VOL. 12. NO. 1 AUGUST 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v12i1.7685

JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

BLOCKCHAIN-POWERED ACADEMIC CERTIFICATION SYSTEM USING NEAR PROTOCOL AND NFTS

Suwarno[1*]; Herman[1]; Elvin Valentino[1]

Information Systems[1]
Universitas Internasional Batam, Department of Information System, Batam, Indonesia[1]
https://uib.ac.id[1]
suwarno.liang@uib.ac.id*, herman@uib.ac.id, 2131017.elvin@uib.edu

(*) Corresponding Author
(Responsible for the Quality of Paper Content)

Abstract— *Academic certificates play a crucial role in today's competitive job market by helping employers assess candidates' qualifications and suitability for specific roles, thereby enhancing employability. However, traditional methods of certificate verification are fraught with challenges, particularly the widespread issue of forgery. This study proposes a blockchain-based academic certification system using the NEAR Protocol to improve the reliability of certificate issuance and verification. The developed decentralized application (DApp) issues certificates as Non-Fungible Tokens (NFTs), enabling tamper-resistant and easily verifiable credentials. The system was developed using Scrum and evaluated through qualitative thematic analysis of structured interview data. The architecture includes a NEAR-based NFT smart contract, RESTful API, and web frontend. Functional and integration testing on the NEAR testnet confirmed successful certificate minting, storage, and verification with low transaction costs. User evaluation results show that 80.48% of response-level feedback (169/210 responses) was positive across the evaluated themes, with 24 of 30 participants expressing willingness to use the system. Compared with Ethereum and Solana, the proposed DApp system demonstrates better cost efficiency. The novelty of the study lies in integrating Scrum-based development, structured user evaluation, and NFT-based credentials closely into a unified academic certification framework. The proposed approach effectively streamlines certificate management and helps mitigate certificate fraud.*

Keywords*: Blockchain, Certificate Verification, Decentralized Application (DApp), NEAR Protocol, NFT.*

Intisari— *Sertifikat akademik memainkan peran krusial dalam pasar kerja yang kompetitif saat ini dengan membantu pemberi kerja menilai kualifikasi dan kesesuaian calon karyawan untuk peran tertentu, sehingga meningkatkan keterampilannya. Namun, metode verifikasi sertifikat tradisional dipenuhi dengan tantangan, terutama masalah pemalsuan yang meluas. Penelitian ini mengusulkan sistem sertifikasi akademik berbasis blockchain menggunakan NEAR Protocol untuk meningkatkan keandalan penerbitan dan verifikasi sertifikat. Aplikasi terdesentralisasi (DApp) yang dikembangkan mencetak sertifikat sebagai Non-Fungible Tokens (NFTs), sehingga menghasilkan kredensial yang tahan manipulasi dan mudah diverifikasi. Sistem dikembangkan menggunakan metodologi Scrum dan dievaluasi melalui analisis tematik kualitatif terhadap data wawancara terstruktur. Arsitektur sistem mencakup smart contract NFT berbasis NEAR, RESTful API, dan antarmuka web. Pengujian fungsional dan integrasi pada NEAR testnet mengonfirmasi keberhasilan proses pencetakan, penyimpanan, dan verifikasi sertifikat dengan biaya transaksi yang rendah. Hasil evaluasi pengguna menunjukkan bahwa 80,48% umpan balik berbasis respons (169/210 respons) bersifat positif pada tema yang dievaluasi, dengan 24 dari 30 partisipan menyatakan kesediaan menggunakan sistem. Dibandingkan dengan Ethereum dan Solana, sistem DApp yang diusulkan menunjukkan efisiensi biaya yang lebih baik. Kebaruan penelitian ini terletak pada integrasi pengembangan berbasis Scrum, evaluasi pengguna terstruktur, dan kredensial NFT berbasis NEAR dalam satu kerangka sertifikasi akademik terpadu. Pendekatan yang diusulkan secara efektif menyederhanakan pengelolaan sertifikat dan membantu memitigasi pemalsuan sertifikat.*

Kata Kunci*: Blockchain, aplikasi terdesentralisasi (DApp), NFT, NEAR Protocol, verifikasi sertifikat.*

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 12. NO. 1 AUGUST 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v12i1.7685

INTRODUCTION

In today's highly competitive job market, academic certificates serve as a benchmark for employers to assess a candidate's qualifications and suitability for a particular role, contributing significantly to their overall employability and hiring decisions [1]. However, traditional methods of verifying academic certificates are plagued with several challenges [2]. One of the major challenges is the prevalence of certificate forgery [3], which makes it difficult for employers and academic institutions to ensure the authenticity of the certificates [4]. This has led to a time-consuming and costly manual verification process that requires significant human resources and expertise [5]. To address this problem, blockchain technology has emerged as a promising solution for academic certificate verification [6].

Blockchain technology has sparked a significant revolution in recent years, with essential components such as cybersecurity [7], cloud computing [8], Internet of Things [9], and big data [10]. Blockchain is a distributed ledger system that enables secure and transparent transactions [11]. The blockchain paradigm leverages key technologies such as peer-to-peer networking, distributed ledgers, consensus mechanisms, and smart contracts [12]. It is widely recognized for its inherent characteristics, including security, transparency, decentralization, auditability, and immutability [13][14]. Consequently, blockchain technology has been adopted across various sectors, including finance, healthcare, supply chain management, government records, and academic records [15].

The previous research conducted by [16] made a system to store academic certificates in blockchain using the Ethereum blockchain. The research presents a blockchain-based system for academic certificate verification using a smart contract named 'AcadCerti'. This system helps to combat the issue of certificate forgeries and counterfeit credentials during admissions and recruitment processes. The key outcomes of this research are the development and testing of the 'AcadCerti' smart contract using Sublime Text 3 as a text editor and Remix Ethereum as an integrated development environment, a methodology for storing certificates on the blockchain to increase transparency and security, and the successful integration of the system with Metamask for front-end chain applications. The results of the test of the 'AcadCerti' smart contract performed using the Remix Ethereum IDE show that the contract functions as planned.

Another research conducted by [17] implemented a blockchain-based system for academic certificate verification using Hyperledger Fabric. The research resulted in the development of a prototype named VECefblock, which is a blockchain-based application tailored to solve the problem of fake diplomas in Vietnam. The architecture, business processes, transaction flows, and data mapping structure were discussed in detail. This prototype was deployed and tested in a cloud environment using Hyperledger Fabric. The study also highlighted how blockchain technology could be applied to education in Vietnam and how it could potentially address the challenge of diploma fraud. The work demonstrated the application of blockchain technology in Vietnam and outlined potential future work, such as scaling up the VECefblock system and building a more effective query data mechanism. However, specific quantitative results from the testing were not provided in the given excerpts.

While prior studies provide strong foundations and demonstrate implementations using major blockchain platforms such as Ethereum and Hyperledger, the existing literature remains largely concentrated on these ecosystems. Comparatively, there is still limited academic exploration addressing how emerging blockchain platforms such as the NEAR Protocol could be utilized for academic certificate issuance and verification. In particular, there is a noticeable lack of studies evaluating the NEAR Protocol in terms of scalability advantages, lower transaction costs, or developer-usability benefits within this specific application domain. This gap indicates that alternative blockchain platforms with potentially lower fees and developer-friendly architectures have not been thoroughly validated for academic credential verification. Therefore, this study evaluates the NEAR Protocol in terms of: (i) transaction cost, (ii) implementation feasibility, and (iii) user acceptance and privacy concerns.

The primary objective of this research is to provide a different approach that makes use of blockchain technology to address the ongoing difficulties related to the issue and verification of academic certificates. The study explores the potential of the NEAR protocol as an alternative blockchain platform for academic certificate verification, in contrast to earlier research that primarily concentrates on well-established blockchain platforms like Ethereum or Hyperledger. The developer-friendly architecture and support for rapid prototyping via a separate testnet environment are two of the NEAR Protocol's many features. This environment streamlines the

VOL. 12. NO. 1 AUGUST 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v12i1.7685

development and testing process by allowing developers to create accounts, simulate transactions, and install smart contracts before mainnet migration [18]. In addition, the NEAR Protocol provides strong scalability through its sharding architecture, which enables parallel transaction processing across multiple shards and allows the network to scale horizontally as demand increases. Its mature developer ecosystem also offers SDK support, human-readable accounts, and efficient tooling that facilitate faster and easier smart contract development [19].

To address this gap, this study proposes and evaluates a blockchain-based academic certification system built on the NEAR Protocol. Specifically, this work makes three main contributions. First, it designs and implements an end-to-end academic credentialing architecture consisting of a NEAR-based NFT smart contract, a RESTful API layer, and a web-based user interface for certificate issuance and verification. Second, it provides an empirical performance evaluation on the NEAR testnet, including functional validation and transaction cost analysis to assess implementation feasibility. Third, it conducts a user-centered evaluation using structured interviews to examine user acceptance and privacy perceptions of the proposed DApp system. Collectively, these contributions position NEAR as a scalable and developer-friendly alternative for blockchain-based academic credential management systems.

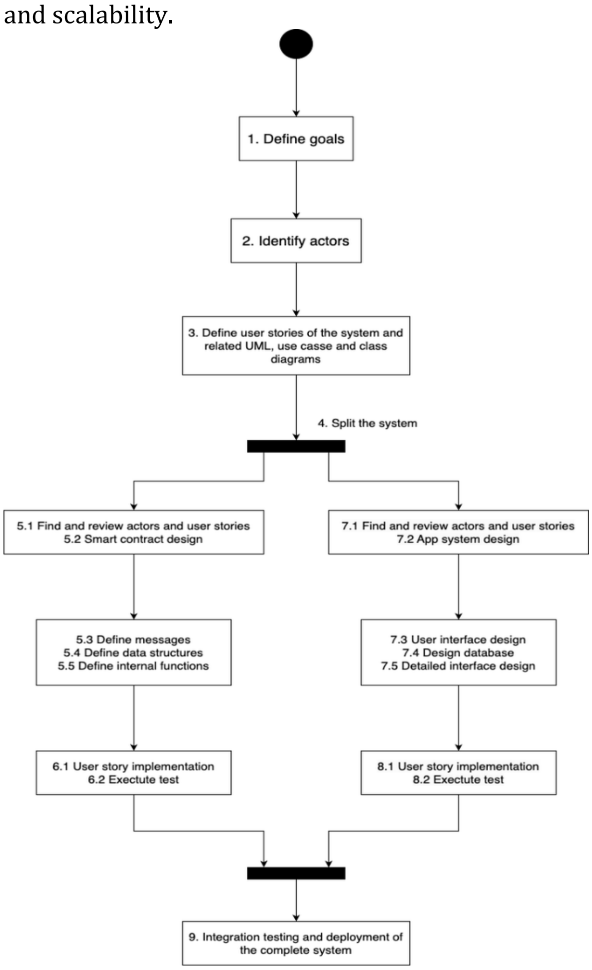
MATERIALS AND METHODS

This study adopts a multi-method research design that combines system development and user evaluation. The system development phase employs the applied Scrum framework, which structures the process into iterative sprints with defined deliverables to support incremental development of the application [20][21], illustrated in Figure 1.

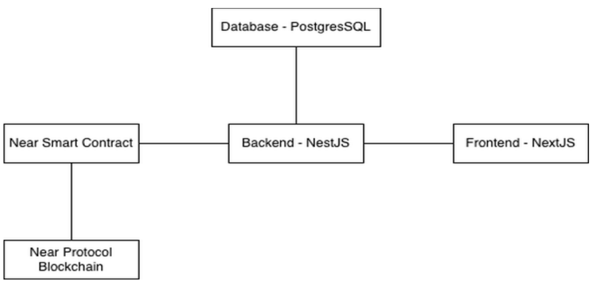
For the evaluation phase, qualitative data are collected through structured interviews with users and analyzed using deductive thematic analysis. The analysis follows a predefined coding protocol to identify themes related to user perceptions, usability, and acceptance of the proposed application.

System Architecture

To support the development process described above, the proposed application integrates a smart contract deployed on the NEAR Protocol blockchain with a conventional web application stack. The overall architecture, illustrated in Figure 2, consists of four main components: (1) the smart contract layer operating on the NEAR blockchain for on-chain certificate minting and verification, (2) a backend service implemented using NestJS that handles business logic and communication with the blockchain, (3) a frontend interface developed using Next.js that provides user interaction for certificate issuance and verification, and (4) a PostgreSQL relational database that supports off-chain persistent storage for auxiliary application data. This hybrid on-chain/off-chain design enables secure certificate validation while maintaining system performance and scalability.



Source: (Research Results, 2025)
Figure 1. Agile Scrum Process



Source: (Research Results, 2025)
Figure 2. System Architecture Diagram

VOL. 12. NO. 1 AUGUST 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v12i1.7685

Structured Interview

The researchers recruited 30 participants with prior experience in traditional digital certification platform for a structured interview to gather feedback on the blockchain-applied certification system. Participants were recruited using purposive sampling through a professional and academic network of researchers to ensure that respondents had prior experience with digital certification platforms, with initial contact conducted via WhatsApp messaging. The inclusion criteria required participants to (i) have previously used a digital certificate verification or issuance platform and (ii) possess basic familiarity with web-based applications. The participant pool consisted of software engineers (n = 10), UI/UX designers (n = 3), and college students (n = 17), representing both technically experienced users and general end users. The distribution reflects the availability of eligible participants within the targeted user groups while ensuring coverage of both technical and non-technical perspectives.

Prior to participation, electronic informed consent was obtained after participants were briefed about the goals and methods of the study. Respondents were free to discontinue participation at any moment. All interview information was anonymized and safely kept for use solely in research. According to institutional guidelines, since the study only collected sensitive personal data and involved low-risk user feedback, formal ethics committee approval was not necessary. As indicated in Table 1, deductive thematic analysis was used to examine the interview data in light of predetermined themes, such as intention to use, acceptance of technology, and certification data management. A structured codebook was used to facilitate consistent coding across transcripts, improving analytical reliability and consistency. An independent qualitative researcher evaluated the coding scheme and thematic interpretations as part of a peer debriefing process to further enhance analytical rigor. The review's comments were utilized to improve theme definitions and guarantee that the dataset was interpreted consistently. To find recurring trends, user issues, and areas for system enhancement, the results were combined [22]. The later interview transcripts showed no significantly new themes, suggesting that thematic saturation had been reached.

Table 1. Interview Questions

Key Theme	Question
Intention of use	Do you feel the need for a blockchain-based academic certification system? Are you willing to use a blockchain-based academic certification system?
Acceptance of technology	Is the information provided by the application clear? Do you understand the information presented by the application? Is it easy to locate features within the application?
Certificate data management and sharing	Are you interested in using a blockchain-based academic certification system for managing certificates? What factors do you consider important when sharing certificate information on the blockchain?

Source: (Research Results, 2025)

RESULTS AND DISCUSSION

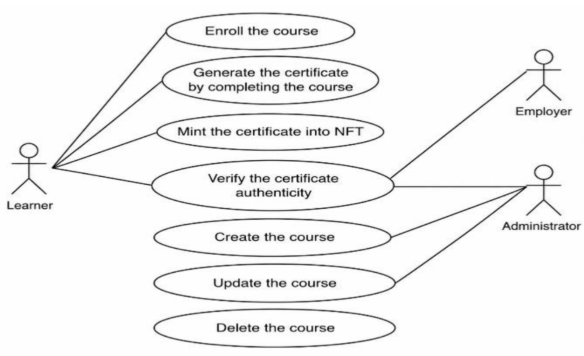
System implementation

A decentralized application (DApp) was developed to leverage blockchain technology for issuing and verifying online course completion certificates. The system enables learner records and associated certificates to be issued, stored, and validated on the NEAR Protocol blockchain network. By utilizing a decentralized ledger, the proposed approach ensures the authenticity, integrity, and traceability of academic certificates, allowing employers, educational institutions, and other authorized parties to perform verification efficiently and reliably.

1. **System Goal**

   The primary goal of the proposed DApp system is to design and implement a blockchain-based academic certification system that issues and verifies academic certificates as Non-Fungible Tokens (NFTs) on the NEAR Protocol.
2. **Actors**

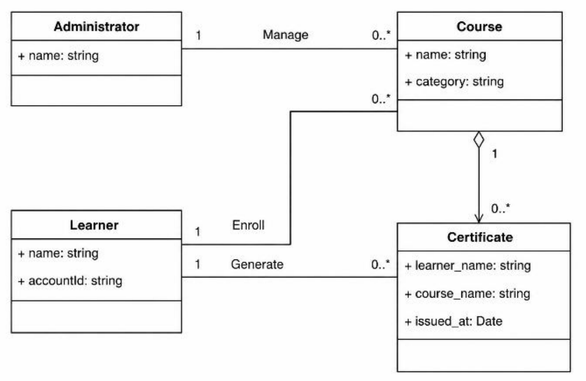
   The key actors involved in this system are:
   a. **Learner:** An individual who completes a course and receives a verifiable certificate.
   b. **Administrator:** Personnel responsible for managing courses and issuing certificates.
   c. **Employer:** A third party who verifies the authenticity of certificates.



Source: (Research Results, 2025)
Figure 3. The User Stories Of The Proposed Dapp System Specification

3. **User Stories**

The key user stories for the system are presented in Figure 3 using UML use case diagrams. These user stories outline the high-level functionalities the system should provide to the actors, without delving into implementation details. Additionally, UML class diagrams in Figure 4 provide information about the entities and data structure, derived from the user stories in Figure 3. It's worth noting that the employer, as a third-party verifier, is not included in Figure 4 as they are not directly involved with the internal system data structures.



Source: (Research Results, 2025)
Figure 4. The standard UML class diagram derived from the user stories

4. **Divide the system into Smart Contract (SC) and App subsystems**

The overall system was divided into two main subsystems. The external application system, which serves as a client to the smart contracts, houses the majority of the core functionality. We developed a UI-based web application that allows students to enroll in courses, complete them, and receive their certificates as NFTs. Additionally, we created a backend service to store and manage user data, course details, and certificate information. This approach helps improve performance, as fetching data directly from the blockchain can be time-consuming. In contrast, the smart contracts subsystem contains only the core blockchain components required to mint NFT certificates for users and store the ownership information in the blockchain.

5. **Design of the SC subsystem**

The smart contract system consists of a single "NFT" smart contract. This contract is responsible for minting the NFT certificate tokens upon issuance and maintaining the ownership information of the NFT tokens. The users must first create their own NEAR wallet to mint their NFT certificates, allowing them to view their minted NFT certificates. To display the certificates in the wallets, the NFT contract needs to implement the NEP-171 non-fungible token standard, which utilizes several standard library contracts shown in Figure 5. The "Mint" library allows for the minting of NFT certificates. The "NFTCore" and "Enumeration" library contracts are used to retrieve the details of the NFT token and the list of NFT tokens by the owner's account ID, respectively. By implementing NEP-171, the NFT contract should have covered the core functionalities of the smart contract system through the blockchain.

6. **Coding of the SC subsystem**

We implemented the NFT smart contract in the TypeScript programming language and tested it using the NEAR Protocol testing framework. As shown in Figure 5, the NFT contract has three public properties or we can call them state variables in terms of smart contract. "tokensPerOwner" is used to store the mapping of the token ids to the owners of the tokens. "tokensById" used to store the mapping of the token ids to the token struct. "tokenMetadaById" used to store the mapping of the token ids to the token metadata. The properties of the smart contract is shown in Listing 1.

Listing 1. Smart Contract State Variables

```
@NearBindgen
export class Contract extends NearContract {
  …
  tokensPerOwner: LookupMap;
  tokensById: LookupMap;
  tokenMetadataById: UnorderedMap;
  …
}
```

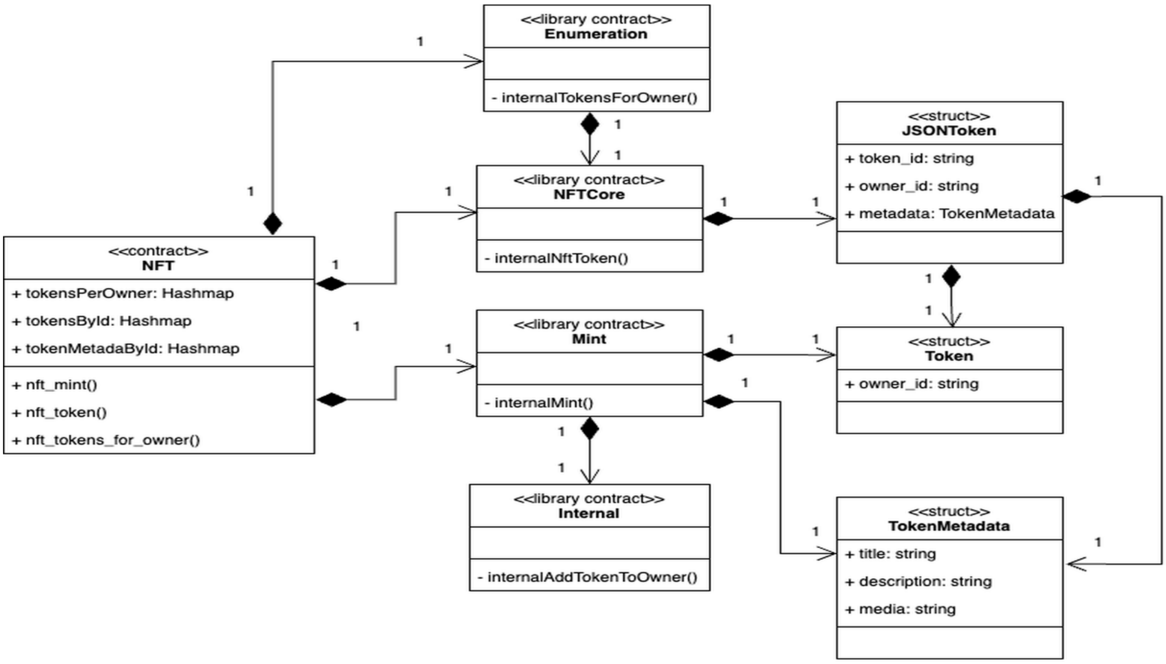
The user can mint an NFT certificate token by calling the "nft_mint" method from the NFT contract. This function will mint the NFT token and assign it to the user's NEAR wallet address according to the parameters given. The function has a "call" decorator which means the function will execute a state change in the smart contract, for which it costs gas. The "nft_mint" code is shown in Listing 2.

Listing 2. NFT Minting Function

```
@call
nft_mint({ token_id, metadata, receiver_id,
perpetual_royalties }) {
   return internalMint({
      contract: this,
      tokenId: token_id,
      metadata: metadata,
      receiverId: receiver_id,
      perpetualRoyalties:
perpetual_royalties,
   });
}
```


Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 12. NO. 1 AUGUST 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v12i1.7685



Source: (Research Results, 2025)
Figure 5. The Modified UML Class Diagram, Showing the Structure of the Required Smart Contracts of the Proposed DApp System

Upon successful minting, the NFT certificate can be viewed in the user's NEAR wallet. The "nft_tokens_for_owner" method needs to be implemented to display the NFTs list in the user's wallet according to the NEP-171 standard. To display the details of the NFT, the NFT contract also needs to implement the "nft_token" method. Unlike "nft_mint" method, the "nft_tokens_for_owner" and "nft_token" methods have a "view" decorator which means the function will not execute a state change in the smart contract, and hence it's free to call. the "nft_tokens_for_owner" and "nft_token" code is shown in Listing 3.

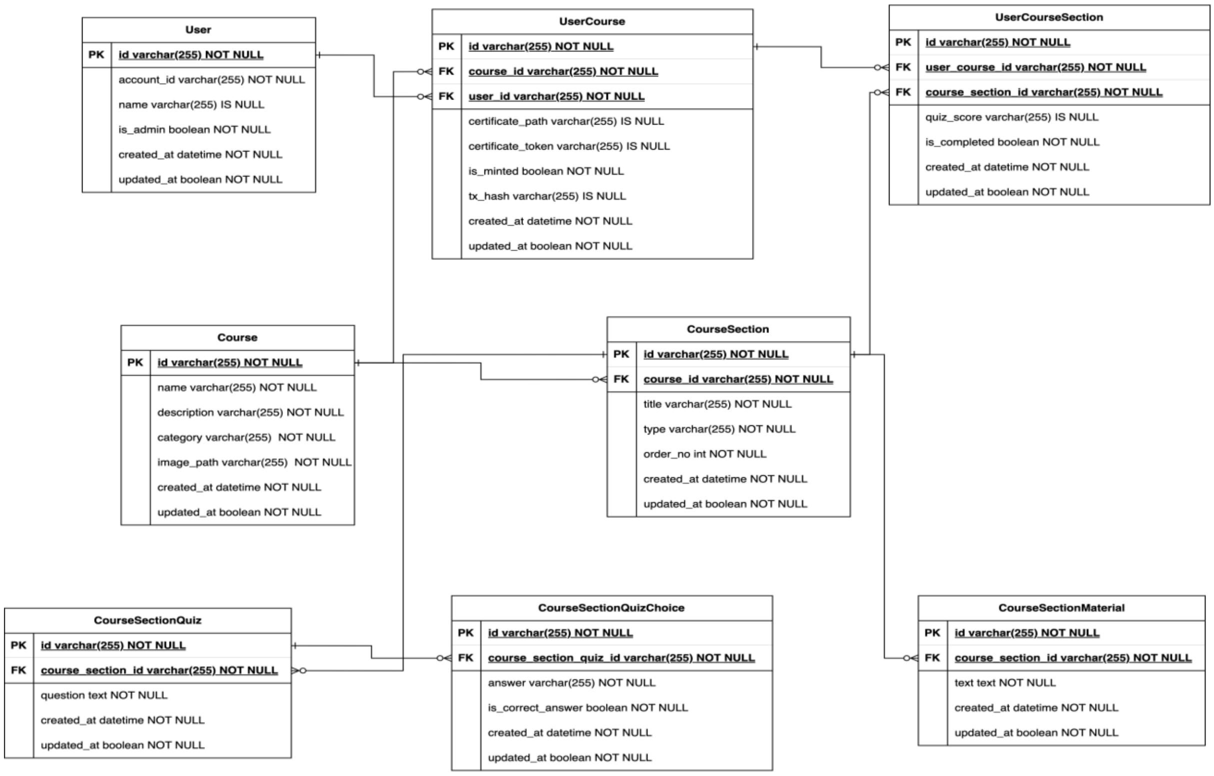
Listing 3. NFT Query Functions
```
@NearBindgen
export class Contract extends NearContract {
  …

  @view
  //get the information for a specific token
ID
  nft_token({ token_id }) {
    return internalNftToken({ contract: this,
tokenId: token_id });
  }
  @view
  //get the total supply of NFTs for a given
owner
  nft_tokens_for_owner({ account_id,
from_index, limit }) {
    return internalTokensForOwner({
      contract: this,
      accountId: account_id,
      fromIndex: from_index,
      limit: limit,
    });
  }
  …
}
```

To ensure the smart contract's proper functioning, we tested the deployed smart contract on the NEAR testnet using the NEAR Protocol Command Line Interface and NEAR Wallet. Since NEAR provides faucet functionality, testnet tokens can be obtained easily, allowing the printing of NFT certificates without any real transaction fees.

7. **Design of the external app subsystem**

The external application system serves as the client interface to the NFT smart contract on the NEAR blockchain. As explained in step 4, we developed both frontend and backend components to handle the overall system functionality. The frontend component is a web application that consists of several pages like a landing page, course enrollment page, certificate page, course materials page, verify certificate page, and user profile page. The backend component is a REST API service that is responsible for storing and managing the user data, course details, and certificate information. The data structure and entities involved in the backend are shown in Figure 6. Notice that we also stored the certificate data and transaction details in the backend database, in addition to on the blockchain, to improve performance and user experience.

VOL. 12. NO. 1 AUGUST 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v12i1.7685



Source: (Research Results, 2025)

Figure 6. The Entity Relationship Diagram.

8. **Coding of the external app subsystem**

We implemented the proposed DApp system using Next.js and developed a RESTful API using Node.js and Nest.js framework. Following the best practices of Next.js development, we separated the pages into components that handle specific functionalities so that it's easier to test and maintain in the long run. The proposed DApp system utilizes the NEAR API to interact with the smart contract directly using a package called "near-api-js".

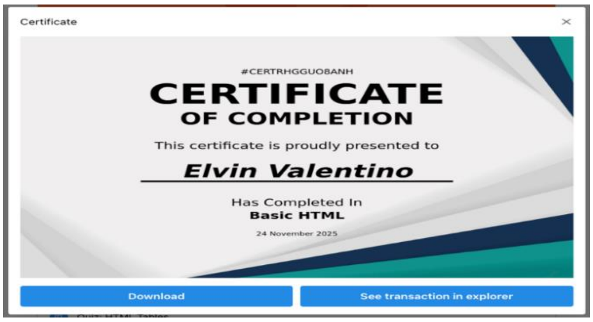
This package provides abstractions over the RPC calls required to interact with the smart contract. To interact with the smart contract, the proposed DApp system prompts the user to connect to their NEAR wallet with the help of the "@near-wallet-selector" package. After the user successfully connects their wallet, the proposed DApp system will store the wallet details in the database via API for user authentication purposes. After the user is authenticated, the user can finally enroll for a course and mint their certificate as an NFT by calling the "nft_mint" method of the NFT smart contract as shown in Listing 4.

Listing 4. Frontend Certificate Minting Integration

```
const mintNft = async () => {
    await wallet.callMethod({
      contractId: CONTRACT_ID,
      method: 'nft_mint',
      args: {
        token_id: course.certificate_token,
        receiver_id: signedAccountId,
        metadata: {
          title: `${course.name}
certificate`,
          description: `Certificate of
completion for ${course.name} course (Please
               do not transfer out this
NFT)`,
          media:
parseImagePath(course.certificate_path),
          copies: 1,
        },
      },
      deposit: new
BN('1000000000000000000000000').toString(),
    });
}
```

After the certificate is successfully minted on the NEAR blockchain, the proposed DApp system will also create a record of the certificate transaction in the database along with the NFT metadata and transaction hash by calling the "nftMinted" method. So whenever the user wants to verify their certificate, the proposed DApp system can fetch the details from the database and display them to the user. We thoroughly tested the proposed DApp system and the backend API through Postman and integration tests to ensure both frontend and backend components are working as expected.

VOL. 12. NO. 1 AUGUST 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v12i1.7685



Source: (Research Results, 2025)
Figure 7. Generated NFT Certificate from the Proposed DApp System

9. Integrate, test and deploy the proposed DApp system.

In this final step, we integrated the frontend web application and backend REST API with the NEAR blockchain-based NFT smart contract. We deployed the NFT smart contract onto the NEAR testnet blockchain network using the NEAR CLI, and the frontend and backend components onto a virtual private server running the Linux Ubuntu operating system. Finally, we conducted manual testing to ensure that the entire proposed DApp system was functioning as expected, including the user flow for course enrollment, certificate minting, and certificate verification. The generated NFT certificate can be seen in the screenshots shown in Figure 7. The proposed DApp system is accessible at https://evcert.netlify.app/.

Functional Testing

Functional and integration testing were performed to validate the core operations of the proposed DApp system. The testing was conducted on the NEAR testnet environment, which replicates mainnet conditions without incurring real transaction costs. Testnet tokens were acquired through the NEAR faucet to facilitate smart contract deployment and transaction execution. The following test criteria were evaluated: (1) smart contract deployment and initialization on the NEAR testnet; (2) NFT certificate minting via the nft_mint function with correct metadata assignment; (3) certificate ownership retrieval using nft_tokens_for_owner; (4) individual certificate detail retrieval using nft_token; (5) frontend-to-backend API communication for user authentication and course enrollment; (6) end-to-end certificate minting workflow from the web interface; and (7) certificate verification by querying on-chain and off-chain records.

All seven test criteria were successfully validated. The smart contract was deployed and initialized without errors. NFT certificates were minted with correct metadata and assigned to the designated receiver accounts. The query functions returned accurate token information and ownership data. The frontend and backend communicated seamlessly through the RESTful API, and the end-to-end certificate minting and verification workflows performed as expected. Integration testing using Postman confirmed that all API endpoints returned correct responses for valid inputs and appropriate error handling for invalid requests. A total of seven functional test cases were executed, all of which passed successfully (100% pass rate). However, detailed latency benchmarking was not the focus of this study, as transaction confirmation time on public blockchains depends heavily on network and validator conditions beyond the application layer.

User Evaluation Findings

As part of the project evaluation, structured interviews were conducted with 30 participants to gather feedback on the proposed DApp system. The interview questions were categorized into three predefined key themes: intention of use (2 questions), acceptance of technology (3 questions), and certificate data management and sharing (2 questions), yielding a total of 7 questions per participant. Each individual response was independently classified as positive, neutral, or negative based on the predefined coding protocol described in the Methods section. The unit of analysis in Table 2 is individual responses rather than participants; accordingly, the denominators reflect the total number of responses per theme (e.g., 30 participants × 2 questions = 60 responses for Intention of Use).

A summary of the response-level results is presented in Table 2. All participant identifiers used in this section (P1–P30) are pseudonymized codes assigned during data collection to ensure respondent anonymity. The direct quotations presented throughout the following thematic discussions were selected as representative examples that best illustrate the predominant sentiments within each theme, rather than extreme or outlying cases, and were identified through consensus among the research team during the thematic analysis process.

Table 2. Interview Result Summary

Key Theme	Positive	Neutral	Negative
Intention of use (2 Questions; n = 60 responses)	48 (80%)	4 (6.67%)	8 (13.33%)
Acceptance of technology	73 (81.11%)	7 (7.78%)	10

Key Theme	Positive	Neutral	Negative
(3 Questions; n = 90 responses)			(11.11%)
Certificate data management and sharing (2 Questions; n = 60 responses)	48 (80%)	5 (8.33%)	7 (11.67%)

Source: (Research Results, 2025)

As shown in Table 2, the overall response distribution across all three themes indicates a predominantly positive reception, with 169 out of 210 total responses (80.48%) classified as positive, 16 (7.62%) as neutral, and 25 (11.90%) as negative. Among the three themes, Acceptance of Technology received the highest proportion of positive responses (81.11%), suggesting that participants generally found the proposed DApp system usable and its information clearly presented. Intention of Use and Certificate Data Management and Sharing both received 80.00% positive responses, indicating comparable levels of user interest and trust in the system. The relatively low proportion of negative responses across all themes (ranging from 11.11% to 13.33%) suggests that major usability or conceptual barriers were not prevalent among the participant group.

To complement the response-level analysis, participant-level summaries were also computed. For Intention of Use, 23 out of 30 participants (76.67%) responded positively to both questions, 4 participants (13.33%) gave mixed responses, and 3 participants (10.00%) responded negatively to both questions. For Acceptance of Technology, 20 out of 30 participants (66.67%) responded positively to all three questions, while the remaining 10 participants (33.33%) provided mixed responses with no participant responding negatively to all three items. These participant-level findings corroborate the response-level results, confirming broad positive reception of the proposed DApp system.

Intention of use

Most participants expressed a strong interest in using a blockchain-based academic certification system due to its security, transparency, and immutability [23]. Participants highlighted that blockchain could minimize certificate forgery and enhance verification efficiency. For instance, participant P5 stated that "blockchain-based academic certification systems increase security, transparency, and efficiency by ensuring immutable, decentralized, and auditable data." Similarly, P25 emphasized that blockchain could "reduce abuse of power and increase fairness in the certification process." Several participants also noted that the system could reduce administrative overhead, while others were motivated by curiosity and the appeal of new technology. P7 shared that they were willing to try the system "to see how the app works with blockchain technology," and P27 described it as "interesting and authentic, adding to our digital assets."

However, a few participants were more skeptical. P1 noted that "even without blockchain, transactions should happen smoothly and securely," while P14 felt the system "seems a little complicated for a regular user." Despite these reservations, the majority expressed willingness to use the system, provided usability and costs such as gas fees remain manageable [24].

Acceptance of technology

Participants generally found the proposed DApp system clear, user-friendly, and easy to navigate. Many appreciated its simple design, well-structured information, and supportive guidance. P17 commented that "the information presented is good and structured… the UI is easy to understand," while P12 found the proposed DApp system "straightforward and clear in purpose." Most participants also indicated they fully understood the information provided, with P11 noting that it was "presented in a clear and structured manner, explaining the key benefits of blockchain technology." Similarly, P28 stated that the information was "well organized, making it easy to follow and understand." Some participants suggested minor improvements, such as clearer instructions for connecting wallets (P10), a search feature (P6), or copyable tokens (P17). Others like P5 mentioned that the main challenge was the general unfamiliarity with blockchain technology, making the first use "a little complicated." [25]. Overall, participants' responses indicated high acceptance of the proposed DApp system's usability, clarity, and purpose.

Certificate data management and sharing

Most participants emphasized security and immutability as essential factors when managing and sharing certificate data on the blockchain. P12 highlighted that "with this technology, we can be safer with blockchain protocols that are more secure," while P18 noted that "the information is immutable… everyone with the internet can access it to ensure authenticity." Participants appreciated that blockchain ensures certificate validity and prevents forgery. P22 stated that the system "gives confidence that my digital certificate is authentic and cannot be forged by others." Others, like P11

VOL. 12. NO. 1 AUGUST 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v12i1.7685

and P25, viewed blockchain's transparency and efficiency as key advantages for long-term adoption [26]. Despite the positive feedback, some concerns were raised about privacy and accessibility. P1 mentioned that "information in the certification application should not be easily accessible from any party other than the user," and P20 warned that certificates "should not contain too much personal data because it can be accessed by anyone." [27]. Overall, participants expressed strong interest and trust in using blockchain-based academic certification systems for certificate management and sharing, acknowledging both the technological benefits and the need for careful attention to privacy.

Cost Analysis

In addition to qualitative findings, a cost analysis was conducted to evaluate the economic feasibility of deploying the certification system on the NEAR Protocol. The NEAR gas fee was measured from actual transaction logs recorded during NFT minting operations on the NEAR testnet. Specifically, the gas consumption for a single nft_mint transaction was observed and converted to NEAR tokens using the protocol's standard gas pricing mechanism. Gas fee estimates for Ethereum and Solana were obtained from prior empirical studies: the Ethereum gas fee is based on the average NFT minting cost reported by [28], and the Solana gas fee is derived from the transaction cost reported by [29] in their implementation of NFT-based e-certificates. On November 26, 2025, cryptocurrency market prices were obtained from CoinMarketCap (https://coinmarketcap.com) in order to facilitate cost comparison in fiat currency. The prices of NEAR, Ethereum (ETH), and Solana (SOL) were around USD 1.89, USD 2,945.15, and USD 138.82, respectively, at the time of recording. The relative variations in operating costs among blockchain networks can be interpreted using these price points as a foundation. The estimated cost of carrying out a single certificate minting transaction across NEAR, Ethereum, and Solana is summarized in Table 3.

Table 3. Cost Comparison

Blockchain	Gas Fee (Token)	Gas Fee (USD)	Source
NEAR Protocol	0.001161 NEAR	0.00219	Testnet Transaction Log
Ethereum	0.009163 ETH	26.98	[28]
Solana	0.0081 SOL	1.12	[29]

Source: (Research Results, 2025)

The findings show that, in comparison to Ethereum and Solana, the NEAR Protocol provides significantly lower transaction fees for certificate minting operations. A single certificate minting transaction on NEAR costs about USD 0.00219 at the current prices, while Ethereum costs about USD 26.98 and Solana costs about USD 1.12. Because of this cost advantage, NEAR is a more cost-effective choice for organizations looking to issue digital certificates on a large scale, especially in situations where a lot of certificates need to be issued with little operating expense.

Discussion

In this study, we built a blockchain-based academic certification system for certificate issuance and verification. The purpose was to make the process of certificate authentication and validation more transparent, secure, and efficient through the use of blockchain technology. With blockchain implementation, we utilized NFT as a means of representing and securely storing the certificate information. We developed the proposed DApp system on the NEAR blockchain protocol using scrum methodology and received feedback through a structured interview process. By utilizing the security and transparency provided by the blockchain [24], we were able to create a system that addresses the issues faced in the traditional certificate issuance and verification process. Which can help academic institutions and employers overcome the challenges related to the trust and verification of academic credentials. They can easily authenticate and access the certificate details on the blockchain, reducing the possibility of fraudulent activities, which also fastens the process as compared to manual verification. Additionally, it can reduce certificate forgery or certificate duplication to ensure its authenticity [30].

Several previous research studies have utilized blockchain-based academic certification systems. A study from [29] implemented a blockchain-based e-certificate as an NFT on the Solana network, using the Scrum methodology for system development and evaluation, but did not conduct user interviews for feedback. Another study from [31] developed a blockchain-based micro-credential system to issue certificates using the Blockcerts open-source project by MIT and conducted user interviews for evaluation. Furthermore, prior works discussed in the literature review demonstrate additional contrasts in architectural design and cost-efficiency. The Ethereum-based approach in [16] exhibited functional reliability yet faced persistent challenges related to high and volatile gas fees, underscoring the need for more economical public blockchain alternatives. In contrast, the Hyperledger Fabric implementation in [17] eliminated gas costs entirely due to its private-network environment but lacked the openness, decentralization, and transparent verification capacity characteristic of public blockchain systems. These comparative findings reinforce the rationale for adopting the NEAR Protocol, which offers substantially lower operational costs than Ethereum while maintaining the transparency and security properties that private blockchains such as Hyperledger Fabric do not provide. However, at the time of this research, there was no study that implemented a blockchain-based academic certification system using both the Scrum methodology and a structured interview process to gather user feedback. Therefore, this study presents a novel approach by implementing a blockchain-based academic certification system in the NEAR Protocol using a multi-method approach, leveraging Agile Scrum for system development and a structured interview method to collect user feedback.

This study demonstrates how a blockchain-based academic certification system was developed using the Agile Scrum methodology. The Scrum approach allowed us to iteratively refine and enhance the proposed DApp system's features, ensuring the final outcome met our expectations. During the development process, we found that the NEAR Protocol made it easier for us as developers to create a smart contract. Testnet tokens were acquired through NEAR faucet on their testnet blockchain network, allowing us to deploy and test our smart contract directly on the testnet. This was in contrast to the challenges of obtaining testnet tokens for Ethereum [32]. The structured interview findings revealed that several participants raised concerns about the privacy implications of storing certificate data on a public blockchain. In particular, participants noted that certificate information should not be easily accessible by unauthorized parties and that certificates should not contain excessive personal data. These concerns are consistent with broader discussions in the literature regarding the tension between blockchain transparency and data privacy requirements, including compliance with regulations such as the General Data Protection Regulation (GDPR) [26][27].

To address these concerns, the following technical mitigation strategies are recommended for future iterations of the system. First, storing only hashed identifiers on-chain. Rather than recording personally identifiable information (PII) directly on the blockchain, only cryptographic hashes of certificate holder identifiers (e.g., SHA-256 hashes of student IDs or email addresses) should be stored on-chain. This approach preserves the ability to verify certificate authenticity by hash comparison without exposing the underlying personal data on the public ledger.

Second, maintaining sensitive metadata off-chain. Detailed certificate information, including the certificate holder's full name, date of birth, and institutional affiliation, should be stored in the off-chain PostgreSQL database or on a decentralized storage platform such as IPFS with access control mechanisms. The on-chain NFT metadata would then contain only a reference pointer (e.g., an IPFS content identifier or API endpoint) rather than the sensitive data itself. Access to the off-chain data can be restricted through authentication and role-based authorization. Third, implementing selective disclosure and encrypted metadata. Future versions of the system could adopt selective disclosure protocols, enabling certificate holders to share only specific credential attributes (e.g., degree title and issuing institution) without revealing all stored data. Additionally, sensitive metadata fields could be encrypted before storage, with decryption keys shared only with authorized verifiers. This approach aligns with emerging standards in verifiable credentials and self-sovereign identity frameworks.

Despite its contributions, this study has several limitations that should be acknowledged. These limitations are organized into methodological, technical, and ecosystem-related categories. Purposive sampling was used to choose the relatively small sample of 30 participants for the user evaluation, which was carried out among the researchers' academic and professional networks. The recruitment strategy and sample size may introduce selection bias because the participants were selected from a specific professional community (college students, software engineers, and UI/UX designers) rather than from a representative population of potential end users, such as university registrars or human resources professionals. As a result, the user evaluation results have limited generalizability to larger populations; therefore, future research should take into account bigger, more varied samples using stratified or randomized sampling techniques.

The functional testing and gas fee measurement were conducted on the NEAR testnet instead of the mainnet due to technological constraints. Although smart contract execution and gas calculations on the testnet are identical to those on the mainnet, there may be variations in network congestion, real-world gas price swings, and validator behavior. Consequently, it is important to consider the reported transaction costs as

VOL. 12. NO. 1 AUGUST 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v12i1.7685

approximations rather than final mainnet values, and further validation on the NEAR mainnet would be necessary for production deployment. Furthermore, the current system design stores certificate metadata, including the certificate title and description, as part of the NFT metadata on the public blockchain. As discussed in the privacy mitigation section, this poses privacy risks, as any network participant can access on-chain data. While no sensitive PII is stored directly on-chain in the current implementation, the certificate title and associated course information may still constitute indirect identifiers when combined with other publicly available data.

Regarding ecosystem-related limitations, the NEAR Protocol is a relatively newer blockchain platform compared to Ethereum and therefore has a smaller developer ecosystem and community support.. This may result in fewer available resources, libraries, and third-party integrations [33], which may slow down the adoption and scalability of applications built on NEAR. Second, although NEAR provides lower transaction fees and easier access to testnet tokens, its long-term sustainability and network stability are still under observation [34], given the rapid changes in blockchain protocols. Third, while the protocol offers scalability through its sharding mechanism [18], it may still face interoperability challenges with other blockchain systems, potentially limiting the widespread recognition and verification of certificates outside the NEAR ecosystem [35].

These limitations highlight that although NEAR offers technical benefits for building blockchain-based academic certification systems, careful consideration must be given to its ecosystem maturity, adoption rate, and compatibility with existing industry standards [33][36]. Lastly, the structured interview feedback showed that although participants acknowledged the great value of blockchain-based certificate data's security, transparency, and immutability, some said that a blockchain-based academic certification system might not be urgently needed or a top priority just yet because they believed traditional certification procedures were still adequate for their present requirements. According to this research, institutional preparedness and awareness of blockchain technology may be just as important in determining user adoption as technical prowess.

CONCLUSION

In this study, the NEAR protocol is used to develop and construct a blockchain-based certificate issuance and verification system. This method addresses issues with traditional certificate administration, like counterfeiting and laborious manual verification, by utilizing blockchain's immutability, transparency, and decentralized trust. Iterative design, continuous feedback, and quicker requirement adaptation were made possible by the agile development technique, which was backed by UML and ER diagrams. A frontend web application, a backend REST API, and an NFT smart contract on NEAR make up the system's three primary parts. Functional and integration testing on the NEAR testnet confirmed successful execution of the core workflows, including certificate minting via the nft_mint function and on-chain verification without transaction failure. User evaluation results indicated strong positive responses across themes, with 80% (48/60) positive responses for intention to use, 81.11% (73/90) for technology acceptance, and 80% (48/60) for certificate data management and sharing. At the participant level, 24 of 30 respondents expressed willingness to use the proposed DApp system. Participants particularly valued the system's traceability and security, while also highlighting concerns related to privacy exposure and the complexity of wallet integration.

From a cost perspective, the NEAR-based implementation demonstrated lower estimated NFT minting fees compared with Ethereum and remained competitive with Solana, indicating its suitability for scalable academic credential deployment. Overall, this study contributes empirical evidence that NEAR can serve as a cost-efficient and developer-friendly alternative for blockchain-based academic certification systems. Based on the insights gathered, future improvements will focus on enhancing user onboarding, privacy controls, and the certification verification workflow; providing clearer in-application usage guidance; implementing search and filtering capabilities for certificate management; simplifying certificate token copying for verification purposes; and improving interoperability through cross-chain verification support or alignment with W3C Verifiable Credentials standards.

REFERENCE

[1] A. kareem and A. C. Shakir, "Review: Verification Process of Academic Certificates Using Blockchain Technology.," *Kirkuk University Journal-Scientific Studies*, vol. 18, no. 1, pp. 62–75, Mar. 2023, doi: 10.32894/kujss.2023.135876.1072.

[2] S. H. Said, M. A. Dida, E. M. Kosia, and R. S. Sinde, "A Blockchain-based Conceptual

Model to Address Educational Certificate Verification Challenges in Tanzania," *Engineering, Technology and Applied Science Research*, vol. 13, no. 5, pp. 11691–11704, Oct. 2023, doi: 10.48084/etasr.6170.

[3] A. de Alwis, A. Shrestha, and T. Sarker, "Exploring Governance for accreditation in the education sector using blockchain technology: a systematic literature review," *Discover Education*, vol. 4, no. 1, p. 57, Dec. 2025, doi: 10.1007/s44217-025-00449-y.

[4] M. Alghamdi *et al.*, "Federated deep blockchain-based system for secure verification of academic transcripts and matching study plans in Saudi universities," *Sci. Rep.*, vol. 16, no. 1, p. 13845, Dec. 2026, doi: 10.1038/s41598-026-43328-8.

[5] A. Razaque *et al.*, "An anti-corruption system for academic achievement verification in kazakhstani higher education using blockchain and artificial intelligence," *Frontiers in Blockchain*, vol. 8, p. 1683522, 2025, doi: 10.3389/fbloc.2025.1683522.

[6] M. A. C. Quispe and A. Pacheco, "Blockchain ensuring academic integrity with a degree verification prototype," *Sci. Rep.*, vol. 15, no. 1, p. 9281, Dec. 2025, doi: 10.1038/s41598-025-93913-6.

[7] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey," *IEEE Trans. Industr. Inform.*, vol. 17, no. 1, pp. 3–19, Jan. 2021, doi: 10.1109/TII.2020.2998479.

[8] A. Punia, P. Gulia, N. S. Gill, E. Ibeke, C. Iwendi, and P. K. Shukla, "A systematic review on blockchain-based access control systems in cloud environment," *Journal of Cloud Computing*, vol. 13, no. 1, p. 146, Dec. 2024, doi: 10.1186/s13677-024-00697-7.

[9] S. Zafar, K. M. Bhatti, M. Shabbir, F. Hashmat, and A. H. Akbar, "Integration of Blockchain and Internet of Things: Challenges and Solutions," *Annales des Telecommunications/Annals of Telecommunications*, vol. 77, no. 1–2, pp. 13–32, Feb. 2022, doi: 10.1007/s12243-021-00858-8.

[10] M. Tota and S. Karmore, "IBMESR: Towards next-generation big data security with integrated blockchain model for efficient, scalable, and robust operations," *Blockchain: Research and Applications*, vol. 7, p. 100337, 2025, doi: 10.1016/j.bcra.2025.100337.

[11] M. Krichen, M. Ammi, A. Mihoub, and M. Almutiq, "Blockchain for Modern Applications: A Survey," *Sensors*, vol. 22, no. 14, p. 5274, Jul. 2022, doi: 10.3390/s22145274.

[12] M. Rifat Hossain, F. A. Nirob, A. Islam, T. M. Rakin, and M. Al-Amin, "A Comprehensive Analysis of Blockchain Technology and Consensus Protocols Across Multilayered Framework," *IEEE Access*, vol. 12, pp. 63087–63129, 2024, doi: 10.1109/ACCESS.2024.3395536.

[13] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing," *Future Internet*, vol. 14, no. 11, p. 341, Nov. 2022, doi: 10.3390/fi14110341.

[14] S. Suwarno, M. Siahaan, and V. Lim, "A Comparative Analysis of the Effectiveness of Hash-Chain-Based and Traditional Logging Audit Trail Systems in Detecting Data Manipulation," *JOIV: International Journal on Informatics Visualization*, vol. 10, no. 4, pp. 1417–1424, Jul. 2026, doi: 10.62527/joiv.10.4.4749.

[15] A. G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, "Emerging Trends in Blockchain Technology and Applications: A Review and Outlook," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 9, pp. 6719–6742, Oct. 2022, doi: 10.1016/j.jksuci.2022.03.007.

[16] S. Pathak, V. Gupta, N. Malsa, A. Ghosh, and R. N. Shaw, "Smart Contract for Academic Certificate Verification Using Ethereum," in *Advanced Computing and Intelligent Technologies: Proceedings of ICACIT 2022*, Springer Science and Business Media Deutschland GmbH, 2022, pp. 369–384. doi: 10.1007/978-981-19-2980-9_29.

[17] B. M. Nguyen, T. C. Dao, and B. L. Do, "Towards a Blockchain-Based Certificate Authentication System in Vietnam," *PeerJ Comput. Sci.*, vol. 6, p. e266, 2020, doi: 10.7717/peerj-cs.266.

[18] L. M. J. D. Torre, R. V. M. Mengoy, R. E. E. Quindoza, N. J. S. Tamondong, and O. D. Tubola, "PUPVOTE: Blockchain-Based Voting System Using NEAR Protocol," in *13th International Conference on Information and Communication Technology Convergence (ICTC)*, IEEE Computer Society, 2022, pp. 1127–1132. doi: 10.1109/ICTC55196.2022.9952594.

[19] R. Sharma, S. Srivastava, A. K. Gaur, S. Chaurasia, and A. Malik, "Solana, Avalanche, and NEAR Protocol: The Next Generation of

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 12. NO. 1 AUGUST 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v12i1.7685

Blockchain Platforms," *Eur.Chem.Bull*, vol. 12, pp. 6102–6110, 2023, doi: 10.48047/ecb/2023.12.si8.518.

[20] W. Behutiye, N. Tripathi, and M. Isomursu, "Adopting Scrum in Hybrid Settings, in a University Course Project: Reflections and Recommendations," *IEEE Access*, vol. 12, pp. 105633–105650, 2024, doi: 10.1109/ACCESS.2024.3434662.

[21] Y. Christian, M. Siahaan, and H. Hansvirgo, "Designing a Web-Based Light Novel Application with an LLM-Powered Chatbot Recommendation System Using Scrum Methodology," *METHOMIKA Jurnal Manajemen Informatika dan Komputerisasi Akuntansi*, vol. 8, no. 2, pp. 174–186, Oct. 2024, doi: 10.46880/jmika.Vol8No2.pp174-186.

[22] J. W. Kim, S. J. Kim, W. C. Cha, and T. Kim, "A Blockchain-Applied Personal Health Record Application: Development and User Experience," *Applied Sciences (Switzerland)*, vol. 12, no. 4, p. 1847, Feb. 2022, doi: 10.3390/app12041847.

[23] S. Pu and J. S. L. Lam, "The Benefits of Blockchain for Digital Certificates: A Multiple Case Study Analysis," *Technol. Soc.*, vol. 72, p. 102176, Feb. 2023, doi: 10.1016/J.TECHSOC.2022.102176.

[24] M. Alshamsi, M. Al-Emran, and K. Shaalan, "A Systematic Review on Blockchain Adoption," *Applied Sciences (Switzerland)*, vol. 12, no. 9, p. 4245, May 2022, doi: 10.3390/app12094245.

[25] A. Alrehaili, M. White, and N. Beloff, "Empowering the adoption of blockchain-based cryptocurrency as a payment method: A user-friendly educational approach," *IET Blockchain*, vol. 5, no. 1, p. e70002, Jan. 2025, doi: 10.1049/blc2.70002.

[26] A. Gómez Vieites, C. Delgado-von-Eitzen, and D. Estévez Garcia, "GDPR-Compliant Academic Certification via Blockchain: Legal and Technical Validation of the GAVIN Project," *Applied Sciences (Switzerland)*, vol. 15, no. 16, p. 9191, Aug. 2025, doi: 10.3390/app15169191.

[27] R. Belen-Saglam, E. Altuncu, Y. Lu, and S. Li, "A Systematic Literature Review of the Tension Between the GDPR and Public Blockchain Systems," *Blockchain: Research and Applications*, vol. 4, no. 2, p. 100129, Jun. 2023, doi: 10.1016/J.BCRA.2023.100129.

[28] A. Musamih, I. Yaqoob, K. Salah, R. Jayaraman, M. Omar, and S. Ellahham, "Using NFTs for Product Management, Digital Certification, Trading, and Delivery in the Healthcare Supply Chain," *IEEE Trans. Eng. Manag.*, vol. 71, pp. 4480–4501, 2024, doi: 10.1109/TEM.2022.3215793.

[29] K. A. R. Artha, S. N. Zain, A. A. Alkautsar, and M. H. Widianto, "Implementation of Smart Contracts for E-Certificate as Non-Fungible Token using Solana Network," in *Proceedings of the 2022 IEEE 7th International Conference on Information Technology and Digital Applications, ICITDA 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1–6. doi: 10.1109/ICITDA55840.2022.9971423.

[30] S. K. Kim, "Blockchain Smart Contract to Prevent Forgery of Degree Certificates: Artificial Intelligence Consensus Algorithm," *Electronics (Switzerland)*, vol. 11, no. 14, p. 2112, Jul. 2022, doi: 10.3390/electronics11142112.

[31] S. Kishore, J. Chan, U. P. Muthupoltotage, N. Young, and D. Sundaram, "Blockchain-Based Micro-Credentials: Design, Implementation, Evaluation and Adoption," in *Hawaii International Conference on System Sciences*, 2021, pp. 6846–6854. doi: 10.24251/hicss.2021.821.

[32] S. Metin and C. Özturan, "Max–Min Fairness Based Faucet Design for Blockchains," *Future Generation Computer Systems*, vol. 131, pp. 18–27, Jun. 2022, doi: 10.1016/J.FUTURE.2022.01.008.

[33] S. S. Mafike and T. Mawela, "An enterprise framework for blockchain interoperability," *Electronic Markets*, vol. 36, no. 1, p. 14, Dec. 2026, doi: 10.1007/s12525-025-00869-6.

[34] M. Thanasi-Boçe and J. Hoxha, "Blockchain for Sustainable Development: A Systematic Review," *Sustainability (Switzerland)*, vol. 17, no. 11, p. 4848, Jun. 2025, doi: 10.3390/su17114848.

[35] A. A. Alzahrani *et al.*, "A Comprehensive Review of Interoperability Challenges and Applications Beyond Cryptocurrencies," *Advances in Artificial Intelligence and Machine Learning*, vol. 5, no. 1, pp. 3373–3388, 2025, doi: 10.54364/AAIML.2025.51193.

[36] M. Jovanovic, N. Kostić, I. M. Sebastian, and T. Sedej, "Managing a Blockchain-Based Platform Ecosystem for Industry-Wide Adoption: The Case of Tradelens," *Technol. Forecast. Soc. Change*, vol. 184, p. 121981, Nov. 2022, doi: 10.1016/j.techfore.2022.121981.