Jurnal Minfo Polgan (JMP)
Volume 15, Nomor 3, September-Desember 2026
DOI : https://doi.org/10.33395/jmp.v15i3.16552
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Penerapan Metode Blockchain Untuk Verifikasi Ijazah Digital Menggunakan Pendekatan Hash Algorithm Verification

[1]Miftahul Rifqi, [2] Yulita Salim, [3]Erick Irawadi Alwi
[1*,2,3]Teknik Informatika/Fakultas Ilmu Komputer, Universitas Muslim Indonesia, Makassar, Indonesia
*Korespondensi: 130220220214@student.umi.ac.id

Submit : 19 Jun 2026 | Diterima : 15 Jul 2026 | Terbit : 28 Agust 2026

ABSTRACT

Digital diploma forgery has become a significant challenge that may reduce trust in the authenticity and integrity of academic documents. Although various verification approaches have been proposed, there remains a need for a more secure and reliable mechanism to ensure document integrity. This study aims to develop a blockchain-based digital diploma verification system by integrating the SHA-256 algorithm, Merkle Tree, and digital signatures to support document authentication. The proposed method generates document hash values using SHA-256, constructs a Merkle Root through the Merkle Tree structure, and verifies the generated Merkle Root and digital signature against the reference data stored on the blockchain. The evaluation was conducted using 14 test documents consisting of one original diploma and thirteen modified diplomas with changes made to different document components. The experimental results indicate that the proposed system was able to distinguish authentic documents from modified ones under the evaluation scenarios. Within the dataset used in this study, the system achieved an Accuracy Verification Rate of 100%, where every document modification produced different hash values and Merkle Roots, enabling the alterations to be detected during the verification process. These findings suggest that the integration of SHA-256, Merkle Tree, digital signatures, and blockchain has the potential to improve the security, integrity, and reliability of digital diploma verification. However, the evaluation was limited to a relatively small dataset, and further studies involving larger datasets and more diverse testing scenarios are recommended to comprehensively assess the proposed approach.

Keywords: Blockchain, Data Integrity, Digital Diploma Verification, Digital Signature, Merkle Tree, SHA-256.

ABSTRAK

Pemalsuan ijazah digital merupakan salah satu tantangan yang dapat menurunkan kepercayaan terhadap keaslian dan integritas dokumen akademik. Berbagai pendekatan verifikasi telah dikembangkan, namun masih terdapat kebutuhan akan mekanisme yang mampu menjamin keutuhan data secara lebih aman dan andal. Penelitian ini bertujuan mengembangkan sistem verifikasi ijazah digital berbasis blockchain dengan mengintegrasikan algoritma SHA-256, Merkle Tree, dan digital signature untuk mendukung proses autentikasi dokumen. Metode yang digunakan meliputi pembangkitan nilai hash menggunakan SHA-256, pembentukan Merkle Root melalui struktur Merkle Tree, serta pencocokan Merkle Root dan digital signature terhadap data referensi yang tersimpan pada blockchain. Evaluasi dilakukan menggunakan 14 dokumen uji yang terdiri atas satu dokumen asli dan tiga belas dokumen yang dimodifikasi pada berbagai komponen data. Hasil pengujian menunjukkan bahwa sistem mampu membedakan dokumen asli dan dokumen yang telah dimodifikasi sesuai dengan kondisi pengujian. Pada dataset yang digunakan dalam penelitian ini, sistem memperoleh Accuracy Verification Rate sebesar 100%, di mana setiap perubahan pada dokumen menghasilkan nilai hash dan Merkle Root yang berbeda sehingga dapat terdeteksi selama proses verifikasi. Temuan ini menunjukkan bahwa integrasi SHA-256, Merkle Tree, digital signature, dan blockchain berpotensi meningkatkan keamanan, integritas, dan keandalan proses verifikasi ijazah digital. Meskipun demikian, pengujian masih terbatas pada jumlah dokumen yang relatif sedikit sehingga diperlukan penelitian lanjutan dengan dataset yang lebih besar dan skenario pengujian yang lebih beragam.

Kata Kunci: Blockchain, Digital Signature, Integritas Data, SHA-256, Merkle Tree, Verifikasi Ijazah Digital.

PENDAHULUAN

Pada era teknologi informasi, terdapat bidang forensik yang mampu membuktikan tindak kejahatan berdasarkan serangkaian tahapan seperti mengidentifikasi, menguji, menganalisis, serta dapat mendokumentasikan bukti yang terdapat pada sumber serta hasil analisa yang dilakukan (M. A. - et al., 2022)(Hidayat et al., 2024)(Afdal et al., 2022)(Akil et al., 2024). Seiring berkembangnya teknologi, ada beberapa cara yang dapat dilakukan untuk memverifikasi dokumen asli atau palsu (Asis & Ilmawan, 2023). Namun demikian, dalam beberapa tahun terakhir, maraknya kasus pemalsuan dokumen di Indonesia telah menjadi permasalahan serius yang mengancam integritas sistem pendidikan nasional serta menurunkan tingkat kepercayaan publik terhadap kredensial akademik. Oleh karena itu, keaslian dan validitas dokumen digital memiliki nilai yang sangat krusial, tidak hanya bagi individu pemiliknya, tetapi juga bagi institusi pendidikan, dunia industri, dan masyarakat secara luas(Putra Santoso & Judhie Putra, 2026)(Afdal et al., 2022).

Teknologi yang semakin canggih tidak hanya dimanfaatkan oleh masyarakat untuk melakukan aktivitas positif, namun banyak juga yang memanfaatkan kehebatan teknologi untuk melakukan tindakan-tindakan negatif yang menjadi ancaman bagi pengguna teknologi khususnya dalam hal pemanfaatan dunia maya (*cybercrime*) (Supardin et al., 2022) (Hidayat et al., 2024)(Pengabdian et al., 2022). Oleh sebab itu, dibutuhkan sebuah sistem verifikasi ijazah yang tidak hanya cepat dan efisien, tetapi juga memiliki tingkat keamanan dan keandalan yang tinggi. Digital forensic adalah suatu ilmu pengetahuan dan keahlian untuk mengidentifikasi, mengumpulkan, menganalisis dan menguji bukti-bukti digital yang menjadi kasus untuk ditangani(Nugraha et al., 2024).

Pemalsuan ijazah tidak hanya terjadi dalam bentuk pemalsuan dokumen fisik, tetapi juga mencakup manipulasi data akademik, penggunaan identitas palsu, serta praktik penerbitan ijazah tanpa proses pendidikan yang sah. Perkembangan teknologi percetakan dan digital editing semakin mempermudah pemalsuan dokumen akademik, sehingga metode verifikasi konvensional menjadi semakin tidak efektif. Dalam konteks rekrutmen tenaga kerja, baik di sektor publik maupun swasta, keberadaan ijazah palsu dapat menyebabkan ketidakadilan kompetitif, menurunkan kualitas sumber daya manusia, serta berpotensi menimbulkan risiko hukum dan administratif. Oleh sebab itu, dibutuhkan sebuah sistem verifikasi ijazah yang tidak hanya cepat dan efisien, tetapi juga memiliki tingkat keamanan dan keandalan yang tinggi(Putra Santoso & Judhie Putra, 2026).

Karakteristik inheren blockchain seperti desentralisasi, immutabilitas (ketidakbisaan data diubah), dan transparansi menjadikannya kandidat ideal untuk merevolusi manajemen data akademik. Kasus manipulasi ijazah, pencurian identitas akademik, dan kehilangan dokumen penting yang belakangan ini terjadi menunjukkan kerentanan sistem informasi akademik tradisional(Abdullah, 2025).

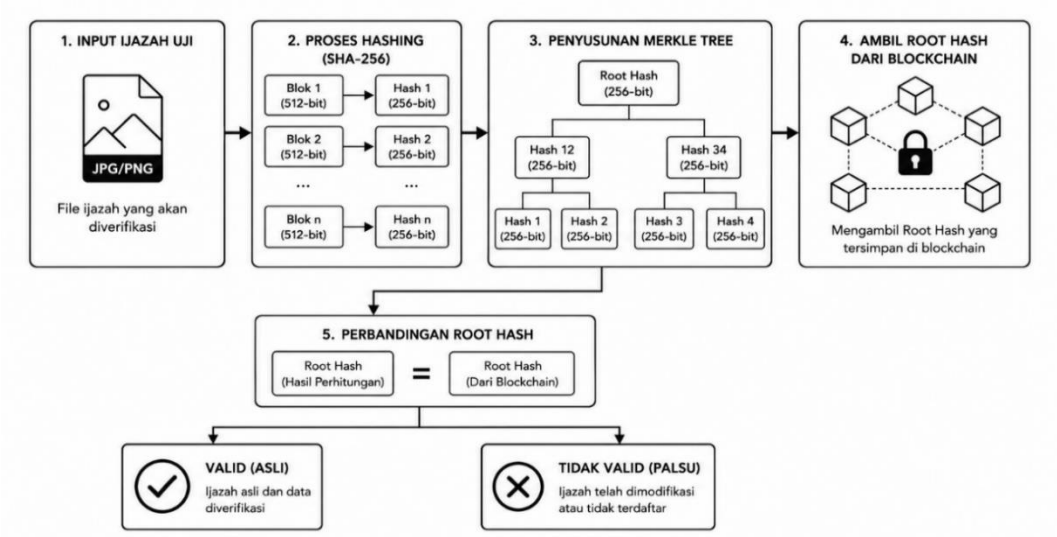
Kebaruan penelitian ini terletak pada integrasi SHA-256, Merkle Tree, Digital Signature, dan Blockchain dalam satu mekanisme verifikasi ijazah digital yang mampu mendeteksi perubahan data secara real-time melalui validasi Root Hash dan tanda tangan digital.

Gambar 1 Konsep dasar fungsi hash SHA-256 dalam menghasilkan identitas digital dokumen.

Gambar 1 menunjukkan proses dasar fungsi hash yang digunakan dalam penelitian ini. Dokumen ijazah digital yang menjadi data masukan diproses menggunakan algoritma SHA-256 untuk menghasilkan nilai hash yang unik(Wadhwani, 2023). Nilai hash tersebut memiliki panjang yang tetap meskipun ukuran dokumen yang diproses berbeda-beda. Dalam sistem yang dikembangkan, hash digunakan sebagai identitas digital dokumen dan menjadi dasar dalam pembentukan *Merkle Tree*. Dengan adanya proses hashing, setiap perubahan sekecil apa pun pada dokumen akan menghasilkan nilai hash yang berbeda sehingga keaslian dan integritas dokumen dapat diketahui melalui proses verifikasi(Kuznetsov, Rusnak, Yezhov, Kanonik, et al., 2024)

METODE PENELITIAN

Metode yang digunakan pada Gambar 2 adalah penerapan algoritma SHA-256 dan struktur Merkle Tree dalam verifikasi ijazah digital berbasis blockchain. Proses verifikasi diawali dengan pembentukan nilai hash menggunakan SHA-256, kemudian nilai hash tersebut disusun ke dalam Merkle Tree hingga menghasilkan Merkle Root sebagai representasi integritas dokumen(Krishnan et al., 2025)(Krishnan et al., 2025). Selanjutnya, nilai Merkle Root yang dihasilkan dibandingkan dengan nilai Merkle Root yang tersimpan pada blockchain. Kesesuaian kedua nilai menunjukkan bahwa dokumen masih asli dan tidak mengalami perubahan, sedangkan perbedaan nilai mengindikasikan adanya modifikasi atau pemalsuan data pada dokumen.



Gambar 2 Proses verifikasi Merkle Root pada sistem ijazah digital berbasis blockchain.

Penelitian ini menguji penggunaan algoritma SHA-256 dan Merkle Tree dalam verifikasi ijazah digital berbasis *blockchain*. Verifikasi dilakukan melalui perbandingan nilai *Merkle Root* hasil perhitungan dokumen dengan nilai *Merkle Root* yang tersimpan pada *blockchain*. Dokumen dinyatakan valid apabila kedua nilai identik, sedangkan perbedaan nilai menunjukkan bahwa dokumen telah mengalami perubahan (Wadhwani, 2023).

Input Ijazah Uji

Pada tahap ini, pengguna mengunggah dokumen ijazah digital berformat JPG atau PNG ke dalam sistem. Sistem kemudian melakukan validasi terhadap format, ukuran file maksimal 2 MB, dan kondisi file untuk memastikan dokumen dapat diproses dengan baik. Setelah lolos validasi, dokumen diproses menggunakan algoritma SHA-256 untuk menghasilkan nilai hash yang digunakan dalam(Mattaparthy & S, 2025) pembentukan Merkle Tree dan proses verifikasi pada blockchain.

$$H_i = SHA256(B_i) \quad (1)$$

Keterangan:

- B_i = blok data ke-iii
- H_i = nilai hash blok ke-iii
- $SHA256$ = fungsi hash kriptografi 256-bit

Proses *hashing*

$$H_{12} = SHA256(H_1 \parallel H_2) \quad (2)$$
$$H_{34} = SHA256(H_3 \parallel H_4) \quad (3)$$

Tahap kedua adalah proses hashing menggunakan algoritma SHA-256. Dokumen ijazah yang telah lolos validasi diproses untuk menghasilkan nilai hash unik sepanjang 256-bit. Nilai hash ini berfungsi sebagai identitas digital dokumen dan digunakan pada proses verifikasi(Abidin, 2025). SHA-256 dipilih karena memiliki tingkat keamanan yang tinggi serta mampu mendeteksi perubahan data sekecil apa pun. Perubahan satu karakter saja pada

dokumen akan menghasilkan nilai hash yang berbeda secara signifikan, sehingga integritas dan keaslian dokumen dapat diverifikasi dengan akurat(Abidin, 2025).

Keterangan:

- ‖ = operasi penggabungan (concatenation)
- H_{12} = hash gabungan dari H_1 dan H_2
- H_{34} = hash gabungan dari H_3 dan H_4

Penyusunan Merkle Tree

Tahap ketiga adalah penyusunan Merkle Tree. Nilai hash yang dihasilkan pada tahap sebelumnya digabungkan secara berpasangan dan diproses kembali hingga menghasilkan satu nilai hash utama yang disebut Merkle Root. Merkle Root berfungsi sebagai identitas digital yang mewakili seluruh isi dokumen. Jika terdapat perubahan pada salah satu bagian dokumen, nilai Merkle Root akan berubah sehingga perubahan tersebut dapat dideteksi melalui proses verifikasi. Nilai Merkle Root inilah yang kemudian digunakan sebagai acuan untuk membandingkan keaslian dokumen dengan data yang tersimpan pada blockchain(Kuznetsov, Rusnak, Yezhov, Kuznetsova, et al., 2024)(Kuznetsov, Rusnak, Yezhov, Kuznetsova, et al., 2024).

$$MR = SHA256(H_{12} \parallel H_{34}) \qquad (4)$$

Keterangan:

- MR = Merkle Root
- Merkle Root merupakan representasi seluruh isi dokumen

Pengambilan Root Hash Dari Blockchain

Tahap keempat adalah pengambilan Merkle Root dari blockchain. Sistem mengambil Merkle Root asli yang telah disimpan saat dokumen pertama kali diregistrasikan. Nilai tersebut digunakan sebagai data pembanding dalam proses verifikasi(Javatpoint, 2023). Blockchain dipilih karena bersifat transparan dan tidak dapat diubah (immutable), sehingga data yang tersimpan lebih aman dan terpercaya. Jika Merkle Root hasil perhitungan dokumen sama dengan Merkle Root yang tersimpan pada blockchain, maka dokumen dinyatakan asli. Sebaliknya, jika nilainya berbeda, dokumen terindikasi telah mengalami perubahan atau pemalsuan(Zhai et al., 2023).

$$MR_{bc} \qquad (5)$$

$$Status = \begin{cases} Valid, & MR_{calc} = MR_{bc} \\ Tidak\ Valid, & MR_{calc} \neq MR_{bc} \end{cases} \qquad (6)$$

Keterangan:

- MR_{bc}= Root Hash yang tersimpan pada blockchain

Perbandingan *Root Hash*

Tahap terakhir adalah membandingkan Merkle Root hasil perhitungan dokumen dengan Merkle Root yang tersimpan pada blockchain. Jika kedua nilai sama, dokumen dinyatakan valid dan asli(M. O. R. M. - et al., 2024). Sebaliknya, jika nilainya berbeda, dokumen dinyatakan tidak valid karena terindikasi mengalami perubahan. Proses ini memungkinkan verifikasi dokumen dilakukan secara cepat, akurat, dan aman dengan memanfaatkan SHA-256, Merkle Tree, dan blockchain(Mattaparthy & S, 2025).

$$V = \begin{cases} Valid, & jika\ MR_{uji} = MR_{bc} \\ Tidak\ Valid, & jika\ MR_{uji} \neq MR_{bc} \end{cases} \qquad (7)$$

Keterangan:

- V = Status verifikasi dokumen
- MR_{uji} = Merkle Root hasil perhitungan dokumen uji
- MR_{bc} = Merkle Root yang tersimpan pada blockchain

Perancangan *root hash*

Perancangan pada penelitian ini difokuskan pada pengujian algoritma SHA-256, Merkle Tree, dan blockchain dalam proses verifikasi ijazah digital untuk menjamin keaslian serta integritas dokumen akademik. Pendekatan ini digunakan sebagai alternatif terhadap proses verifikasi konvensional yang memerlukan waktu relatif lama dan masih memiliki risiko terjadinya pemalsuan dokumen(Abdulrahman Syed, 2025).

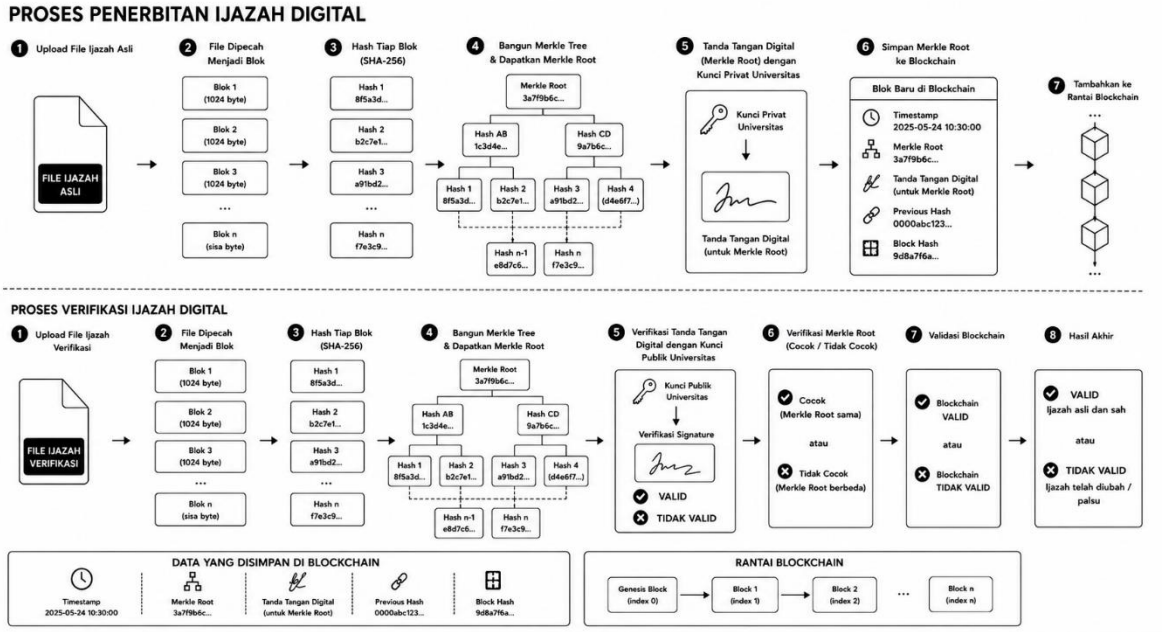
Pengujian dilakukan melalui beberapa tahapan, yaitu input data dokumen, validasi dokumen, proses hashing menggunakan SHA-256, pembentukan Merkle Tree, penyimpanan Root Hash pada blockchain, pengambilan data dari blockchain, proses verifikasi, serta pencatatan aktivitas verifikasi. Seluruh tahapan tersebut digunakan untuk mengevaluasi kemampuan algoritma dalam mendeteksi perubahan data pada dokumen ijazah digital(Capece et al., 2020).

Proses diawali dengan penggunaan dokumen ijazah dalam format JPG atau PNG sebagai data uji. Dokumen kemudian melalui tahap validasi untuk memastikan format, ukuran, dan integritas data sesuai dengan kebutuhan pengujian(Djajadi et al., 2023). Setelah validasi selesai, algoritma SHA-256 digunakan untuk menghasilkan nilai hash yang merepresentasikan isi dokumen secara unik.

Nilai hash yang diperoleh selanjutnya diproses menggunakan struktur Merkle Tree hingga menghasilkan Root Hash sebagai representasi digital dari keseluruhan data dokumen. Root Hash tersebut kemudian disimpan pada blockchain sebagai data referensi yang bersifat permanen dan sulit dimodifikasi(Javatpoint, 2023).

Tahap berikutnya dilakukan dengan membandingkan Root Hash hasil perhitungan dokumen uji dengan Root Hash yang tersimpan pada blockchain. Apabila kedua nilai hash identik, maka dokumen dinyatakan valid dan tidak mengalami perubahan. Sebaliknya, apabila ditemukan perbedaan nilai hash, maka dokumen terindikasi telah mengalami modifikasi sehingga dinyatakan tidak valid(Priyadarshini et al., 2025).

Selain itu, proses pengujian juga memanfaatkan pencatatan aktivitas verifikasi untuk mendukung transparansi dan keterlacakan hasil pengujian. Kombinasi algoritma SHA-256, Merkle Tree, dan blockchain menunjukkan kemampuan yang baik dalam menjaga integritas data serta mendeteksi perubahan dokumen secara cepat, akurat, dan aman(Marian et al., 2025)(Quispe & Pacheco, 2025).



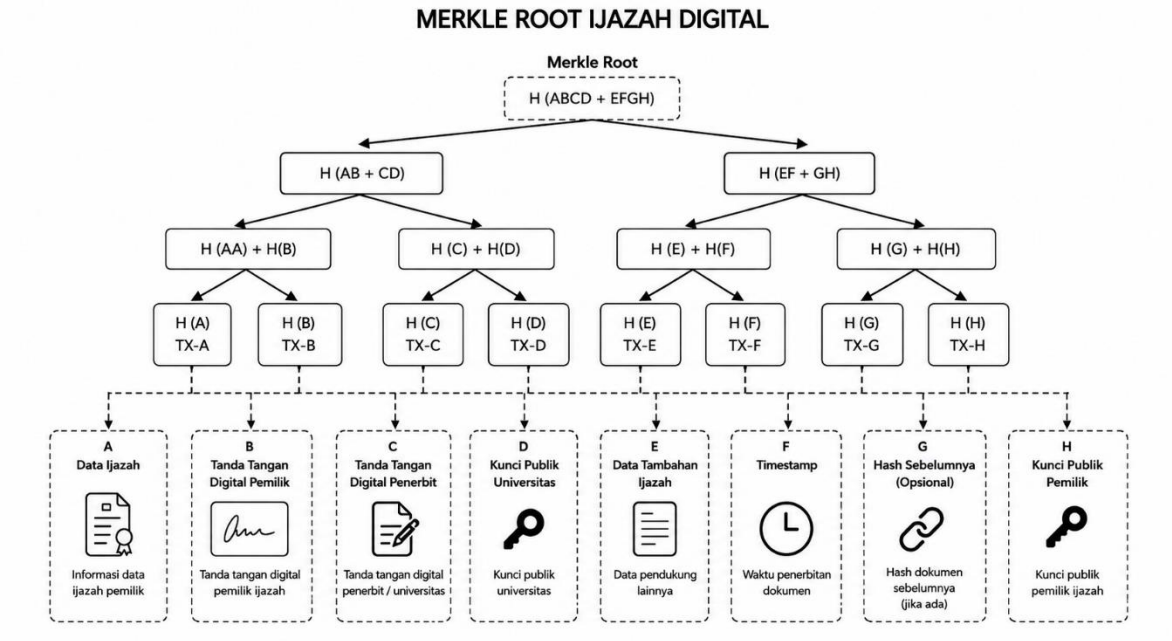
Gambar 3 Proses penerbitan dan verifikasi ijazah digital berbasis blockchain.

Berdasarkan Gambar 3 pengujian dilakukan melalui dua tahap utama, yaitu pembentukan data referensi dan verifikasi dokumen. Pada tahap pembentukan data referensi, dokumen ijazah diproses menggunakan algoritma SHA-256 untuk menghasilkan nilai hash yang unik. Nilai hash tersebut kemudian disusun menggunakan Merkle Tree hingga

menghasilkan Merkle Root sebagai representasi integritas dokumen. Selanjutnya, Merkle Root disimpan pada blockchain bersama digital signature sebagai data referensi(M. O. R. M. - et al., 2024).

Pada tahap verifikasi, dokumen yang diuji diproses kembali menggunakan algoritma yang sama untuk menghasilkan Merkle Root baru. Nilai yang diperoleh kemudian dibandingkan dengan Merkle Root yang tersimpan pada blockchain. Selain itu, digital signature juga diverifikasi untuk memastikan keaslian sumber dokumen. Dokumen dinyatakan valid apabila nilai Merkle Root dan digital signature sesuai dengan data referensi yang tersimpan. Sebaliknya, perbedaan nilai menunjukkan adanya perubahan atau modifikasi pada dokumen(Iavich & Kuchukhidze, 2025).

Melalui tahapan tersebut, pengujian dilakukan untuk mengevaluasi kemampuan algoritma SHA-256, Merkle Tree, digital signature, dan blockchain dalam menjaga integritas, keaslian, serta konsistensi data pada dokumen ijazah digital(Han et al., 2025).



Gambar 4 Pembentukan Merkle Root menggunakan SHA-256 dan Merkle Tree

Gambar 4 menunjukkan proses pembentukan Merkle Root dari komponen data ijazah digital yang diproses menggunakan algoritma SHA-256. Nilai hash yang dihasilkan kemudian disusun dalam struktur Merkle Tree hingga menghasilkan satu nilai hash akhir (Merkle Root) yang mewakili keseluruhan dokumen(Tri Ade Nia et al., 2024)(Tri Ade Nia et al., 2024). Nilai tersebut digunakan dalam proses verifikasi, di mana perubahan pada salah satu komponen data akan menghasilkan Merkle Root yang berbeda sehingga integritas dan keaslian dokumen dapat diverifikasi(Begimbayeva et al., 2026).

Formulasi Merkle Root
Hash Tingkat Pertama (Leaf Node)
A = H(Data Ijazah)
B = H(Tanda Tangan Digital Pemilik)
C = H(Tanda Tangan Digital Penerbit)
D = H(Kunci Publik Universitas)
E = H(Data Tambahan Ijazah)
F = H(Timestamp)
G = H(Hash Sebelumnya)
H = H(Kunci Publik Pemilik)
Keterangan:

- H(x) = fungsi hash SHA-256
- A–H = hash dari setiap komponen dokumen

Hash Tingkat Kedua

$$AB = H(A \parallel B)$$
$$CD = H(C \parallel D)$$
$$EF = H(E \parallel F)$$
$$GH = H(G \parallel H)$$

Keterangan:

- ‖ menyatakan operasi penggabungan (*concatenation*)

Hash Tingkat Ketiga

$$ABCD = H(AB \parallel CD)$$
$$EFGH = H(EF \parallel GH)$$

Pembentukan Merkle Root

$$MR = H(ABCD \parallel EFGH)$$

Keterangan:

- MR = Merkle Root
- MR merupakan representasi seluruh isi dokumen ijazah digital

Formulasi tersebut menggambarkan tahapan pembentukan Merkle Root melalui proses penggabungan hash secara bertingkat hingga diperoleh satu nilai hash akhir. Nilai tersebut selanjutnya digunakan sebagai acuan dalam proses verifikasi dokumen pada blockchain(Nadimsyah & Ezar Al Rivan, 2024).

HASIL DAN PEMBAHASAN

Pengujian sistem dilakukan menggunakan dataset yang terdiri dari dokumen ijazah asli dan dokumen ijazah hasil modifikasi. Dataset tersebut digunakan untuk menguji kemampuan sistem dalam mendeteksi perubahan data melalui mekanisme hashing SHA-256, Merkle Tree, Digital Signature, dan Blockchain. Adapun rincian dataset pengujian dapat dilihat pada Tabel.3

Tabel 1 dataset pengujian sistem verifikasi ijazah digital

No	Nama Dataset	Jenis Dokumen	Modifikasi yang Dilakukan	Status Dokumen
1	Ijazah_Asli.jpg	Ijazah Asli	Tidak ada	Valid
2	Ijazah_Mod_01.jpg	Ijazah Modifikasi	Perubahan Nama Pemilik	Tidak Valid
3	Ijazah_Mod_02.jpg	Ijazah Modifikasi	Perubahan NIM	Tidak Valid
4	Ijazah_Mod_03.jpg	Ijazah Modifikasi	Perubahan NIK	Tidak Valid
5	Ijazah_Mod_04.jpg	Ijazah Modifikasi	Perubahan Tempat Lahir	Tidak Valid
6	Ijazah_Mod_05.jpg	Ijazah Modifikasi	Perubahan Tanggal Lahir	Tidak Valid
7	Ijazah_Mod_06.jpg	Ijazah Modifikasi	Perubahan Program Studi	Tidak Valid
8	Ijazah_Mod_07.jpg	Ijazah Modifikasi	Perubahan Nomor Ijazah	Tidak Valid
9	Ijazah_Mod_08.jpg	Ijazah Modifikasi	Perubahan Tanggal Kelulusan	Tidak Valid
10	Ijazah_Mod_09.jpg	Ijazah Modifikasi	Perubahan Nama Rektor	Tidak Valid
11	Ijazah_Mod_10.jpg	Ijazah Modifikasi	Perubahan Nama Dekan	Tidak Valid
12	Ijazah_Mod_11.jpg	Ijazah Modifikasi	Perubahan Foto Pemilik	Tidak Valid
13	Ijazah_Mod_12.jpg	Ijazah Modifikasi	Perubahan Tanda Tangan	Tidak Valid
14	Ijazah_Mod_13.jpg	Ijazah Modifikasi	Perubahan Logo Universitas	Tidak Valid

Dataset pengujian terdiri atas 14 dokumen ijazah digital yang meliputi 1 dokumen ijazah asli dan 13 dokumen hasil modifikasi. Dokumen modifikasi dibuat dengan mengubah satu komponen data pada dokumen asli, seperti nama pemilik, NIM, NIK, tempat lahir, tanggal lahir, program studi, nomor ijazah, tanggal kelulusan, identitas pejabat penandatangan, foto, tanda tangan, dan logo universitas. Dataset ini digunakan untuk menguji kemampuan sistem dalam mendeteksi perubahan dokumen melalui perbandingan nilai hash SHA-256, Merkle Root, digital signature, dan data yang tersimpan pada blockchain.

Tabel 2 Hasil *Accuracy Verification Rate*

	Jumlah Dokumen	Hasil Verifikasi Benar	Hasil Verifikasi Salah
Ijazah Asli	1	1	0
Ijazah Modifikasi	13	13	0
Total	14	14	0

Perhitungan Accuracy Verification Rate menggunakan rumus:

$$Accuracy = \frac{Jumlah\ Verifikasi\ Benar}{Total\ Dokumen\ Uji} \times 100\% = 100\% \quad (8)$$

Sehingga :

$$Accuracy = \frac{14}{14} \times 100\% = 100\% \quad (9)$$

Hasil pengujian menunjukkan bahwa sistem mampu melakukan verifikasi dokumen dengan akurasi sebesar 100%. Hasil tersebut didukung oleh penggunaan algoritma SHA-256 yang menghasilkan nilai hash unik untuk setiap dokumen, sehingga setiap perubahan data dapat terdeteksi melalui perbedaan nilai hash. Selain itu, penerapan Merkle Tree, Digital Signature, dan Blockchain memperkuat proses verifikasi dalam menjaga integritas dan keaslian dokumen. Meskipun demikian, pengujian masih terbatas pada 14 dokumen sehingga diperlukan penelitian lanjutan dengan jumlah data dan variasi manipulasi yang lebih beragam.

Tabel 3 *Confusion Matrix*

	Prediksi Valid	Prediksi Tidak Valid
Aktual Valid	1 (TP)	0 (FN)
Aktual Tidak Valid	0 (FP)	13 (TN)

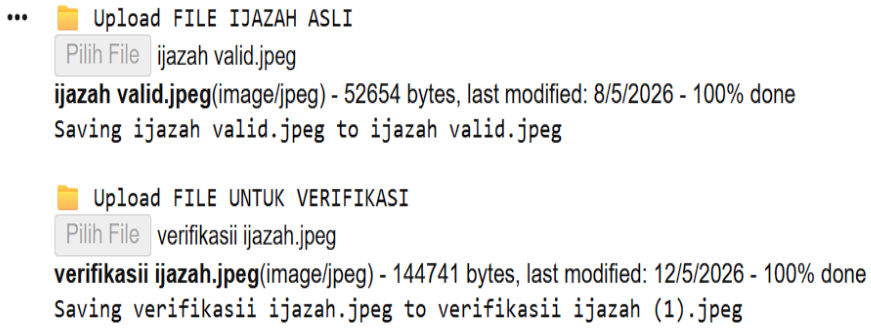
Dari tabel 3 dapat menghasilkan:

- Accuracy = 100%
- Precision = 100%
- Recall = 100%
- F1-Score = 100%

Table 4 Perbandingan Penelitian yang Diusulkan dengan Penelitian Sebelumnya

Peneliti	Tahun	Metode	SHA-256	Merkle Tree	Digital Signature	Blockchain	Hasil
Priyadarshini et al.	2025	Blockchain Certificate Validation	×	×	×	✓	Memverifikasi sertifikat digital berbasis blockchain untuk meningkatkan keaslian dokumen.
Quispe & Pacheco	2025	Degree Verification Blockchain	×	×	×	✓	Menjamin integritas dokumen akademik melalui teknologi blockchain.
Krishnan et al.	2025	Merkle Tree Certification	×	✓	×	✓	Menggunakan Merkle Tree dan blockchain untuk verifikasi dokumen akademik.
Mattaparthy et al.	2025	Blockchain Verification	×	×	×	✓	Mengimplementasikan blockchain untuk validasi dan penyimpanan data dokumen digital.
Penelitian Ini	2026	SHA-256 + Merkle Tree + Digital Signature + Blockchain	✓	✓	✓	✓	Mencapai Accuracy Verification Rate sebesar 100% pada 14 dokumen uji serta mampu menjaga integritas dan keaslian dokumen digital melalui verifikasi hash, Merkle Root, dan digital signature.

Berdasarkan hasil perbandingan dengan penelitian sebelumnya, penelitian ini menawarkan pendekatan yang lebih komprehensif melalui integrasi SHA-256, Merkle Tree, Digital Signature, dan Blockchain dalam satu mekanisme verifikasi ijazah digital. Integrasi tersebut memungkinkan sistem tidak hanya memvalidasi keberadaan data pada blockchain, tetapi juga memeriksa integritas dan keaslian dokumen melalui verifikasi hash, Merkle Root, dan tanda tangan digital. Hasil pengujian menunjukkan bahwa seluruh dokumen uji berhasil diidentifikasi sesuai dengan kondisi sebenarnya dengan Accuracy Verification Rate sebesar 100%. Temuan ini menunjukkan bahwa metode yang diusulkan mampu mendeteksi perubahan Data secara efektif serta mendukung proses verifikasi dokumen digital yang lebih aman dan terpercaya.



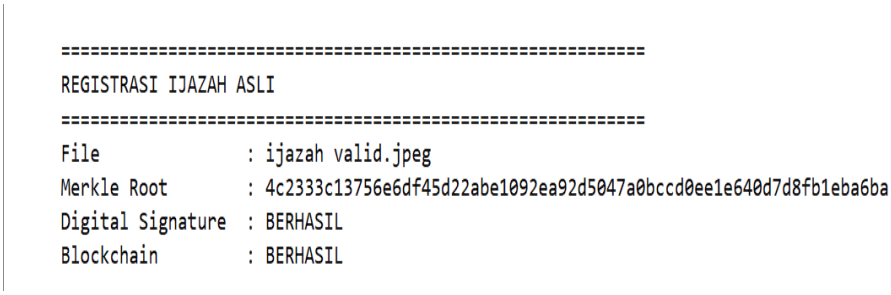
Gambar 5 Tahap input dokumen ijazah asli dan dokumen verifikasi

Berdasarkan hasil pengujian pada Gambar 5 dokumen *ijazah valid.jpeg* dan *verifikasi ijazah.jpeg* berhasil diunggah ke sistem dengan status 100% selesai. Sistem dapat menerima dan menyimpan file berformat JPEG dengan baik sehingga dokumen siap diproses pada tahap verifikasi. Hasil ini menunjukkan bahwa fitur unggah dokumen berfungsi sesuai dengan kebutuhan sistem.

Tabel 5 *Hash*, Blok, Data, Integritas, *Merkle*.

HASH SETIAP BLOK	
Block 1 :	15649b3dcc9e81f6b217396e5c25c297c6e01f8d653978e579e11c5aadccae94
Block 2 :	7ccbfe88947702660469510934 7b78a051b766068f9fe3aaff8c1887739005e7
Block 3 :	acec74bf5ec4f93a2d197430feb5b22c587b13c3b4d8365c39e35fe0bac49812
Block 4 :	e1781f0f4d3bff6cc36d05a450bacfb1b3195fb6cb403f138ae7d70b591ea420
Block 5 :	8fb13144837de8d54951fa2efe01c7eb677ad937e96104e7c0e900655adf43e3

Hasil pengujian menunjukkan bahwa sistem berhasil menghasilkan nilai hash SHA-256 untuk setiap blok data. Meskipun diproses menggunakan algoritma yang sama, setiap blok menghasilkan nilai hash yang berbeda karena memiliki isi data yang berbeda. Nilai hash yang dihasilkan memiliki panjang tetap 256-bit (64 karakter heksadesimal) dan digunakan sebagai dasar pembentukan Merkle Tree. Hasil ini menunjukkan bahwa proses hashing berjalan dengan baik dan mampu mendukung verifikasi integritas dokumen digital.



Gambar 6 Proses registrasi dan penyimpanan data ijazah ke blockchain

Berdasarkan hasil registrasi pada Gambar 6 sistem berhasil menghasilkan Merkle Root dan digital signature yang valid. Hasil ini menunjukkan bahwa mekanisme hashing SHA-256 dan tanda tangan digital dapat digunakan untuk membangun identitas unik dokumen sebelum disimpan ke blockchain. Dengan demikian, setiap perubahan pada dokumen dapat dideteksi pada tahap verifikasi.

Tabel 6 *Hash* blok unik menjaga integritas data

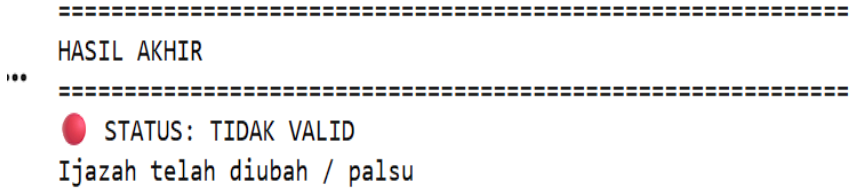
HASH SETIAP BLOK	
Block 1 :	bbbd2ec1e0387b82807f6739fdcb975474159db548722edc83d6688171e38bc7
Block 2 :	d83f602059fcd6935f1974d33678b274f43f771da918584034f64730cd8d8155
Block 3 :	36cecf5882dfa65a16c07b986b862eaa6f361b13aeb231cec4777b24fbdaea28
Block 4 :	ee8378befb535fc5809c94e04479c13a54a6c12ac908275b86af40152f104024
Block 5 :	f68d4029daee4445774929b9ebc14a854cab3c837c7b73cc0e49957d50a44acf

Berdasarkan hasil pengujian, sistem berhasil menghasilkan nilai hash SHA-256 untuk setiap blok data dari Block 1 hingga Block 5. Setiap blok menghasilkan nilai hash yang berbeda meskipun diproses menggunakan algoritma yang sama. Hal ini menunjukkan bahwa setiap blok data memiliki identitas digital yang unik. Seluruh nilai hash yang dihasilkan memiliki panjang tetap 64 karakter heksadesimal sesuai dengan karakteristik algoritma SHA-256.

Nilai hash tersebut digunakan sebagai dasar dalam pembentukan Merkle Tree untuk menghasilkan Merkle Root yang mewakili keseluruhan dokumen. Perbedaan nilai hash pada setiap blok menunjukkan bahwa sistem mampu menjaga integritas data dan mendeteksi perubahan pada dokumen. Hasil ini membuktikan bahwa proses hashing berjalan dengan baik dan dapat digunakan untuk mendukung verifikasi keaslian dokumen digital.

Gambar 7 Verifikasi gagal karena signature tidak valid.

Berdasarkan hasil pengujian pada Gambar 7 proses verifikasi ijazah berhasil dilakukan oleh sistem. Hasil verifikasi menunjukkan bahwa Merkle Root tidak sesuai dengan data yang telah diregistrasi sebelumnya sehingga mengindikasikan adanya perubahan pada dokumen. Selain itu, status Signature TIDAK VALID menunjukkan bahwa tanda tangan digital gagal diverifikasi dan keaslian dokumen tidak dapat dibuktikan. Meskipun data pada blockchain masih berstatus valid, dokumen tetap dinyatakan tidak valid karena hasil verifikasi Merkle Root dan digital signature tidak sesuai. Hasil ini menunjukkan bahwa sistem mampu mendeteksi perubahan atau pemalsuan dokumen secara efektif.



Gambar 8 Status validasi ijazah terdeteksi tidak valid

Berdasarkan hasil pengujian pada Gambar 8 sistem memberikan status TIDAK VALID terhadap dokumen yang diverifikasi. Status ini menunjukkan bahwa dokumen tidak sesuai dengan data yang telah diregistrasi sebelumnya, yang ditunjukkan oleh Merkle Root yang tidak cocok dan digital signature yang tidak valid. Oleh karena itu, dokumen dinyatakan telah mengalami perubahan atau pemalsuan. Hasil ini menunjukkan bahwa sistem mampu mendeteksi dokumen yang tidak memiliki integritas dan keaslian yang valid.

```
============================================================
ISI BLOCKCHAIN
============================================================

BLOCK #0
Timestamp     : 1778767452.8058474
Merkle Root   : 0
Previous Hash : 0
Block Hash    : 48ca1e1a717175df09438bae8a603d1b20e2232d803e6e0141ccff16595b2df5

BLOCK #1
Timestamp     : 1778767452.809108
Merkle Root   : 4c2333c13756e6df45d22abe1092ea92d5047a0bccd0ee1e640d7d8fb1eba6ba
Previous Hash : 48ca1e1a717175df09438bae8a603d1b20e2232d803e6e0141ccff16595b2df5
Block Hash    : fcd8aa3c1d2e894c13717287427214b6a6926f34d67af49cf5c03b28d3cc4247
```

Gambar 9 Tampilan isi blockchain pada proses verifikasi data ijazah

Berdasarkan hasil pengujian pada Gambar 9 sistem berhasil menampilkan struktur blockchain yang digunakan untuk menyimpan data ijazah digital. Blockchain terdiri dari Block #0 sebagai *genesis block* dan Block #1 yang berisi data ijazah yang telah diregistrasi. Setiap blok memiliki informasi berupa *timestamp*, *Merkle Root*, *Previous Hash*, dan *Block Hash* yang berperan dalam menjaga integritas data. Keterkaitan antara Block #1 dan Block #0 melalui nilai *Previous Hash* menunjukkan bahwa data telah tersimpan dalam rantai blockchain secara berurutan. Hasil ini menunjukkan bahwa mekanisme blockchain telah diterapkan dengan baik untuk menjaga keamanan dan integritas data ijazah digital.

KESIMPULAN

Penelitian ini berhasil mengimplementasikan sistem verifikasi ijazah digital berbasis blockchain melalui integrasi algoritma SHA-256, Merkle Tree, dan digital signature. Mekanisme verifikasi dilakukan dengan membandingkan nilai hash, Merkle Root, dan digital signature yang dihasilkan dari dokumen uji terhadap data referensi yang tersimpan pada blockchain. Berdasarkan hasil pengujian terhadap 14 dokumen yang terdiri atas satu dokumen asli dan tiga belas dokumen yang telah dimodifikasi, sistem mampu mengidentifikasi kondisi setiap dokumen sesuai dengan hasil pengujian yang dilakukan, dengan Accuracy Verification Rate sebesar 100% pada dataset penelitian ini. Setiap perubahan pada komponen dokumen menghasilkan nilai hash dan Merkle Root yang berbeda, sehingga perubahan tersebut dapat dideteksi secara konsisten selama proses verifikasi. Temuan penelitian ini menunjukkan bahwa integrasi SHA-256, Merkle Tree, digital signature, dan blockchain dapat menjadi pendekatan yang menjanjikan dalam mendukung proses verifikasi ijazah digital yang lebih aman, menjaga integritas data, serta meningkatkan kepercayaan terhadap keaslian dokumen akademik. Meskipun demikian, hasil penelitian ini masih didasarkan pada jumlah dokumen uji yang relatif terbatas. Oleh karena itu, penelitian selanjutnya disarankan melibatkan dataset yang lebih besar, variasi skenario manipulasi yang lebih beragam, serta pengujian pada lingkungan implementasi yang lebih luas agar kinerja, skalabilitas, dan keandalan pendekatan yang diusulkan dapat dievaluasi secara lebih komprehensif.

REFERENSI

-, M. A., Alwi, E. I., & As'ad, I. (2022). Analisis Forensik Terhadap Serangan Ddos Ping of Death Pada Server. *Cyber Security Dan Forensik Digital*, *5*(1), 23–31. https://doi.org/10.14421/csecurity.2022.5.1.3423

-, M. O. R. M., -, M. S. S. S., -, M. N. D. M., -, M. T. B. C., & -, P. S. R. B. (2024). Digital Document Verification System Using Blockchain. *International Journal For Multidisciplinary Research*, *6*(2), 1–6. https://doi.org/10.36948/ijfmr.2024.v06i02.16798

Abdullah, S. (2025). Implementasi Blockchain untuk Keamanan Data Akademik dalam Sistem Informasi Perguruan Tinggi. *Go Infotech: Jurnal Ilmiah STMIK AUB*, *31*(1), 149–160. https://doi.org/10.36309/goi.v31i1.371

Abdulrahman Syed. (2025). Blockchain's Cryptographic Backbone: Mastering Hash Functions, Digital Signatures & Merkle Trees. *Journal of Scientific Research and Technology*, (12), 254–259. https://doi.org/10.61808/jsrt384

Abidin, M. F. (2025). Blockchain-Based Digital Document Verification Using SHA-256 on the Internet Computer Protocol. *Journal of Electrical, Electronic, Information, and Communication Technology (JEEICT)*, *7*(2), 64–68.

Afdal, A. M., Salim, Y., & Manga, A. R. (2022). Analisis Bukti Digital Forensik Pada Discord Menggunakan Metode National Institute of Standards Technology. *Buletin Sistem Informasi Dan Teknologi Islam*, *3*(4), 293–300. https://doi.org/10.33096/busiti.v3i4.1425

Akil, M., Alwi, E. I., Abdullah, S. M., Informatika, S. T., Komputer, F. I., Indonesia, U. M., Website, K., Testing, P., Security, W., & Testing, P. (2024). *ANALISA KEAMANAN WEBSITE TERHADAP SERANGAN HTML INJECTION MENGGUNAKAN METODE PENETRASION TESTING WEBSITE SECURITY ANALYSIS AGAINST HTML INJECTION USING THE METHOD PENETRASION TESTING*. *01*(01), 42–50.

Asis, M. A., & Ilmawan, L. B. (2023). Implementasi Quick Response (QR) Code pada Aplikasi Pengajuan Surat Keterangan Pendamping Ijazah (App-SKPI). *Buletin Sistem Informasi Dan Teknologi Islam*, *4*(1), 9–14. https://doi.org/10.33096/busiti.v4i1.1611

Begimbayeva, Y., Ussatova, O., Karyukin, V., Mutanov, G., Kistaubayev, Y., & Turdaliyev, M. (2026). Enhancing Trust and Sustainability in Higher Education Through Blockchain-Based Academic Document Verification. *Sustainability (Switzerland)*, *18*(7), 1–20. https://doi.org/10.3390/su18073547

Capece, G., Ghiron, N. L., & Pasquale, F. (2020). Blockchain technology: Redefining trust for digital certificates. *Sustainability (Switzerland)*, *12*(21), 1–12. https://doi.org/10.3390/su12218952

Djajadi, A., Lestari, K. S., Englista, L. E., & Destaryana, A. (2023). Blockchain-Based E-Certificate Verification and Validation Automation Architecture to Avoid Counterfeiting of Digital Assets in Order to Accelerate Digital Transformation. *CCIT Journal*, *16*(1), 68–85. https://doi.org/10.33050/ccit.v16i1.2367

Han, L., Hu, G., Li, X., Xia, F., Wang, S., & You, L. (2025). A Novel Lattice-Based Blockchain Infrastructure and Its Application on Trusted Data Management. *IEEE Transactions on Network Science and Engineering*, *12*(4), 2524–2536. https://doi.org/10.1109/TNSE.2025.3550158

Hidayat, A. Q. I., Alwi, E. I., & Gaffar, A. W. M. (2024). Analisis bukti video TikTok dengan metode DFRWS. *Jurnal Minfo Polgan*, *13*(1), 1138–1146.

Iavich, M., & Kuchukhidze, T. (2025). *Post-Quantum Digital Signature : Verkle-Based HORST*. 1–23.

Javatpoint. (2023). *Blockchain Merkle Tree - Javatpoint*. (May), 69–72. https://www.javatpoint.com/blockchain-merkle-tree

Krishnan, S., Rajendran, S., & Zakariah, M. (2025). A secured accreditation and equivalency certification using Merkle mountain range and transformer based deep learning model for the education ecosystem. *Scientific Reports*, *15*(1), 1–21. https://doi.org/10.1038/s41598-025-06789-x

Kuznetsov, O., Rusnak, A., Yezhov, A., Kanonik, D., Kuznetsova, K., & Karashchuk, S. (2024). Enhanced Security and Efficiency in Blockchain with Aggregated Zero-Knowledge Proof Mechanisms. *IEEE Access*, *12*, 49228–49248. https://doi.org/10.1109/ACCESS.2024.3384705

Kuznetsov, O., Rusnak, A., Yezhov, A., Kuznetsova, K., Kanonik, D., & Domin, O. (2024). Merkle trees in blockchain: A Study of collision probability and security implications. *Internet of Things (Netherlands)*, *26*, 1–17. https://doi.org/10.1016/j.iot.2024.101193

Marian, C. V., Mitrea, D. A., Rusu, D. S., & Vasilateanu, A. (2025). Transparent Digital Governance: A Blockchain-Based Workflow Audit Application. *Applied Sciences (Switzerland)*, *15*(21), 1–26. https://doi.org/10.3390/app152111694

Mattaparthy, L., & S, V. L. (2025). Online Document Verification using Blockchain Technology. *International Journal For Multidisciplinary Research*, *7*(3), 1–8. https://doi.org/10.36948/ijfmr.2025.v07i03.46084

Nadimsyah, A. Z., & Ezar Al Rivan, M. (2024). Implementasi Secure Hash Algorithm-256 dan Advanced Encryption Standard Untuk Verifikasi Tanda Tangan Digital. *Journal of Information System Research (JOSH)*, *6*(1), 229–239. https://doi.org/10.47065/josh.v6i1.5942

Nugraha, A., Alwi, E. I., & Gaffar, A. W. M. (2024). Penerapan Model Investigasi Forensik Komputer Umum dalam Analisis Forensik Video CCTV. *Jurnal Minfo Polgan*, *13*(1), 1130–1137. https://doi.org/10.33395/jmp.v13i1.13963

Pengabdian, J., Global, M., Kejahatan, D., Bagi, S., Siswi, S., & Negeri, S. M. A. (2022). *SOSIALISASI AMAN BERMEDIA SOSIAL DI ERA DIGITAL AGAR TERHINDAR DARI KEJAHATAN SIBER BAGI SISWA/SISWI SMA NEGERI 13 MAROS*. *1*(2), 67–70.

Priyadarshini, R., Pandey, R., Ankit, K. C., Bhandari, D., Khadka, B., Kumar Barik, R., & Jyoti Saikia, M. (2025). A Faster, Integrated, and Trusted Certificate Authentication and Issuer Validation System Based on Blockchain. *IEEE Access*, *13*(February), 27037–27049. https://doi.org/10.1109/ACCESS.2025.3539180

Putra Santoso, R., & Judhie Putra, R. R. (2026). Blok IPFS Blockchain Untuk Orisinalitas Ijazah Pendidikan Tinggi. *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI)*, *4*(3), 1993–1999. https://doi.org/10.62712/juktisi.v4i3.780

Quispe, M. A. C., & Pacheco, A. (2025). Blockchain ensuring academic integrity with a degree verification prototype. *Scientific Reports*, *15*(1), 1–15. https://doi.org/10.1038/s41598-025-93913-6

Supardin, H., Satra, R., & Asis, M. A. (2022). Analisis Perbandingan Tools Forensik Digital Pada Instagram Messenger Menggunakan Metode Nasional Institute of Standards and Technology. *Buletin Sistem Informasi Dan Teknologi Islam*, *3*(4), 274–283. https://doi.org/10.33096/busiti.v3i4.1380

Tri Ade Nia, Rudyanto Ompungsunggu, Arrant Ardi Sianipar, Jesimanta, J., & Yoramo Waruwu. (2024). Merkle-Damgård as the Foundation of Hash Cryptography: A Study of Advantages and Limitations. *Jurnal Teknik Indonesia*, *3*(01), 24–29. https://doi.org/10.58471/ju-ti.v3i01.652

Wadhwani, S. (2023). Certificate Verification and Counterfeit Detection using Blockchain. *International Journal for Research in Applied Science and Engineering Technology*, *11*(11), 1288–1294. https://doi.org/10.22214/ijraset.2023.56705

Zhai, X., Pang, S., Wang, M., Qiao, S., & Lv, Z. (2023). TVS: a trusted verification scheme for office documents based on blockchain. *Complex and Intelligent Systems*, *9*(3), 2865–2877. https://doi.org/10.1007/s40747-021-00617-1