Journal of Computer Science and Artificial Intelligence
ISSN: 3078-8242 (Print), ISSN: 3078-2309 (Online) | Vol. 4, No. 3, 2025

Research on Model and Core Functions of a Blockchain-Based Learning Record Authentication System

Xuekai Sun [1, 2, *], Robiatul A'dawiah Jamaluddin [1]

[1] Faculty of Engineering, Science and Technology, Kuala Lumpur University of Science and Technology, Jalan Ikram-UNITEN 43000 Kajang, Selangor Darul Ehsan Malaysia

[2] School of Mechanical and Electrical Engineering, Weifang University of Science and Technology, No. 1299, Shouguang City, Weifang City, Shandong Province, China

[*] **Corresponding author**: Xuekai Sun (Email: 223923752@s.klust.edu.my)

Abstract: Academic record authentication plays a pivotal role in enhancing university students' comprehensive employability and revitalizing their personal learning experiences as credible digital assets. Based on the practical needs of academic record authentication and its convergence with blockchain technology, this paper designs a model for a blockchain-based academic record authentication management system. It systematically elaborates on the functional design and implementation methods across various layers of the system architecture, with a focus on the composite blockchain ledger structure and academic archives storage solutions employed in the logical and data layers. Additionally, it outlines the core modules in the presentation and application layers, including authentication management, smart contract management, and record query and analysis. Finally, the paper concludes with a summary and prospects for the system's application in future educational scenarios.

Keywords: Academic Record Authentication, Blockchain, System Architecture, Smart Contract.

1. Introduction

Academic records refer to the systematic documentation of knowledge, skills, and competencies acquired by learners through educational activities. From the perspective of educational providers, academic records can be classified into two main categories: formal academic records and non-formal academic records [1]. Formal academic records are obtained through structured, goal-oriented learning within nationally recognized educational institutions or training organizations. These are typically presented in standardized formats such as course transcripts, degree certificates, diplomas, and credit certifications. In contrast, non-formal academic records arise from various forms of learning including on-the-job training, continuing education, micro-credential programs, soft skills development, and self-directed learning. These records manifest in diverse forms such as training certificates, project portfolios, practical experience documentation, and skill assessment results. The absence of unified standards and normalization frameworks for non-formal academic records presents significant challenges in their recognition, accumulation, and transfer [2].

The integration of blockchain technology offers a transformative approach to academic records management. By leveraging blockchain's inherent characteristics of decentralization, immutability, and transparency, both formal and non-formal academic records can be securely stored and reliably verified. This technology enables the creation of a unified, tamper-proof system for recording learning achievements regardless of their origin [3]. For non-formal records specifically, blockchain provides the missing framework for standardization and credibility assessment. Through smart contracts and distributed consensus mechanisms, blockchain facilitates the authentication, accumulation, and transfer of diverse learning achievements while maintaining the privacy and control of learners' data. This technological foundation supports the development of a more inclusive and comprehensive ecosystem for recognizing lifelong learning experiences.

2. Construction of the Authentication System Model

2.1. Requirements Analysis

The development of a blockchain-based academic record authentication system is primarily driven by four core demands emerging from the digital transformation of education: the need to break down data silos and facilitate mutual recognition of academic records by establishing a decentralized trust mechanism to overcome the data barriers created by centralized systems across educational institutions [4]; the need to ensure the authenticity and integrity of records by leveraging the immutability of blockchain to trace the origin, verify the content, and audit the history of each credential, thereby fundamentally eliminating credential fraud; the need to safeguard learner data sovereignty and privacy by shifting from an institution-centric to a learner-centric paradigm, enabling individuals to control the usage of their data through digital identity authorization and supporting trusted verification under the principle of minimal disclosure[5]; and the need to support the authentication of diverse forms of academic achievement, as the rise of micro-credentials and project-based learning requires a system flexible enough to provide standardized certification for both formal qualifications and informal learning outcomes, thereby fostering an inclusive ecosystem for learning recognition [6].

2.2. Core System Components

The proposed blockchain-based academic record authentication system involves three core participating roles and operates on several key data objects. The primary participants are: 1) the Learner, who is the rights-holder of the academic records and maintains permissions for their storage,

presentation, and authorized verification[7]; 2) the Issuing Institution, such as universities, training organizations, and certifying bodies, which acts as the issuing authority responsible for creating and digitally signing academic credentials; and 3) the Verifying Institution, including employers and admissions offices, which constitutes the user entity requiring efficient verification of credential authenticity. The system's functionality is enabled by critical data objects adhering to open standards. These include Verifiable Credentials (VCs), which serve as the core digital assets encapsulating academic record metadata and digital signatures according to W3C standards; Decentralized Identifiers (DIDs), which provide a self-sovereign identity management framework for all participants based on the DID standard; and Smart Contracts, which are deployed on the blockchain to automate the execution of business logic for notarization and verification processes [8].

2.3. Model Design

This research constructs a blockchain-based academic record authentication system employing a layered architecture to ensure modularity, scalability, and security. The framework comprises four core layers [9]. The certification system for academic records is shown in Figure 1.

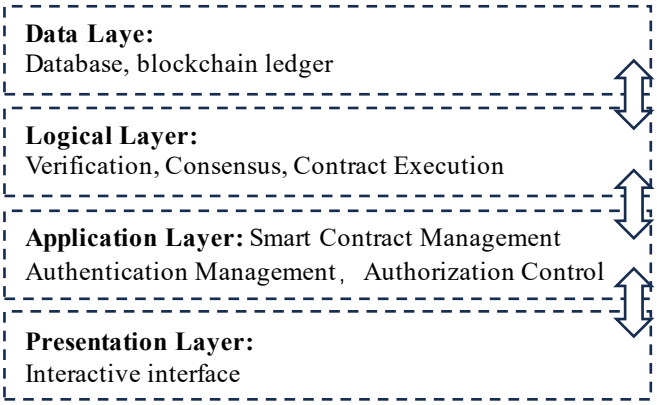

Figure 1. System structure model

The Data Layer serves as the trust foundation of the system, utilizing a composite blockchain ledger structure to store key hashes of academic records on-chain, thereby ensuring data immutability and traceability. Simultaneously, it manages complete record files through off-chain storage solutions to balance performance and cos [10]t.

The Logical Layer acts as the intelligent core of the system, integrating an optimized BFT consensus algorithm to maintain consistency among distributed nodes. It also deploys smart contracts responsible for notarization, verification, and permission management, encoding business rules into self-executing digital protocols.

Building upon the Logical Layer, the Application Layer encapsulates core functional modules for different users, including authentication management for educational institutions, a smart contract management interface for system administrators, and record query and analysis services for learners and verifying parties.

The Presentation Layer functions as the bridge for user-system interaction, providing users with streamlined and intuitive operational experiences through various front-end interfaces such as web portals and mobile applications. It seamlessly bridges the underlying complex blockchain technology with practical educational authentication scenarios [11].

3. Functional Design of Core Modules

3.1. The Design of The Blockchain Ledger

Each system maintains an independent blockchain ledger, which organizes data in a chain structure composed of sequentially generated blocks. Each block contains key information such as the block number, hash of the previous block, timestamp, and Merkle tree [12]. The Merkle tree structure consists of a root node, intermediate nodes, and leaf nodes. The leaf nodes store specific authentication record data, while the intermediate nodes and root node contain hash values of their child nodes. By comparing the hash values of the Merkle tree's root node and intermediate nodes, the system can efficiently verify whether the data in the leaf nodes remains consistent, thereby determining if the authentication records have been tampered with. The structure of the system's blockchain ledger is illustrated in Figure 2.

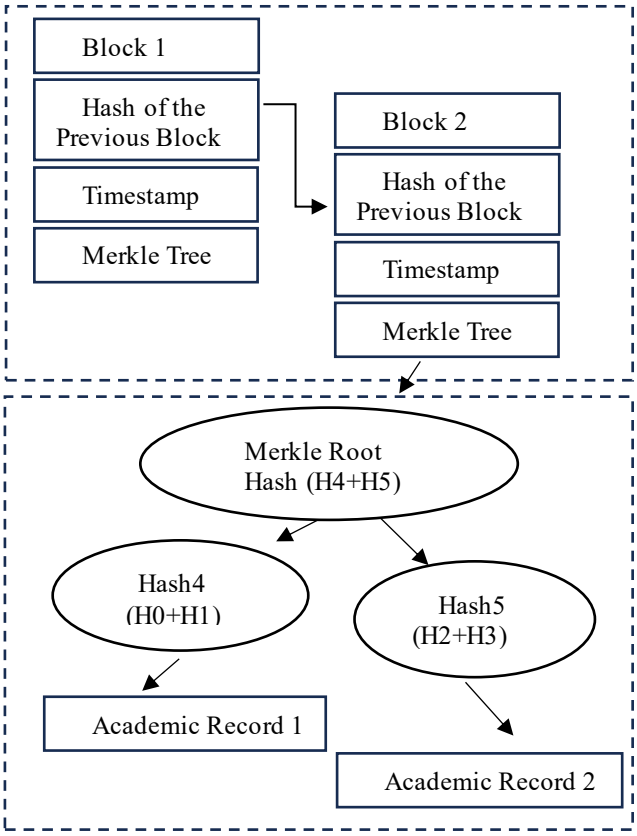

Figure 2. Blockchain Ledger Design

3.2. System Storage

The storage architecture of the system employs a hybrid design of "on-chain anchoring and off-chain storage" to achieve an optimal balance between security and efficiency. Specifically, the system utilizes cryptographic hash algorithms to generate unique digital fingerprints for each academic record. Only these hash values along with key metadata (such as record identifiers, issuing institution digital signatures, timestamps, etc.) are stored on the blockchain, leveraging the immutability of the distributed ledger to provide a trusted anchor for data authenticity [13]. The complete academic record files (including detailed transcripts, scanned certificates, etc.) are stored in encrypted form in off-chain storage systems, which can be implemented based on distributed file systems like IPFS or traditional cloud servers.

3.3. Authentication Process

The authentication process of the system is built upon verifiable credentials and smart contracts as its core technological foundations, establishing a decentralized, user-centric trusted authentication loop. The entire workflow consists of two main phases - credential issuance and credential verification - involving three key roles: the issuer, the holder (learner), and the verifier [14].

During the issuance phase, the issuing institution first generates a verifiable credential containing complete academic information and a digital signature for the learner. The system then calculates the credential's hash value and invokes a notarization smart contract to anchor this hash and other key information onto the blockchain. This process utilizes consensus mechanisms to ensure the immutability of the notarization record. Finally, the complete verifiable credential, including the blockchain transaction certificate, is securely delivered to the learner's digital wallet, achieving the transfer of academic record sovereignty [15].

In the verification phase, learners can voluntarily choose to present their credentials to verifiers. The verifier's system automatically extracts the credential hash and queries the verification smart contract on the blockchain to authenticate the notarization record's validity, integrity, and issuer identity [16]. The smart contract automatically performs hash comparison and status checks, immediately returning a "valid" or "invalid" verification result. This process operates without involving the original issuing institution, ensuring both verification efficiency and learner privacy protection.

This process design enables trust transfer and automated verification through blockchain technology, guaranteeing the immutability, traceability, and efficient verification of academic records. Simultaneously, it fully embodies learners' sovereign control over personal data, establishing a solid foundation for building an open and trusted educational certification ecosystem.

4. Conclusion

The blockchain-based academic record authentication system provides learners with credible qualification certification. Utilizing distributed ledger technology, the system ensures the immutability of academic records, enabling multiple stakeholders including educational institutions, instructors, students, and employers to participate equally in the authentication process. The system comprehensively records both formal and informal learning experiences while implementing automated verification through smart contracts, significantly improving authentication efficiency and reducing operational costs. Furthermore, the system enables multidimensional analysis of learning outcomes through in-depth examination of authentication records, providing data support for learners to demonstrate their competencies and for teachers to implement personalized, data-driven teaching approaches, thereby strongly facilitating the development of lifelong learning systems.

The system also innovatively supports smart contract-based collaborative learning models. In teaching scenarios, instructors and students can jointly establish learning objectives and evaluation criteria through smart contracts, effectively stimulating learning initiative. Learning teams can utilize smart contracts to clarify member responsibilities and outcome distribution, establishing collaborative learning communities with well-defined rights and obligations. This innovative application provides substantial support for student-centered teaching methodologies such as problem-based learning and project-driven instruction. Through the deep integration of blockchain with artificial intelligence and big data technologies, the system achieves efficient educational application operations while ensuring data security and privacy protection. Beyond academic authentication, the system can be extended to multiple scenarios including research achievement management and educational quality assessment, offering innovative practical solutions for digital transformation in education.

References

[1] Khashan O A, Alamri S, Alomoush W, et al. Blockchain-Based Decentralized Authentication Model for IoT-Based E-Learning and Educational Environments [J]. Computers, Materials & Continua, 2023, 75(2).

[2] Chinnasamy P, Subashini B, Ayyasamy R K, et al. Blockchain based electronic educational document management with role-based access control using machine learning model [J]. Scientific Reports, 2025, 15(1): 18828.

[3] Ouf S, Ahmed S, Helmy Y. A blockchain based deep learning framework for a smart learning environment [J]. Scientific Reports, 2025, 15(1): 19519.

[4] Hagui I, Msolli A, ben Henda N, et al. A blockchain-based security system with light cryptography for user authentication security [J]. Multimedia Tools and Applications, 2024, 83(17): 52451-52480.

[5] Qu J, Shao J. Research on the Construction System of Learning Outcome Certification System Based on Blockchain [C]//2024 International Conference on Computers, Information Processing and Advanced Education (CIPAE). IEEE, 2024: 853-857.

[6] Dewangan N K, Chandrakar P. Implementing blockchain and deep learning in the development of an educational digital twin [J]. Soft Computing, 2024, 28(9-10): 6619-6636.

[7] Ayare A A, Jadhav V A, Banatwala M K, et al. A systematic review on blockchain-based framework for storing educational records using interplanetary file system [J]. Cureus Journals, 2025, 2(1).

[8] Aslam M S, Altaf A, Iqbal F, et al. Novel model to authenticate role-based medical users for blockchain-based IoMT devices [J]. Plos one, 2024, 19(7): e0304774.

[9] Soni P, Islam S K H, Pal A K, et al. Blockchain-based user authentication and data-sharing framework for healthcare industries [J]. IEEE Transactions on Network Science and Engineering, 2024, 11(4): 3623-3638.

[10] Said S H, Sinde R S, Kosia E M, et al. A Comprehensive Blockchain-Based System for Educational Qualifications Management and Verification to Counter Forgery [J]. IEEE Access, 2025.

[11] Farabi A, Khandaker I, Jahan N, et al. ShikkhaChain: A Blockchain-Powered Academic Credential Verification System for Bangladesh [J]. arXiv preprint arXiv:2508.05334, 2025.

[12] Cardenas-Quispe M A, Pacheco A. Blockchain ensuring academic integrity with a degree verification prototype [J]. Scientific Reports, 2025, 15(1): 9281.

[13] Al-Ghuraybi H A, AlZain M A, Soh B. Exploring the integration of blockchain technology, physical unclonable function, and machine learning for authentication in cyber-physical systems [J]. Multimedia Tools and Applications, 2024, 83(12): 35629-35672.

[14] Alabdulatif A. Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users [J]. Information, 2025, 16(3): 219.

[15] Singh T, Vaid R. Preserving security in terms of authentication on blockchain-based wireless sensor network (WSN) [J]. * Int. J. Comput. Netw. Appl.*, 2024, 11(3): 2024.

[16] Le H V A, Nguyen Q D N, Tadashi N, et al. Blockchain-Based Decentralized Identity Management System with AI and Merkle Trees [J]. Computers, 2025, 14(7): 289.