

IMPLEMENTASI *BLOCKCHAIN* PADA SISTEM MANAJEMEN IDENTITAS BERBASIS *WEB* UNTUK VERIFIKASI SERTIFIKAT DIGITAL

Chandra Sidiq Prayoga ¹, Maulana Ardhiansyah ²

^{1,2}Teknik Informatika, Universitas Pamulang, Jl. Surya Kencana No. 1, Pamulang, Tangerang Selatan, Indonesia, 15417

e-mail: ¹chandrasidiq76@gmail.com, ²dosen00374@unpam.ac.id

Info Artikel

Riwayat Artikel:

Received Nov 03, 2025

Revised Dec 17, 2025

Accepted Dec 21, 2025

Abstract – Digital certificate security and authenticity have become critical issues in digital identity management due to the increasing number of forged certificates, which reduce public trust and slow down verification processes. This study aims to develop a web-based digital certificate management system integrated with blockchain technology to enhance security, transparency, and verification accuracy. The system employs MySQL and MongoDB for data management, while certificate files are stored in a decentralized manner using the InterPlanetary File System (IPFS). Certificate hash values are recorded through smart contracts deployed on the Polygon blockchain network, with MetaMask used for transaction authorization. The system was developed using the Waterfall method and evaluated through functional testing involving administrators, users, verifiers. The results indicate that the implemented blockchain architecture effectively ensures data integrity, prevents certificate forgery, and enables transparent and tamper-resistant verification, thereby improving the security, trust, and efficiency of digital certificate verification at LPK Pilitera.

Keywords: Blockchain, Digital Certificate, Identity Management, IPFS, Web-Based System

Corresponding Author:

Chandra Sidiq Prayoga

Email: chandrasidiq76@gmail.com



This is an open access article under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license.

Abstrak Indonesia – Keamanan dan keaslian sertifikat digital menjadi permasalahan penting dalam manajemen identitas di era digital akibat maraknya pemalsuan sertifikat yang menurunkan kepercayaan publik dan memperlambat proses verifikasi. Penelitian ini bertujuan mengembangkan sistem manajemen sertifikat digital berbasis website yang terintegrasi dengan teknologi blockchain untuk meningkatkan keamanan, transparansi, dan akurasi verifikasi. Sistem dikembangkan menggunakan MySQL dan MongoDB untuk pengelolaan data, serta interplanetary file system (IPFS) untuk penyimpanan file sertifikat secara terdesentralisasi, dengan pencatatan hash sertifikat dilakukan melalui smart contract pada jaringan Polygon menggunakan MetaMask. Metode pengembangan yang digunakan adalah Waterfall dengan pengujian oleh admin, pengguna, dan verifikasi. Hasil penelitian menunjukkan bahwa arsitektur blockchain yang dibangun mampu menjamin integritas data, mencegah pemalsuan sertifikat, dan menyediakan proses verifikasi yang transparan, sehingga terbukti meningkatkan keamanan, kepercayaan, dan efisiensi verifikasi sertifikat digital di LPK Pilitera.

Kata Kunci: Blockchain, Sertifikat Digital, Manajemen Identitas, IPFS, Berbasis Website

1. PENDAHULUAN

Perkembangan teknologi digital yang pesat telah membawa perubahan signifikan dalam pengelolaan data dan dokumen resmi, termasuk sertifikat digital yang digunakan sebagai bukti kompetensi individu di berbagai lembaga pelatihan dalam institusi pendidikan [1]. Namun, meningkatnya kasus pemalsuan

sertifikat dan manipulasi data digital menimbulkan tantangan serius terhadap keaslian dokumen serta menurunkan tingkat kepercayaan publik terhadap sertifikat yang diterbitkan [2]. Kondisi tersebut tidak hanya menghambat proses verifikasi, tetapi juga berpotensi menurunkan kredibilitas lembaga penerbit sertifikat

Permasalahan serupa juga dihadapi oleh Lembaga Pelatihan Kerja Ilmu Sejahtera (LPK Piltera), di mana proses penerbitan dan verifikasi sertifikat masih dilakukan secara manual tanpa integrasi sistem keamanan digital. Proses ini berpotensi menimbulkan kesalahan administrasi, duplikasi data, serta kesulitan dalam melakukan validasi keaslian sertifikat oleh pihak ketiga. Oleh karena itu, dibutuhkan sistem yang mampu menjamin keaslian, keamanan, dan transparansi dalam pengelolaan sertifikat digital.

Teknologi *blockchain* menawarkan solusi yang kuat untuk mengatasi permasalahan tersebut karena memiliki karakteristik terdesentralisasi, transparan, dan memiliki integritas data yang tinggi [3]. Setiap data yang tersimpan pada *blockchain* diverifikasi oleh banyak node dalam jaringan dan dicatat secara permanen, sehingga hampir tidak memungkinkan untuk dimanipulasi [4]. Selain itu, *blockchain* mendukung penerapan tanda tangan digital (*digital signature*) yang dapat memperkuat validitas identitas dan sertifikat digital yang diterbitkan.

Teknologi *blockchain* sendiri pertama kali diperkenalkan oleh Satoshi Nakamoto melalui sistem mata uang kripto Bitcoin, yang memperkenalkan konsep desentralisasi dan integritas data berbasis kriptografi [5]. Dalam perkembangannya, teknologi ini meluas ke berbagai bidang seperti bisnis, pemerintahan, dan pendidikan [6].

Beberapa penelitian terdahulu telah mengeksplorasi penerapan teknologi *blockchain* dalam proses verifikasi dokumen digital. Penelitian oleh Swastika et al., (2022), menunjukkan bahwa penggunaan *smart contract* pada jaringan *Ethereum* lokal (*Geth*) layak digunakan untuk penerbitan dan validasi sertifikat digital, namun sistem tersebut masih bergantung pada penyimpanan berkas di server lokal [7]. Alfina & Syafrinal (2022), mengembangkan sistem verifikasi ijazah berbasis *blockchain* dengan kombinasi metode *Peak Signal to Noise Ratio (PSNR)* untuk mendeteksi kesamaan citra ijazah, tetapi penelitian tersebut lebih berfokus pada proses deteksi dan verifikasi dibandingkan penyimpanan berkas secara terdesentralisasi [8]. Sementara itu, Wjiyanto (2024), merancang aplikasi verifikasi sertifikat berbasis *website* menggunakan *Ganache*, *Truffle*, *Flask*, dan *Web3.js* yang efektif dalam validasi *hash* sertifikat, namun belum mengintegrasikan sistem penyimpanan terdistribusi seperti *InterPlanetary File System (IPFS)* [9].

Berdasarkan keterbatasan penelitian-penelitian sebelumnya, kebaruan penelitian ini terletak pada aspek infrastruktur penyimpanan dan jaringan *blockchain* yang digunakan. Berbeda dengan penelitian terdahulu yang masih bergantung pada server lokal [10] atau belum menerapkan penyimpanan terdesentralisasi [11], penelitian ini mengintegrasikan *IPFS* sebagai media penyimpanan sertifikat digital sehingga file sertifikat tersimpan secara permanen, terdistribusi, dan tidak mudah dihapus. Selain itu, jaringan *blockchain* yang digunakan adalah *Polygon* sebagai solusi *layer-2 Ethereum* yang lebih efisien dari segi biaya dan memiliki kecepatan transaksi yang lebih baik, sehingga lebih realistis untuk diterapkan pada lingkungan lembaga pelatihan seperti LPK Piltera.

Penelitian ini bertujuan untuk mengembangkan sistem manajemen sertifikat digital berbasis *website* yang terintegrasi dengan teknologi *blockchain* guna meningkatkan keamanan, keaslian, dan akurasi proses verifikasi sertifikat digital, serta mendukung peningkatan kepercayaan dan efisiensi dalam pengelolaan data sertifikat di LPK Piltera.

2. PENELITIAN YANG TERKAIT

Teknologi *blockchain* telah banyak diteliti dan diterapkan dalam sistem verifikasi dokumen digital karena karakteristiknya yang bersifat terdesentralisasi, transparan, dan memiliki integritas data yang tinggi [3]. Karakteristik tersebut menjadikan *blockchain* sebagai teknologi yang relevan dalam meningkatkan keamanan dan keaslian sertifikat digital.

Penelitian oleh Swastika et al., (2022) mengimplementasikan *smart contract* pada jaringan *Ethereum* lokal (*Geth*) untuk proses penerbitan dan validasi sertifikat digital. Hasil penelitian menunjukkan bahwa *blockchain* mampu digunakan sebagai media verifikasi sertifikat, namun masih bergantung pada penyimpanan berkas di server lokal sehingga memiliki keterbatasan dari sisi keamanan dan skalabilitas [7].

Penelitian oleh Alfina & Syafrinal (2022) mengembangkan sistem verifikasi ijazah berbasis *blockchain* dengan metode *Peak Signal to Noise Ratio (PSNR)* untuk mendeteksi kesamaan citra ijazah,

namun penelitian tersebut lebih menekankan pada proses deteksi dan belum mengintegrasikan penyimpanan berkas secara terdesentralisasi [8].

Sementara itu, penelitian oleh Wijayanto (2024) merancang aplikasi verifikasi sertifikat berbasis *website* menggunakan *Ganache*, *Truffle*, *Flask*, dan *Web3.js* yang efektif dalam validasi *hash* sertifikat digital. Meskipun sistem tersebut mampu memverifikasi keaslian sertifikat, penyimpanan data masih bergantung pada infrastruktur terpusat dan belum memanfaatkan teknologi penyimpanan terdistribusi seperti *InterPlanetary File System (IPFS)* [9].

Berdasarkan penelitian-penelitian terdahulu, dapat disimpulkan bahwa sebagian besar sistem verifikasi sertifikat digital berbasis *blockchain* masih memiliki keterbatasan pada aspek penyimpanan berkas dan efisiensi jaringan *blockchain* yang digunakan. Penelitian ini dilakukan untuk mengatasi keterbatasan tersebut melalui integrasi penyimpanan sertifikat berbasis *IPFS* dan pemanfaatan jaringan *Polygon* sebagai *blockchain* yang lebih efisien dalam satu sistem manajemen sertifikat digital berbasis *website*. Dengan demikian, penelitian ini memberikan kontribusi dalam meningkatkan keamanan, keandalan, dan efisiensi proses verifikasi sertifikat digital.

3. METODE PENELITIAN

Metodologi penelitian merupakan langkah-langkah yang diterapkan untuk mempermudah proses penelitian dan mencapai tujuan yang telah ditetapkan. Adapun metodologi yang digunakan dalam penelitian ini meliputi metode pengumpulan data dan metode pengembangan sistem.

a. Metode Pengumpulan Data

Metode pengumpulan data dilakukan melalui beberapa cara, yaitu: Studi Pustaka, studi ini dilakukan dengan mempelajari berbagai literatur yang berkaitan dengan teknologi *blockchain*, sistem manajemen identitas, serta penerapan sertifikat digital berbasis *web* [12]. Selain itu, dilakukan juga kajian terhadap penelitian-penelitian terdahulu yang relevan sebagai landasan teori dan pembanding dalam pengembangan sistem. Wawancara, metode wawancara dilakukan dengan pihak LPK Pelita Ilmu Sejahtera (LPK Piltera) untuk memperoleh informasi terkait alur kerja, kebutuhan sistem, serta kendala yang dihadapi dalam proses penerbitan dan verifikasi sertifikat secara manual. Observasi, observasi dilakukan dengan mengamati langsung proses administrasi dan manajemen sertifikat di lingkungan LPK Piltera, guna memahami permasalahan yang ada dan menentukan kebutuhan sistem yang tepat.

b. Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan dalam penelitian ini adalah metode *Waterfall*. Metode ini dipilih karena memberikan pendekatan yang sistematis dan berurutan dalam pengembangan perangkat lunak [11]. Adapun tahapan dalam metode *Waterfall* meliputi:

1. *Requirements Definition* (Analisis Kebutuhan)

Pada tahap ini dilakukan komunikasi dengan pihak pengguna untuk memahami kebutuhan dan batasan sistem yang akan dikembangkan. Informasi diperoleh melalui wawancara dan observasi di LPK Piltera, kemudian dianalisis untuk menentukan kebutuhan fungsional dan nonfungsional sistem.

2. *System Design* (Perancangan Sistem)

Tahap ini mencakup perancangan arsitektur sistem, struktur basis data, serta rancangan antarmuka pengguna. Sistem dirancang untuk mengintegrasikan *blockchain Ethereum* dengan *MySQL* sebagai basis data pengguna dan *MongoDB* sebagai penyimpanan metadata sertifikat digital [13].

3. *Implementation* (Implementasi)

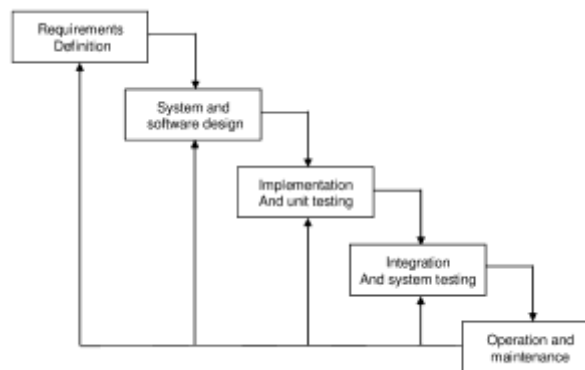
Pada Tahap ini sistem mulai dikembangkan menggunakan bahasa pemrograman *PHP* untuk *backend* serta *HTML*, *CSS*, dan *JavaScript* untuk *frontend*. Proses pengembangan dilakukan menggunakan *Visual Studio Code*, dengan integrasi ke *blockchain* melalui *MetaMask* [14].

4. *Integration & Testing* (Integrasi dan Pengujian)

Setiap modul sistem diintegrasikan dan diuji menggunakan metode *Black Box Testing* untuk memastikan semua fungsi berjalan sesuai kebutuhan, seperti *login admin* dan pengguna, *upload* sertifikat, penyimpanan *hash* di *blockchain*, serta proses verifikasi sertifikat [15].

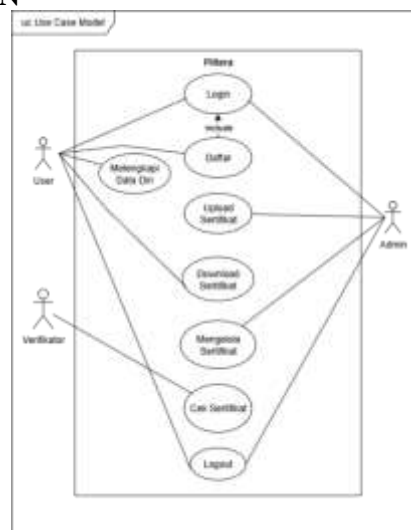
5. *Operation & Maintenance* (Operasi dan Pemeliharaan)

Tahapan terakhir adalah implementasi sistem yang telah diuji ke dalam lingkungan operasional di LPK Piltera. Selanjutnya dilakukan pemeliharaan dan evaluasi untuk memperbaiki kesalahan yang mungkin muncul serta meningkatkan fungsi sistem sesuai kebutuhan di masa mendatang.



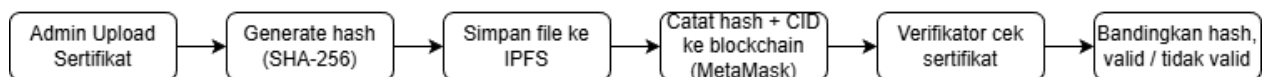
Gambar 1. Model Waterfall Ian Sommerville

4. HASIL DAN PEMBAHASAN



Gambar 2. Use Case Diagram

Dalam diagram tersebut, *admin* dapat melakukan *login*, menambah dan mengelola data pengguna, serta mengunggah sertifikat. *User* dapat melakukan *login* dan melihat daftar sertifikat yang dimilikinya berdasarkan NIK. Sedangkan verifikator hanya dapat melakukan verifikasi melalui halaman utama dengan memasukkan nomor sertifikat atau NIK peserta.



Gambar 3. Alur Proses Blockchain pada Sistem Verifikasi Sertifikat Digital

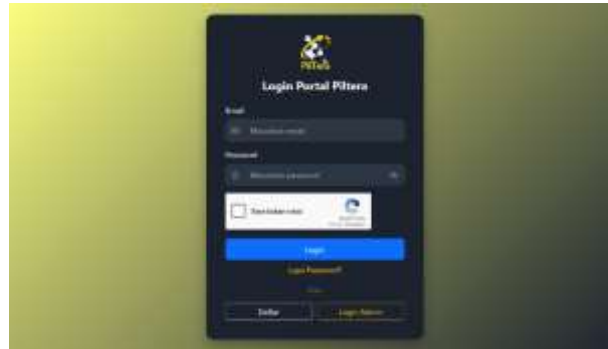
Alur proses *blockchain* pada sistem dimulai ketika *admin* mengunggah sertifikat digital ke dalam sistem. Sistem kemudian menghasilkan nilai *hash* sertifikat menggunakan algoritma *SHA-256* sebagai identitas unik sertifikat. File sertifikat selanjutnya disimpan secara terdesentralisasi menggunakan *InterPlanetary File System (IPFS)*, sedangkan nilai *hash* sertifikat dicatat ke dalam jaringan *blockchain* melalui *smart contract* dengan otorisasi transaksi menggunakan *MetaMask*.

Pada proses verifikasi, pengguna atau pihak verifikator memasukkan Nomor Sertifikat atau NIK peserta melalui halaman verifikasi. Sistem membandingkan nilai *hash* sertifikat yang tersimpan di *blockchain* dengan *hash* hasil perhitungan ulang dari sertifikat yang diverifikasi. Apabila kedua nilai *hash* sesuai, maka sertifikat dinyatakan asli dan valid, sedangkan perbedaan nilai *hash* menunjukkan bahwa sertifikat tidak valid atau telah mengalami perubahan.

Tahap implementasi dilakukan setelah tahap perancangan selesai. Implementasi bertujuan menerjemahkan hasil desain ke dalam bahasa pemrograman yang dapat dijalankan oleh sistem. Sistem ini dikembangkan menggunakan *PHP* sebagai bahasa *backend*, *HTML*, *CSS*, dan *JavaScript* sebagai *frontend*, serta *MySQL* dan *MongoDB* sebagai basis data. Integrasi dengan *MetaMask* dan *Ethereum* digunakan untuk mencatat *hash* sertifikat ke *blockchain*.

Berikut beberapa tampilan antarmuka yang terdapat dalam sistem:

a. Halaman *Login*



Gambar 3. Halaman *Login*

Menampilkan form untuk masuk ke sistem, terdapat *button Login Admin* untuk menuju ke halaman *login admin*.

b. Halaman *Dashboard Admin*



Gambar 4. Halaman *Dashboard Admin*

Pada halaman *dashboard admin* dapat melihat daftar *user*, mengunggah sertifikat, serta mengelola data sertifikat yang telah diterbitkan

b. Halaman *Dashboard User*



Gambar 5. Halaman *Dashboard User*

Halaman *dashboard user* menampilkan daftar sertifikat yang dimiliki user berdasarkan NIK, dan *user* dapat mengelola akun seperti ubah profil dan ubah *password*.

c. Halaman Verifikasi Sertifikat (Indeks)



Gambar 6. Halaman Verifikasi Sertifikat

Halaman verifikasi sertifikat dapat diakses tanpa *login* oleh pihak verifikator untuk memeriksa keaslian sertifikat dengan memasukkan NIK dan Nomor Sertifikat.

Setelah sistem diimplementasikan, dilakukan tahap pengujian untuk memastikan setiap fungsi berjalan dengan benar. Pengujian dilakukan menggunakan metode *Black Box Testing*, yang berfokus pada pengujian fungsi utama sistem berdasarkan kebutuhan pengguna.

Tabel I. Pengujian *Black Box*

No	Fitur yang Diuji	Hasil yang Diharapkan	Hasil Pengujian	Status
1	<i>Login Admin dan User</i>	Sistem menerima kredensial valid dan menolak yang salah	Sesuai	Berhasil
2	<i>Upload Sertifikat</i>	File tersimpan dan <i>hash</i> tercatat di <i>blockchain</i>	Sesuai	Berhasil
3	Verifikasi Sertifikat	Sertifikat dapat diverifikasi dengan <i>hash blockchain</i>	Sesuai	Berhasil
4	Lihat Sertifikat oleh <i>User</i>	Menampilkan daftar sertifikat berdasarkan NIK	Sesuai	Berhasil
5	Cek Sertifikat oleh Verifikator	Dapat dilakukan tanpa <i>login</i>	Sesuai	Berhasil

Berdasarkan hasil pengujian, seluruh fitur berjalan sesuai dengan rancangan awal. Proses unggah dan penyimpanan sertifikat berjalan dengan baik, serta hash transaksi tercatat permanen di jaringan *Polygon*. Hal ini membuktikan bahwa penerapan *blockchain* dapat meningkatkan keamanan, keaslian, dan transparansi sertifikat digital.

5. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa penerapan teknologi *blockchain* pada sistem manajemen sertifikat digital berbasis *website* berhasil meningkatkan keamanan, keaslian, dan transparansi proses verifikasi sertifikat. Pencatatan *hash* sertifikat menggunakan algoritma *SHA-256* ke dalam jaringan *blockchain* memastikan bahwa setiap perubahan pada sertifikat dapat terdeteksi, sehingga risiko pemalsuan dapat diminimalkan. Integrasi *InterPlanetary File System (IPFS)* sebagai media penyimpanan sertifikat memungkinkan penyimpanan file secara terdesentralisasi dan mengurangi ketergantungan pada server terpusat. Selain itu, penggunaan jaringan *Polygon* memberikan efisiensi biaya dan kecepatan transaksi yang lebih baik dibandingkan jaringan utama *Ethereum*, sehingga sistem lebih realistis untuk diterapkan pada lingkungan lembaga pelatihan seperti LPK Pilitera. Dengan demikian, sistem yang dikembangkan tidak hanya layak secara teknis, tetapi juga memberikan dampak signifikan terhadap peningkatan kepercayaan dan efisiensi proses verifikasi sertifikat digital sesuai dengan tujuan awal penelitian.

DAFTAR PUSTAKA

- [1] K. Kumutha, S. Jayalakshmi, and P. SriPriya, "Data security mechanism of Hyperledger Fabric and its application in academic documents verification system," *International Journal of Health Sciences*, vol. 6, no. S3, pp. 4394–4403, 2022.
- [2] R. Saputra and M. Hidayat, "Pemanfaatan blockchain untuk sistem verifikasi ijazah digital," *Jurnal Sistem Informasi dan Teknologi (SISFOTEK)*, vol. 9, no. 2, pp. 33–40, 2022.
- [3] S. A. Chic and M. F. Bilqisthi, "Tantangan dan peluang blockchain di era digital dalam bidang keamanan data dan transaksi digital," *Journal of Comprehensive Science (JCS)*, vol. 3, no. 11, 2024.
- [4] U. Rahardja, M. Mulyati, and F. Budiarty, "Pengaruh teknologi blockchain terhadap keabsahan ijazah," *Jurnal Manajemen Retail Indonesia*, vol. 2, pp. 11–19, 2021.
- [5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [6] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York, NY, USA: Penguin, 2016.
- [7] W. Swastika, H. Wirasantosa, and O. H. Kelana, "Rancang bangun website akademik dengan penyimpanan sertifikat digital menggunakan teknologi blockchain," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 9, no. 1, p. 33, 2022.
- [8] A. Alfina and S. Syafrinal, "Model sistem verifikasi dokumen ijazah digital berbasis teknologi blockchain," *SMARTICS Journal*, vol. 8, no. 2, pp. 59–65, 2022, doi: 10.21067/smartics.v8i2.7718.
- [9] H. Wijayanto, "Aplikasi verifikasi sertifikat berbasis website menggunakan blockchain," *Infact: International Journal of Computers*, vol. 8, no. 02, pp. 35–42, 2024, doi: 10.61179/jurnalinfact.v8i02.586.
- [10] M. Ubaidillah and R. Murti, "Penerapan Teknologi Blockchain dalam Pengolahan Data," *Jurnal Teknologi dan Sistem Informasi*, vol. 9, no. 2, pp. 45–52, 2021.
- [11] R. S. Pressman, *Rekayasa Perangkat Lunak: Pendekatan Praktisi* (Edisi 7). Yogyakarta: Andi, 2012. Fathansyah. (2012). *Basis Data*. Bandung: Informatika.
- [12] H. P. Fitriani, N. Andriyani, C. Anggraeni, M. F. Ashofwani, and A. M. Miftah, "Analisis penggunaan blockchain untuk pengelolaan di bidang pendidikan," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 1, pp. 1041–1045, 2025.
- [13] I. Afrianto, A. Sufa, and T. R. D. Suseno, "Pemodelan sistem pencatatan data akademik sekolah berbasis teknologi blockchain," 2023.
- [14] M. Ardiansyah and R. Nugraha, "Penerapan model rapid application development pada aplikasi helpdesk trouble ticket PT. Satkomindo Mediyasa," *Jurnal Teknologi Informasi dan Komputer*, vol. 6, no. 2, pp. 22–29, 2022.
- [15] B. D. Fathansyah and R. Ketiga, *Informatika*, Bandung, Indonesia, 2012.