Available online at
https://jcrinn.com/
https://crinn.conferencehunter.com/

Journal of Computing Research and Innovation 11 (1) 2026

Journal of Computing Research and Innovation

NFT-Based Authentication in Education: ERC-721 Token Use for Moodle LMS Security and Credentialing

Danang H B Saputro[1*], Noor A Setiawan[2], Azkario R Pratama[3], Avinanta Tarigan[4]

[1,2,3]*Dept. of Electrical and Information Engineering, Universitas Gadjah Mada, D. I. Yogyakarta, Indonesia.*
[4]*Dept. of Computer System, Gunadarma University, Jawa Barat, Indonesia.*

ARTICLE INFO

Article history:
Received 6 November 2025
Revised 1 January 2026
Accepted 23 February 2026
Online first
Published 1 March 2026

Keywords:
Blockchain
Decentralized Authentication
NFT Identity
E-Learning

DOI:
10.24191/jcrinn.v11i1.622

ABSTRACT

The increasing adoption of blockchain technology in education has introduced alternative approaches to identity verification beyond centralized credential systems. This study proposes and implements a decentralized authentication mechanism for Moodle LMS using ERC-721 non-fungible tokens (NFTs) verified through MetaMask. Developed as a proof-of-concept following a design science methodology, the system links on-chain identity tokens to Moodle accounts without storing usernames or passwords. The architecture integrates Ethereum smart contracts, nonce-based digital signature verification, and Moodle's Role-Based Access Control (RBAC) framework. Functional testing confirms that access is granted exclusively to users possessing valid ERC-721 tokens and verified wallet signatures. Replay attack simulations demonstrate effective resistance through nonce validation, while ensuring that no sensitive credential data is exposed during the authentication process, in contrast to default Moodle login mechanisms. Performance evaluation using Apache JMeter indicates stable operation under moderate loads. Although scalability and token management limitations remain, the results demonstrate the technical feasibility and enhanced security advantages of NFT-based authentication for learning management systems.

1. INTRODUCTION

Learning Management Systems (LMS) like Moodle have become central to digital education by supporting content delivery, instructor-student interaction, and online assessments (Wang et al., 2020). Traditional LMS authentication methods typically rely on centralised credential storage, which introduces a single point of failure and creates vulnerabilities related to unauthorised access, privacy breaches, and data tampering (Pal, 2020). Centralised systems also raise concerns about long-term scalability and institutional trust (Bashir, 2017).

[1*] Corresponding author. *E-mail address*: dananghandokobelutsaputro@mail.ugm.ac.id

https://doi.org/10.24191/jcrinn.v11i1.622

Blockchain technology, as a distributed ledger system, provides a promising alternative by decentralising identity management and eliminating reliance on centralised authorities (Ramasamy & Khan; 2024). Non-fungible tokens (NFTs) based on the ERC-721 standard offer a secure way to represent user identities as unique, tamper-proof digital assets. When paired with cryptographic wallets like MetaMask, these identities can be authenticated through digital signatures, replacing the need for conventional username-password mechanisms (Paul et al., 2022). This type of token-based authentication has been shown to be more secure and efficient than older methods (Karataş, 2018).

Several studies have explored blockchain applications in educational contexts; however, they fall short of implementing decentralised authentication workflows, particularly on platforms like Moodle. The limitations of selected blockchain-based educational systems are summarised in Table 1, highlighting the absence of decentralised authentication mechanisms integrated directly into Moodle.

Table 1. Comparison of prior blockchain-based educational systems and their authentication limitations

Study	Approach	Key Limitation
Karataş (2021)	SCORM data integrated with Moodle and stored on blockchain	No support for decentralized authentication or access control
Chukowry et al. (2022)	Smart contract based digital badges for achievement validation	Not integrated with Moodle; no login or access authorization
Leka et al. (2020)	Digital certification using Ethereum and IPFS	No LMS integration; lacks token-based access management
Baldi et al. (2019)	Public Key Infrastructure (PKI)-based digital certificates	Still centralized; does not implement tokenized access in LMS

The gap in existing research reveals that, while blockchain-based credential verification has gained attention, decentralised authentication, particularly using ERC-721 tokens natively integrated into the Moodle LMS, remains underexplored. To the best of our knowledge, no prior study has implemented a direct login mechanism that links on-chain identity to active LMS sessions. This research addresses that gap by introducing a decentralised authentication framework that integrates ERC-721 identity tokens with Moodle via MetaMask. This approach eliminates the need for centralised credential storage by leveraging Ethereum smart contracts for stateless user authentication while maintaining compatibility with Moodle's existing Role-Based Access Control (RBAC) model.

The study serves as a proof-of-concept (PoC) to evaluate the technical feasibility of NFT-based login systems within LMS environments. By combining these principles with blockchain-enabled identity verification, the proposed plugin offers a secure, user-controlled alternative to traditional login methods without compromising usability. Considering the increasing frequency of data breaches in educational institutions (Thennakoon, 2024) and the growing momentum behind self-sovereign identities, decentralised authentication systems have become both relevant and necessary. This study contributes a novel ERC-721-based login solution fully integrated into Moodle, offering a practical model for secure, privacy-preserving, and scalable user authentication in modern educational platforms.

2. METHODOLOGY

This section talks about the proposed decentralised login system's architecture, design rationale, and authentication workflow. The system uses MetaMask-enabled Ethereum authentication to connect ERC-721-based identity tokens with the Moodle LMS. The design focuses on making sure that Moodle's RBAC, stateless verification, and tamper-proof identity validation systems all work together.

https://doi.org/10.24191/jcrinn.v11i1.622

2.1 System design

The architecture of the decentralised authentication system, as illustrated in Fig. 1, is composed of interdependent components that operate across two primary domains: the blockchain environment and the Moodle environment. Each domain plays a specific role in enabling secure, token-based user login while maintaining interoperability with existing LMS infrastructure.

On the frontend, the login page of Moodle initiates the authentication sequence. When a user accesses the page, a unique cryptographic challenge (nonce) is generated and presented to the user via the MetaMask browser extension. MetaMask prompts the user to digitally sign the nonce using their private key. Upon successful signature, the interface displays the token ownership status and transmits the result to the server.

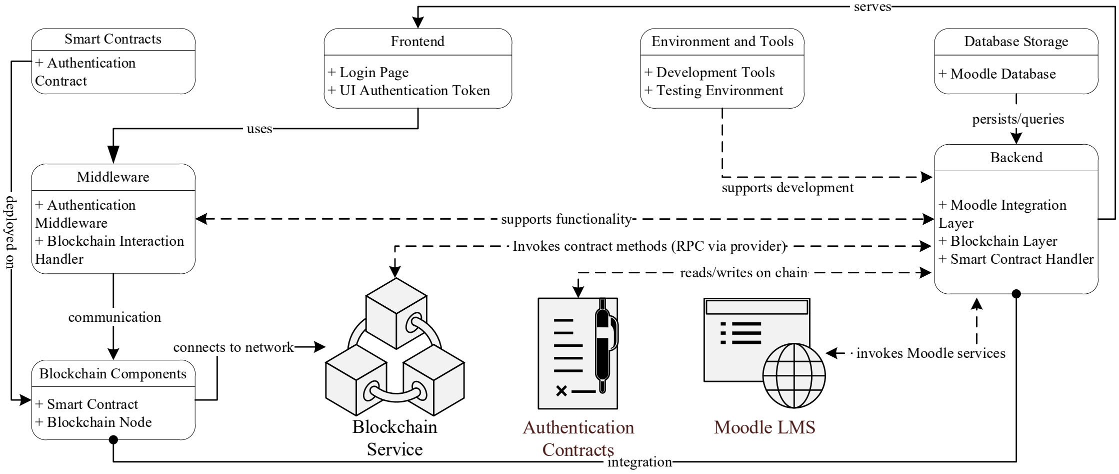

Fig. 1. Architecture of the ERC-721–based decentralized authentication system integrated with Moodle LMS.

This data is received by the middleware layer, which consists of two sub-components. The Authentication Middleware is responsible for validating the digital signature and enforcing security policies, while the Blockchain Interaction Handler communicates with the deployed smart contract through standard Ethereum functions, such as ownerOf() and balanceOf(). These interactions are facilitated by a provider (e.g., Alchemy or Infura), and, if necessary, the system subscribes to on-chain events such as Transfer to monitor changes in token ownership.

At the backend, the system includes three layers: the Moodle Integration Layer, the Blockchain Layer, and the Smart Contract Handler. These components collectively bind the verification result to an existing Moodle user account, establish a session, and apply RBAC based on the Moodle capabilities system. In the event of token transfer, the backend is designed to detect and re-bind the new token holder appropriately.

The smart contract, deployed on the Ethereum Sepolia testnet, manages the issuance and validation of User Identity Tokens conforming to the ERC-721 standard. Each token is associated with user-specific metadata, accessible via the tokenURI function. These tokens are inherently non-transferable unless explicitly allowed by the system design, ensuring strong binding between user identity and token ownership.

The Moodle database functions as the source of user and role-based information, which is utilized for mapping the user's id and the identity token's metadata payload.

https://doi.org/10.24191/jcrinn.v11i1.622

Finally, the environment and tooling layer provides the necessary configuration for development, testing, and deployment. This includes access to the Sepolia test network, API keys for blockchain gateways, and test harnesses to automate and validate system behaviour under various conditions

2.2 Authentication Workflow

The authentication process, as shown in Fig. 2, begins when the user accesses the Moodle login page through a web browser. The interface component then triggers a request to connect a digital wallet via the MetaMask extension. Once the user grants consent, the authorised wallet address is returned to the frontend component as an initial cryptographic identifier for subsequent validation.

The next stage involves communication between the frontend and the middleware. The frontend transmits the wallet address (and, when available, the token identifier) to the backend service. The middleware then invokes a Web3 library to interact with an Ethereum node and the ERC-721 smart contract on the test network. Ownership validation is performed by reading on-chain state through function calls such as ownerOf(tokenId) or, alternatively, balanceOf(address) to confirm the presence of an identity token within the specified collection.

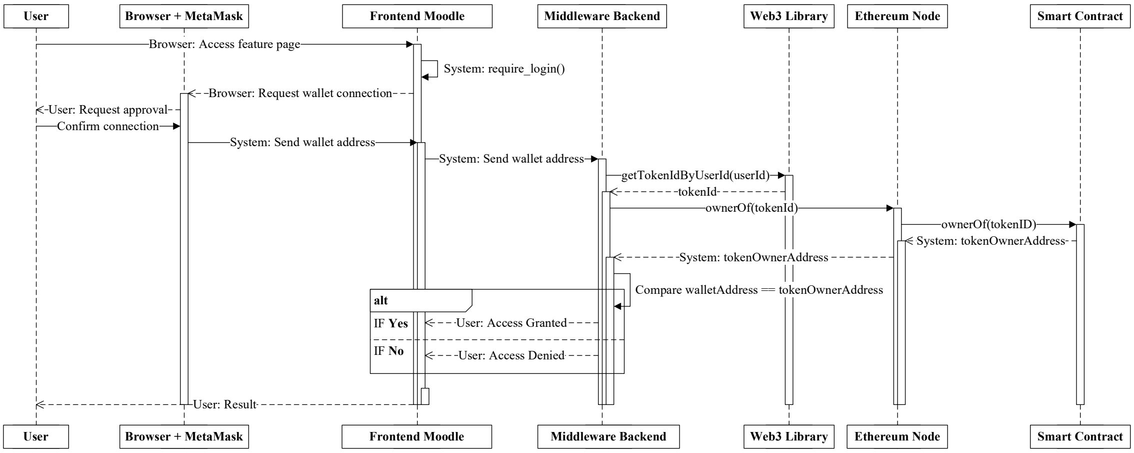

Fig. 1. Authentication workflow illustrating wallet connection, nonce signing, on-chain token verification, and session establishment.

The result on the chain is compared to the wallet address that was given at the start. If a match is confirmed, the middleware sends a success signal to the Moodle integration layer to start a session and grant access. On the other hand, access is denied if there is a mismatch or no token. To make security stronger, a production implementation should have a challenge-response system. In this system, the user signs a unique nonce, and then the backend checks the signature to stop address spoofing and replay attacks.

2.3 Plugin implementation

The Moodle plugin is implemented in PHP and comprises three core modules: login.php, which handles authentication requests; request_nonce.php, which generates and validates unique nonces; and web3p/web3.php, which provides the interface to the Ethereum blockchain. Client-side integration uses JavaScript and the Web3.js library to enable MetaMask interactions and signature generation. The backend verifies these signatures and cross-checks token data on the blockchain before granting access. The implementation of the plugin leverages the following development tools and environments: Ethereum Sepolia Testnet for blockchain interactions; Solidity v0.8.19 and Remix IDE for smart contract

https://doi.org/10.24191/jcrinn.v11i1.622

development and deployment; Moodle 4.1 (PHP 8.1) for the LMS platform; and the MetaMask browser extension for client-side wallet management.

2.4 Integration with Moodle RBAC

While authentication is conducted on-chain, role assignment continues to be managed by Moodle. After successful login, user roles such as "student" or "teacher" are assigned based on Moodle's internal metadata. This hybrid design maintains compatibility with existing LMS role structures while benefiting from the added security of blockchain-based verification.

The integration flow with Moodle's RBAC, depicted in Fig. 3, begins by establishing the user's Moodle context. Each user (e.g., Bob as a student and Jane as a teacher) authenticates through the Ethereum-based login operation, which includes MetaMask sign-in and identity-token validation. After successful validation, an access-permission signal is issued to Moodle. Moodle's RBAC maps the verified wallet address to the corresponding Moodle identity and evaluates role assignments and capabilities according to institutional policy. If policy evaluation succeeds, Moodle establishes an application session and performs a completion check to confirm that required conditions are met (e.g., account status and course enrolment). When the check passes, the system routes the user to the role-appropriate dashboard (Student Dashboard for Bob and Teacher Dashboard for Jane); otherwise, access is denied, and the flow terminates.

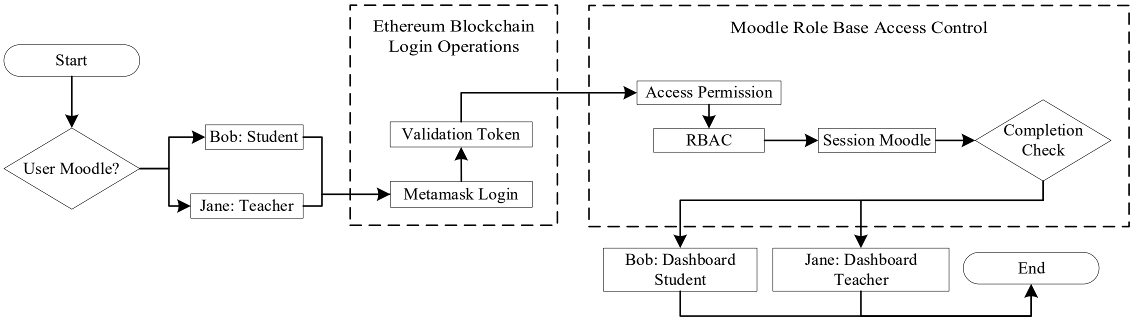

Fig. 2. Integration Flow between Ethereum-based authentication and RBAC

2.5 Smart contract

The system's backbone is a smart contract written in Solidity and deployed on the Ethereum Sepolia testnet using the Remix IDE. It adheres to the ERC-721 specification and provides token issuance through a custom minting function. Listing 1 illustrates the token minting function used for user identity binding.

Listing 1: ERC-721 token minting function for user identity binding

```
function mintTo(address recipient, string memory userId) public {
  _nextTokenId++;
  _safeMint(recipient, _nextTokenId);
    userIds[_nextTokenId] = userId;
    userIdToTokenId[userId] = _nextTokenId;
}
```

https://doi.org/10.24191/jcrinn.v11i1.622

This design maintains an immutable and verifiable link between user identities and their ERC-721 tokens by verifying on-chain ownership at login and updating the off-chain binding based on contract events.

2.6 Design evaluation approach

To ensure that the developed authentication plugin fulfils its intended objectives, this study adopts a structured evaluation strategy grounded in the principles of design science research. In particular, the evaluation phase aligns with the framework proposed by Hevner et al. (2004), which emphasizes the need to rigorously demonstrate the utility, quality, and effectiveness of technological artifacts through both empirical and analytical methods.

The evaluation criteria in this study encompassed functionality, performance, security, and integration compatibility with the existing LMS infrastructure. A combination of methods was employed to assess the artefact across these dimensions. Functional testing (black-box) was conducted to verify the correctness of the authentication process, ensuring that access was granted exclusively to users possessing valid ERC-721 tokens. Performance benchmarking was performed using Apache JMeter to simulate concurrent login attempts and evaluate system scalability, latency, and error rates. Security testing included replay attack simulations conducted with Fiddler Classic, which analysed HTTP Archive (HAR) logs by resubmitting previously signed nonces to assess the system's ability to detect and prevent session hijacking. Finally, descriptive evaluation was performed through informed argumentation, offering justification for architectural decisions such as the use of Ethereum smart contracts and MetaMask integration based on supporting literature.

These multi-method evaluation strategies reflect the iterative and incremental nature of design science, whereby feedback from each assessment cycle informs artifact refinement. By integrating both empirical validation and theoretical justification, this study ensures that the developed authentication system is not only technically viable but also contextually grounded and aligned with practical implementation needs in educational environments.

3. IMPLEMENTATION AND RESULT

The smart contract was deployed on the Sepolia network. Identity tokens were issued to test accounts via the minting function. A nonce-based login interface was integrated directly into Moodle's login system, allowing users to be authenticated through MetaMask instead of traditional passwords.

After verifying the digital signature and confirming token ownership, the plugin mapped Ethereum addresses to corresponding Moodle user IDs, granting access based on Moodle's native RBAC. This integration ensured backward compatibility with existing course and user management features. As shown in Listing 2, the client retrieves and signs a nonce for authentication.

Listing 2: MetaMask-based login with ERC-721 token verification

```
metamaskButton.addEventListener('click', async () => {
    if (typeof window.ethereum !== 'undefined') {
      const provider = new ethers.providers.Web3Provider(window.ethereum);
      await provider.send("eth_requestAccounts", []);
       const signer = provider.getSigner();
       const wallet = await signer.getAddress();

 // Step 1: Request nonce from server
```

```
        const {nonce}= await (await fetch(
`${M.cfg.wwwroot}/local/token_auth/request_nonce.php?wallet=   ${wallet}`
   )).json();

 // Step 2: User signs nonce
        const signature = await signer.signMessage(nonce);

 // Step 3: Send signature to server for verification
        await fetch(`${M.cfg.wwwroot}/local/token_auth/login.php`, {
        method: 'POST',
        headers: { 'Content-Type': 'application/json' },
        body: JSON.stringify({ wallet, signature })
      });
   }
});
```

The plugin was evaluated to determine its ability to authenticate users through ownership of ERC-721 identity tokens, and the results of these test scenarios are presented in Table 2. Test scenarios were designed to simulate various combinations of user credentials and digital signatures, representing potential real-world login attempts. As presented in Table 2, the system consistently verified token presence and matched signatures to confirm identity before granting access. Only users possessing both a valid ERC-721 token and a verified wallet signature were granted access. In contrast, attempts without tokens or with unmatched credentials were accurately rejected. These results confirm the plugin's effectiveness in enforcing token-bound access control and upholding the intended security policy.

Table 2. Functional authentication testing results for ERC-721 token and signature verification scenarios

No	User Category	Token ID	Wallet Owner	Verification Result
1	Possesses Identity Token (ERC-721)	Detected	Detected	Access Granted
2	Does Not Possess Identity Token (ERC-721)	Not Detected	Not Processed	Access Denied
3	Valid Signature but No Token	Not Detected	Not Processed	Access Denied

3.1 Replay attack resistance evaluation

Replay attack resilience was evaluated by resubmitting previously signed nonces to both the plugin endpoint and Moodle's default login (/login/index.php). Testing was conducted using Fiddler Classic with HAR log inspection. The replay attack evaluation results are presented in Table 3, which show that the plugin consistently returned HTTP 400 (Bad Request) when reused nonces were submitted, effectively rejecting reused nonces and preventing session hijacking. Moreover, login via the plugin did not expose any user credentials in the request or response payloads. In contrast, the default Moodle login returned HTTP 303 and revealed sensitive data, including the plaintext username and password, within the HTTP headers and body. This result confirms that the plugin offers a more secure and privacy-preserving authentication mechanism. As shown in Table 3, the plugin consistently rejected reused nonces, whereas the default login system permitted partial responses.

Table 3. Replay attack evaluation comparing default Moodle login and plugin-based authentication

No	Scenario	Endpoint/URL	Code Result	Description Result
1	Moodle Default Login	/login/index.php	303	Allowed partial response; session data exposed (less secure)
2	Plugin-Based Login	/local/plugin/login.php	400	Rejected reused nonce; preserving data confidentiality (secure)

https://doi.org/10.24191/jcrinn.v11i1.622

These results demonstrate the plugin's superior resistance to replay attacks, preserving session confidentiality and mitigating credential reuse risks.

3.2 Performance Evaluation

Table 4. Performance Benchmarking Results Under Varying Ramp-Up Conditions Using Apache JMeter

No	Ramp Up	User	Latency (ms)	Error (%)	Throughput (request/s)
1	100	100	868	0.00%	0.99
2	90	100	880	0.00%	1.1
3	80	100	858	0.00%	1.2
4	70	100	856	0.00%	1.4
5	60	100	861	0.00%	1.6
6	50	100	863	0.00%	2.0
7	40	100	846	0.00%	2.5
8	30	100	870	0.00%	3.2
9	20	100	949	0.00%	4.8
10	10	100	1,352	30.00%	9.1

System scalability and responsiveness were evaluated using Apache JMeter. Login requests were simulated with a total of 100 users under varying ramp-up intervals (100, 90, ..., 10 seconds). Metrics observed included: Latency (average time per request), Throughput (requests per second), Error rate (failed attempts). These performance benchmarking results, as summarised in Table 4, illustrate how a reduced ramp-up time increases system strain, affecting both latency and reliability.

3.3 Discussion: Feasibility and limitations

This implementation confirms the technical feasibility of NFT-based authentication within LMS environments. However, as a proof-of-concept, the system is not yet ready for large-scale deployment due to several limitations, including network latency, RPC bottlenecks, the lack of token revocation mechanisms, and reliance on third-party browser wallet extensions such as MetaMask. Future iterations should consider optimisations that enhance scalability, reliability, and user autonomy. Potential directions include implementing off-chain verification to minimise on-chain overhead, adopting rollup chains for improved transaction throughput, and integrating with Decentralised Identity (DID) frameworks to support more flexible, user-centric identity models that maintain usability while strengthening security.

4. CONCLUSIONS

This paper presents a novel decentralized authentication approach for Moodle LMS using ERC-721 NFTs verified via MetaMask. The proposed plugin eliminates centralized credential storage by linking user identity to on-chain tokens, thereby enhancing transparency, tamper resistance, and privacy-preserving authentication. As the first fully integrated ERC-721 login implementation for Moodle, the system demonstrates the architectural feasibility and functional soundness of blockchain-based identity management in educational platforms. Evaluation results indicate that the system functions correctly under moderate loads, maintaining stable throughput and a secure nonce-based login flow. Replay attack testing confirms improved security compared to default Moodle authentication, while performance metrics suggest suitability for small-scale deployments. However, limitations related to throughput, key management, and resilience against advanced threats highlight the need for further optimization before large-scale production adoption. Future work will focus on enhancing scalability through Layer-2 solutions, integrating decentralized identifiers (DIDs), and implementing token revocation or delegation mechanisms, guided by core principles of the Technology Acceptance Model (TAM), particularly perceived usefulness and ease of use, to support future usability testing and long-term adoption in real educational environments.

5. ACKNOWLEDGEMENTS

The authors gratefully acknowledge Universiti Teknologi MARA (UiTM), Malaysia, for providing publication support for this work.

6. CONFLICT OF INTEREST STATEMENT

The authors declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

7. AUTHORS' CONTRIBUTIONS

Danang H. B. Saputro: Conceptualisation, methodology, formal analysis, investigation, software development, and writing-original draft; **Noor A. Setiawan**: Conceptualisation, supervision, and validation; **Azkario R. Pratama**: Supervision, writing-review and editing, and validation; **Avinanta Tarigan**: Supervision, validation, and writing-review and editing.

8. REFERENCES

Baldi, M., Chiaraluce, F., Kodra, M., & Spalazzi, L. (2019). Security analysis of a blockchain-based protocol for the certification of academic credentials. *arXiv preprint arXiv:1910.04622*. https://doi.org/10.48550/arXiv.1910.04622

Bashir, I. (2017). *Mastering blockchain: Deeper insight into decentralization, cryptography, Bitcoin, and popular blockchain frameworks*. Packt Publishing Limited.

Chukowry, V., Nanuck, G., & Sungkur, R. K. (2021). The future of continuous learning – Digital badge and microcredential system using blockchain. *Global Transitions Proceedings*, *2*, 248–253. https://doi.org/10.1016/j.gltp.2021.08.026

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Karataş, E. (2018). Developing Ethereum blockchain-based document verification smart contract for Moodle Learning Management System. *Gazi University Journal of Science Part B: Art, Humanities, Design and Planning*, *6*(4), 399–406. https://doi.org/10.17671/GAZIBTD.452686

Leka, E., & Selimi, B. (2021). Development and evaluation of blockchain-based secure application for verification and validation of academic certificates. *Advances in Emerging Technology and Innovation*, *5*(2), 1–10. https://doi.org/10.33166/AETIC.2021.02.003

Pal, N. (2020). *The emergence of decentralized web in the education field: A case study on challenges of learning systems based on decentralized learning model* [Master's thesis, Uppsala University].

Paul, P., Aithal, P. S., & Saavedra Marroquin, M. (2022). Blockchain in educational development: Potentialities and issues—Towards sophisticated digital education systems. *International Journal of Applied Sciences and Engineering (IJASE)*, *11*(2), 1–12. http://dx.doi.org/10.2139/ssrn.4400249

Ramasamy, L. K., & Khan, F. (2024). *Blockchain for global education* (1st ed.). Springer Cham. https://doi.org/10.1007/978-3-031-52123-2

https://doi.org/10.24191/jcrinn.v11i1.622

Sporny, M., Longley, D., & Chadwick, D. (2025). *Verifiable credentials data model v1.1: W3C Recommendation*. World Wide Web Consortium. https://www.w3.org/TR/vc-data-model-1.1/

Thennakoon, N. S. (2024). Leveraging blockchain technology to enhance the security of educational credentials in e-learning systems. *International Journal of Innovative Science and Research Technology (IJISRT)*, *9*(11), 707–712. https://doi.org/10.38124/ijisrt/ijisrt24nov638

Wang, X., Chen, W., Qiu, H., Eldurssi, A., Xie, F., & Shen, J. (2020). A survey on the e-learning platforms used during COVID-19. In *2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (pp. 808–814). IEEE. https://doi.org/10.1109/IEMCON51383.2020.9284840