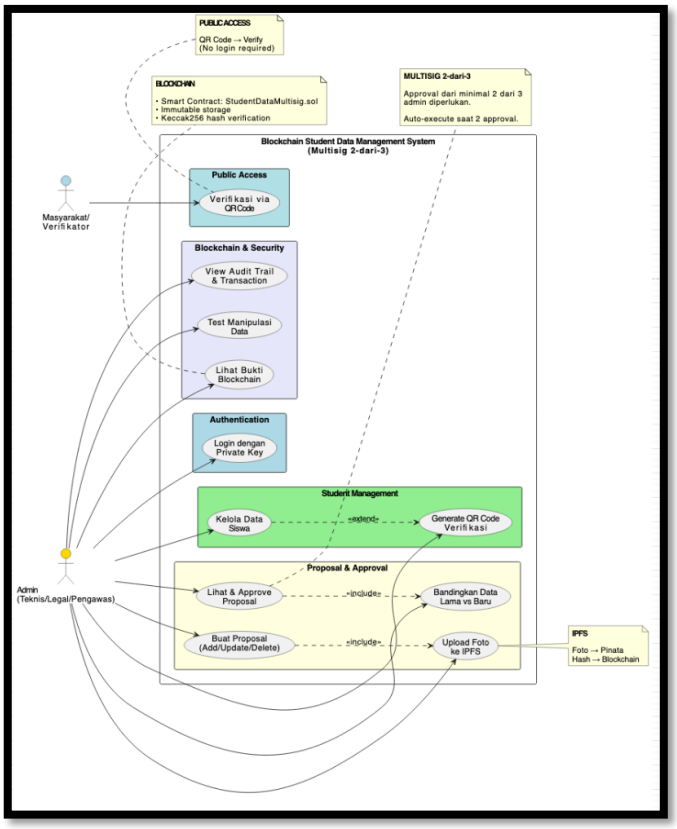

Figure 2. Use Case Diagram

User interactions are modeled using a Use Case Diagram to illustrate how three administrative actors interact with the React JS interface and Smart Contract functions. The Technical Administrator acts as the data initiator, the Legal Administrator validates and approves data, and the Supervisory Administrator oversees auditing and procedural compliance.

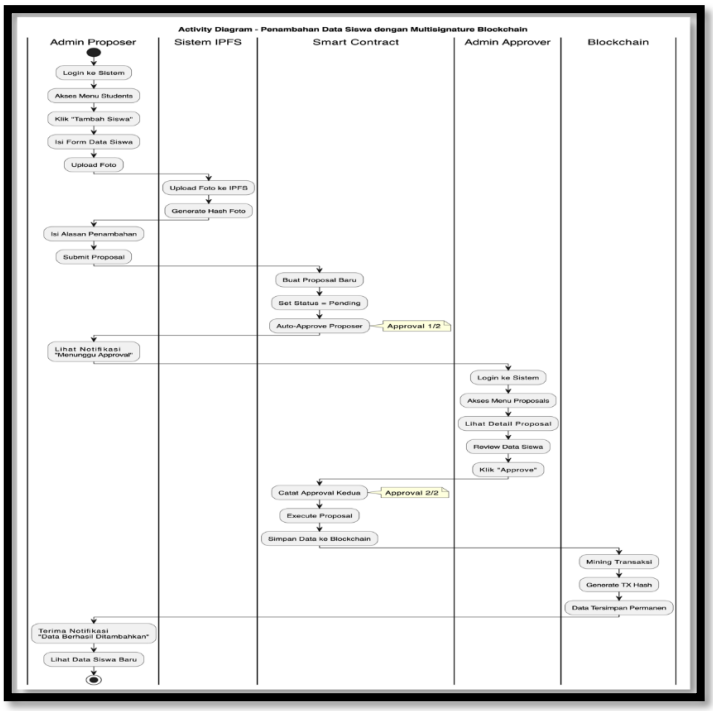

Figure 3. Activity Diagram of Student Data Addition

Based on the diagram, the student data addition process begins with the Admin Proposer accessing the *Add Student* menu to input student information and upload a photo. The system automatically stores the photo on the IPFS network and generates a unique hash as a reference. The student data and photo hash are then submitted as a proposal to the Smart Contract. The Smart Contract records the proposal with a *pending* status and initial approval from the proposer. Subsequently, an Admin Approver verifies the consistency between digital data and physical documents and provides approval. Once the required number of approvals is met, the Smart Contract permanently records the student data on the blockchain, followed by transaction mining as proof of data immutability.

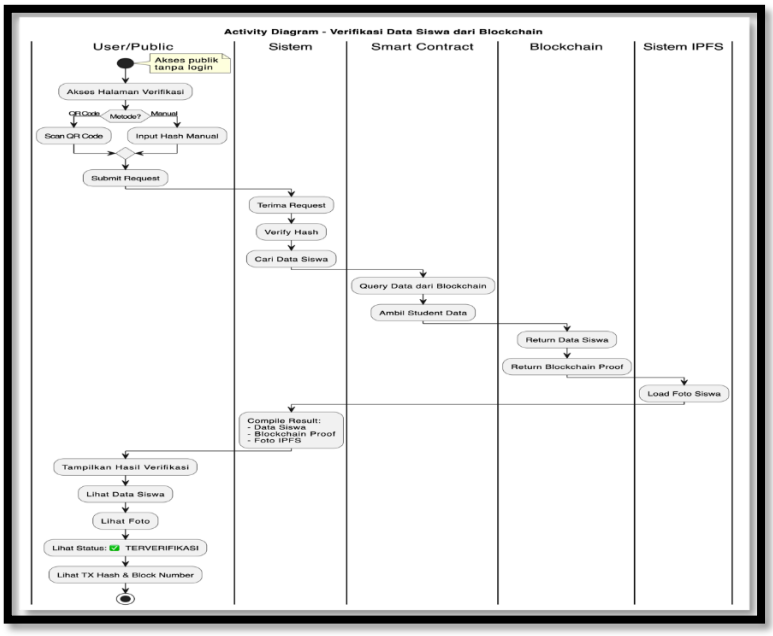

Figure 4. Activity Diagram of Student Data Verification

As illustrated in Figure the data verification mechanism involves coordinated interaction between the application layer, Smart Contract, and decentralized storage (IPFS). Public users access the verification

page through a React JS–based web interface and submit verification requests either by scanning a QR code or entering an identity hash manually. The request is processed by the Node.js backend, which validates the hash format and forwards the query to the blockchain network. The Smart Contract retrieves student identity data from the blockchain and obtains the associated CID to fetch the student photo from IPFS. The system then displays the verification result with a *Verified* status, along with the transaction hash and block number as cryptographic proof of data authenticity and immutability.

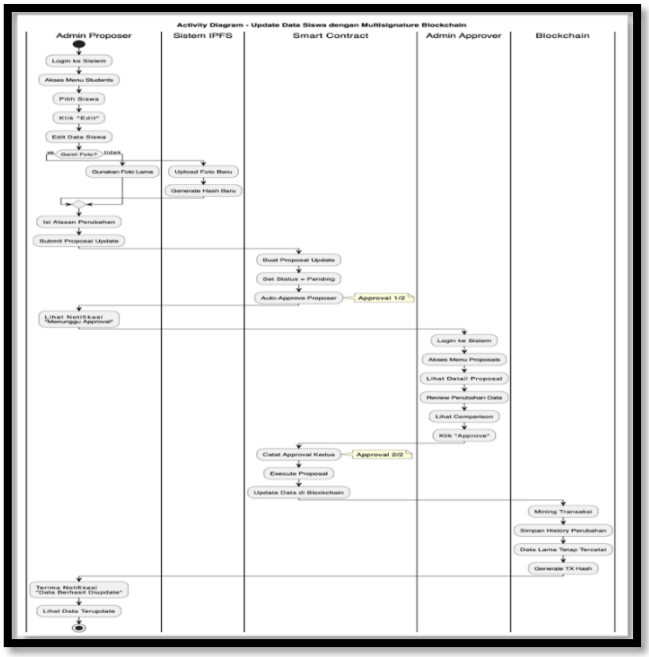

Figure 5. Activity Diagram of Student Data Update

As shown in Figure the student data update process begins when the Admin Proposer selects an active student record to be revised. The system allows updates to both textual data and biometric data. If a new photo is submitted, the system uploads it to IPFS and generates a new hash; otherwise, the existing photo hash is retained. The proposer is required to provide a reason for the update to support accountability. The Smart Contract then creates an update proposal with a *pending* status and records an initial approval. An Admin Approver reviews the proposed changes using a side-by-side data comparison before granting approval. Once consensus is reached, the Smart Contract executes the update while preserving the full history of changes on the blockchain for audit purposes.

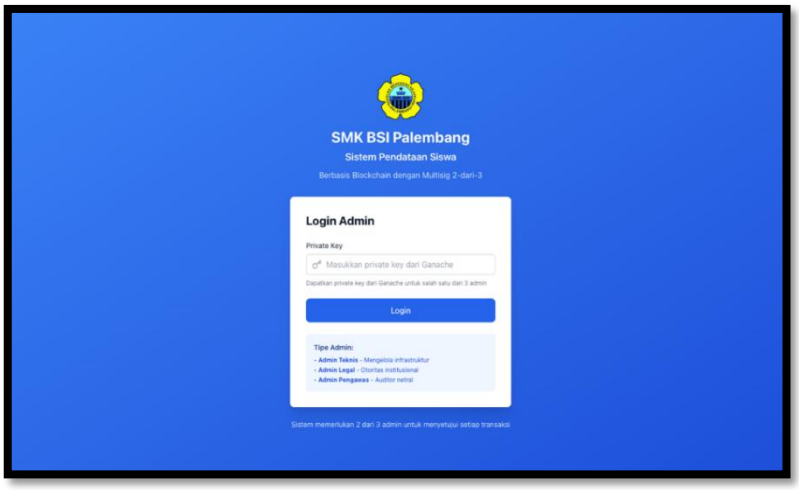

Figure 6. Admin Login Page

On this interface, the system transparently displays the active user roles and applicable consensus rules. Users are informed that every transaction validation or identity data modification requires a Multi-

signature mechanism, with approval from at least two of three administrators: Technical, Legal, and Supervisory Admins. In addition to security enforcement, visual elements such as the prominent display of the SMK Bina Sriwijaya Palembang logo and institutional identity reinforce ownership and institutional legitimacy within the data ecosystem.

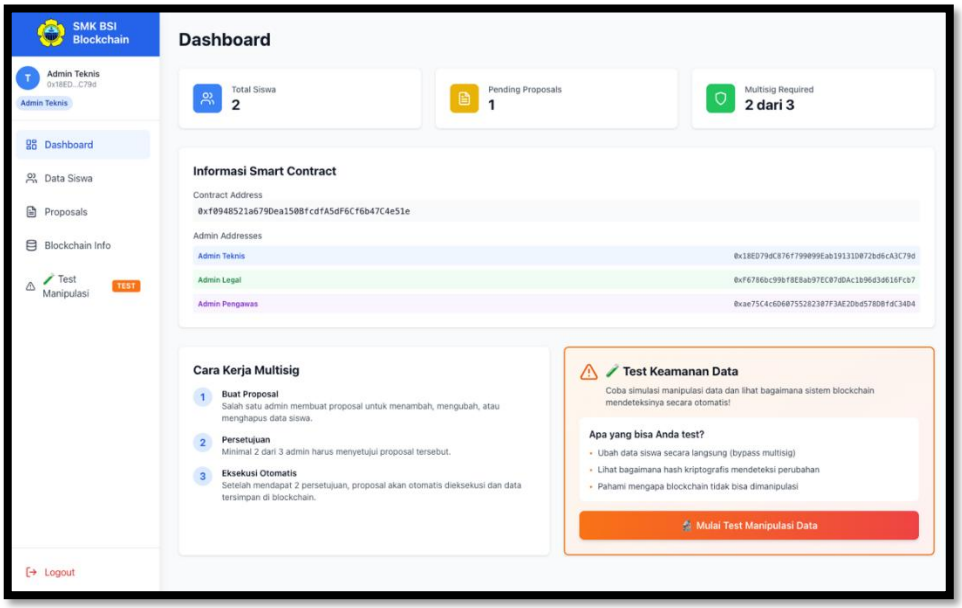

Figure 7. Main Dashboard Page

This view represents the main dashboard interface. As shown in the figure, the implementation displays real-time metrics, including "2 Total Students" already recorded on the blockchain and "1 Pending Proposal" requiring attention. The *Smart Contract Information* section transparently presents the contract address (0xf09...) and the list of registered administrator addresses. On the right side, an educational panel explaining the *Multisig Mechanism* and quick access to the *Data Manipulation Test* feature are provided, enabling technical administrators to efficiently perform system audits.

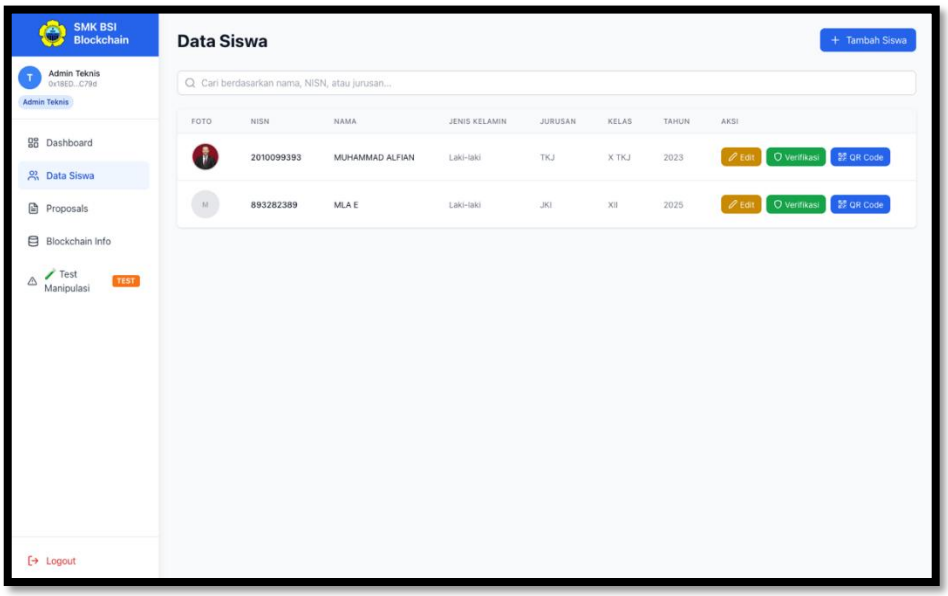

Figure 8. Student Data Management Page

The Student Data Management page implements CRUD (Create, Read, Update, Delete) functionality. On this page, student records that have been successfully written to the blockchain ledger are displayed in an interactive table format. Each row represents a unique student entity and is associated with its own transaction hash.

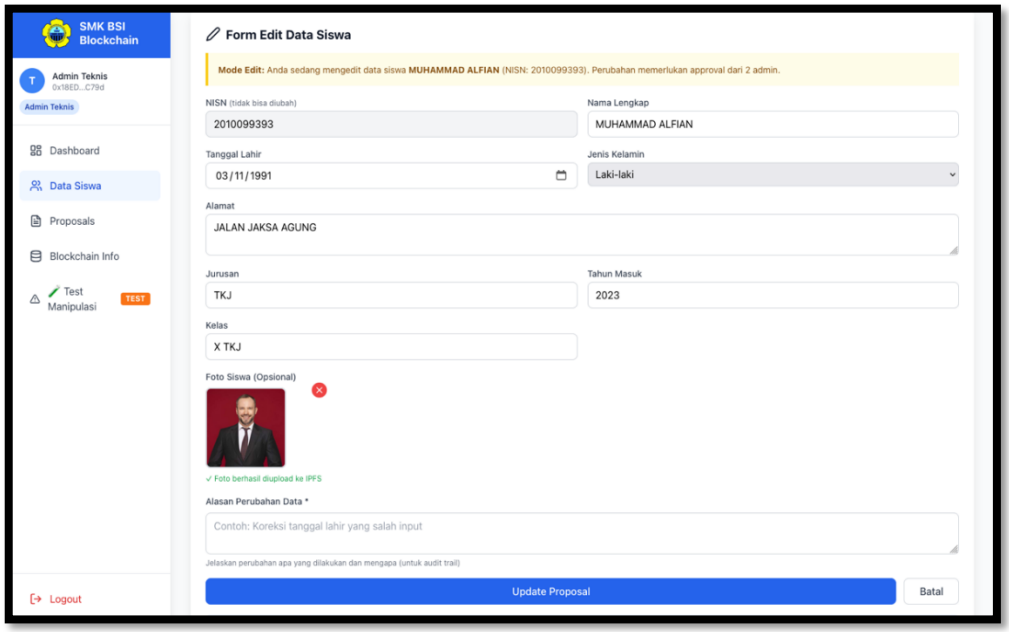

Figure 9. Edit Data Form Page

When the Edit button is selected, the system does not immediately modify the data but instead opens a proposal submission form. This implementation captures the intended changes and packages them into a proposal that awaits approval from other administrators.

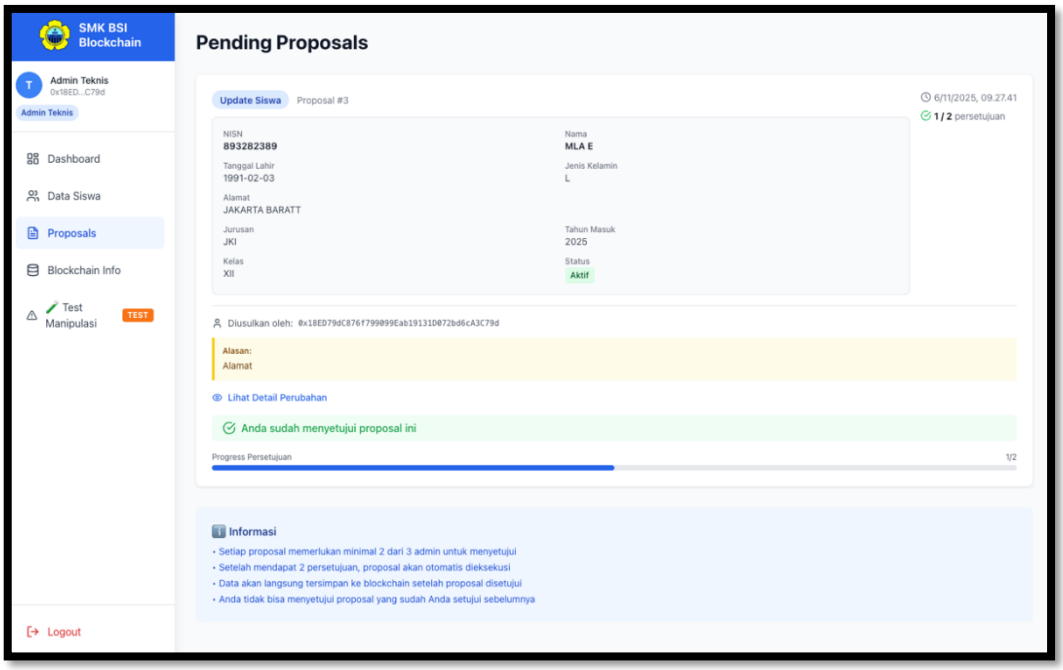

Figure 10. Proposal Approval Page

The core functionality of the system is implemented on the Proposal page. This interface allows administrators to view a list of pending data change requests. It is a critical component, as it visually facilitates the execution of the two-out-of-three consensus mechanism.

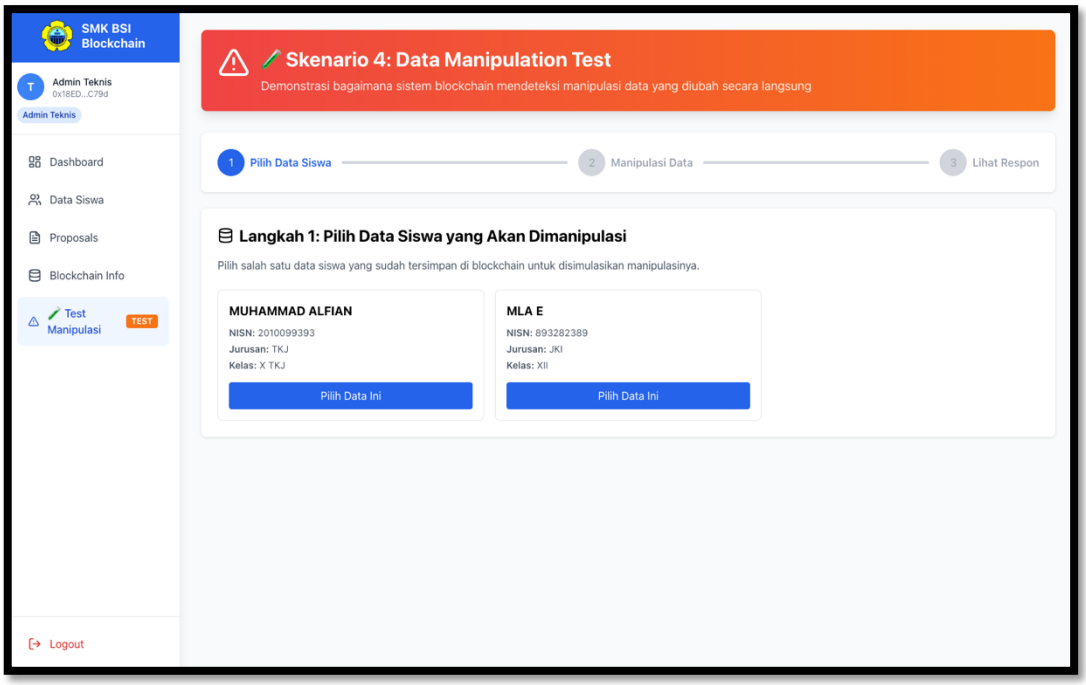

Figure 11. Data Manipulation Test Page

As a final validation step, the Test Manipulation feature is implemented to demonstrate system resilience. This page simulates an attack scenario in which a user attempts to forcibly modify student data without following the authorized proposal procedure.

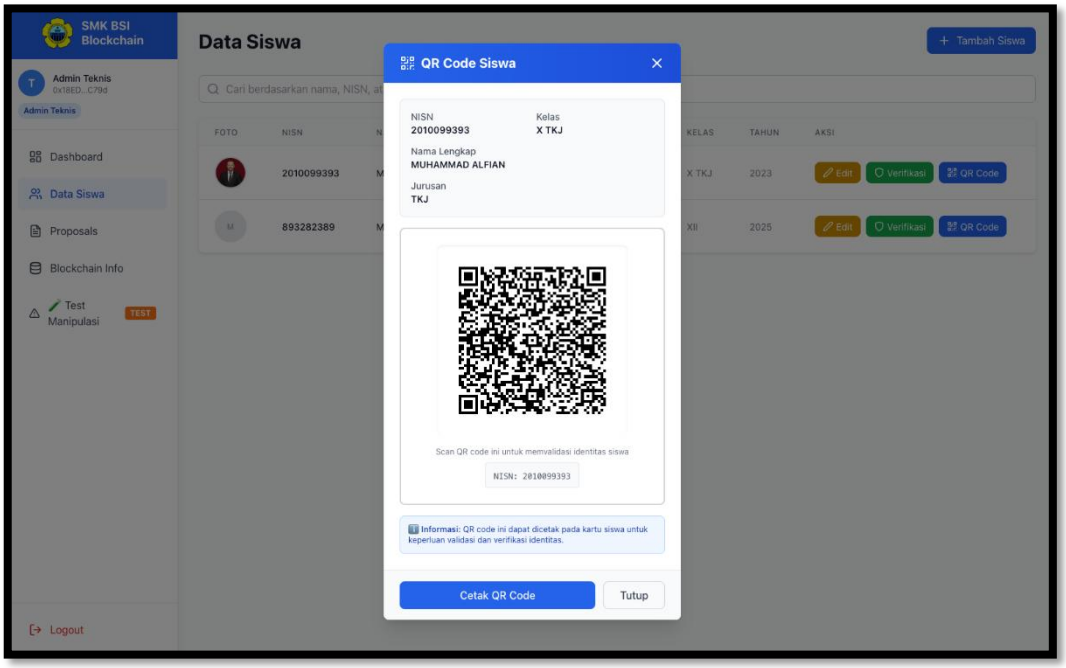

Figure 12. QR Code Page

To bridge blockchain-stored data with real-world access requirements, the system implements a QR code–based Digital Identity feature. This feature is specifically designed to enable instant third-party verification without requiring system login. Its purpose is to provide a transparent proof mechanism, allowing the public such as higher education institutions or potential employers to verify a student's status at SMK Bina Sriwijaya Palembang using only a mobile device.

Testing

Functional testing was conducted using the Black Box Testing method, where the focus was placed on evaluating the application's input and output behavior without examining the internal code during execution. The testing covered several key scenarios, including Admin Login, proposal creation, multi-level approval using a multi-signature (Multisig) mechanism, and public verification through QR codes. Each scenario was tested to ensure that the system responded in accordance with the defined functional requirements. Based on the testing results, all core system features operated as expected and produced valid outputs, indicating that the application meets functional requirements and is suitable for implementation.

Table 1. Testing Black-Box

No	Test Scenario	Test Steps	Expected Result	Actual Result	Status
1	Valid Admin Login	Enter the private key of a registered admin (Technical/Legal/Supervisor) on the login page.	The system redirects the user to the main dashboard.	Admin successfully accesses the dashboard and the role is correctly detected.	Passed
2	Invalid Admin Login	Enter a random private key that is not registered in the Smart Contract.	The system rejects access and displays an error message.	A red warning message appears: "Not an admin address."	Passed
3	Student Data Input (Proposal)	Admin A fills in the add student form and clicks the save button.	Data is not immediately activated and the status becomes *Pending* (1/2 Approval).	A success notification appears: "Waiting for approval from another admin." Data does not appear in the main table.	Passed
4	Proposal Approval	Admin B (different account) clicks the Approve button on the proposal.	Proposal status changes to *Executed* and data is recorded on the blockchain.	Status changes to *Executed*. Student data appears in the active student list.	Passed
5	Public Verification	A visitor scans the QR code or accesses the unique verification URL.	The system displays valid student data with a green verification indicator.	Student Name, NISN, and Major are displayed with a "✓ Blockchain Verified" badge.	Passed

4. CONCLUSION

Based on the design, implementation, and testing activities carried out during the Independent Study project entitled *"Blockchain-Based Digital Identity Data Management System"* at SMK Bina Sriwijaya Palembang, it can be concluded that the developed system was successfully implemented and operated reliably. The web-based application ran smoothly without critical errors during demonstration, supported by a responsive front-end built with React JS and Vite, and a stable back-end developed using Node.js. The use of Ganache as a local Ethereum blockchain simulation proved effective in recording and validating identity-related transactions. All Smart Contract functions operated correctly, enabling secure data storage, hash verification, and protection against data manipulation through blockchain immutability. Furthermore, the system provided tangible benefits for the partner institution by reducing data redundancy and improving the efficiency of student data verification processes compared to

conventional methods. Based on testing results and partner feedback, the implemented solution enhanced data security, transparency, and trustworthiness, demonstrating that blockchain technology can serve as a robust and practical foundation for managing digital identity data in educational institutions.

REFERENCES

Cahya Pramuditya, A. (2023). *PENGUJIAN USABILITY PADA PROTOTYPE SISTEM INFORMASI PEMASARAN PT. PRIMISSIMA MENGGUNAKAN METODE USABILITY TESTING*. *2*(2), 98–103.

Chic, S. A., & Bilqisthi, M. F. (2024). Tantangan dan Peluang Blockchain di Era Digital dalam Bidang Keamanan Data dan Transaksi Digital. *Journal of Comprehensive Science (JCS)*, *3*(11).

Fadhilah, A. M. I., Nurdiawan, O., & Basyisyar, F. M. (2023). Pengembangan sistem informasi berbasis web smart contract pada blockchain berbasis nft. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *7*(1), 776–783.

Famuji, T. S., Masitha, A., Samodro, M. M. J., Fanani, G. P. I., & Pertiwi, Y. (2025). MODEL PERANCANGAN SISTEM TERDESENTRALISASI UNTUK KEAMANAN DATA GENETIKA MANUSIA BERBASIS BLOCKCHAIN DAN IPFS. *Rabit: Jurnal Teknologi Dan Sistem Informasi Univrab*, *10*(2), 241–258.

Fitrian, H. P., Andriyani, N., Anggraeni, C., Ashofwani, M. F., & Miftah, A. M. (2025). Analisis penggunaan blockchain untuk pengelolaan di bidang pendidikan. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(1), 1041–1045.

Fitriani, F. (2021). Analisis penilaian pembelajaran berbasis teknologi informasi dan implikasinya terhadap peningkatan kualitas pendidikan SD/MI. *Genderang Asa: Journal of Primary Education*, *2*(2), 30–42.

Hose, F., Censaka, F., Wijaya, R. A., Tanuwijaya, C., & Ng, J. (2025). Analisis Peran Blockchain dalam Zero-Trust Architecture untuk Penguatan Identitas Digital dan Privasi Data. *JIMU: Jurnal Ilmiah Multidisipliner*, *4*(01), 568–5778.

Kuswayati, S., & Rusdan, M. (2023). Prototype of Sales Information System Based on Educational Book Consultan Data and Senior Educational Book Consultant. *Jurnal Sistem Informasi Dan Teknologi Informasi*, *1*(2), 69–73.

Putra, E. P., & Setiadi, F. (2025). Faktor Kunci Keberhasilan Implementasi Blockchain dalam Identitas Berdaulat untuk Mendukung Target Pembangunan Berkelanjutan. *Jurnal Teknologi Dan Sistem Informasi Bisnis*, *7*(2), 253–261.

Rakhmansyah, M., Rahardja, U., Santoso, N. P. L., Khoirunisa, A., & Faturahman, A. (2021). Smart digital signature berbasis blockchain pada pendidikan tinggi menggunakan metode swot. *ADI Bisnis Digital Interdisiplin Jurnal*, *2*(1 Juni), 39–47.

Simanungkalit, A. (2024). Teknologi blockchain: Solusi untuk keamanan data dalam transaksi digital. *Circle Archive*, *1*(6).

Slam, B. E., Irawan, F., Efranda, N., & Herikson, R. (2025). Pengujian Sistem Identitas Digital Siswa Berbasis Blockchain untuk Keamanan dan Transparansi Menggunakan Black-Box Testing. *Journal Software, Hardware and Information Technology*, *5*(2), 72–83.

Suminar, L. R., & Nugroho, A. A. (2023). Adopsi Teknologi Blockchain di Sektor Publik: Peluang Pembentukan Sistem Identitas Digital Nasional di Era VUCA. *Dinamika Governance: Jurnal Ilmu Administrasi Negara*, *12*(4).

Tanadi, M., Prathama, Y., Stanley, E., Wimanho, V., Ashyqi, F., & Ng, J. (2025). Pemanfaatan Teknologi Blockchain untuk Digital Signature dan Manajemen Dokumen Akademik di Era Digital. *JIMU: Jurnal Ilmiah Multidisipliner*, *3*(04).

Vaher, K., Simanjuntak, A., & Sugiharto, E. (2025). Securing academic records with blockchain technology a data-driven approach for university management. *Jurnal MENTARI: Manajemen, Pendidikan Dan Teknologi Informasi*, *4*(1), 52–62.