Mrs. Vidhya Rani M, 2026, 14:1
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Comprehensive Literature Review on Block Chain Enabled Deep Learning Frameworks for Smart Learning Environments

[1]Mrs. Vidhya Rani M, [2]Dr. Vijayalakshmi S

[1]Ph.D Research Scholar, Department of computer science Sri Ramakrishna College of Arts and Science for Women Coimbatore, Tamil Nadu, India.

[2]HoD CSDA, Department of computer science Sri Ramakrishna College of Arts and Science for Women Coimbatore, Tamil Nadu, India.

Abstract- The integration of Blockchain Technology (BCT) and Deep Learning (DL) has emerged as a transformative approach to addressing the challenges of data security, transparency, and personalization in smart learning environments (SLEs). Blockchain provides decentralized, tamper-proof storage of learner records and ensures data authenticity, while deep learning offers powerful predictive analytics for personalized and adaptive education. This paper presents a literature review on blockchain-enabled deep learning frameworks in education, examining recent advances, architectural models, and practical implementations. The review highlights how existing studies have applied blockchain for credential verification, secure content sharing, and distributed trust management, while deep learning techniques have been employed for student performance prediction, intelligent tutoring, and adaptive feedback. Despite these advancements, significant research gaps remain, particularly in the areas of real-time deployment, scalability, latency, interoperability across institutions, and privacy-preserving learning analytics. By systematically analyzing current trends, this review identifies open challenges and future directions for developing efficient, secure, and scalable blockchain.DL frameworks tailored to smart learning environments.

Keywords - blockchain, deep learning, federated learning, smart learning, credentialing, privacy, Latency.

I. INTRODUCTION

Smart learning environments (SLEs) are reshaping education by integrating intelligent analytics, secure content sharing, and adaptive personalized learning. However, challenges such as data privacy, trust, and interoperability persist. Recently, the convergence of Blockchain Technology (BCT) and Deep Learning (DL) has been proposed as a promising solution, offering decentralized trust management along with predictive intelligence.

Shafay et al. [1] examined the integration of blockchain with deep learning and identified open research challenges in ensuring model integrity and decentralized coordination. Ning et al. [2] presented a comprehensive taxonomy of blockchain-based federated learning (BC-FL) architectures, categorizing coordination mechanisms and smart contract governance models. Yurdem et al. [3] reviewed federated learning techniques and emphasized privacy preservation benefits relevant to education systems.

Ouf et al. [4] introduced a blockchain-supported deep learning framework for smart learning environments, combining immutable credential storage with predictive analytics for student performance monitoring. Together, these studies establish the conceptual foundation for blockchain-enabled intelligent educational infrastructures. Recent research emphasizes the integration of blockchain-based decentralized storage with deep learning-driven analytics for applications such as student performance prediction, plagiarism detection, automated assessment, secure content management, and personalized learning pathways.

However, the majority of existing approaches remain at the conceptual or experimental stage, with limited deployment in real-world learning environments. Key challenges include ensuring low-latency data access, scalability of blockchain systems, computational efficiency of DL models, and cross-institutional interoperability.

Therefore, this literature review critically examines A Blockchain-Based Deep Learning Framework for Smart Learning Environments (2025) and related research. It provides an overview of existing frameworks, identifies their strengths and limitations, and highlights research gaps that must be addressed to realize fully functional, scalable, and secure blockchain-DL-powered educational systems.

Blockchain-Based Credential Verfication

Ensuring authenticity of academic credentials represents one of the earliest applications of blockchain in education. Credential security is a foundational application.

Blockchain has been extensively explored for academic credential verification. Alsobhi et al. [5] developed a blockchain-based microcredentialing framework ensuring immutable academic badge issuance and preventing certificate forgery. Ullah et al. [6] analyzed blockchain adoption in smart learning environments through an extended technology acceptance model, highlighting institutional readiness factors. Li et al. [7] conducted a comprehensive survey of blockchain-based federated learning systems, emphasizing decentralized trust mechanisms. Cardenas-Quispe et al. [8] proposed a blockchain prototype for secure academic degree issuance, demonstrating tamper-resistant verification workflows.

Zhang et al. [9] investigated deep learning applications in decentralized systems, illustrating the feasibility of integrating intelligent analytics within distributed environments. Kumar et al.

[20] further demonstrated practical academic credential verification using blockchain technology to reduce validation time and eliminate fraudulent alterations.

While these systems enhance authenticity and transparency, they typically operate independently of predictive intelligence modules.

Overview of Blockchain and Deep Learning Integration in Education

Recent advancements have highlighted the potential of combining blockchain technology (BCT) and deep learning (DL) to address challenges in educational environments, including data security, transparency, and personalized learning mechanisms. Ouf et al. [4] proposed a framework integrating blockchain with deep learning to enhance e-learning systems by ensuring secure data storage and accurate student performance prediction. Their architecture demonstrates how decentralized ledgers can be combined with neural networks to create intelligent and tamper-resistant academic ecosystems.

Blockchain-Based Frameworks in Smart Learning Environments

Several studies have explored the application of blockchain technology in smart learning environments (SLEs).

Ouf et al. [4] developed a framework utilizing an Ethereum private blockchain integrated with the InterPlanetary File System (IPFS) for decentralized learner data storage. Their approach ensures integrity and confidentiality through encrypted wallet mechanisms and distributed storage models.
Singh et al. [10] introduced a blockchain-based framework for secure knowledge transactions, incorporating immutable versioning systems that record all academic interactions. This mechanism enhances trust, traceability, and transparency in digital education processes by maintaining a tamper-resistant audit trail.

Deep Learning Applications in Smart Learning

Deep learning techniques have been widely employed to analyze learner behavior, predict academic performance, and support adaptive learning systems.

Shafay et al. [1] presented a thematic taxonomy of blockchain deep learning integration, covering blockchain types, deep learning architectures, key

service domains, and open research challenges. Their study emphasizes the importance of secure model training in decentralized environments.

Alsobhi et al. [5] investigated micro-credential management systems using blockchain, outlining the technical requirements for secure higher-education credentialing infrastructures.

Ullah et al. [6] applied the Technology Acceptance Model (TAM) to analyze blockchain adoption in smart learning environments, highlighting user perception, trust, and institutional readiness as critical adoption factors.

These studies collectively illustrate how deep learning models can be mapped to block chain-secured infrastructures to enhance intelligent academic services while preserving security.

Hybrid Blockchain and Deep Learning Frameworks

Integrating blockchain and deep learning offers a comprehensive and secure architecture for modern educational ecosystems.

Rakha et al. (2025) proposed a secured accreditation and equivalency certification system utilizing Merkle Mountain Range structures alongside transformer-based deep learning models to ensure data integrity and privacy. (If Rakha et al. is part of your reference list, assign the correct reference number accordingly. If not, it must be added properly to the reference list.) Ouf et al. [4] further demonstrated the integration of blockchain-based secure storage mechanisms with deep learning-based performance prediction, forming a unified smart learning framework that enhances reliability, automation, and transparency within e-learning systems.

Blockchain-Enabled Federated Learning

Federated learning enables collaborative model training across institutions without exchanging raw data. Liu et al. [10] analyzed blockchain-enabled federated learning mechanisms, emphasizing secure aggregation and malicious update detection. Aggarwal et al. [11] identified non-identically distributed (non-IID) data as a significant challenge affecting model convergence.

Ali et al. [12] proposed an edge–fog–cloud blockchain-integrated federated architecture to reduce latency and enhance resource allocation efficiency. Pandya et al. [13] examined scalability constraints in large-scale federated networks and highlighted communication overhead concerns.

These contributions demonstrate that BC-FL enhances trust and transparency but introduces additional computational and communication complexity.

Edge Computing and Intelligent SLE Architectures

Smart learning environments generate high-volume real-time data. Yurdem et al. (2024) emphasized edge intelligence to reduce network load and enhance privacy preservation in distributed learning systems [3]. Ouf et al. (2025) incorporated edge nodes for preprocessing student interaction data before federated aggregation to minimize communication overhead and improve scalability [4]. Alsobhi et al. (2023) suggested decentralized node management strategies to enable faster and more secure credential validation processes [5]. Edge-enabled architectures significantly improve real-time responsiveness; however, they require secure coordination mechanisms and well-defined governance frameworks to ensure system reliability.

Deep Learning and Attention-Based Distributed Models

Deep neural networks play a central role in predictive educational analytics. Alphonse et al.

[14] introduced an attention-integrated federated learning model capable of capturing multi-scale student behavior patterns across distributed datasets. Zheng et al. [15] proposed selective parameter update mechanisms to reduce communication overhead in attention-based federated systems.

Yoneda et al. [16] applied federated ranking techniques to detect at-risk students across institutions without compromising data privacy. These attention-driven distributed models

significantly improve prediction accuracy; however, they increase computational requirements and system complexity.

Blockchain-Based Credential Management

Blockchain-enabled credential systems are widely discussed as a foundational layer for smart learning ecosystems. Shafay et al. [1] state that integrating distributed ledgers with intelligent systems enhances data integrity and trust in decentralized applications. Alsobhi et al.

[5] explain that blockchain-based micro-credential frameworks improve transparency and reduce fraudulent certificate issuance by storing hashed academic records on-chain while maintaining detailed documents off-chain. Cardenas-Quispe et al. [8] demonstrate that degree issuance prototypes using consortium blockchains significantly reduce verification time compared to traditional manual processes. These studies collectively show that permissioned blockchains are preferred in academic contexts due to governance control and scalability considerations.

Federated Learning with Blockchain

Federated learning (FL) combined with blockchain is emerging as a dominant paradigm for privacy-preserving educational analytics. Ning et al. [2] argue that blockchain can securely coordinate federated aggregation by recording model updates immutably and preventing malicious participation. Liu et al. [10] further state that blockchain-enabled FL improves accountability and auditability in distributed training environments. Ullah et al. [6] emphasize that institutional trust increases when transparent consensus mechanisms are used in collaborative AI systems. These findings suggest that blockchain acts as a coordination and validation layer, while FL ensures student data remain locally stored.

Deep Learning for Student Performance Prediction

Deep learning models play a central role in smart learning analytics. Ouf et al. [4] report that hybrid blockchain–deep learning architectures can simultaneously support credential verification and performance forecasting with improved accuracy and reduced latency. Zhang et al. [9] note that neural network models, particularly recurrent and attention-based architectures, effectively capture temporal academic behavior. Li et al. [7] observe that integrating secure blockchain layers with deep models reduces risks of model tampering and adversarial interference. Collectively, these studies demonstrate that combining predictive intelligence with secure infrastructure enhances system reliability.

Edge Computing Integration

Edge-enabled blockchain frameworks reduce computational delay in smart learning systems. Aggarwal et al. [11] and Ali et al. [12] indicate that edge nodes can preprocess data and perform lightweight inference before interacting with blockchain networks. Such architectures minimize bandwidth usage and improve scalability in multi-institution deployments. Authors emphasize that hybrid edge–cloud models are particularly suitable for real-time educational analytics.

Security, Privacy, and Explainability Considerations

Security and privacy remain central design challenges. Shafay et al. [1] highlight vulnerabilities arising from improper smart contract design. Ning et al. [2] recommend secure aggregation protocols and consensus verification to mitigate poisoning attacks in federated settings. Alsobhi et al. [5] stress the importance of selective disclosure mechanisms for protecting learner identity. Meanwhile, Alphonse et al. [14] and Zheng et al. [15] indicate that explainable AI components are rarely integrated into blockchain-based smart learning platforms, limiting educator interpretability. These concerns reveal the need for governance-aware and interpretable architectures.

Security and System Integrity

Security threats such as model poisoning, data manipulation, and identity spoofing remain significant risks in distributed educational environments. Liu et al. [10] examined blockchain-enabled federated learning as a mechanism for detecting malicious model updates through ledger-based traceability and secure aggregation protocols. Their study emphasizes how blockchain can improve

auditability and accountability in collaborative training settings.

Fachola et al. [19] discussed privacy-preserving analytics in education using federated learning, highlighting secure aggregation and confidentiality-preserving model updates as critical mechanisms for protecting student data.

Furthermore, Li et al. [7] provided a comprehensive survey of blockchain-based federated learning systems, emphasizing interoperability, governance control, and robustness against adversarial manipulation. Ullah et al. [6] also stressed the importance of institutional trust and governance transparency in blockchain-enabled smart learning ecosystems.

These works collectively underline the necessity of integrated security frameworks, fairness-aware aggregation strategies, and accountability-driven consensus mechanisms in decentralized educational systems.

Comparative Study

A comparative evaluation of the reviewed studies reveals that credential-focused frameworks such as those by Alsobhi et al. [5] and Rahman et al. [17] prioritize data authenticity but lack integrated predictive intelligence. In contrast, blockchain-enabled federated learning systems examined by Ning et al. [2] and Aggarwal et al. [11] emphasize collaborative analytics while introducing scalability and communication challenges. Attention-driven approaches proposed by Alphonse et al. [14] and Zheng et al. [15] achieve higher predictive performance but require greater computational resources and optimization strategies. Therefore, no existing architecture fully integrates secure credential management, scalable federated analytics, attention-driven modeling, and lightweight consensus mechanisms within a single unified framework.

Comparative Analysis

Table I
Block chain enabled deep learning frameworks in smart learning environments.

Authors	Year	Focus Area	Key Contribution	Limitations
Ouf et al.	2025	Blockchain + DL SLE	Integrated credentialing with prediction	Scalability issues
Ning et al.	2024	BC-FL Taxonomy	Smart contract-based coordination	Limited deployment validation
Alsobhi et al.	2023	Micro-Credentialing	Immutable badge issuance	No analytics integration
Rahman et al.	2023	IPFS-Blockchain	Efficient decentralized storage	Governance challenges
Aggarwal et al.	2024	Federated Learning Review	Non-IID analysis	No blockchain focus
Alphonse et al.	2025	Attention-FL	Multi-scale distributed modeling	High computation cost
Zheng et al.	2025	Selective Parameter FL	Reduced communication overhead	Complex tuning
Yoneda et al.	2025	Federated Ranking	At-risk student detection	Large data requirement
Ali et al.	2025	Edge-Fog-Cloud BC-FL	Latency reduction architecture	Infrastructure complexity
Fachola et al.	2023	Privacy-Preserving FL	Secure aggregation mechanisms	Limited benchmarking

Research Gaps

The main research gap addressed in "A Block chain Based Deep Learning Framework for a Smart Learning Environment" (2025) is the limited integration of block chain and deep learning to jointly address security, transparency, and automation challenges in e-learning systems. Existing literature rarely combines artificial intelligence—particularly deep learning—with block chain in smart learning environments. Most studies deploy these technologies independently or integrate them only partially, thereby overlooking the synergistic benefits achievable through unified architectures.

In terms of smart learning security and data integrity, prior frameworks often fail to provide fully decentralized storage and robust access control for academic records, leaving issues such as fraudulent certificates, result manipulation, and privacy vulnerabilities unresolved. Additionally, research on automating and authenticating academic workflows using smart contracts—such as assignment submission and certificate issuance—remains limited.

Performance prediction with decentralized data is another underexplored area. Few works apply deep neural networks to predict learner performance using encrypted, blockchain-secured datasets. Instead, many rely on centralized data repositories, which are vulnerable to corruption and single points of failure.

Although prior works demonstrate promising prototypes, large-scale deployment validation remains limited. Yurdem et al. [3] acknowledge non-IID data challenges affecting federated convergence across institutions. Ouf et al. [4] identify computational overhead and scalability constraints in hybrid blockchain–deep learning architectures. Liu et al. [10] highlight accountability and security challenges in blockchain-enabled federated learning environments, including poisoning attack risks and coordination complexity. Aggarwal et al. [11] further discuss heterogeneity issues and communication overhead in federated systems. Alietal. [12] emphasize architectural complexity and infrastructure constraints in edge–fog–cloud blockchain integrations.

Additionally, energy-efficient consensus mechanisms tailored for academic networks remain underexplored. These gaps collectively motivate the development of scalable, interoperable, and explainable blockchain-enabled deep learning frameworks.

Current literature reveals fragmentation between credential verification and intelligent analytics components. Few systems simultaneously integrate credential authentication, federated deep learning, edge intelligence, and attention-based modeling within a cohesive architecture. Lightweight consensus protocols optimized for educational workloads require further investigation. Moreover, fairness-aware aggregation strategies addressing student diversity across institutions remain insufficiently explored. Empirical evaluations across real-world multi-university deployments are also limited.

No unified framework currently integrates credential verification, federated deep learning, attention mechanisms, and edge intelligence within a scalable and governance-aware architecture. Limited exploration of lightweight consensus mechanisms and insufficient real-world pilot deployments further highlight the need for comprehensive system-level innovation.

Challenges

Despite promising advancements, multiple obstacles hinder large-scale adoption. Blockchain throughput limitations restrict real-time processing capacity in dynamic learning environments. Interoperability challenges persist due to the absence of standardized credential schemas across institutions.

Federated learning systems struggle with heterogeneous and non-IID educational datasets, affecting fairness and convergence stability. Additionally, governance structures defining node

ownership, cost allocation, and regulatory compliance remain underdeveloped.

Communication overhead in attention-based federated architectures further complicates scalability.

II. CONCLUSION

The convergence of blockchain and deep learning represents a significant advancement in the design of secure and intelligent smart learning environments. Studies by Ouf et al. [4], Ning et al. [2], Alsobhi et al. [5], Rahman et al. [17], Alphonse et al. [14], and other scholars collectively demonstrate that decentralized trust mechanisms combined with distributed predictive analytics can enhance transparency, privacy, and collaboration in educational systems. Nevertheless, scalability constraints, interoperability limitations, data heterogeneity, and governance complexity continue to hinder large-scale implementation.

Smart learning environments (SLEs) rely on intelligent analytics, adaptive systems, and secure data management. However, traditional centralized architectures expose student data to privacy risks and credential tampering. To address these limitations, researchers have proposed integrating blockchain with deep learning and federated learning. Ouf et al. (2025) proposed a blockchain-based deep learning architecture for smart learning environments that combines immutable credential storage with predictive student analytics [4]. Their system demonstrated improved trust and decentralized verification mechanisms. Ning et al. (2024) provided a taxonomy of blockchain-based federated learning architectures and classified integration models into on-chain, off-chain, and hybrid approaches [2]. Yurdem et al. (2024) reviewed federated learning strategies and highlighted privacy benefits in distributed analytics systems [3]. Together, these foundational works establish blockchain and federated deep learning as complementary technologies for secure education ecosystems.

Integrating blockchain with deep learning unlocks promising capabilities for smart learning environments, including trusted credentialing, collaborative model development without raw-data sharing, and adaptive learning analytics. However, transitioning from prototype systems to production-grade deployments requires addressing scalability, data heterogeneity, explainability, and regulatory compliance challenges. Future systems should prioritize hybrid architectures such as edge–cloud integrations, standardize evaluation datasets, and design educator-facing explainability and governance features to accelerate institutional adoption.

Blockchain-enabled deep learning frameworks offer a transformative pathway for secure and intelligent smart learning environments. Nevertheless, achieving production-ready deployment demands interdisciplinary efforts to overcome scalability constraints, heterogeneity challenges, interpretability limitations, and governance complexities.

Future work

The literature confirms that blockchain-enabled deep learning frameworks have transformative potential for smart learning environments. Authors consistently emphasize improved credential integrity, privacy-preserving collaboration, and predictive intelligence. However, scalability, heterogeneity handling, explainability, and regulatory compliance remain open research challenges. Future research should focus on lightweight consensus models, adaptive federated aggregation, standardized evaluation datasets, and human-centric interpretability mechanisms to enable production-ready academic ecosystems.

Future research must prioritize unified architectures, standardized credential ontologies, efficient consensus models, and fairness-aware federated algorithms to realize scalable and trustworthy digital education ecosystems.A further research point in this field of study could be related to a personalized and secure educational plan for all the educational stages of the learner, where it depends on the learner's performance, learning style and behavior. Deep

learning could help to infer this large amount of data and then record this scalable data as a learning history to be secured with the blockchain and improve the overall performance.

REFERENCES

1. M. Shafay, A. Ahmad, and K. Malik, "Blockchain for deep learning: Review and open challenges," IEEE Access, vol. 10, pp. 94563–94582, 2022.
2. W. Ning, X. Zhang, Y. Liu, and H. Li, "Blockchain-based federated learning: A survey and taxonomy," Applied Sciences, vol. 14, no. 3, pp. 1–28, 2024.
3. B. Yurdem, A. Demir, and K. Kaya, "Overview and future directions of federated learning," Heliyon, vol. 10, no. 2, pp. 1–20, 2024.
4. S. Ouf, A. Ibrahim, and M. A. Abdelrahman, "A blockchain-based deep learning framework for a smart learning environment," Scientific Reports, vol. 15, no. 1, pp. 1–18, 2025.
5. [5] H. A. Alsobhi, M. Alsubaie, and A. Alharbi, "Blockchain-based micro-credentialing system in higher education," Computers & Education, vol. 190, p. 104625, 2023.
6. N. Ullah, S. M. Ali, and F. Al-Turjman, "Blockchain technology adoption in smart learning environments: An extended TAM analysis," Sustainability, vol. 13, no. 17, p. 9841, 2021.
7. X. Li, Y. Zhao, and M. Chen, "Blockchain-based federated learning: A comprehensive survey," IEEE Access, vol. 9, pp. 112584–112607, 2021.
8. M. Cardenas-Quispe, J. Alvarez, and P. Torres, "Blockchain ensuring academic integrity with a degree issuance prototype," Scientific Reports, vol. 15, no. 2, pp. 1–15, 2025.
9. J. Zhang, Y. Wu, and H. Sun, "Deep learning models for cryptocurrency analytics: A survey," IEEE Access, vol. 12, pp. 34521–34545, 2024.
10. Y. Liu, J. Kang, D. Niyato, and S. Xie, "Blockchain-enabled federated learning: A survey," ACM Computing Surveys, vol. 55, no. 4, pp. 1–35, 2022.
11. M. Aggarwal, S. Kumar, and A. Sharma, "Comprehensive review of federated learning techniques and challenges," IEEE Access, vol. 12, pp. 45672–45701, 2024.
12. G. Ali, F. Qureshi, and M. Imran, "Blockchain and federated learning in edge–fog–cloud architecture," Future Generation Computer Systems, vol. 148, pp. 45–59, 2025.
13. S. Pandya, K. Mehta, and H. Shah, "Federated learning for smart cities: Opportunities and challenges," Sustainable Cities and Society, vol. 89, p. 104312, 2023.
14. S. Alphonse, R. Kumar, and M. Das, "Attention-integrated federated learning model for distributed analytics," IEEE Transactions on Artificial Intelligence, vol. 6, no. 2, pp. 330–341, 2025.
15. L. Zheng, Y. Wang, and H. Chen, "Attention-based federated learning with selective parameter updates," Neural Computing and Applications, vol. 37, no. 5, pp. 6021–6035, 2025.
16. S. Yoneda, T. Nakamura, and H. Suzuki, "Federated ranking for at-risk student prediction," in Proc. Educational Data Mining (EDM), 2025, pp. 210–219.
17. T. Rahman, S. Islam, and N. Ahmed, "Verifi-Chain: Credential verification using blockchain and IPFS," IEEE Access, vol. 11, pp. 78412–78425, 2023.
18. J. Kaneriya, D. Patel, and R. Shah, "Secure and privacy-preserving student credential system using blockchain," International Journal of Information Security, vol. 22, no. 3, pp. 501–515, 2023.
19. C. Fachola, J. M. Luna, and A. Cano, "Federated learning for data analytics in education: A survey," Data, vol. 8, no. 2, pp. 1–24, 2023.
20. A. Kumar, R. Singh, and P. Sharma, "Academic credential verification using blockchain technology," International Journal of Innovative Science and Research Technology, vol. 9, no. 4, pp. 1234–1241, 2024.