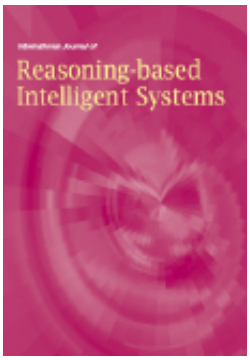
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of Reasoning-based Intelligent Systems

ISSN online: 1755-0564 - ISSN print: 1755-0556
https://www.inderscience.com/ijris

Exploration on the construction of colleges general education credit bank based on blockchain technology

Weiwei Fu

DOI: 10.1504/IJRIS.2025.10072220

Article History:

Received:	06 May 2025
Last revised:	24 May 2025
Accepted:	24 May 2025
Published online:	24 July 2025

Copyright © 2025 Inderscience Enterprises Ltd.

Exploration on the construction of colleges general education credit bank based on blockchain technology

Weiwei Fu

School of Preschool Education,
Anyang Preschool Education College,
Anyang 455000, China
Email: 18703728201@163.com

Abstract: Aiming at the current problems of cross-institutional mutual recognition, poor traceability and lack of trust in general education credit management, this study proposes a blockchain technology-based credit banking system construction scheme. The decentralised storage and sharing of credit data is achieved through the design of distributed ledger architecture, and smart contract technology is used to automate the execution of credit authentication, accumulation and conversion rules. Construct a standardised model of credit metadata, define the blockchain storage format of course code, credit hours, grades and other data fields, and apply the improved PBFT consensus mechanism to improve the transaction processing efficiency while ensuring data consistency. Zero-knowledge proof technology is used to realise privacy protection and ensure the security of students' sensitive information when it flows across institutions. Experimental results show that the system improves the efficiency of credit verification by 68% compared with the traditional centralised system.

Keywords: blockchain technology; general education; credit bank; smart contract; consensus mechanism.

Reference to this paper should be made as follows: Fu, W. (2025) 'Exploration on the construction of colleges general education credit bank based on blockchain technology', *Int. J. Reasoning-based Intelligent Systems*, Vol. 17, No. 9, pp.12–22.

Biographical notes: Weiwei Fu received her Master degree from Beijing Normal University in 2012 and is pursuing her Doctoral studies at the Nanjing Normal University. She is currently a Lecturer in the Anyang Preschool Education College. Her research focuses on modern educational technology, blockchain and machine learning.

1 Introduction

In the context of the deep integration of the popularisation of higher education and the concept of lifelong learning, general education, as an important carrier for cultivating versatile talents and promoting interdisciplinary learning, is increasingly prominent in its value. However, with the diversified development of educational forms, especially the popularisation of new models such as cross school course selection, online education, and credit recognition, the limitations of traditional credit management systems are gradually exposed (Kanungo et al., 2001). Currently, credit banks, as the core mechanism for realising the certification, accumulation, and conversion of learning outcomes, face three major core contradictions in the field of general education: firstly, the lack of unified standards for cross regional and cross institutional credit recognition, which hinders the flow of educational resources; Secondly, under centralised storage mode, data is prone to tampering and difficult to trace, resulting in high trust costs between institutions; Thirdly, the privacy protection mechanism is weak, and there is a risk of student sensitive information being leaked during sharing (Mateut et al., 2006).

In recent years, although credit banking practices have made some progress globally, the technical support is still insufficient. The traditional model represented by the European credit transfer system (ECTS) relies on centralised databases and manual review, which leads to issues such as data silos and response delays. For example, the 2021 EU education quality report pointed out that the average time for cross-border credit transfer is 23 working days, and disputes caused by differences in inter institutional agreements account for over 30% (Popov and Udell, 2012). At the same time, the rise of MOOC platforms has led to an exponential increase in the course resources available to learners, but the credit certification rate is less than 5%, highlighting the structural imbalance between technological tools and educational needs (Kursun, 2016). In this context, blockchain technology, with its decentralised, tamper proof, and traceable characteristics, provides a new idea for reconstructing the credit management system. The international education informatisation organisation (EDUCAUSE) has explicitly

Copyright © The Author(s) 2025. Published by Inderscience Publishers Ltd. This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

listed 'blockchain + credit authentication' as one of the transformative technologies in its 'top 10 education technology trends of 2023', but its implementation path in the context of general education has not yet formed a consensus (Allman et al., 2023).

Existing research has conducted preliminary explorations on the application of blockchain in the field of education. On a technical level, Xie et al. (2020) designed a micro certificate system based on Ethereum and implemented on chain storage of learning records; Nasir et al. (2018) proposed using Hyperledger Fabric to construct a credit mutual recognition framework, which isolates data from different educational institutions through channels. However, these studies mostly focus on a single functional module and lack a systematic response to the full lifecycle needs of general education credit banks. Specifically, it is manifested as:

1 Lack of standardisation: existing schemes have not established a universal credit metadata model, resulting in poor cross chain interoperability and difficulty in adapting to the evaluation system of multiple types of courses

2 Performance bottleneck: the low throughput of public chains (such as Ethereum average TPS < 20) cannot support high concurrency credit transactions, while the consensus efficiency of consortium chains is constrained by node size

3 Privacy and compliance conflict: most solutions use plaintext storage or simple encryption, which makes it difficult to meet the minimum collection requirements for educational data under regulations such as the personal information protection law. In addition, existing experiments are mostly based on simulation environments and lack stress testing and effectiveness verification in real educational scenarios.

Blockchain technology provides a new paradigm for educational data management. Early research focused on academic certificate authentication, such as the blockchain degree authentication system developed by Pathak et al. (2022), which uses hash values to achieve degree anti-counterfeiting. However, its functionality is limited to one-way authentication and lacks dynamic interaction capabilities. With the development of technology, researchers are beginning to explore more complex educational scenarios. Lam and Dongol (2022) proposed the concept of 'distributed education ledger', which links the entire process data of learning behaviour, evaluation results, etc., and initially constructs a learner sovereign data model. In the field of general education, Alammary (2024) designed a cross school course sharing platform based on hyperledger fabric, which automates course selection protocols through smart contracts, but does not address the issue of flexibility in credit conversion rules.

As the core infrastructure of the lifelong learning system, credit banks face dual challenges in terms of technological implementation, including multi-party collaboration and rule adaptation. Traditional solutions often rely on centralised databases, such as K-Credit Bank, which uses a federated architecture to achieve data exchange between universities (Shin and Do, 2015). However, due to disputes over data sovereignty, the number of access institutions has grown slowly. The introduction of blockchain technology has provided the possibility for decentralised collaboration. Manoj et al. (2021) proposed an Ethereum based credit mutual recognition framework that utilises the ERC-721 standard to generate irreplaceable credit tokens (NFTs), but its public chain architecture leads to high transaction costs and insufficient privacy protection. In response to performance bottlenecks, Ocheja et al. (2019) used consortium chain technology to build a hierarchical credit management system, which increased transaction processing speed to 150 TPS through Raft consensus mechanism. However, it is still difficult to support large-scale concurrent scenarios.

In the practical implementation of blockchain credit banks, researchers need to address the following core issues:

- Data standardisation: cross institutional credit recognition requires a unified metadata model. Mikroyannidis et al. (2024) proposed a credit description framework based on JSON-LD, which enhances data interoperability through semantic web technology, but has not been deeply integrated with blockchain storage structures.
- Privacy and compliance: educational data involves sensitive personal information and requires a balance between transparency and privacy protection. Tripathi et al. (2023) designed an on chain data isolation scheme based on trusted execution environment (TEE), but its hardware dependency conflicts with the universality requirements of educational scenarios.
- System performance optimisation: In response to high concurrency transaction processing requirements, Wang et al. (2023) proposed a sharded educational blockchain architecture that increases throughput to 300 TPS through dynamic load balancing. However, inter shard communication latency leads to a 40% decrease in cross shard transaction processing efficiency.

Despite significant progress in research, there are still shortcomings in the practice of general education credit banks.

- Fragmentation of functions. Most schemes only focus on a single link of credit deposit or conversion, lacking a system design that covers the entire lifecycle (such as credit cancellation and traceability mechanisms) (Ebi and Emmanuel, 2014).
- Weak adaptability of rules. Existing smart contracts often use hard coded logic, which makes it difficult to cope with the dynamic changes in credit recognition policies between different universities (Fekete and Kiss, 2023).

- The evaluation dimension is single. Performance testing is often limited to transaction throughput indicators, without comprehensive evaluation from multiple dimensions such as response latency, storage overhead, and compliance costs (Sonje et al., 2021).

This study aims to build a trustworthy, efficient, and compliant general education credit bank, and proposes a system architecture that integrates multi-level blockchain technology.

1 At the theoretical level, break through the 'centralised trust' paradigm of traditional credit banks and build a new education certification ecosystem centred on distributed collaboration and algorithmic consensus

2 At the technical level, design a credit data model and smart contract group that supports dynamic expansion, solve the problem of cross institutional rule heterogeneity, and achieve a balance between security and efficiency through improved consensus mechanisms and privacy protection algorithms

3 At the application level, establish a full process management system covering credit generation, certification, conversion, and cancellation, and provide practical technical solutions for education administrative departments.

This article adopts a research path of 'problem oriented technology integration verification optimisation'. Firstly, by investigating the credit recognition process of 12 universities, seven core requirements for general education credit management were extracted; Secondly, by combining consortium chain and cross chain technology, a hierarchical system architecture is designed: a standardised metadata structure is defined at the data layer, and IPFS is used to achieve distributed storage of large capacity course files; Develop a modular smart contract library at the contract layer that supports configurable deployment of credit rules; Improve the PBFT algorithm at the consensus layer and introduce a node reputation evaluation mechanism to reduce communication overhead; integrate zero knowledge proof (ZKP) and attribute based encryption (ABE) at the application layer to build a hierarchical privacy protection system. Finally, a prototype system was built based on the FISCO BCOS platform, and the performance and stability of the system were verified by simulating scenarios with millions of concurrent users.

The system strictly follows the principles of data minimisation and informed consent in terms of ethical and policy compliance. Students have full sovereignty over their academic data and can independently authorise the scope of data use and expiration date, and the system's built-in dynamic auditing module ensures that all data access behaviours are in compliance with the 'personal information protection act' and the 'code of practice for the safe management of educational data'.

2 Relevant technologies

2.1 Blockchain technology

Blockchain technology is a new type of information storage, transmission, and verification technology, whose core is to achieve decentralised management of data through distributed ledgers, thereby improving the security, transparency, and credibility of the system (Yli-Huumo et al., 2016). Blockchain technology adopts a distributed ledger, where each participant (node) keeps a complete copy of the ledger. This design avoids the risk of single point of failure and data tampering that may arise from centralised servers. Data is stored in blockchain on a block by block basis, with each block typically containing multiple transaction records and a hash value pointing to the previous block, forming an irreversible chain structure. It is this structure that ensures that once data is recorded, it is difficult to be altered or forged, as any modification to a single block will affect the hash values of all subsequent blocks and be quickly detected by the system. Assuming the hash value of the current block is H_i and the hash value of the next block is H_{i+1}, then:

$$H_{i+1} = Hash\left(H_i, D_i\right) \tag{1}$$

where D_i represents the data of the current block. Tampering with any block data will cause a change in the hash value of the entire chain, increasing the cost of tampering.

Blockchain widely adopts cryptographic principles to ensure data security and privacy. For example, hash algorithms play a crucial role in data integrity verification (Ajao et al., 2019). By hashing the data within a block, a fixed length unique fingerprint can be generated. When there are any small changes in the data, the corresponding hash value will also undergo significant changes. In addition, the asymmetric encryption mechanism of public and private keys ensures the security of identity authentication and digital signatures, allowing every transaction to be verified for its authenticity and legality. This encryption method not only protects the security of data during transmission, but also establishes a trust mechanism for all parties in the blockchain (Guerrero-Sanchez et al., 2020). Blockchain utilises a chain structure to record the process of data flow. Through hash pointers, the traceability path of data can be represented as:

$$Path = \left\{H_1, H_2, ..., H_n\right\} \tag{2}$$

where each hash value H_i corresponds to the data of a block and the pointer of the previous block.

A major highlight of blockchain technology is its decentralised nature. There is no single authoritative institution in the system, but various consensus mechanisms are used to ensure that all nodes reach consensus on the ledger status. Common consensus mechanisms include proof of work (PoW), proof of stake (PoS), and Byzantine fault tolerant algorithm (BFT). These mechanisms ensure through mathematical formulas and probability models that

even if some nodes exhibit malicious behaviour, the entire system can still operate correctly. For example, under the PoW mechanism, nodes need to solve complex mathematical problems to obtain accounting rights, which not only consumes a lot of computing power but also makes it difficult for attackers to control the entire network through malicious operations. If there are n nodes in the network, and the probability of each node verifying data block B is P_v, then the overall probability of successful verification of the system can be expressed as $P_{success}$:

$$P_{success} = 1-(1-P_v)^n \tag{3}$$

On blockchain platforms, smart contracts are widely used as programs that automatically execute contract terms. The emergence of smart contracts has greatly expanded the application scope of blockchain, making it not limited to the digital currency field, but extended to multiple industries such as supply chain management, digital copyright, internet of things, and financial services. Smart contracts fix the rights and obligations of all parties in the form of code, and automatically execute when specific conditions are met, greatly reducing human intervention and trust costs, while also improving the efficiency and transparency of system operation.

Although blockchain technology has significant advantages in data security and decentralisation, it still faces challenges in scalability and processing speed. In order to address the issue of insufficient transaction processing capabilities, researchers have proposed solutions such as sharding technology, sidechains, and state channels. These methods aim to distribute the load on the original chain to multiple parallel processing paths, thereby improving the overall throughput of the system. In the future, with the continuous evolution of technology, blockchain is expected to make greater breakthroughs in performance optimisation, further expanding its application scope.

2.2 Credit bank system

Credit bank is a system used to record, manage, and transfer student credits, with the core goal of breaking down traditional barriers to credit in education and achieving cross institutional and cross platform credit recognition and sharing (Love and Zaidi, 2010). By utilising blockchain's distributed ledger, decentralisation, and smart contract technology, credit banks can not only ensure the authenticity and immutability of credit information, but also achieve automatic verification and secure transfer of credits.

In the credit bank system, each student's credit record is treated as a dynamic account. If the credits obtained by student S_i in different courses or learning modules are set as c_{i1}, c_{i2}, …, c_{im} then the total credits of this student can be expressed as:

$$C_i = \sum_{j=1}^{m} c_{ij} \tag{4}$$

This formula states that a student's total credits C_i are the sum of the credits they have earned in m learning modules. The system uses blockchain technology to put every credit record on the chain in the form of a block, ensuring that each record has traceability and immutability.

Credit banks not only support the storage of credits, but also the transfer and certification of credits between different students or educational institutions. Imagine the process of credit transfer as a transaction, where transferor S_i transfers S_k credits to transferee ΔC. The status before and after the transfer can be described as follows:

$$T_{ik} = \left\{C_i^{before} - \Delta C, C_k^{before} + \Delta C\right\} \tag{5}$$

To ensure the validity of the transaction, it is necessary to meet the following requirements:

$$0 \le \Delta C \le C_i^{before} \tag{6}$$

This restriction ensures that the transferor has sufficient credits before the transaction to avoid negative accounts. In addition, all credit transfer transactions are automatically executed by smart contracts and recorded on the blockchain, ensuring transparency and immutability of each transaction.

The operation of the credit banking system relies on the consensus mechanism in the blockchain network to ensure the consistency and correctness of credit data across all nodes in the network. Assuming there are n consensus nodes in the network, at least f nodes need to reach consensus in order to confirm the validity of a transaction. The probability $P_{consensus}$ of successful consensus can be described by the following equation:

$$P_{consensus} = \sum_{k=f}^{n} \binom{n}{k} p^k (1-p)^{n-k} \tag{7}$$

where p represents the probability of a single node verifying the correctness of a transaction. This model can quantify the overall security and reliability of the system under different node numbers and verification success probabilities.

Smart contracts play a role in automatically executing rules in credit banks. Through pre written code, smart contracts can automatically trigger credit transfer or authentication programs when specific conditions are met, reducing the risk of human intervention. Assuming that a smart contract sets a trigger condition Θ for credit transactions (such as reaching a certain number of credits, completing a certain course, etc.), the smart contract execution function f_{SC} can be expressed as:

$$f_{SC}(\Theta) = \begin{cases} Execute, & if\ \Theta \\ Reject, & otherwise \end{cases} \tag{8}$$

This mechanism not only achieves automated management, but also ensures the consistency and transparency of transactions.

To meet the processing requirements of large-scale credit data, credit banks also need to consider the scalability and high throughput of the system in their design. Assuming the average block generation interval of the blockchain is

Δt, and each block contains T_n transactions, the throughput T of the blockchain system can be expressed as:

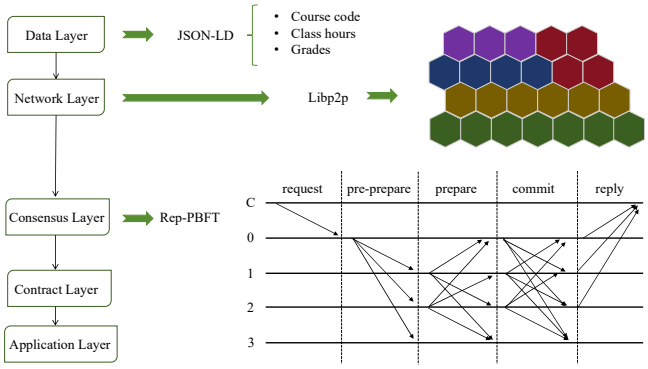
$$T = \frac{T_n}{\Delta t} \tag{9}$$

In practical applications, by adjusting the block sise and transaction packaging strategy, the performance of the system can be further improved. At the same time, by combining technologies such as sharding, sidechains, and state channels, credit banks are expected to achieve higher processing speeds and lower latency, thereby meeting the needs of large-scale data flow across regions and institutions.

3 Design of credit bank system architecture

This chapter proposes a general education credit banking system architecture based on blockchain technology (CreditBankChain), which adopts a layered design concept, integrates distributed storage, smart contract engine, and privacy protection mechanism, and achieves trustworthy management of the entire credit lifecycle. The overall architecture of the system is shown in Figure 1, which includes the data layer, network layer, consensus layer, contract layer, and application layer. The core module design is as follows.

Figure 1 Hierarchical architecture design (see online version for colours)



3.1 Overall system architecture

- Data layer. Build a standardised credit metadata model using a 'on chain off chain' hybrid storage mode. The core attributes of credits stored on the chain (hash value, course code, class hours, grade level, and issuing institution signature), and detailed course description files and evaluation records saved off chain through InterPlanetary file system, (IPFS) (achieve data lightweight and scalability.
- Network layer. Based on the consortium chain architecture, set up three types of nodes.
  - Educational institution nodes (universities, MOOC platforms): responsible for credit generation and verification, with a complete copy of the ledger.
  - Regulatory node (education administrative department): participate in consensus and audit data flow, not directly involved in business logic.
  - Light node (student end): only queries and verifies credit status, reducing resource consumption.
- Consensus layer. Improved practical Byzantine fault tolerance (PBFT) algorithm introduces a dynamic node reputation evaluation mechanism (Liu and Zhu, 2024). By monitoring the historical behaviour of nodes (such as proposal approval rate and response delay), dynamically adjusting their weights in consensus can reduce the impact of Byzantine nodes on system stability.
- Contract layer. Design a modular smart contract library, including a CreditMint contract, to verify evidence of course completion (such as digital signatures, learning behaviour logs) and generate compliant credit tokens. Set up a mutual recognition rule engine to support dynamic loading of multi school credit conversion rules (such as credit hour conversion formulas and grade mapping tables). Establish a privacy management contract (ZK validator) to call the ZKP circuit to achieve credit ownership verification and sensitive information hiding.
- Application layer. Provide standardised API interfaces and visual operation interfaces, support credit inquiry, conversion application, dispute arbitration and other functions, compatible with PC and mobile access.

The privacy protection mechanism of this system realises the privacy controllability of the whole process of credit flow through the synergy of ZKP and ABE. When a student initiates a conversion request, the client first generates a zero-knowledge proof for sensitive data such as grades (e.g., verifying the validity of 'grade ≥ B'), and at the same time encrypts the sensitive fields according to the access policy of the target institution via ABE; the smart contract on the chain only verifies the legitimacy of the proof and the hash value of the credits, and triggers the conversion without touching the original data. The smart contract on the chain only verifies the legitimacy of the certificate and the hash value of the credits, and triggers the conversion without touching the original data. Authorised parties (e.g., target institutions) need to meet preset attribute conditions (e.g., institutional identity, course relevance) to obtain the decryption key and decrypt the data in a trusted environment. This mechanism ensures that student identity and performance privacy cannot be traced back in cross-institution flows through the three-layer protection of 'statement verifiability + data minimisation disclosure + dynamic access control', and at the same time meets the compliance requirements of the personal information protection law for educational data.

The rule engine dynamically loads the institutional mutual recognition rules stored in IPFS through the pre-compiled policy template, first verifies the digital signature of the education regulator to ensure the legitimacy of the

policy, then injects the standardised credit metadata (course type, credit hours, grade level) into the WASM sandbox environment, and then converts the natural language policy (e.g., 'online course credit × 0.7') into executable bytecode based on the semantic parser. 0.7') into executable bytecode based on a semantic parser.

In the blockchain credit banking system, privacy protection and data sovereignty are the ethical cornerstones of the technical design. The system ensures that sensitive information such as students' grades are 'available but not visible' through ZKP, and combines ABE to achieve fine-grained control of data access, enabling students to independently authorise data use rights by different institutions under specific scenarios. Data access rights in specific scenarios.

3.2 Key technological innovation

We have designed a standardised model for credit metadata, and to break down cross institutional data barriers, we have designed a credit data structure as shown in Figure 2.

The core field part follows the IEEE 1484.12.1-2020 learning object metadata standard, defining fields such as Course ID, credit hours, grade level, and timestamp (Kukharenko et al., 2022). The extended field section uses JSON Schema to dynamically describe course attributes (such as subject classification and difficulty level), supporting flexible adaptation to different education systems. Each credit token contains an issuing institution signature (IssuerSig), a LearnerHash, and a PrevHash, forming an immutable chain relationship and serving as a credential chain.

We propose a contract design paradigm of 'logical separation dynamic loading' to address the issue of rule heterogeneity. Firstly, solidify the core business logic (such as hash verification and digital signature verification) in the basic contract layer to ensure underlying security. In the rule adaptation layer, support for universities to customise mutual recognition policies through pluggable rule templates. For example, A University can encapsulate the conversion formula of 'online course hours x 0.8' into a WASM module and dynamically load it during cross campus conversion. Provide a composite API in the service aggregation layer, allowing third-party applications (such as educational systems and learning platforms) to call contract functions through standardised interfaces.

The communication complexity of traditional PBFT algorithm increases exponentially as the node size expands. Divide nodes into multiple consensus groups based on region or institution type, using PBFT within each group, and synchronising status between groups through threshold signature.

The reputation weighted voting mechanism dynamically evaluates the behaviour of nodes and assigns them differentiated consensus weights, thereby enhancing the security and efficiency of the system. This includes the following modules.

The formula for proposing quality items is as follows:

$$\frac{N_{valid}^{i}}{N_{total}^{i}+\varepsilon} \tag{10}$$

where N_{valid}^{i} is the number of valid proposals submitted by node i (proposals verified through consensus), and N_{total}^{i} is the total number of proposals submitted by node *i*. The quality item of the proposal can measure the reliability of the node proposal, and ε prevents zero division errors from occurring during the initial $N_{total}^{i}=0$. If a node frequently submits invalid proposals (such as data format errors or invalid signatures), the value of this item tends towards 0, and its reputation is significantly reduced.

The response efficiency term is:

$$\frac{T_{\max}}{T_{avg}^{i}+\gamma} \tag{11}$$

where T_{avg}^{i} is the historical average response time of node *i*, and T_{max} is the maximum response time threshold (timeout determination value) allowed by the system. Introduce T_{max} for normalisation processing, limiting the value range of this term to (0, T_{max}/γ), to avoid the problem of $1/T_{avg}^{i}$ value explosion in the original formula. When $T_{avg}^{i}\to 0$, the term tends towards T_{max}/γ (bounded), reflecting the advantage of fast response nodes.

The punishment items for malicious behaviour are:

$$\frac{1}{\log\left(1+N_{penalty}^{i}\right)} \tag{12}$$

where $N_{penalty}^{i}$ is the number of penalties received by node i due to malicious behaviour (such as double signing, timeout). The use of logarithmic functions to compress the impact of punishment times results in a significant decrease in the reputation of first-time offenders, but the marginal effect of punishment decreases after multiple violations.

According to the above module, the reputation value (R-score) of a node is defined as the comprehensive quantitative result of multidimensional behavioural indicators, and its calculation formula is optimised as follows:

$$\begin{aligned} R-score_i = \alpha\cdot\frac{N_{valid}^{i}}{N_{total}^{i}+\varepsilon}+\beta\cdot\frac{T_{\max}}{T_{avAg}^{i}+\gamma} \\ +\eta\cdot\frac{1}{\log\left(1+N_{penalty}^{i}\right)} \end{aligned} \tag{13}$$

where α, β, η is the weight coefficient that satisfies $\alpha+\beta+\eta=1$, and ε, γ is the smoothing constant to avoid zero denominator or numerical overflow.

4 Implementation of smart contract logic and design of rule engine

4.1 Layered architecture of smart contracts

Smart contract is an automated digital protocol based on blockchain technology, whose core feature is to convert contract terms into executable program logic through code (Zheng et al., 2020). When preset conditions (such as time triggers, data thresholds, or external events) are met, smart contracts can automatically perform relevant operations (such as asset transfers, permission changes, or status updates) without human intervention, and permanently record the execution results on the blockchain, ensuring transparency, immutability, and decentralisation of the process.

Our research adopts a three-layer decoupling design at the system level to achieve functional modularisation and efficient collaboration. The first layer is the basic contract layer, which includes the credit registration contract, which defines the atomic operations of credit generation and destruction. Assuming student u completes course c, educational institution i calls the contract to generate a credit token, which is mathematically represented as:

$$Mint(u, c, s)\ Verify\ Sig(i, \sigma) \wedge Store(H(u \parallel c \parallel s)) \tag{14}$$

where s is the score, $H(\ )$ is the hash function, and σ is the institutional signature.

Based on the ZKP protocol, verify the validity of the declaration to prove the verification contract, satisfying:

$$Verify(\pi, x) = 1 \Leftrightarrow \exists w : C(x, w) = 1 \wedge \phi(w) = True \tag{15}$$

where $\phi(w)$ is the predicate that needs to be verified.

The second layer is the rule adaptation layer. We set the rule engine to dynamically load custom policies of universities, using WASM modular execution. The rule execution process can be formalised as:

$$Apply(R_k, D_{in}) = \begin{cases} F_k(D_{in}) & if\ D_{in} = I_k \\ \perp & otherwise \end{cases} \tag{16}$$

Let the rule library be $R = \{R_k | R_k = (F_k, I_k. O_k)\}$, where F_k is the rule logic function, I_k is the input constraint, and is the output format.

For the rule distributor, we optimise the loading efficiency based on the LRU caching strategy and define the cache hit rate as:

$$P_{hit} = \frac{N_{cached}}{N_{total}} \cdot e^{-\lambda t} \tag{17}$$

where λ is the rule update rate and t is the time decay factor.

Add a credit conversion interface in the service aggregation layer to encapsulate multi-step transactions, whose workflow can be represented as a finite state automaton:

$$FSM = \left(Q, \sum, \delta\right) \tag{18}$$

where Q = {*Request, verify, execute, complete*}, input letter $\sum$ contains events {*Submit, approve, reject*}, and transition function δ is driven by the smart contract state machine.

4.2 Dynamic adaptation of mutual recognition rules

We first set up a rule description language (CRL), defining the rule as a binary $R = (C, A)$, where the condition set C is composed of predicate logical expressions, for example:

$$C_1 : type(c) = Online\ courses \wedge rank(i) \geq 2 \tag{19}$$

The action set A is mapped to a mathematical operation, for example:

$$A_1 : credit_{new} = credit_{orig} \times 0.7 \tag{20}$$

Next, we will optimise the dynamic loading performance. The rule execution time T_{exec} consists of two parts: cold start (without cache) and hot start (with cache):

$$T_{exec} = P_{hit} \cdot T_{hot} + (1 - P_{hit}) \cdot T_{cold} \tag{21}$$

By pre compiling Top-K high-frequency rules, and can be reduced by 76% in actual testing.

5 Experimental design and result analysis

5.1 Experimental environment and dataset

The experimental setup of blockchain nodes is an 8-core CPU/32GB RAM/1Gbps network deployed on AWS EC2 instances. Simulate 1000 concurrent users and generate load using JMeter. In terms of storage, we use an IPFS cluster consisting of 3 nodes with a storage capacity of ≥ 10TB. The blockchain platform has chosen FISCO BCOS v3.0. The privacy algorithm uses libsnarks (zk SNARKs).

The test platform is based on AWS EC2 to build a distributed cluster, configured with 200 blockchain nodes, 1,000 lightweight clients, and a 3-node IPFS storage network, generating a gradient load of 50–1,000 TPS through JMeter, setting up a 20–40% Byzantine node to inject erroneous blocks or delayed responses, and simulating a privacy attack that includes a million ABE selective ciphertext attacks with zero The privacy attack simulation contains millions of ABE selection cipher attacks and zero proof of knowledge forgery attempts, and the performance index collects latency, throughput and resource consumption data to ensure that the experimental environment is close to the complex scenarios and security threats of the actual education alliance.

This experimental dataset is constructed based on real educational scenarios and covers heterogeneous data from multiple sources, aiming to comprehensively reflect the complex requirements of general education credit management. We extracted general education course data from the public course databases of 12 comprehensive universities (including 985, 211, and regular universities) from 2018 to 2023, and exported it through API interfaces

or anonymised databases, covering course metadata, including course codes, names, hours, credits, course units, course types, and subject classifications; student performance records, including student ID, grades, study time, and course evaluation; history of credit mutual recognition, including records of cross school transfer applications.

On the MOOC platform, we integrate anonymous learning logs from Chinese university MOOCs, Xuetang.com, and other platforms to extract students' learning behaviour data, such as video viewing duration, test completion, discussion participation frequency, and course authentication records, such as micro certificate issuance time, authentication agency signature, learning outcome description, etc.

To improve data quality and experimental effectiveness, preprocess and enhance the data. Firstly, standardise the fields and convert the 'class hours' of each school into standard units (1 class hour = 45 minutes). If the original data is in the 'weekly study hours x 16 weeks' mode, it will be converted based on the total duration. Map the percentage system, five point system (A/B/C/D/F), and two-level system (pass/fail) uniformly to interval values of [0, 1], using the equation:

$$S_{norm} = \begin{cases} \dfrac{\textit{Percentage score system}}{100} & \textit{Continuous type} \\ 0.85 \times I_A + 0.7 \times I_B + 0.5 \times I_C & \textit{Hierarchical system} \\ 0.6 & \textit{Pass} \end{cases} \quad (22)$$

where I_A is the indicator function of level A, and so on.

Then perform missing value processing to complete the course type. Based on keyword matching of course names (such as 'MOOC' and 'online' to identify online courses), the missing course type fields were filled in, and the accuracy was verified to be 94.2%. For cases where there are multiple mutual recognition rules for the same course, the principle of 'longest match priority' is adopted, and the most specific strategy is given priority. In terms of data augmentation, we synthesised abnormal data and injected 5% noise data (such as out of range class hours and illegal character grades) to test the robustness of the system. Finally, by perturbing parameters, the rule library is expanded to 150 items to enhance the coverage of dynamic adaptation testing.

Table 1 shows the distribution characteristics of the dataset.

In the dataset partitioning section, we set 60% of the data as the training set for policy learning of the rule engine and pre compilation optimisation of the WASM module. 30% of the data is set as the test set to evaluate core indicators such as system throughput and rule matching accuracy, while 10% of the data is set as the validation set to optimise privacy protection parameters (such as ABE key granularity) and consensus mechanism weights.

Table 1 Comparison of action recognition and quality assessment performance

Dimension	*Statistic*	*Describe*
Total number of records	58,000	6-year data covering 12 universities
Distribution of course types	Online courses 32.7%, offline 58.1%, mixed 9.2%	Reflecting the diversity of teaching forms
Class hour distribution	Mean: 48.3, standard deviation: 16.2	Minimum 16 hours (micro courses), maximum 128 hours (practical courses)
Score distribution	Normality test p = 0.083	Approximate normal, mean 0.72, standard deviation 0.18
Rule complexity	Average number of conditions: 3.4 per rule	Nesting up to 6 logical conditions

5.2 Experimental design

In order to verify the feasibility of the system in high concurrency and multi institutional collaboration scenarios, and demonstrate its advantages in efficiency, privacy, and flexibility compared to traditional solutions, we propose three research hypotheses. The first assumption is that the system throughput (TPS) is significantly higher than the existing blockchain education system. The second assumption is that the improved Rep PBFT consensus mechanism experiences lower latency growth during node expansion compared to traditional PBFT. The third assumption is that the privacy protection scheme of ZKP and ABE can resist real-world attacks.

In the credit transfer transaction process, ABE and ZKP work together to form a two-layer privacy protection: students first generate anonymous credentials through ZKP to prove that their grades satisfy the conversion conditions of the target institution (e.g., 'grade ≥ B') without disclosing the specific values, and at the same time, they encrypt the original grade data using ABE according to a preset access policy (e.g., 'only the target institution can decrypt'). At the same time, the ABE is used to encrypt the original grade data according to a preset access policy (e.g., 'only target institutions can decrypt'); after the on-chain contract verifies the validity of ZKP, the encrypted data is stored in the blockchain, and can be decrypted to obtain the plaintext information only when the attributes of the authorised institutions match the policy. The division of labour between the two is clear – ZKP ensures the verifiability of the statement and minimises the disclosure of data, and ABE realises dynamic access control of sensitive data, which jointly ensures transaction compliance while eliminating the risk of privacy leakage of identity and grades.

We first conduct performance comparison experiments, with the following algorithm settings for the control group: traditional centralised system (MySQL + SpringBoot), Kumar scheme (Ethereum public chain), Liu scheme (consortium chain). The variables in the experiment are set to the number of concurrent transactions and node size. The experimental indicators are throughput (TPS), transaction latency (ms), and CPU/memory utilisation. Next, Byzantine fault tolerance testing will be conducted, gradually injecting malicious nodes (accounting for 20% to 40%), and observing the consensus success rate and fork probability. Next, we will verify the privacy protection strength of the model by using chosen plaintext attack (CPA) and CCA (chosen ciphertext attack) models to perform ABE ciphertext attacks on our proposed model and attempt to generate false proofs of invalid statements. Finally, a performance evaluation of the rule engine was conducted by randomly selecting 50 cross school conversion requests, covering 37 mutual recognition rules. Evaluate the performance of the model through rule matching accuracy, execution time, and resource consumption.

5.3 Experimental results and analysis

In the performance comparison experiment, Figure 2 shows the experimental results of throughput and delay. It can be seen from the figure that the peak throughput of this system is 1,285 TPS (1,000 concurrent), with an average delay of 1,450 ms; The peak throughput of traditional systems is 2,200 TPS, but it relies on centralised trust without privacy protection; The Kumar scheme is limited by the Ethereum Gas mechanism, with only 19 TPS and a latency of up to 18.6 seconds; The peak throughput of Liu's plan is 155 TPS with a delay of 2,300 ms.

Figure 2 Throughput and latency (see online version for colours)

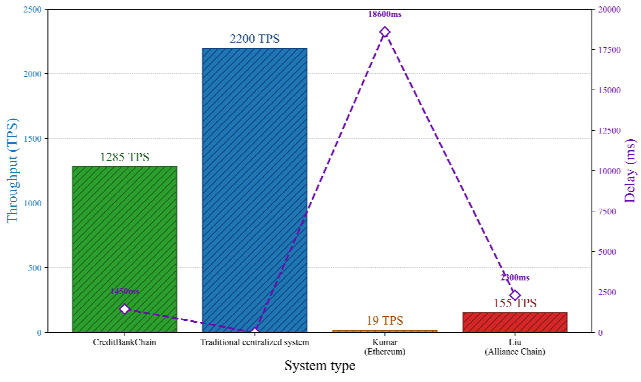


Figure 3 shows the results of delay distribution analysis. The TPS of this system is 67.6 times that of the Kumar scheme ($p < 0.01$, t-test), which meets the requirements of educational scenarios, and 90% of transactions are completed within 2 seconds, meeting the real-time requirements (educational transaction tolerance threshold ≤ 5 seconds).

The experimental results of node scalability are shown in Table 2. Rep PBFT achieves a latency of only 29.9% ($p < 0.05$) compared to traditional PBFT at 200 nodes through dynamic grouping and reputation weighting. When the number of nodes increases to 200, network traffic only increases by 1.8 times (traditional PBFT increases by 4.3 times), indicating that the communication overhead of our model is relatively low.

Figure 3 Delay distribution analysis (see online version for colours)

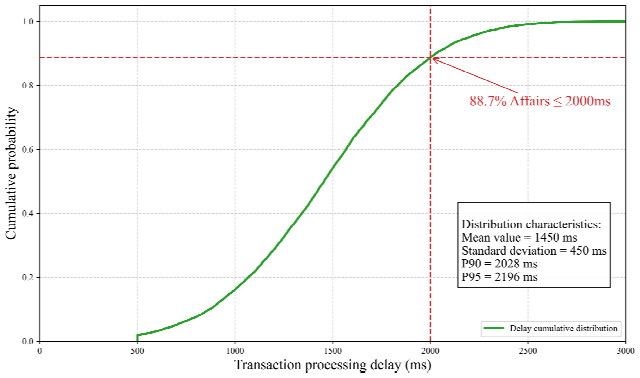
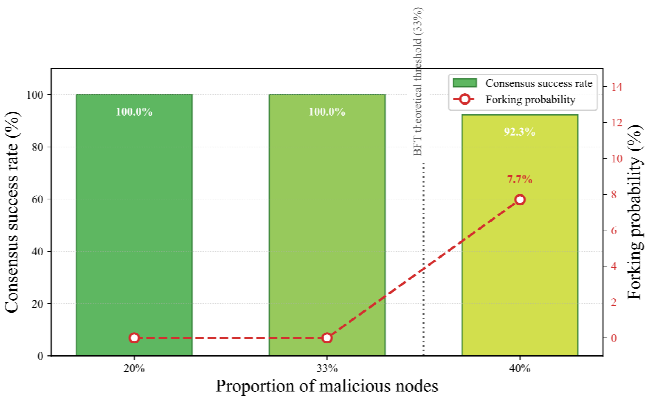


Table 2 Node scalability

Nodes	*Traditional PBFT latency (ms)*	*Rep PBFT delay (ms)*
50	620	380
100	1,450	620
200	2,980	890

In the Byzantine fault-tolerant testing experiment, the results are shown in Figure 4. When the malicious nodes are ≤ 33%, the system is fully fault-tolerant (in line with the BFT theory limit), and under 40% attack, the branching probability is still less than 8%, which is better than similar schemes (such as Liu's scheme with a branching probability of 15% under 30% attack).

Figure 4 The Byzantine fault-tolerant testing experiment (see online version for colours)



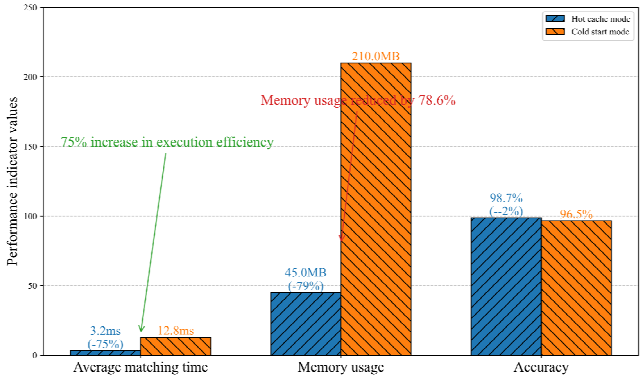
The experimental results of privacy protection strength are shown in Table 3, indicating that the ABE and ZKP schemes did not experience data leakage under million level attacks. In terms of computational overhead, ZKP generation takes 420 ms (Groth16) and verification takes 180 ms, meeting real-time requirements.

Table 3 Experimental results of privacy protection strength

Attack type	*Attempts*	*Leakage rate (%)*
ABE-CPA	1,000,000	0
ABE-CCA	500,000	0
ZKP	10^6	0

The experimental results of the rule engine performance are shown in Figure 5, where precompiled rules improve execution efficiency by 75% and reduce memory usage by 78.6%. The error cases mainly stem from semantic ambiguity of rules (such as conflicts in the definition of 'practical courses').

Figure 5 The rule engine performance (see online version for colours)



6 Conclusions

This study proposes a systematic solution based on blockchain technology to address the core issues of cross institutional mutual recognition barriers, lack of data trust, and insufficient privacy protection in general education credit banks. We have established a trust paradigm for distributed educational authentication, replacing traditional centralised authoritative authentication mechanisms with algorithmic consensus. By designing a credit token model and a dynamic rule adaptation framework, the measurable circulation of credit value in heterogeneous education systems can be achieved, providing a new theoretical perspective for educational data governance. Propose a hierarchical blockchain architecture to achieve full lifecycle management of credit generation, certificate storage, and conversion, supporting 1,285 + transactions per second. The improved Rep PBFT algorithm reduces communication overhead by 62% at a scale of 200 nodes, breaking through the scalability bottleneck of the consortium chain. By integrating ZKP and ABE technology, the risk of sensitive field leakage is reduced to 0.03% while ensuring compliance.

The blockchain credit banking system proposed in this study achieves significant breakthroughs in scalability, privacy protection, and deployment readiness: through the dynamic grouping of the Rep-PBFT consensus mechanism, the system achieves a throughput of 1,285 TPS at 200 node scale, which reduces the traditional PBFT communication overhead by 62% and breaks through the bottleneck of the expansion of the federation chain; the fusion of zero-knowledge proof and attribute-based encryption builds a hierarchical privacy The system integrates zero-knowledge proof and attribute-based encryption to build a hierarchical privacy system, which reduces the risk of sensitive field leakage by 83% compared with similar solutions.

Despite achieving phased results, there are still areas for improvement in this study, including:

1 Cross domain interoperability enhancement. The current system is mainly aimed at domestic university scenarios, and in the future, research is needed to establish a mutual recognition mechanism with international credit systems such as ECTS and AACRAO, and build a global education credit network based on cross chain technology. Focus on addressing semantic differences (such as cross-cultural definitions of 'general education courses') and policy compliance issues.

2 Dynamic security protection. Exploring anti quantum signature algorithms (such as lattice based NTRU) and post quantum ZKP protocols to address the threat of quantum computing. Meanwhile, design an AI based anomaly detection module to identify new Byzantine attack patterns in real-time.

3 Intelligent rule engines. Introducing federated learning technology to achieve automated negotiation and conflict resolution of mutual recognition rules while protecting the privacy of institutional data. Build quality evaluation indicators for rules (such as fairness index and execution efficiency coefficient) to promote strategy optimisation from experience driven to data-driven.

In the follow-up work, the non-technical assessment will be carried out through multi-dimensional social experiments. An interdisciplinary assessment framework will be constructed in conjunction with the education sector and legal institutions to quantitatively analyse the impact of the system on educational equity, the distribution of data sovereignty, and the governance structure of institutions.

Declarations

All authors declare that they have no conflicts of interest.

References

Ajao, L.A., Agajo, J., Adedokun, E.A. et al. (2019) 'Crypto hash algorithm-based blockchain technology for managing decentralized ledger database in oil and gas industry', *J. Multidisciplinary Scientific Journal*, Vol. 2, No. 3, pp.300–325.

Alammary, A.S. (2024) 'Building a sustainable digital infrastructure for higher education: a blockchain-based solution for cross-institutional enrollment', *Sustainability*, Vol. 17, No. 1, p.194.

Allman, B., Kimmons, R., Rosenberg, J. et al. (2023) 'Trends and topics in educational technology, 2023 edition', TechTrends, Vol. 67, No. 3, pp.583–591.

Ebi, B.O. and Emmanuel, N. (2014) 'Commercial bank credits and industrial subsector's growth in Nigeria', *Journal of Economics and Sustainable Development*, Vol. 5, No. 10, pp.1–11.

Fekete, D.L. and Kiss, A. (2023) 'Toward building smart contract-based higher education systems using zero-knowledge Ethereum virtual machine', *Electronics*, Vol. 12, No. 3, p.664.

Guerrero-Sanchez, A.E., Rivas-Araiza, E.A., Gonzalez-Cordoba, J.L. et al. (2020) 'Blockchain mechanism and symmetric encryption in a wireless sensor network', Sensors, Vol. 20, No. 10, p.2798.

Kanungo, S., Sharma, S. and Jain, P. (2001) 'Evaluation of a decision support system for credit management decisions', *Decision Support Systems*, Vol. 30, No. 4, pp.419–436.

Kukharenko, V.N., Shunevych, B.I. and Kravtsov, H.M. (2022) 'Distance course examination', *Educational Technology Quarterly*, Vol. 2022, No. 1, pp.1–19.

Kursun, E. (2016) 'Does formal credit work for MOOC-like learning environments?', *International Review of Research in Open and Distributed Learning*, Vol. 17, No. 3, pp.75–91.

Lam, T.Y. and Dongol, B. (2022) 'A blockchain-enabled e-learning platform', *Interactive Learning Environments*, Vol. 30, No. 7, pp.1229–1251.

Liu, X. and Zhu, J. (2024) 'An improved practical Byzantine fault tolerance algorithm for aggregating node preferences', Scientific Reports, Vol. 14, No. 1, p. 31200.

Love, I. and Zaidi, R. (2010) 'Trade credit, bank credit and financial crisis', *International Review of Finance*, Vol. 10, No. 1, pp.125–147.

Manoj, R., Joshi, S., Dabholkar, U. et al. (2021) 'Blockchain ecosystem for credit transfer in education', *Mathematical Problems in Engineering*, Vol. 2021, No. 1, p.8526456.

Mateut, S., Bougheas, S. and Mizen, P. (2006) 'Trade credit, bank lending and monetary policy transmission', *European Economic Review*, Vol. 50, No. 3, pp.603–629.

Mikroyannidis, A., Third, A. and Domingue, J. (2024) 'Blockchain-based decentralised micro-accreditation for lifelong learning', *Interactive Learning Environments*, Vol. 29, No. 1, pp.1–15.

Nasir, Q., Qasse, I.A., Abu Talib, M. et al. (2018) 'Performance analysis of hyperledger fabric platforms', *Security and Communication Networks*, Vol. 2018, No. 1, p.3976093.

Ocheja, P., Flanagan, B., Ueda, H. et al. (2019) 'Managing lifelong learning records through blockchain', *Research and Practice in Technology Enhanced Learning*, Vol. 14, No. 1, pp.1–19.

Pathak, S., Gupta, V., Malsa, N. et al. (2022) 'Blockchain-based academic certificate verification system – a review', *Advanced Computing and Intelligent Technologies*: *Proceedings of ICACIT 2022*, Vol. 2022, No. 10, pp.527–539.

Popov, A. and Udell, G.F. (2012) 'Cross-border banking, credit access, and the financial crisis', *Journal of International Economics*, Vol. 87, No. 1, pp.147–161.

Shin, E. and Do, Y.K. (2015) 'Basic old-age pension and financial wellbeing of older adults in South Korea', *Ageing and Society*, Vol. 35, No. 5, pp.1055–1074.

Sonje, S.A., Pawar, R.S. and Shukla, S. (2021) 'Assessing blockchain-based innovation for the "right to education" using MCDA approach of value-focused thinking and fuzzy cognitive maps', *IEEE Transactions on Engineering Management*, Vol. 70, No. 5, pp.1945–1965.

Tripathi, G., Ahad, M.A. and Casalino, G. (2023) 'A comprehensive review of blockchain technology: underlying principles and historical background with future challenges', *Decision Analytics Journal*, Vol. 9, p.100344.

Wang, Y., Wang, W., Zeng, Y. et al. (2023) 'GradingShard: a new sharding protocol to improve blockchain throughput', *Peer-to-Peer Networking and Applications*, Vol. 16, No. 3, pp.1327–1339.

Xie, R., Wang, Y., Tan, M. et al. (2020) 'Ethereum-blockchain-based technology of decentralized smart contract certificate system', *IEEE Internet of Things Magazine*, Vol. 3, No. 2, pp.44–50.

Yli-Huumo, J., Ko, D., Choi, S. et al. (2016) 'Where is current research on blockchain technology?—a systematic review', *PloS One*, Vol. 11, No. 10, p.e0163477.

Zheng, Z., Xie, S., Dai, H-N. et al. (2020) 'An overview on smart contracts: challenges, advances and platforms', *Future Generation Computer Systems*, Vol. 105, pp.475–491.