Digital Certification Security Framework Using Multi Hybrid Cryptography and QRL Blockchain

Roy Mubarak[*1,2], Imam Riadi[3], Tole Sutikno[4]
[1]Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Department of Informatics, Universitas Mercu Buana, Jakarta, Indonesia
[3]Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[4]Department of Electrical Engineering, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
E-mail: [*1]**2537083002@webmail.uad.ac.id**, [2]roy.mubarak@mercubuana.ac.id,
[3]imam.riadi@uad.ac.id, [4]tole@ee.uad.ac.id,

Abstract

Academic certificates in the modern era, due to the extensive use of digital technology, face various risks of counterfeiting and long-term cryptographic exposure due to advances in computing power. Existing frameworks often lack comprehensive protection utilizing multi-cryptographic technologies. To address this, we propose a secure digital certification framework by implementing robust integration defense mechanisms. In the first layer, core encryption is achieved using a high-dimensional hyperchaotic system combined with dynamic DNA coding. It is then connected to a Quantum Resilient Ledger (QRL) to ensure decentralized, immutable, and future-proof verification. We evaluate this framework across various certificate formats (JPG, PNG, BMP, TIFF, and GIF). Experimental results demonstrate high operational efficiency, with cryptographic processing times ranging from 0.12 to 0.19 seconds and fast QRL anchoring times between 1.66 and 2.32 seconds. The system achieves an ideal information entropy of 8, a uniform histogram, and a correlation coefficient close to zero, confirming high randomness. Furthermore, the proposed scheme demonstrates strong resilience against differential attacks with near-ideal NPCR (~99.61%) and UACI (~33.47%). This holistic approach provides a highly secure, efficient, and decentralized solution for protecting digital academic credentials.

Keywords— *Digital Certificate, Hyperchaotic Maps, Blockchain, Quantum Resistant Ledger*

1. INTRODUCTION

Personal data security is a necessity in today's digital era, where internet user activity has increased year after year, impacting user behaviour [1]. Users are often unaware that their systems may be targeted [2]. Information security is the protection of information from all potential threats to ensure business continuity, minimize business risk, and maximize or accelerate return on investment and business opportunities [3]. Data protection and security are necessary to address threats such as damage, natural disasters, and cybercrime [4]. There is no denying that life, in all its forms, has entered the digital era, and many activities are now performed digitally [5]. Data protection and security threats also occur in the education sector. Without robust validation, the education ecosystem is vulnerable to data manipulation, which can harm students, educational institutions, and employers. The threat of falsified educational certificates is becoming increasingly sophisticated as the transition from physical documents to digital. Current studies have discussed that certificate forgery has become a global problem and has damaged trust in educational institutions [6] [7]. While traditional encryption techniques often struggle with the complexity of modern data, optimizing encryption algorithms is needed to protect visual data [8].

There is an urgent need for decentralized and tamper-resistant security solutions. Blockchain technology has emerged as an ideal candidate due to its promising characteristics of transparency, immutability, and decentralization, which promise higher levels of encryption and data security to address internal, malicious, peripheral, and incidental threats [9]. Blockchain technology is also used as an excellent alternative for protecting personal data, particularly

educational certificates, as a complement to encryption technology. The two technologies can be combined very easily. Blockchain has the capability to achieve these standards since it is a truly distributed technology. Blockchain is a technology that involves third parties in the process of exchanging information. Information on the Blockchain can be in the form of data entry in transaction form, assets, identities, and other information that is packaged in digital form [10]. Therefore, research is also directed at developing hybrid blockchain systems with IPFS for off-chain storage. Blockchain demonstrates that this architecture can satisfy user privacy rights, such as the Right to Be Forgotten, which are often difficult to implement on immutable blockchains [11]. Blockchain technology is widely adopted to automate verification, for example, the use of Smart Contracts to eliminate intermediaries. Storage efficiency is also improved through the integration of IPFS [12][13]. Blockchain is a technology that combines tools, methods, and configurations to address specific problems or use cases. Blockchain technology differs from traditional centralized approaches by enabling secure on-chain data management across a distributed and interconnected network of nodes [14]. Blockchain technology uses a consensus mechanism that allows transaction data to be securely stored on the network after verification and validation, without third-party interference [15]. Blockchain technology combines several security concepts to ensure the confidentiality of information. One concept in blockchain technology is similar to that in distributed databases [16]. One use of blockchain technology is in the security and verification process of digital certificates. This technology enables secure, encrypted, and immutable data recording, providing transparency and trust throughout the production and distribution process [17].

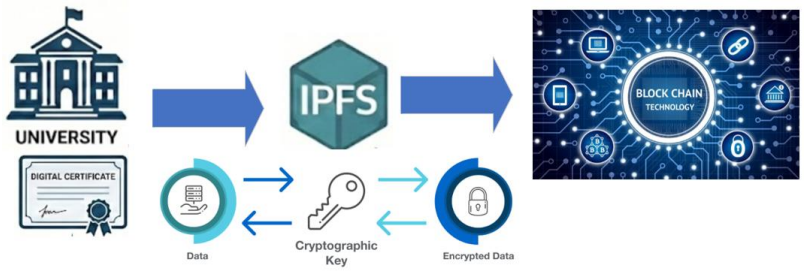


Figure 1. Blockchain for Academic Certificate

The potential of this technology has become a pivotal solution in the higher education ecosystem, specifically in developing trustworthy and sustainable diploma management infrastructures to mitigate the risks of academic certificate forgery, which increasingly threatens institutional reputation and public confidence. Not only is it needed for the university's reputation, but on a practical level, attempts to verify degrees are typically bureaucratic, and the weaknesses of this system are preyed upon by actors in the educational ecosystem seeking to game it [18]. Ghani et al. [19] proposed modernizing educational record management by integrating decentralized blockchain technology to ensure data security, privacy, and immutability. Blockchain is a decentralized method to handle authentication and tamper-resistant transactions with integrity through a wide number of users, often known as nodes [20]. Blockchain Technology is a distributed and decentralized ledger system connected to nodes across the network. Each node shares access to the ledger and its records. The records stored are immutable. Therefore, no one can change or tamper with a record after it enters the ledger. Four types of blockchain networks are available: public, private, permissioned, and consortium. Users could choose which network to use based on their needs [21]. Transaction data is converted into a hash value using a Merkle tree, optimizing data storage management and regulating accessibility [22]. As a result, blockchain ensures immutability, meaning that any modification to a block would affect all subsequent blocks within the distributed ledger [23].

However, the reliability of current blockchain and digital security frameworks faces an existential threat from rapid advancements in quantum computing [24].

This global phenomenon introduces an urgent timeline for transition, as predictive models estimate that quantum processors capable of compromising current cryptographic standards could realistically emerge between 2033 and 2040 [25]. Most existing infrastructures rely on classical algorithms like RSA and ECDSA, which are highly vulnerable to quantum-based attacks.

Specifically, Shor's algorithm can completely break RSA and ECC [26]. Meanwhile, Grover's algorithm introduces a quadratic speedup that halves the effective security level of symmetric systems and hash functions, such as SHA-256 [25]. To fill this gap, we proposed a framework, which we renamed to "Digital Certification Security Framework Using Multi-Hybrid Cryptography and QRL Blockchain".

2. RESEARCH METHODS

The research method includes a literature review, process flow and the proposed method. Literature review includes: state of the art, gap analysis, contribution, and comparison with existing research. The process flow includes: input of student metadata and student digital certificates by academic admins and certificate verification by students. The proposed method includes analysis, architecture, methods used, and implementation.

2.1. Literature Review

We have found some studies related to the implementation of Blockchain Technology. A literature review shows that there is growing interest in this topic, with several institutions already attempting to implement blockchain solutions

2.1.1. State of The Art

The evolution of digital certification frameworks can be synthesized into three primary thematic categories:

- The first category focuses on Ledger Integrity through Classical Cryptography and Conventional Blockchain. These studies aim to transition paper-based systems to decentralized ledgers using established algorithms such as ECDSA, RSA, and standard hashing to ensure transparency and anti-tampering [27][28] [29]. Mechanisms like Byzantine consensus, hybrid networks, and Merkle-based traceability have proven effective for basic credential verification and administrative traceability [30][31]. Furthermore, innovations in hashed mapping and decentralized applications have further optimized verification speed and global accessibility [32][7][33].
- The second category addresses Data Privacy, Web3, and Regulatory Compliance, particularly regarding the GDPR. Researchers here utilize modern primitives such as Non-Fungible Tokens (NFTs), Rejectable Soul bound Tokens, and Zero-Knowledge Proofs (ZKPs) to protect the privacy of certificate owners [34][35]. These frameworks often incorporate Decentralized Identifiers (DIDs) and Layer-2 scaling solutions like zk-Rollups to achieve privacy-preserving credential management without compromising institutional trust [36][37][38][39].
- The third category involves Automation and Intelligent Detection via AI and Machine Learning Integration. These studies synergize blockchain with deep learning models, such as Transformers, BERT, and CNNs, to automate credential evaluation, equivalency estimation, and sophisticated fraud detection [40][41]. These systems aim to transform diploma verification into an autonomous, transparent process through intelligent data mining and pattern recognition [42][43]

2.1.2. Gap Analysis

Despite progress in these four categories, critical research gaps remain. While the first three categories offer robust integrity, privacy, and automation, they largely rely on standard blockchain networks such as BSV Blockchain, Ethereum, and Remix/Ganache and have not yet utilized post-quantum-protected blockchain networks like QRL

2.1.3. Contribution

To bridge this gap, this research proposes a multi-cyprography 6D hyper-chaotic system with DNA mutation for randomized encryption and integration with QRL Blockchain. The significance of this work is three-fold.

- This research significantly expands the literature on multi-layer Cryptography and QRL Blockchain integration. It demonstrates a novel multi-layered architecture that secures a digital certification.
- The framework provides a tangible, highly secure solution for higher education institutions to combat certificate forgery. It offers an instant, unforgeable verification system that maintains structural visual integrity without sacrificing image quality, ensuring that certificates cannot be backdated or tampered with visually.
- The proposed architecture aligns with global data protection regulatory trends. By securely decoupling encrypted visual payloads from decentralized ledger anchors and utilizing advanced steganography, the system inherently supports privacy-preserving standards compliant with international regulations such as the European Union's General Data Protection Regulation (GDPR) and Indonesia's Personal Data Protection Law (UU PDP).

2.1.4. Comparison with Existing Reasearch

Table 1 illustrate of summary of comparison of existing research and the position of this research

Table 1. Comparison with Existing Research

Research	Object	Blockchain Type & Network	Storage	Digital Signature	Algorithm
[7]	Digital Diploma	Binance Smart Chain (BSC)	IPFS & Blockchain	ECDSA	SHA-256 Hashing
[27]	FiDigital Certificate	BSV Blockchain	Blockchain & Database	ECDSA	AES encryption for on-chain data.
[30]	Digital Certificate	Private P2P Network	Blockchain & Database	Private key	AES-256, SHA-256, ECDSA.
[32]	Digital Certificate	Ethereum	Blockchain	RSA	RSA encryption/ decryption on hashes.
[33]	Academic document	Ethereum (Remix / Ganache)	Blockchain & Local/Cloud Database	Standard digital signatures.	Implicit cryptographic algorithms.
[36]	Digital Certificate	Ethereum Layer-2 (zk-Rollups, Arbitrum).	IPFS	RSA-2048 / ECDSA	SHA-256, SHA-512 Hashing.
[38]	Privacy-preserving verification	Dual-blockchain (Public & Private)	IPFS Encrypted	DID & zk-SNARKs	AES encryption for off-chain data.

[41]	Accreditation	Cerberus++ (Distributed Ledger)	Blockchain / MMR.	ECDSA	Extended MD5 + MultiPRNA + Runge-Kutta chaotic system.
This Research	**Digital Certificate**	**Blockchain (QRL)**	**Blockchain & MongoDB**	**XMSS (eXtended Merkle Signature Scheme)**	**SHA-256 (Secure Hash Algorithm), Hybrid Chaotic 6D-DNA Encoding Quantum Walk**

Table 1 explains about the comparison of the proposed digital certificate security architecture with various frameworks from previous research, highlighting a strategic transition from classical cryptography towards Post-Quantum Security. Unlike conventional systems that are vulnerable to future computational attacks due to their reliance on traditional digital signature algorithms such as ECDSA or RSA, this framework innovatively utilizes the Quantum Resistant Ledger (QRL) network alongside the eXtended Merkle Signature Scheme (XMSS) authentication algorithm to guarantee absolute document validity on-chain.

Furthermore, in terms of data protection at the database level (MongoDB), this architecture fundamentally outperforms standard encryption methods through the implementation of a 6D Hyper-Chaotic hybrid cryptographic engine which operates with an extra layer of entropy via the x7 parameter—combined with DNA Encoding and Quantum Walk methods. This strategic approach ensures that the developed framework maintains an extremely lightweight server computational load (zero-overhead) while simultaneously delivering a level of security algorithm complexity that far exceeds the protection standards established in previous literature.

2.2. Process Flow

a. Process Flow Input Student Metadata & Student Digital Certificate

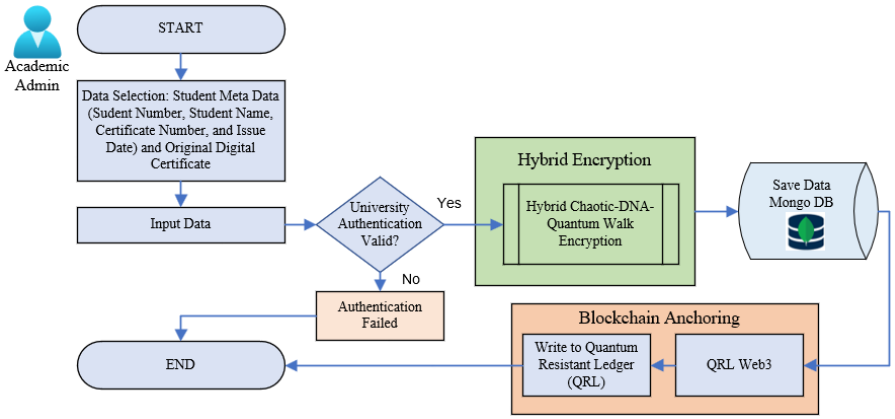


Figure 2. Input Data Process Flow

Figure 2 shows that the workflow begins with the selection of student metadata and the original digital certificate, followed by a university authentication check. If the authentication is valid, the data undergoes a complex "Chaotic-DNA-Quantum Walk Hybrid Encryption" before being securely stored in a MongoDB database. Finally, the system performs blockchain tethering using Web3 QRL to write the data to a Quantum Resistant Ledger (QRL), ensuring certificate invulnerability and long-term security before the process concludes.

b. Certificate Verification

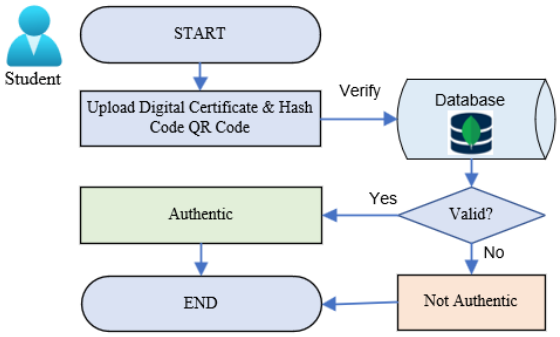


Figure 3. Certificate Verification Process Flow

Figure 3 shows that the process begins with students uploading their digital certificates along with their Hashed QR Codes. This submitted data is then matched and verified against existing database records. Based on this verification step, the system determines whether the certificate is valid; if it matches, the result is declared "Authentic," while if it fails the check, it is marked as "Inauthentic," thus ending the verification workflow.

2.3. Proposed Framework

This research proposes a framework that synergizes hybrid cryptography and Quantum Resistant Ledger (QRL) as shown in Figure 4. Proposed Framework.

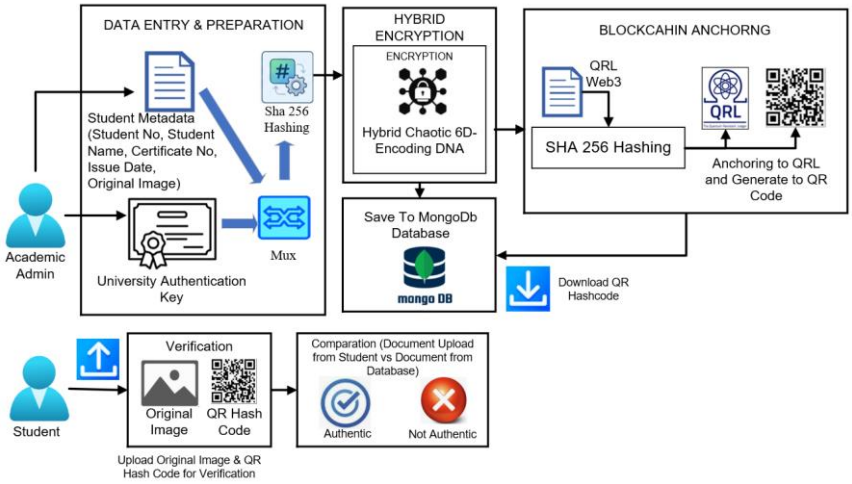


Figure 4. Proposed Framework

2.3.1. Selection of Student Metadata and Digital Certificate

In this research, student data consist of essential academic identity attributes commonly used in higher education certification systems, including: student number, student name, date of issuance, and institutional validation metadata. These data are organized into structured digital records prior to the encryption stage. To ensure interoperability across educational institutions and digital verification platforms, the student information is transformed into standardized machine-readable formats before being processed by the proposed security architecture. Figure 5-9 shows the student data input page and upload of digital certificate documents.



Figure 5. Digital Certificate (jpg format)



Figure 6. Digital Certificate (png format)



Figure 7. Digital Certificate (bmp format)



Figure 8. Digital Certificate (tiff format)



Figure 9. Digital Certificate (gif format)

Each image format possesses different characteristics in terms of compression mechanism, color representation, and storage structure, thereby providing a comprehensive evaluation environment for the robustness of the proposed steganographic model. Figure 5-9 illustrates examples of digital certificate formats utilized in this research, including PNG, JPG, BMP, GIF, and TIFF-based certificates.

2.3.2. Data Input

The process initiates at the frontend interface, where the system collects essential student metadata alongside (Student ID, Name, Certificate Number, Date) and the original digital certificate image. Figure 10 illustrate Input Metadata & Base64 Process.

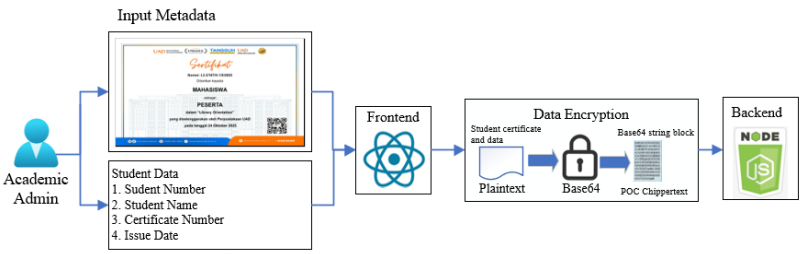


Figure 10. Input Metadata and Base64 Process

To streamline data transmission and reduce server load, this original image is immediately converted into a Base64 string format directly within the user's local browser environment. Once

this local conversion is complete, the combined payload containing both the text metadata and the Base64 image string is securely transmitted to backend using a standard HTTP POST protocol.

2.3.3. Multi-Cryptographic

In this phase, student metadata is combined with the University Secret Key and processed through the SHA-256 algorithm to generate a unique digital fingerprint. This hash then serves as the seed to trigger the 6D Hyper-Chaotic Engine. The resulting chaotic trajectory determines the randomization and encoding of the image matrix into a distributed DNA sequence using the Quantum Walk method.

a. Hyper-Chaotic Encryption

The core of the proposed this framework is a high-dimensional nonlinear system. To achieve a higher degree of complexity and a broader key space, the traditional chaotic maps are extended into a 6-Dimensional (6D) state space.

$$\left.\begin{aligned} x_1 &= a(x_2 - x_1) + x_4 \\ x_2 &= cx_1 - x_2 - x_1x_3 + x_5 \\ x_3 &= x_1x_2 - bx_3 + x_6 \\ x_4 &= dx_4 - x_1x_3 \\ x_5 &= ex_1 + x_2x_3 \\ x_6 &= fx_6 - gx_1 \end{aligned}\right\} \quad (1)$$

The system is defined by the following set of first-order differential equations. Parameter and State Variable Definitions:

- State Variables x1, x2, … x6 represent the six interdependent coordinates of the chaotic system in the phase space. The non-linear cross-terms (such as x1 x3 and x1 x2) are responsible for generating the sensitive dependence on initial conditions.
- Control Parameters (a, b, c, d, e, f, g) system constants that govern the stability and chaotic behaviour.

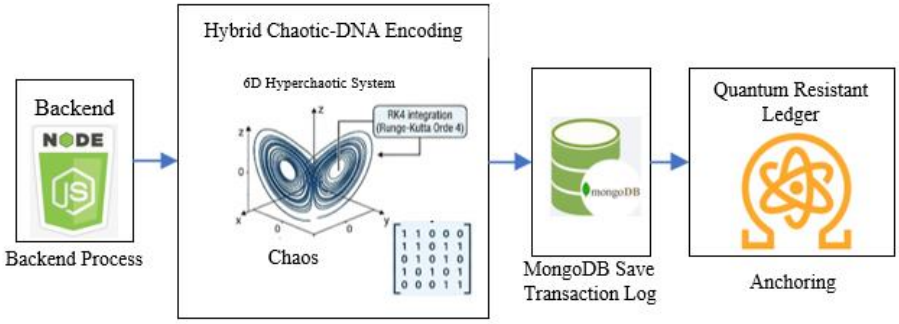


Figure 11. Multi-Cryptographic and Anchoring

Figure 11 illustrate the Multi-Cryptographic and Anchoring process. To ensure the mathematical precision required for cryptographic synchronization, the continuous-time system is discretized using the 4th-order Runge-Kutta (RK4) numerical method. This approach provides a high degree of accuracy for the chaotic keystream generation. The next state yn+1 is calculated as:

$$y_{n+1} = y_n + \frac{h}{6}(k_1 + 2k_2 + 2k_3 + k_4) \quad (2)$$

$$\left.\begin{aligned} k_1 &= f(t_n, y_n) \\ k_2 &= f(t_n + h/2, y_n + h/2.k_1) \\ k_3 &= f(t_n + h/2, y_n + h/2.k_2) \\ k_4 &= f(t_n + h, y_n + hk_3) \end{aligned}\right\} \quad (3)$$

b. DNA Quantum Scrambling

The resulting chaotic sequences are mapped into a DNA nucleotide space A, C, G, T. To maximize diffusion, the system performs a permutation process where the DNA string positions are scrambled based on the sorted indices of the quantum-influenced chaotic sequence.

$$P = \text{sort}(\text{indices}(Q_W)) \quad (4)$$

2.3.4. Storage Offloading & Database

To maintain a zero-overhead architecture and ensure the server remains highly responsive, the backend employs a strategic storage offloading mechanism before interacting with the database. Instead of injecting the massive Base64 strings of the original and encrypted images directly into the database, The Backend proses saves them as static text files within a local server directory. Consequently, the MongoDB database is only tasked with storing the lightweight file reference names, the hash, and the student metadata, which is symmetrically encrypted using AES-256 to uphold strict privacy-by-design principles.

2.3.5. Post-Quantum Blockchain Anchoring Phase (QRL Zond)

Simultaneous to the database logging, the digital signature and authentication processes are offloaded entirely to the Quantum Resistant Ledger (QRL) Zond Testnet to achieve true post-quantum security. The Backend establishes a direct RPC connection with the blockchain network and embeds the phase3_hash into an EIP-1559 Type 2 transaction payload as an immutable proof of existence. Figure 7 illustrate Quantum-Resistant Ledger (QRL) Anchoring Process.

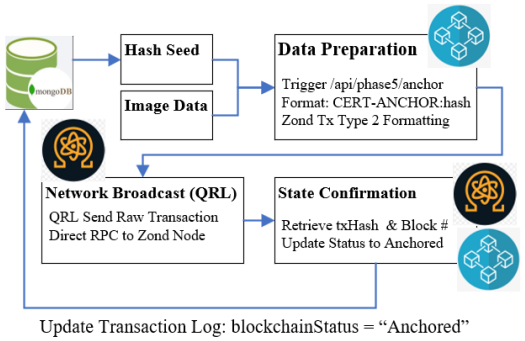


Figure 12. Quantum Resistant Ledger

Before this transaction is broadcasted to the network, it is cryptographically signed using the extended Merkle Signature Scheme (XMSS), a robust hash-based algorithm that guarantees the document's authenticity and renders the transaction impervious to future quantum computing attacks. By writing to the QRL, the framework utilizes quantum-secured protocols to mitigate transaction vulnerabilities such as Maximal Extractable Value (MEV) attack using secure sources of randomness [44].

2.3.6. Performance Evaluation Metrices

To rigorously validate the security, robustness, and visual quality of the proposed framework, a comprehensive set of evaluation metrics is employed. These metrics are processed through a dedicated performance evaluator module, which provides empirical evidence of the system's resilience to cryptographic attacks and high-fidelity steganographic performance.

a. Entropy Analysis

Quantifies data randomness to verify resistance against pattern-based and frequency analysis attacks. s represents the image source or the set of pixel intensities. i denotes the specific pixel intensity value, ranging from 0 to 255 for standard 8-bit images. P(si) represents the probability of occurrence of the pixel intend.

$$H(s) = -\sum_{i=0}^{255} P(s_i) \log_2 P(s_i) \quad (5)$$

b. Histogram Analysis

Verifies the statistical uniformity of the pixel distribution to ensure no plain image information is leaked. Represents the frequency of each pixel intensity, typically calculated as h(v)= nv where v is the pixel intensity level (0-255) and nv is the total count of pixels with that specific intensity.

c. Correlation Coefficient

Evaluates the statistical independence of adjacent pixels (horizontal, vertical, diagonal) to ensure they are uncorrelated

$$\rho_{xy} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2 \cdot \sum_{i=1}^{N}(y_i - E(y))^2}} \quad (6)$$

d. Number of Pixels Change Rate (NPCR)

Measures encryption sensitivity to a single-pixel-change by calculating the percentage of different pixels between two cipher images. D(i,j)= 1 if the pixels at coordinates (i,j) in the two images are different, and D(i,j) = 0 otherwise.

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (7)$$

e. Unified Average Changing Intensity (UACI)

Calculates the average intensity difference between two encrypted images resulting from a one-pixel alteration.

$$\text{UACI} = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \quad (8)$$

2.3.7. Output

In the final phase, when the academic administrator accesses the document details page, the system quickly reconstructs the visual elements by retrieving data from MongoDB and reading the corresponding uploaded text files. This highly optimized retrieval process allows the dashboard to seamlessly and simultaneously display the decrypted student data, the original document image, and the visual evidence of the Chaotic-DNA encrypted matrix. Furthermore, the interface provides real-time verification by displaying the blockchain transaction hash and its bound status, providing comprehensive and mathematically proven digital certificate validation.

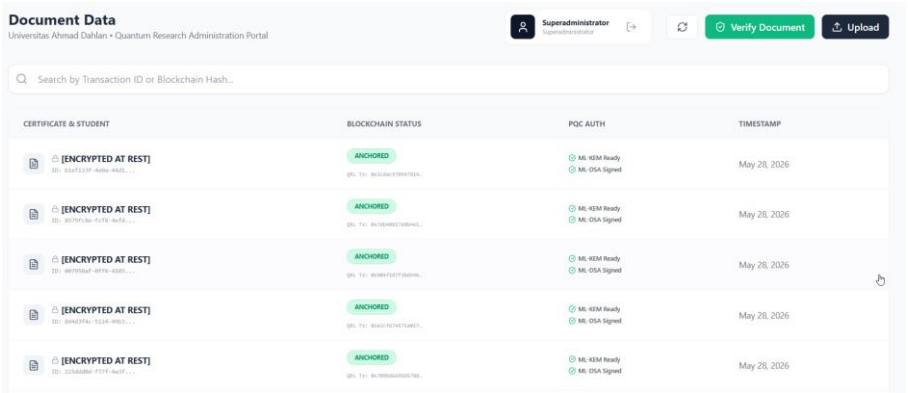


Figure 13. Data Recoding

Figure 13 is the output in the form of a list that comes from the data input process, multi-encryption and blockchain QRL anchoring.

Figure 14 Data Integrity illustrates the system's final verification panel, which serves as the ultimate cryptographic proof of a digital certificate's authenticity within the proposed framework.

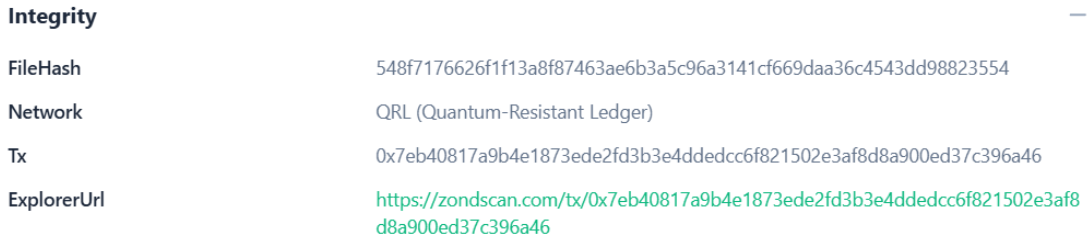
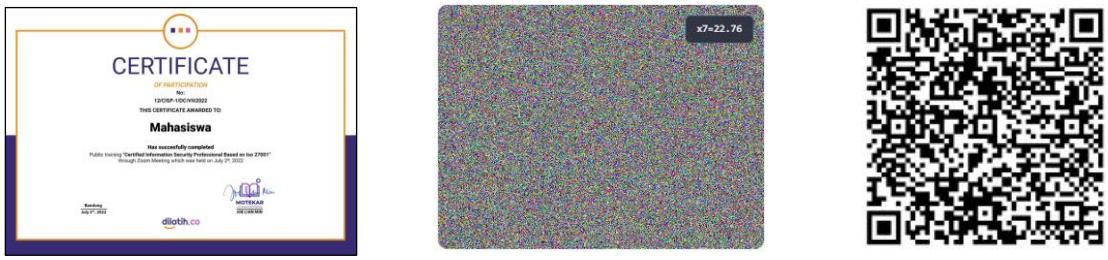


Figure 14. Data Integrity

As depicted in the figure, the panel displays the File Hash, acting as an immutable digital fingerprint generated from the document's original metadata, which is permanently anchored to the QRL (Quantum-Resistant Ledger) network to guarantee post-quantum security.

2.3.8. Verification

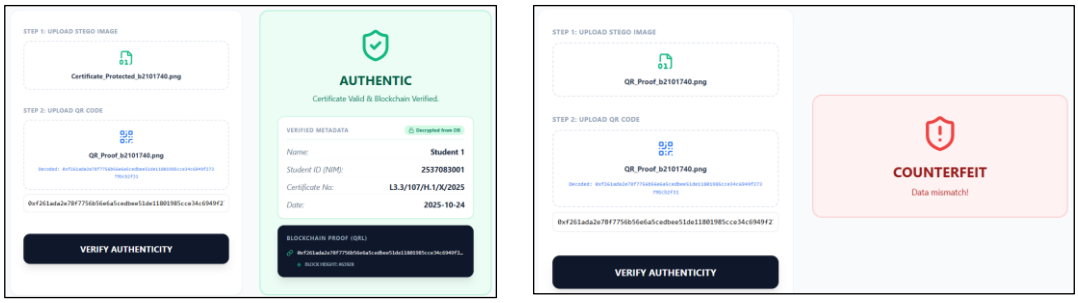
Figure 15.a displays the original image, Figure 15.b encryption image resulting from the multi-layer encryption and 15.c QR Hash Code. The verification process is carried out by students.



(a) **(b)** **(c)**

Figure 15. Output (a) Original Image; (c) QR Hash Code

The system outputs a final verdict: a perfect match between the orignial-image and the QR hash yields an “Authentic” status (Figure 16.a), where as any discrepancy flags the document as “Counterfeit” (Figure 16.b)



(a) **(b)**

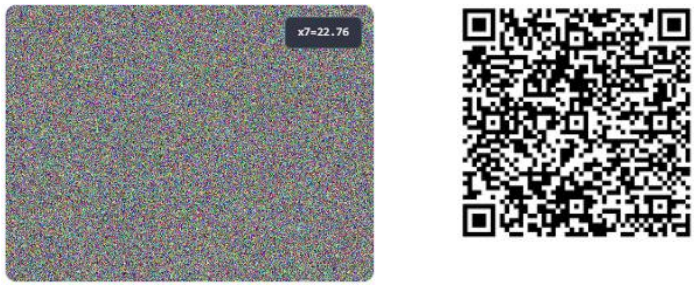
Figure 16. Verification Result (a) Authentic; (b) Counterfeit

3. RESULTS AND DISCUSSION

The proposed digital certification security framework was successfully implemented and evaluated against comparable methodologies.

3.1. Image Encryption

The multi-encryption process carried out on digital diploma documents produces digital encrypted documents and hash codes in the form of QR Codes as represented in Figure 14.a and Figure 14.b.



(a) **(b)**

Figure 17. Result (a) Image Encryption; (b) QR Hashing Result

3.2. Quantum Resistant Ledger (QRL)

The network provides a Transaction Hash and Block Number, delivering an immutable, timestamped state confirmation that prevents ledger tampering or backdating. Blockchain Anchoring Workflow:

- Data Preparation. The server retrieves the certificate's SHA-256 hash and formats it into a blockchain-compatible hex string.
- Transaction Building & Signing. A Zond-compatible transaction is constructed with the necessary gas and fee parameters, then securely signed offline using the server's private key.
- Network Broadcast: The signed transaction payload is broadcast directly to the Quantum-Resistant Ledger (QRL) Zond network via RPC API.
- Anchoring & Logging: Upon processing, the QRL network provides a cryptographic proof (Transaction Hash and Block Number). The system subsequently updates the transaction log to "Anchored," establishing a permanent and immutable link to the post-quantum blockchain.

Table 2 QRL Result presents the comprehensive outcomes of the blockchain anchoring process across various digital certificate file formats, including JPG, PNG, BMP, TIFF, and GIF.

Table 2 QRL Result

Certificate	Hash ID	URL
Certificate a (jpg)	0x904f1d7f3bd4462e488ba4a121ff759981093d0909ac38e59dcb4890dfc7c108	https://zondscan.com/tx/0x904f1d7f3bd4462e488ba4a121ff759981093d0909ac38e59dcb4890dfc7c108
Certificate b (png)	0x7eb40817a9b4e1873ede2fd3b3e4ddedcc6f821502e3af8d8a900ed37c396a46	https://zondscan.com/tx/0x7eb40817a9b4e1873ede2fd3b3e4ddedcc6f821502e3af8d8a900ed37c396a46
Certificate c (bmp)	0x709b86695d5788fd0585b239db0c555169cc0e16dc2468cb1a5ac1381c103cff	https://zondscan.com/tx/0x709b86695d5788fd0585b239db0c555169cc0e16dc2468cb1a5ac1381c103cff
Certificate d (tiff)	0x3cdac970947814df959af95856d414b2c020e6fd552453d0822903ffde097d98	https://zondscan.com/tx/0x3cdac970947814df959af95856d414b2c020e6fd552453d0822903ffde097d98
Certificate e (gif)	0xa3cf674571a017f0a8d65ae4769ad9394bdca38ef18423251342ff0a40058312	https://zondscan.com/tx/0xa3cf674571a017f0a8d65ae4769ad9394bdca38ef18423251342ff0a40058312

This data clearly demonstrates the framework's versatility and robustness in processing diverse document types without compatibility issues. For each respective certificate, the table displays a unique cryptographic Hash ID, which represents the specific on-chain transaction identifier generated upon successful anchoring to the Quantum Resistant Ledger (QRL). Furthermore, the corresponding URL column provides direct links to Zond scan, the official QRL block explorer. These URLs serve as transparent, publicly accessible proofs, allowing any third-party validator to independently verify the transaction's existence, integrity, and post-quantum security status directly on the decentralized network, entirely independent of the internal university database.

3.3. Performance Evaluation Metrices

These metrics are processed through a dedicated performance evaluator module, which provides empirical evidence of the system's resilience to cryptographic attacks and high-fidelity steganographic performance. Table 3 represent performance evaluation metrices across all tested formats (JPG, PNG, BMP, TIFF, GIF)

These metrics are processed through a dedicated performance evaluation module, which provides empirical evidence on the system's resilience to cryptographic attacks and high-fidelity steganographic performance. Table 3 presents the performance evaluation metrics consisting of Entropy, Histogram, Corr. Coeff, NPCR, UACI, PSNR, MSE, SSIM and BER across all tested formats (JPG, PNG, BMP, TIFF, GIF).

Table 3 Performance Evaluation Metrices & Duration

Certificate	Size (Kb)	Crypto Time(s)	Anchor Time(s)	Entropy	Histogram	Corr.Coeff	NPCR (%)	UACI (%)
Certificate a (jpg)	504	0.1964	2.0168	8	Uniform	0.00082	99.610	33.476
Certificate b (png)	603	0.1348	1.6632	8	Uniform	-0.00843	99.611	33.469
Certificate c (bmp)	874	0.1865	2.1590	8	Uniform	-0.00926	99.611	33.477
Certificate d (tiff)	229	0.1207	1.6912	8	Uniform	0.01093	99.609	33.469
Certificate e (gif)	243	0.1205	2.3256	8	Uniform	-0.02059	99.609	33.467

Table 3 presents the information entropy. In all tested formats (JPG, PNG, BMP, TIFF, GIF), the encrypted payload achieves a perfect Information Entropy value of 8. This indicates a state of ideal randomness, proving that Hyper-Chaotic-DNA Multi-Encryption randomization completely eliminates predictable patterns, making statistical attacks mathematically impossible. The correlation coefficients for all formats are close to absolute zero (e.g., 0.00082 for JPG and 0.00843 for BMP). This confirms that adjacent pixels in the encrypted payload are completely statistically independent, successfully obscuring any visual relationships present in the original data. The system's sensitivity to plaintext modification is evaluated using the NPCR and UACI metrics. The framework consistently recorded NPCR values exceeding 99.60% (ranging from 99.609% to 99.611%) and UACI values approaching the theoretically optimal threshold of approximately 33.47% (ranging from 33.467% to 33.477%). These near-ideal scores validate that a single bit change in the original metadata or seed triggers a completely different encryption avalanche, effectively neutralizing the appeal of differential cryptanalysis.

Furthermore, encryption time using 6D Chaotic DNA is very light, completing within a narrow time range of 0.1205 seconds to 0.1964 seconds. Anchoring the blockchain to the QRL network is the most time-consuming phase due to the required network broadcast protocol, yet it maintains a stable latency ranging from 1.6632 seconds to 2.3256 seconds. Overall, it confirms that this framework provides advanced multi-hybrid cryptographic security integrated with the QRL Blockchain network successfully without incurring excessive computational burden or latency.

3.4. Secure Transaction Lodging

All transactions are stored in a MongoDB database. Although the initial student metadata is derived directly from secure administrative input rather than being pulled from an existing MongoDB database, a robust backend storage mechanism is essential for recording post-processing transaction logs. The proposed framework uses MongoDB exclusively as a secure NoSQL-based transaction ledger to archive final cryptographic artifacts, evaluation metrics, and Quantum-Resistant Ledger (QRL) anchor confirmations.

The stored JSON-formatted documents encapsulate critical operational data, including transaction IDs, multi-cryptographic results, Phase-3 SHA-256 hash seeds, and QRL network receipts. The adoption of a NoSQL database architecture aligns perfectly with the document-based, hierarchical structure of the encrypted payload and the React.js frontend. Furthermore, to adhere to strict privacy principles from the design stage, this database serves solely as an immutable audit trail. All sensitive metadata stored in these logs is encrypted at rest using AES-256, thus neutralizing the database as a potential attack vector.

4. CONCLUSION

This research successfully developed and implemented a multi-cryptographic digital certification framework integrated with the robust QRL Blockchain network, designed to secure academic credentials from both classical forgery and emerging post-quantum threats. Its core innovation, a 6D hyper-chaotic system integrated with DNA-Quantum randomization, achieves near-ideal randomness, evidenced by an Information Entropy of 8 and optimal NPCR or UACI values. Finally, linking certificates to a Quantum-Resistant Ledger (QRL) establishes a decentralized and mathematically verifiable ecosystem for global educational credentialing.

To advance this field, several future research avenues are proposed Computational Optimization for Edge Devices. Future development will focus on optimizing the computational burden of a 6D hyper-chaotic machine to support real-time certificate issuance and verification on resource-constrained mobile hardware and IoT edge nodes. Adaptive Fibonacci Steganography technology is also added, exploring the integration of texture-based or Region-of-Interest (ROI) detection to adaptively adjust Fibonacci gaps, further enhancing resilience against advanced AI-based steganalysis. Decentralized Identity (DID) Integration, combining the framework with the Self-Sovereign Identity (SSI) standard to empower students with full ownership of their digital credentials while maintaining post-quantum anonymity. Cross-Chain Interoperability, investigating protocols for secure cross-chain tethering between various post-quantum blockchains to ensure credential longevity and global interoperability across institutional ledgers. Resilience Against Generative AI Attacks, conducting extensive stress testing against GAN (Generative Adversarial Networks)-based image manipulation to ensure the SPHINCS+ integrity seal remains robust against AI-synthesized certificate forgery.

5. REFERENCES

[1] M. Zulfadhilah, Y. Prayudi, and I. Riadi, “Cyber Profiling using Log Analysis and K-Means Clustering A Case Study Higher Education in Indonesia,” *IJACSA - Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 7, pp. 430–435, 2016, doi: https://doi.org/10.14569/IJACSA.2016.070759.

[2] I. Ardymulya and I. Riadi, “Denial Of Services Log Analysis Using Density K-Means Method,” *J. Theor. Appl. Inf. Technol.*, vol. 83, no. 2, pp. 299–302, 2016, [Online]. Available: http://www.jatit.org/volumes/Vol83No2/18Vol83No2.pdf

[3] Rosmiati, I. Riadi, and Y. Prayudi, “A Maturity Level Framework for Measurement of Information Security Performance,” *Int. J. Comput. Appl.*, vol. 141, no. 8, pp. 1–6, 2016, doi: https://doi.org/10.5120/IJCA2016907930.

[4] R. Umar, I. Riadi, and R. S. Kusuma, “Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method,” *IJID (International J. Informatics Dev.*, vol. 10, no. 1, pp. 53–61, 2021, doi: https://doi.org/10.14421/ijid.2021.2423.

[5] R. Umar, I. Riadi, M. Ihya, and A. Elfatiha, “Security analysis of web-based academic information system using OWASP framework,” *Kinet. Game Technol. Inf. Syst. Comput.*

Network, Comput. Electron. Control, vol. 4, no. 4, 2024, doi: https://doi.org/10.22219/kinetik.v9i4.2015.

[6] T. Ifeyemi, A. Oyedeji, and F. Adebiyi, "A Blockchain-Based Digital Educational Certificate Verification System," *J. Eng. Technol. Ind. Appl.*, vol. 10, no. 49, pp. 35–41, 2024, doi: https://doi.org/10.5935/jetia.v10i49.1145.

[7] S. H. Said, R. S. Sinde, E. M. Kosia, and M. A. Dida, "A Comprehensive Blockchain-Based System for Educational Qualifications Management and Verification to Counter Forgery," *IEEE Access*, vol. 13, no. February, pp. 31562–31589, 2025, doi: https://doi.org/10.1109/ACCESS.2025.3542545.

[8] A. Tiwari, P. Diwan, T. D. Diwan, M. Miroslav, and S. P. Samal, "A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image communication," *Sci. Rep.*, vol. 15, no. 1, p. 14151, 2025, doi: 10.1038/s41598-025-95995-8.

[9] R. Mubarak, I. Riadi, and T. Sutikno, "Integrasi Blockchain dan Algoritma Kriptografi Untuk Perlindungan Data Pribadi : Tinjauan Literatur Sistematis 2021-2025," *J. Inform. Darmajaya*, vol. 25, no. 2, pp. 72–87, 2025, doi: https://doi.org/10.30873/jurnalinformatika.v25i110.

[10] A. Fadlil, I. Riadi, and A. Nugrahantoro, "Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology Modification," *J. Hari. Reg.*, vol. 11, no. 3, pp. 155–166, 2020, doi: https://doi.org/10.24843/LKJITI.2020.v11.i03.p04.

[11] R. M. Gonçalves, M. M. da Silva, and P. R. da Cunha, "Olympus: a GDPR compliant blockchain system," *Int. J. Inf. Secur.*, vol. 23, no. 2, pp. 1021–1036, 2024, doi: https://doi.org/10.1007/s10207-023-00782-z.

[12] R. Abdelmagid, M. Abdelsalam, and F. K. Alsheref, "A Blockchain Framework for Academic Certificates Authentication," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 7, pp. 297–305, 2024, doi: http://dx.doi.org/10.14569/IJACSA.2024.0150729.

[13] S. A. Sultana, C. Rupa, R. P. Malleswari, and T. R. Gadekallu, "IPFS-Blockchain Smart Contracts Based Conceptual Framework to Reduce Certificate Frauds in the Academic Field," *MDPI*, vol. 14, no. 8, pp. 1–19, 2023, doi: https://doi.org/10.3390/info14080446.

[14] I. Riadi, A. Z. Ifani, and R. S. Kusuma, "Optimization and Evaluation of Authentication System using Blockchain Technology," *Emerg. Sci. J.*, vol. 4, no. February, pp. 225–240, 2022, doi: http://dx.doi.org/10.28991/esj-2021-SP1-015.

[15] I. Riadi, T. Ahmad, R. Sarno, P. Purwono, and A. Ma, "Developing Data Integrity in an Electronic Health Record System using Blockchain and InterPlanetary File System (Case Study : COVID-19 Data)," *Emerg. Sci. J. Vol.*, vol. 4, no. February, pp. 190–206, 2022, doi: http://dx.doi.org/10.28991/esj-2021-SP1-013.

[16] I. Riadi, R. Umar, I. Busthomi, and A. Wirawan, "Block-hash of blockchain framework against man-in-the- middle attacks," *Regist. J. Ilm. Teknol. Sist. Inf.*, vol. 8, no. 1, pp. 1–9, 2022, doi: https://doi.org/10.26594/register.v8i1.2190.

[17] B. Dwi *et al.*, "Evaluating The Acceptance of Blockchain Technology In The Supply Chain of Lombok Traditional Weaving Industry Using Extended Technology Acceptance Model," *Janapati*, vol. 14, no. 2, pp. 408–420, 2025, doi: https://doi.org/10.23887/janapati.v14i2.92595.

[18] R. Mubarak, I. Riadi, and T. Sutikno, "Integration of blockchain and cryptographic algorithms for education certification and verification : a systematic literature," *J. Soft Comput. Explor.*, vol. 7, no. 1, pp. 117–131, 2026, [Online]. Available: https://joscex.shmpublisher.com/index.php/journal/article/view/23/13

[19] A. Ghani, A. Zinedine, and M. El Mohajir, "A Trustful and Sustainable Diploma Management System in the Higher Education Institutions : A Blockchain-based Solution," *Int. J. Comput. Digit. Syst. 2025*, vol. 18, no. 1, pp. 1–13, 2025, doi: http://dx.doi.org/10.12785/ijcds/1571145627.

[20] R. T. H. Hasan and S. Y. Ameen, "Security Enhancement of IoT and Fog Computing Via Blockchain Applications," *J. Soft Comput. Data Min.*, vol. 2, no. 2, pp. 26–38, 2021, doi: https://doi.org/10.30880/jscdm.2021.02.02.003.

[21] S. E. Arief, R. F. Pamenang, and R. F. Sari, "JSCDM Blockchain-Based Cheat Detection System for Multiplayer Online Games," *J. Soft Comput. Data Min.*, vol. 6, no. 2, pp. 1–14, 2025, doi: https://doi.org/10.30880/jscdm.2025.06.02.001.

[22] E. Zaghloul, T. Li, M. W. Mutka, and J. Ren, "Bitcoin and Blockchain: Security and Privacy," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10288–10313, 2020, doi:

10.1109/JIOT.2020.3004273.
[23] S. K. Nanda, S. K. Panda, and M. Dash, "Medical supply chain integrated with blockchain and IoT to track the logistics of medical products," *Multimed. Tools Appl.*, vol. 82, no. 21, pp. 32917–32939, 2023, doi: 10.1007/s11042-023-14846-8.
[24] N. R. Reddy, S. Suryadevara, K. G. R. Reddy, R. Umamaheswari, R. Guttula, and R. Kotoju, "Quantum secured blockchain framework for enhancing post quantum data security," *Sci. Rep.*, vol. 15, no. 1, p. 31048, 2025, doi: https://doi.org/10.1038/s41598-025-16315-8.
[25] M. Švarcmajer, D. Šabanović, M. Köhler, and I. Lukić, "Predictive Modeling of Quantum Computing Development and Its Impact on Blockchain Security," *IEEE Access*, vol. 14, no. May, 2026, doi: https://doi.org/10.1109/ACCESS.2026.3689963.
[26] Y. Wang and E. S. Ismail, "A Review on the Advances , Applications , and Future Prospects of Post-Quantum Cryptography in Blockchain and IoT," *IEEE Access*, vol. 13, no. June, pp. 112962–112977, 2025, doi: https://doi.org/10.1109/ACCESS.2025.3584473.
[27] M. Al Hemairy, M. A. Talib, A. Khalil, A. Zulfiqar, and T. Mohamed, "Blockchain-based framework and platform for validation, authentication & equivalency of academic certification and institution's accreditation: UAE case study and system performance (2022)," *Educ. Inf. Technol.*, vol. 29, no. 14, pp. 18203–18232, 2024, doi: https://doi.org/10.1007/s10639-024-12493-6.
[28] L. Sardar, "Fake Me If You Can : Unforgeable Digi-Physical Academic Certificates With Instant Verifiability," *IEEE Access*, vol. 13, no. June, pp. 118334–118353, 2025, doi: https://doi.org/10.1109/ACCESS.2025.3583184.
[29] A. Djajadi, K. S. Lestari, L. E. Englista, and A. Destaryana, "Blockchain-Based E-Certificate Verification and Validation Automation Architecture to Avoid Counterfeiting of Digital Assets in Order to Accelerate Digital Transformation," *CCIT J.*, vol. 16, no. 1, pp. 68–85, 2023, doi: https://doi.org/10.33050/ccit.v16i1.2367.
[30] M. A. C. Quispe and A. Pacheco, "Blockchain ensuring academic integrity with a degree verification prototype," *Sci. Rep.*, vol. 15, no. 1, p. 9281, 2025, doi: https://doi.org/10.1038/s41598-025-93913-6.
[31] O. S. Oluwaseyi and R. O. Akinyede, "Utilizing Blockchain Technology for University Certificate Verification System," *Int. J. Appl. Inf. Syst.* –, vol. 12, no. 45, pp. 23–40, 2024, doi: https://doi.org/10.5120/ijais2024451977.
[32] R. Priyadarshini *et al.*, "A Faster , Integrated , and Trusted Certificate Authentication and Issuer Validation System Based on Blockchain," *IEEE Access*, vol. 13, no. January, pp. 27037–27049, 2025, doi: https://doi.org/10.1109/ACCESS.2025.3539180.
[33] K. Soumya, K. S. Sharat, and N. Sreenivas, "Academic certificate fraud detection by Web-based intelligent access control system: An effective role of Blockchain technology," *Int. J. Inf. Manag. Data Insights*, vol. 6, no. 1, p. 100386, 2026, doi: 10.1016/j.jjimei.2025.100386.
[34] C. Delgado-von-eitzen, L. Anido-rif, and M. J. Fernández-Iglesias, "NFTs for the Issuance and Validation of Academic Information That Complies with the GDPR," *MDPI*, vol. 14, no. 2, p. 706, 2024, doi: https://doi.org/10.3390/app14020706.
[35] R. Pericàs-Gornals, M. Mut-Puigserver, M. M. Payeras-Capellá, M. Á. Cabot-Nadal1, and J. Ramis-Bibiloni, "Digital credentials management system using rejectable soulbound tokens," *Ann. Telecommun.*, vol. 79, no. 11, pp. 843–855, 2024, doi: https://doi.org/10.1007/s12243-024-01032-6.
[36] M. Fartitchou, I. Lamaakal, K. El Makkaoui, and Y. Maleh, "BlockMEDC : Blockchain Smart Contracts System for Securing Moroccan Higher Education Digital Certificates," *IEEE Access*, vol. 13, no. March, pp. 39152–39175, 2025, doi: https://doi.org/10.1109/ACCESS.2025.3546177.
[37] A. G. Vieites, C. Delgado-von-eitzen, and D. E. Garcia, "GDPR-Compliant Academic Certification via Blockchain : Legal and Technical Validation of the GAVIN Project," *MDPI*, vol. 15, no. 9191, pp. 1–34, 2025, doi: https://doi.org/10.3390/app15169191.
[38] J. A. B. Moya, J. Ayoade, and M. A. Uddin, "A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System," *MDPI*, vol. 25, no. 11, pp. 1–24, 2025, doi: https://doi.org/10.3390/s25113450.
[39] X. Xu, "Zero-knowledge proofs in education: a pathway to disability inclusion and equitable learning opportunities," *Smart Learn. Environ.*, vol. 11, no. 1, p. 7, 2024, doi: 10.1186/s40561-024-00294-w.
[40] S. Boonkrong, "Design of an academic document forgery detection system," *Int. J. Inf.*

Technol., vol. 17, no. 9, pp. 5175–5187, 2024, doi: https://doi.org/10.1007/s41870-024-02006-6.

[41] S. Krishnan, S. Rajendran, and M. Zakariah, "A secured accreditation and equivalency certification using Merkle mountain range and transformer based deep learning model for the education ecosystem," *Sci. Rep.*, vol. 15, no. 22511 |, pp. 1–21, 2025, doi: https://doi.org/10.1038/s41598-025-06789-x.

[42] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "DIAR : a blockchain - based system for generation and verification of academic diplomas," *Discov. Appl. Sci.*, vol. 6, no. 6, p. 297, 2024, doi: https://doi.org/10.1007/s42452-024-05984-1.

[43] K. Tan-vo *et al.*, "Optimizing Academic Certificate Management With Blockchain and Machine Learning : A Novel Approach Using Optimistic Rollups and Fraud Detection," *IEEE Access*, no. August, pp. 168135–168159, 2024, doi: https://doi.org/10.1109/ACCESS.2024.3486029.

[44] N. K. Sinai and H. P. In, "Q-RTOP : Quantum-Secure Random Transaction Ordering Protocol for Mitigating Maximal Extractable Value Attacks in Blockchains With a Priority Gas-Fee Policy," *IEEE Access*, vol. 12, no. December 2023, pp. 10036–10046, 2024, doi: http://doi.org/10.1109/ACCESS.2024.3351830.