Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Combinatorial Press

Blockchain Applications and Challenges in Cross-Institutional Educational Evaluation Data Sharing

Wei Yue[1,✉], Yufeng Zhou[2], Yongtao Nie[1]

[1] *Innovation and Entrepreneurship Guidance Center, Weifang Engineering Vocational College, Weifang, Shandong, 262500, China*

[2] *School of Marxism, Weifang Engineering Vocational College, Weifang, Shandong, 262500, China*

ABSTRACT

Data empowers educational evaluation, and blockchain technology aids in the governance of educational evaluation data. The union of big data and blockchain technology has prompted the development of educational evaluation toward digitalization and precision of educational evaluation. This paper combines the multifaceted governance utility of blockchain technology for educational evaluation data and proposes to improve the consensus mechanism in educational evaluation information sharing. The PBFT consensus algorithm is updated with node contribution reward and punishment mechanism, the consensus nodes are selected by Fibonacci function characteristics, and the consistency protocol is optimized, so as to design a practical Byzantine fault-tolerant algorithm NCG-PBFT based on node contribution grouping, and analyze the credit value, throughput, normal block out delay, and the number of communications of NCG-PBFT consensus algorithm. Build a comprehensive education quality evaluation platform and bring in the improved PBFT consensus algorithm to test the operation performance of the comprehensive education quality evaluation platform. When the request frequency tends to be stable, the education comprehensive evaluation system of NCG-PBFT consensus algorithm is able to improve the system throughput by 74.54% compared with the PBFT algorithm, which is able to meet the performance and stability requirements of the education comprehensive quality evaluation system.

Keywords: PBFT consensus algorithm, blockchain technology, throughput, education evaluation

1. Introduction

Teaching evaluation is mainly the evaluation of students' learning effect and the evaluation of teachers' teaching work process, including the evaluation of teachers' teaching work (teaching design, organization, implementation, etc.) and the evaluation of apprentices' learning effect (i.e., learning achievement) [1-2]. The main goal of the blockchain concept teaching evaluation reform is to promote

✉ Corresponding author.
E-mail address: 19506533327@163.com (W. Yue).
Received 14 October 2024; Revised 05 December 2024; Accepted 10 March 2025; Published Online 16 April 2025.
DOI: 10.61091/jcmcc127b-012

the diversification of teaching evaluation and the disclosure of information within a certain range. This reform is closely linked to informatization [3-4].

At present, the positioning of talent cultivation objectives of each applied university is closely aligned with social needs, but the way of realizing talent cultivation is relatively backward, and there are the problems of solidified teaching mode, teacher-centered teaching method, single assessment system, single evaluation subject, and non-objective assessment results, and innovation and entrepreneurship ability cultivation is based on the classroom, the lack of practical experience, and the poor initiative [5-8]. At present, the teaching of colleges and universities lacks the characteristics of "polycentricity", "non-tampering" and "socialization", so the introduction of blockchain technology into the "teaching-evaluation-innovation" system, and the research on the innovation and development of application-oriented universities from the perspective of technological innovation, in order to build and operate a teaching evaluation system based on blockchain technology, is not only an important breakthrough in strategically building an educational power in the new era and shaping new advantages in education development, but also a necessary measure to give full play to technological innovation, link the digital ecology of higher education, and accelerate the digital transformation of application-oriented university education [9-12].

“Blockchain+” is an innovative technology-based mindset that ensures the security, authenticity, reliability and traceability of data. Blockchain technology is deeply integrated with traditional industries to meet the needs of digital transformation through innovation and iteration, in order to realize the “Blockchain + N” industry enterprise change, and create a new industry with blockchain technology as the innovative elements and infrastructure [13-15]. The blockchain consensus mechanism, traceability mechanism, anti-tampering mechanism, collective maintenance and high degree of autonomy mechanism established with the technological revolution can ensure that the introduction of blockchain can effectively resolve common problems such as business-as-usual, lack of trust, and data silos in the cultivation of higher education talents, and promote the change of education [16-18].

This paper analyzes the advantages of educational evaluation based on big data and blockchain technology. It interprets the development of data-enabled educational evaluation from three aspects: logical unification, efficiency reshaping, and evaluation depth. Combined with the development of blockchain technology, it organizes the role of blockchain technology on educational data governance in points. Propose PBFT consensus algorithm, improve the algorithm step by step, and propose NCG-PBFT consensus algorithm in education evaluation information sharing. Analyze the credit score reward Rsr, credit score penalty Rsp, and node credit values under honest behavior and faulty behavior of the improved consensus algorithm. Propose a comparison method to examine the throughput, normal block out delay, and the number of communications of the improved consensus algorithm. Construct a multilayer education comprehensive quality evaluation platform and analyze the platform operation performance using the improved NCG-PBFT consensus algorithm.

2. Educational evaluation based on big data and blockchain technology

Educational evaluation based on big data and blockchain technology improves the digital governance of education. Digital empowerment, using digital technology, thinking, and cognition, improves the scientific nature of education evaluation and breaks down the traditional digital barriers in education. Solve the information asymmetry in the construction of teaching resources and imperfections in the certification/evaluation system due to the long-term, ambiguous and complex nature of educational activities. With the relevance of blockchain technology, using the holistic nature of big data technology, integrating blockchain technology with the certification/evaluation system, resource circulation system, learning credit system, establishing an educational resources database, decentralized certificate certification/evaluation system, intelligent learning resources, forming an educational

integration, sharing the “digital dividend”, and providing a reference for the improvement of the educational system. Provide reference for the improvement of education system [19-20].

2.1. Data-enabled education evaluation

In the research related to big data and educational evaluation, data-enabled educational evaluation has been unidimensionally regarded as a simple superposition of data, technology and educational evaluation at the level of “things”. However, data-enabled education evaluation is not only a combination of the three relationships. As an important part of the digitization of education, it focuses on the shift from traditional forms of educational evaluation to data-enabled. Double deconstruction of the internal logic of data-enabled education evaluation from the level of “things” and “people” will help break through the dependence on the “path” of education evaluation and realize the transformation of the education evaluation paradigm.

1) Value-added orientation: realizing the balance and unity between the logic of educating people and the logic of screening and discernment. Educational evaluation is one of the main forms of existence of education, and the view of educational evaluation guides the view of education. The technology represented by big data is shaping a new type of educational evaluation. The value-added orientation of educational evaluation is promoted through data empowerment, which helps to realize the balance and unity between the logic of educating people and the logic of screening.

With the extension of technology in the field of education, data-based educational evaluation is not only a means of educating people, but also an initiative for educating people in the digital age.

In terms of the evaluation standard system, the “people-oriented” standard is supplemented by the “data + professional research and judgment” support, focusing on the comprehensive quality of the students' investigation. In terms of evaluation targets, it encourages mutual benefit among multiple subjects and advocates a symbiotic relationship of synergistic “growth”. In the evaluation process, ensure that the data source is real and reliable, educate people in the evaluation process, and promote educating people through evaluation, so as to realize the comprehensive educating of the evaluation results.

2) Data-driven: helping to remodel and reshape evaluation quality and evaluation efficiency. "Data" is an important production tool to achieve "resource empowerment". "Education data" is the core enabling tool to achieve "quality and efficiency" of schools. Data-empowered education evaluation emphasizes the use of fine reorganization of educational elements and educational resources in the process of digital transformation to drive educational evaluation activities. Data-driven brings new trends and technologies, and its connotation lies in creating a new model of education evaluation characterized by virtual education evaluation field, fair education evaluation concept, and high-quality edu cation evaluation results.

3) Paradigm transformation: promoting the depth of data-driven and educational evaluation. Convergence of data-enabled education evaluation should not just be an overlay of data-driven and education evaluation, but an all-round deep integration of data-driven and education evaluation. This paradigm shift emphasizes the data-driven penetration of educational evaluation in terms of “governance,” “tools,” and “awareness,” thus contributing to the generation of a new ecology of educational evaluation. In this sense, the paradigm shift in educational evaluation encompasses a shift in governance represented by data decision-making, a shift in tools centered on data support, and a transformation of consciousness represented by data thinking.

2.2. The utility of blockchain technology for education data governance:

1) The decentralized nature of blockchain ensures the accuracy of education data mining and analysis. Through the use of blockchain technology, the education data monitoring platform is able to follow up the class size of each school in real time, and can also record and update the school planning layout and teacher training in a timely and accurate manner. On the basis of automatic analysis of big data,

the existing weak points can be precisely identified, and targeted and precise measures can be implemented to avoid the phenomenon of duplication of investment in educational resources.
2) The decentralization of blockchain dissolves the monopoly of educational data control. No one or more entities can control the storage and processing of data information and its integrity. The openness, borderlessness, and permissionlessness of blockchain technology can provide everyone with equal access to the technology and the network it builds.
3) The reliability of blockchain improves the verifiability of educational data use. Information can be kept constant and distributed over time in the blockchain. Any system participant can verify the authenticity of the data and ensure that it has not been tampered with. Network operation is not affected by the failure of a single node. In addition to system transparency and no tampering of data, blockchain technology has significant operational traceability features that make the use of educational data on the blockchain traceable, permanent and accountable, enabling the checking of the authenticity of diplomas and certificates verifying the skills and achievements of learners.
4) The security of the blockchain guarantees the copyrightability of educational data outcomes. Information and communications are secure if they are considered as blockchain transactions based on cryptographic protocols. Using blockchain technology, it is possible to confirm data attributes using verification of database records, as well as trace back to the root cause to ensure that the blockchain is able to store the entire process of data from its collection to its computational analysis, thus enabling a strong trust endorsement of the data quality and the establishment of trust between the entities involved.
5) The privacy of blockchain lays down the security of educational data sharing. The main difficulty and challenge of open data sharing is how to open data while protecting individual privacy. At present, databases in education are still threatened by multiple parties. One is hacker attacks. The second is the failure of software and hardware. The third is the system administrator's negligent operation to tamper with or lose the relevant data. Comparatively speaking, the consensus-based encryption algorithm adopted by blockchain technology is more capable of ensuring the privacy of educational data. Any attempt to change just a bit of information will break the existing chain. The use of blockchain data desensitization technology satisfies the need for privacy protection during the sharing of data.
6) The self-sovereignty and trust of blockchain optimizes the fairness and efficiency of educational data articulation. The key to the realization of blockchain self-sovereignty lies in empowering users to identify themselves while maintaining control over the storage and management of their personal data.

3. Consensus mechanisms in sharing information on education evaluation

3.1. PBFT Consensus Algorithm

The kernel of PBFT is composed of the following three main protocols: checkpointing protocol, consistency protocol, and view switching protocol. The checkpointing technique and consistency protocol must be used when the system is working normally. The view switching protocol and replacement of the master node can be enabled only when the master node is abnormal or the system works slowly [21].

3.1.1. PBFT conformance protocols. The approximate flow of the consistency protocol of the algorithm is as follows: assuming that there are 3f+1 nodes in the system (f is the number of Byzantine nodes that can be tolerated by the system), in the pre-preparation phase, the master node collects the transaction information to pack the block and broadcasts it to the whole network. In the preparation phase, each node, after receiving transaction information, simulates the execution of these transactions, calculates the Hash digest required for the new block and broadcasts the preparation information to the whole network. In the confirmation phase, if a node receives a Hash digest equal to its own from 2f other nodes, it broadcasts a confirmation message to the whole network. In the reply

phase, if a node receives 2f confirmation messages it can submit a new block to the local blockchain and the state database, and finally reaches a consensus. The PBFT algorithm consistency protocol flow is shown in Fig. 1.

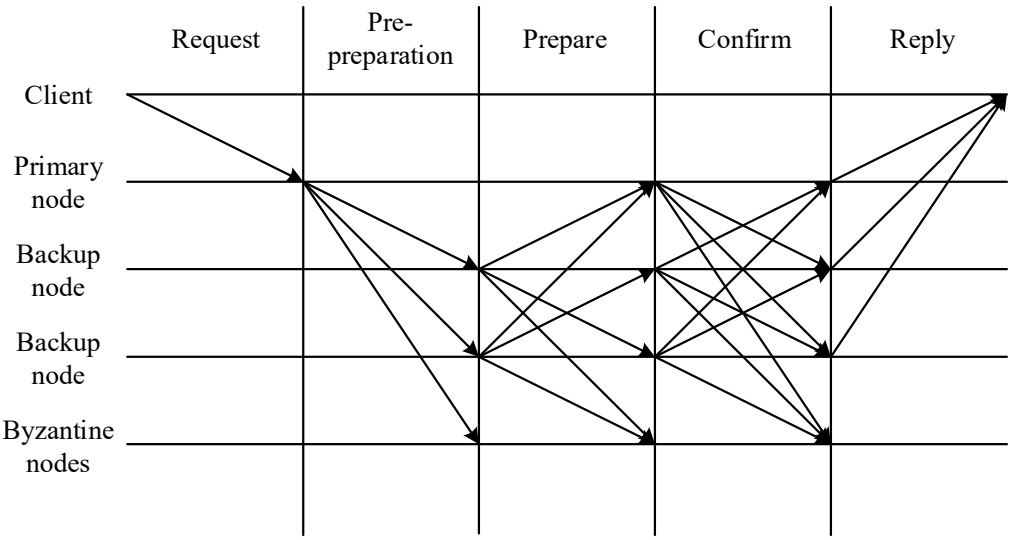

Fig. 1. The consistency protocol process for the proposed ft algorithm

3.1.2. Checkpoint protocols. Due to the consistency protocol every request executed by the system, the node has to record the log (including the messages sent in the request phase, pre-preparation phase, preparation phase, and acknowledgement phase). If the system does not clean up in time it will lead to a large amount of resources being occupied, affecting the availability of the system. As some nodes are unable to execute requests after starting from a certain sequence number due to network delay. Therefore, the periodic checkpointing protocol in order to synchronize the state of all nodes within the system, this is actually a block chasing process, the node through the blockchain timed broadcast of the state of the world or other nodes to send messages to be informed of the node's block lagging behind, and then to start the block chasing process.The checkpointing protocol of the PBFT algorithm is a good solution to the excessive logging caused by the waste of system resources, the availability of the reduced and the checkpointing protocol of PBFT algorithm well solves the problems of wastage of system resources due to too many logs, reduced availability and inconsistency of node state due to Byzantine nodes.

3.1.3. View switching protocol. Every node in the blockchain has to work under the same configuration information which is known as view. In PBFT algorithm after the failure of the master node, the master node needs to be replaced by running the view switching protocol. After the failure of the master node, the master node is elected according to equation (1):

$$\begin{cases} V = V + 1 \\ P = V \bmod |N| \end{cases} \tag{1}$$

Where P represents the number of the master node, V denotes the view number and |N| denotes the number of nodes within the system.

There are two triggering conditions for the view switching protocol.

A/No pre-prepared message broadcast by the master node is received within the fixed time T1.

B/ No new block is generated by the system within the fixed time T2.

And T2>T1, the system automatically triggers the view switching protocol when one of the above conditions is satisfied. The specific process is as follows:

First, view number +1, sends view-change message to all nodes.

Second, all nodes when received 2f+1 (f denotes the number of tolerable Byzantine nodes within the system) view-change messages, send view-change-ack confirmation messages to the master node in the new view. The corresponding new master node in the new view will collect view-change-ack messages from other nodes.

Finally, when 2f acknowledgement messages are collected, the new-view message is assembled and broadcasted to be sent to all nodes, after which the consistency protocol is executed based on the local link data.

3.2. Proposal and Design of NCG-PBFT Consensus Algorithm

The current blockchain-based information sharing system is mainly developed in a federation chain environment, where information between nodes is interacted and shared through the PBFT consensus algorithm. However, the PBFT consensus algorithm still has many problems. Its communication complexity is O (n^2) level, if the number of nodes in the educational institution is large, the communication pressure will be larger and the consensus efficiency is low.The master node in the PBFT consensus algorithm is selected in order, and the malicious node can launch a denial-of-service attack on the node before its number, which leads to the failure of the master node in front of it, and thus is elected as the new master node. At the same time, there is no reward and punishment mechanism for malicious nodes and honest nodes, and the probability of malicious nodes doing evil is not improved.

To address the above problems, this paper makes improvements on the basis of PBFT consensus algorithm and proposes a practical Byzantine fault-tolerant algorithm NCG-PBFT based on the grouping of nodes' contribution degree.It effectively improves the consensus efficiency and makes it more suitable for the sharing scenario of educational information. The algorithm divides all the nodes in the network system into four major categories according to their duties, which are consensus nodes, master nodes, monitoring nodes and other nodes.

3.2.1. Node contribution reward and punishment mechanism. Adding the contribution reward and punishment mechanism to the NCG-PBFT consensus algorithm, the nodes are divided into three levels according to their contribution, which improves the security of the system.

This paper introduces the design of contribution reward and punishment mechanism based on the idea of dynamic reputation evaluation model designed. The calculation method of node contribution degree and the way of node category updating will be introduced in the following.

The initial value of the contribution degree of a newly registered node in the system is set as: $C_{init} = 0.5$. The node contribution value is calculated as shown in equation (2):

$$T_{n=}exp\{[(\sum_{x=1}^{n} z(x) - \lambda \times \sum_{x=1}^{n} h(x)) - (v \times \sum_{x=1}^{n} g(x) + \rho \times \sum_{x=1}^{n} l(x))] / n - 1\} \tag{2}$$

Where $\Sigma_{x=1}^{n} z(x)$ denotes the total number of times the consensus node has successfully reached consensus in the historical consensus process. λ represents the penalty factor for consensus node consensus failure, and $\Sigma_{x=1}^{n} h(x)$ represents the total number of times the consensus node has failed to reach consensus in the previous consensus process. v represents the consumption factor for successful consensus of the master node, and $\Sigma_{x=1}^{n} g(x)$ represents the total number of times that the consensus node has succeeded in consensus as the master node in the consensus over. The penalty factor for the failure of the master node consensus is denoted by ρ, and $\Sigma_{x=1}^{n} l(x)$ represents the sum of the number of times that the node fails to reach consensus as the master node in the consensus process. The value of λ, v, ρ in the above equation can be changed according to the actual situation.

The calculation of the final node contribution also needs to take into account the network stability value, which is calculated based on the time that each node has continuously joined the network, as shown in equation (3):

$$P_n = \frac{2}{1+exp(-(t_{present} - t_{begin}))} \tag{3}$$

Where $t_{present}$ represents the current time value and t_{begin} represents the time value of the node's previous access to the network. The final node's contribution is:

$$C_{final} = C_{init} + \gamma T_n + (1-\gamma)P_n \tag{4}$$

Where γ is an adjustment parameter that adjusts the node contribution and network stability value as a percentage of the node's final contribution. When a node becomes a malicious node, the contribution degree of the node is directly set to 0 and it is removed from the blockchain network system.

According to the calculation of the above formula, as shown in equation (5), the contribution degree of each node is:

$$C = \begin{cases} C_{init} & \text{Node is a newly registered node} \\ C_{final} & \text{Node is a non-evil node} \\ 0 & \text{Node is the evil node} \end{cases} \tag{5}$$

3.2.2. Consensus node selection mechanismIn NCG-PBFT consensus algorithm, all nodes except monitoring nodes are sorted in descending order of node contribution. In NCG-PBFT consensus algorithm, the total number of nodes is set to $N(N \geq 5)$, the total number of nodes with contribution not less than C_{imit} is set to $N_r(N \geq 5), Group_i \in \{Group_1, Group_2, Group_h\}$ denotes the blockchain nodes in the ith group and $Group_k$ denotes the last group of blockchain nodes. The consensus nodes are selected using the Fibonacci function property, and the recursive nature of the Fibonacci function is as follows $(n \geq 3, n \in N^*)$:

$$\begin{cases} S(1) = S(2) = 1 \\ S(n) = S(n-1) + S(n-2) \end{cases} \tag{6}$$

All the nodes in the blockchain whose contribution is not less than C_{imit} are categorized into h groups in total using the Bonnacci function, and there are $S(h-1)$ nodes in Grouph. $Node_{mn}$ denotes the n th node in Groupm, where $1 \leq m \leq h-1, 1 \leq n \leq S(m)$.

3.2.3. Master node selection mechanism. The consensus nodes are selected and all the consensus nodes are ranked in descending order according to the node contribution. The top two consensus nodes will be used as candidate master nodes and other consensus nodes are utilized to vote for these two candidate master nodes. When consensus nodes vote, they can perform three operations: support, oppose, and abstain.

The voting result is calculated as shown in equation (7):

$$\begin{cases} R_{ab} = C_{ab} + \sum_{m=1}^{k-1}\sum_{n=1}^{up} Vote_{mn} + \sum_{n=1}^{num} Vote_{kn} \\ up = upper\left(\frac{S(m)}{2}\right) \\ num = upper\left(\frac{N_r - \sum_{t=1}^{k-1} S(t)}{2}\right) \end{cases} \tag{7}$$

Where, R_{ab} is the voting score received by the b rd candidate master node in group a. C_{ab} denotes the contribution value of the b th candidate master node in group a. $1 \le a \le 2, b = 1, Votemm$ denotes the total number of votes cast by the n th consensus node in group m. 1, -1 and 0 are the values corresponding to support, oppose and abstain respectively.

The candidate master node that finally obtains a large voting score will be elected as the master node, and if the two candidate master nodes finally obtain equal voting scores, the consensus node with the first ranked contribution value before the voting will be selected as the master node.

3.2.4. Optimizing Conformance Protocols. In this paper, the consistency protocol is improved according to the idea of optimizing the consistency protocol, and the two-by-two interaction of the PBFT consensus algorithm is turned into a one-way sending.The execution process of NCG-PBFT algorithm is shown in Fig. 2. Among them, node 0 is the master node in the NCG-PBFT consensus algorithm, nodes 1, 2, and 3 are consensus nodes, and node 3 is a Byzantine node. The remaining nodes are the nodes in the NCG-PBFT consensus algorithm whose contribution is greater than or equal to Cinit but have not become consensus nodes. The dotted lines in the figure show the boundaries of the stages in the consensus, arrows indicate that the source node sends the message to the receiver node, arrows with dotted lines indicate that the message has been tampered with, and f indicates the number of Byzantine nodes in the consensus node.

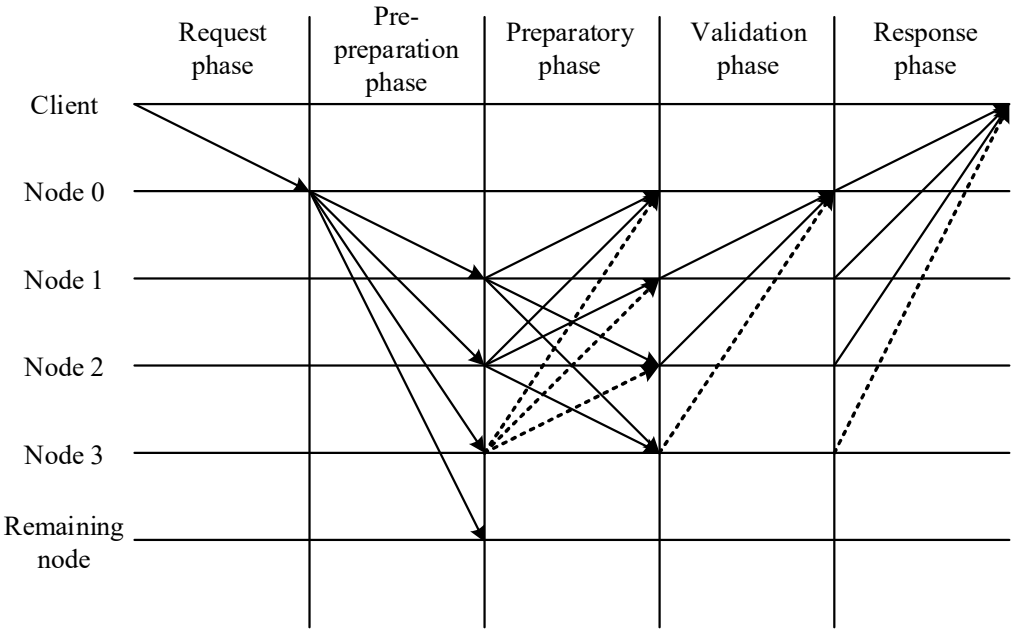

Fig. 2. NCG-PBFT Algorithm Flowchart

4. Application of the NCG-PBFT consensus algorithm to educational evaluation

4.1. Algorithm experiment and performance analysis

This chapter analyzes the communication overhead, security and activity of NCG-PBFT algorithm. Multi-node communication is simulated using docker and go language is used as the programming language, node credit value changes, throughput and latency are tested and compared with the PBFT algorithm to verify the effectiveness of the NCG-PBFT algorithm. The environment configuration is shown in Table 1.

Table 1. Environmental configuration

Configuring	Model/version
Processor	AMD Ryzen 7 4800U
Memory	32GB
Operating system	ubuntu20.04.4
docker	docker 20.10.21

4.1.1. Change in credit value. The experiment tested the trend of node credit value when nodes do honest behavior with different credit score reward Rsr. The number of nodes n is set to 25, Msr to 0.01, Chigh to 0.8, and 500 times consensus is performed. The trend of node credit value growth is shown in Fig. 3. When Psr=0.05, the NCG-PBFT algorithm node credit value can reach up to 0.95.With the increase of Rsr, the node credit value growth becomes faster. When the credit threshold of advanced nodes is reached, the growth rate becomes slower, showing the trend of first fast and then slow. After many rounds of consensus, the node credit value is maintained at a high level.

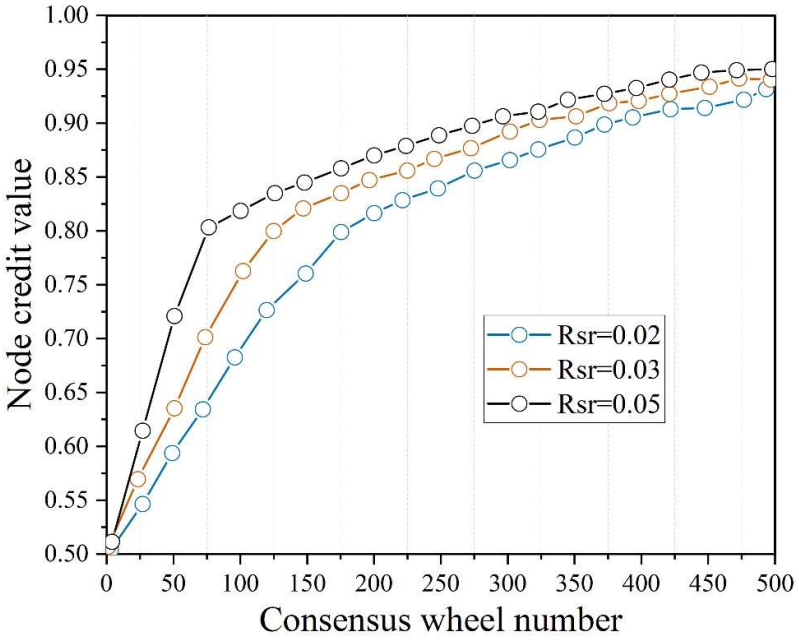

Fig. 3. Node credit value growth trend

The experiments tested the change in credit values of nodes after consecutive failures with different credit scores penalizing Rsp. The nodes are set to start failing after performing 50 honest behaviors for 50 consensus rounds.

The trend of node credit value is shown in Fig. 4, with credit score penalty Rsp=0.2 and number of consensus rounds=50, the node credit value is at [0,0.1]. The credit value starts to decline from a

higher level, and the rate of decline gradually becomes slower, and the higher the credit score penalty Rsp is, the faster the credit value declines. The Rsp and credit threshold can be set according to different situations, when the credit score penalty is high, the node will be downgraded from a normal node to a low-level node as long as the node makes multiple errors.

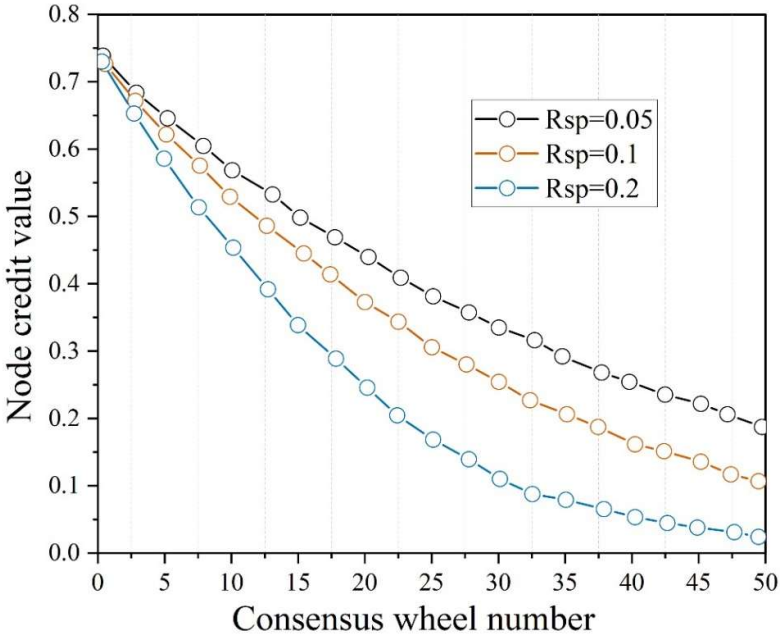

Fig. 4. Node credit value change trend

The experiment tested the growth of the credit value of nodes doing honest behavior after a failure and compared it with the nodes that did not have a failure. The nodes were set up to perform 50 consensus sessions, in which they performed honest behavior, 10 faulty behaviors and 20 faulty behaviors, with Rsr of 0.02, Rsp of 0.05, Msr of 0.01, and Chigh of 0.8, for 300 consensus sessions.

Comparison of honest node and faulty node credit value growth is shown in Fig. 5, the more the number of node faults, the lower its credit value. With continuously doing honest behavior, the node credit value grows gradually. Influenced by the historical behavior as well as the use of evaluation factors, nodes with historical failures want to be elected as the master node, they need to do more honest behaviors to reach the credit threshold and have the right to elect the master node. And nodes with multiple failures or even malicious behaviors need to pay a bigger price. Thus the chance of Byzantine behavior in the system will be greatly reduced.

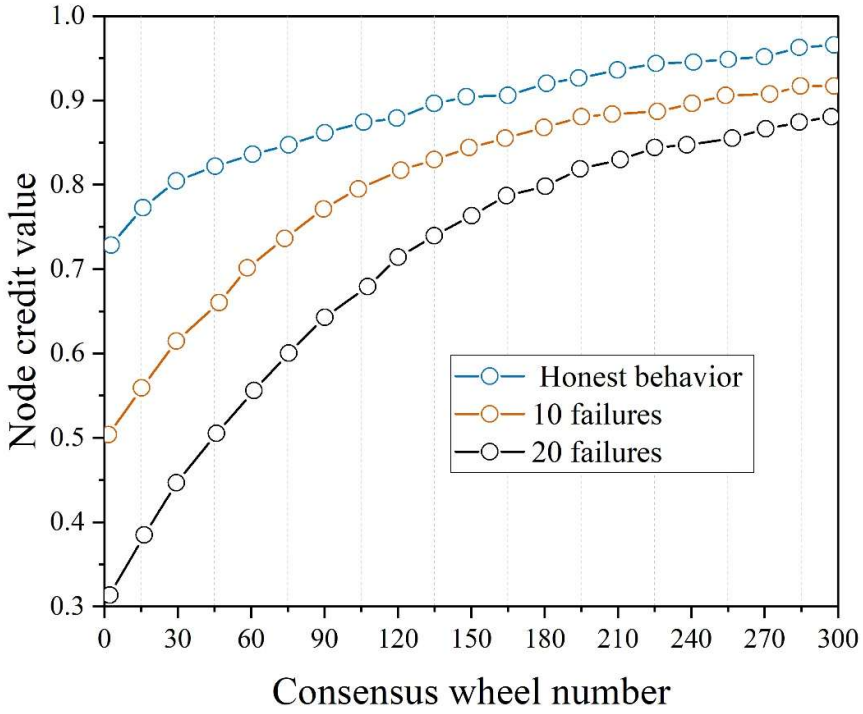

Fig. 5. The honest node is compared with the value growth of the fault node

4.1.2. Algorithm throughput experiment and analysis. The experiments test the throughput and latency of PBFT and the improved algorithm NCG-PBFT under different number of nodes respectively. 4 to 16 nodes are simulated through docker containers, the number of Byzantine nodes is set according to the maximum fault tolerance of the PBFT algorithm, and the number of transactions per transaction is set to 1000, and the experiments are conducted for several times and the average value is taken.

Throughput TPS is the number of transactions that can be processed per second, which is an important indicator of blockchain performance, and the TPS calculation formula is as follows:

$$TPS = \frac{Transactions}{time} \tag{8}$$

Where $Transactions$ is the number of transactions completed in the consensus process and $time$ is the time spent in the consensus process.

The results of throughput comparison for different number of nodes are shown in Table 2. As the number of nodes increases, the communication overhead for each round of consensus increases and the throughput decreases sharply. NCG-PBFT has higher throughput than PBFT under the same conditions. As the number of nodes increases, the more obvious the throughput effect improves. Due to the gradual increase in the number of Byzantine nodes, the original algorithm suffers from frequent view switching due to errors in the master node. The NCG-PBFT algorithm can penalize the error nodes, and the Byzantine nodes are not easy to be elected as master nodes. After a period of consensus, the system tends to stabilize, and the overall throughput is improved by about 9%.

Table 2. Comparison of throughput of different nodes

Node number	PBFT(pen/second)	NCG-PBFT (pen/second)
4	1989.663	1999.594
8	969.124	1056.221
12	573.787	695.865
15	556.639	635.946

18	521.405	611.288

4.1.3. Normal block out delay analysis. In a blockchain network, the normal out-of-block latency represents the time it takes for a node to successfully generate a new block. This value directly affects the performance of the entire blockchain network. In general, the shorter the normal block out delay of the consensus algorithm, the faster the transaction processing speed of the whole blockchain network will be. Therefore, the normal block out delay is one of the important indicators for testing the performance strength of consensus algorithms.

In this paper, NCG-PBFT is compared with PBFT and C-PBFT for normal block out delay, and the test data are shown in the table.

NCG-PBFT and PBFT normal block out delay test data is shown in Table 3.

With the increase in the number of nodes, the block out delay of PBFT consensus algorithm increases exponentially. And compared to NCG-PBFT consensus algorithm, the increase in the number of nodes does not have a significant impact on the block-out delay of the three clustered networks with k=4, 7, and 10. And under the condition of the same number of consensus nodes, the larger the value of k is, the fewer the number of communications to complete a consensus. Only when k=1, the block out delay grows more rapidly, but it is still much lower than the delay of PBFT. This result is due to the fact that the consensus algorithm in this paper is a PBFT consensus optimization algorithm based on clustering, which divides a large WSN into k non-empty clusters, each of which completes the first consensus step independently. Then the cluster head node of each cluster completes the inter-cluster consensus, and this process significantly reduces the communication overhead. Accordingly, the block out delay is also reduced.

Table 3. NCG-PBFT and PBFT normal out block delay test data

Number of nodes	NCG-PBFT				PBFT
	Avg(ms)				Avg(ms)
	K=1	K=4	K=7	K=10	
40	82	35	21	16	165
60	275	65	55	32	873
90	1200	300	197	174	2854
100	1367	400	231	189	3601
110	1822	430	265	234	4723
130	2965	783	440	301	6957

The NCG-PBFT and C-PBFT normal block out delay test data is shown in Table 4. Again, the block out delay of NCG-PBFT is lower for the same value of k.

Table 4. NCG-PBFT and C-PBFT normal out block delay test data

Number of nodes	NCG-PBFT		C-PBFT	
	Avg(ms)			
	K=4	K=10	K=4	K=10
40	410	321	758	450
50	632	400	1120	623
60	905	550	1784	804
70	1352	670	2565	1121
80	1695	803	3041	1287
90	2113	992	3956	1770
100	2670	1210	4875	1986

4.1.4. Algorithm communication count experiment and analysis. One of the important manifestations of the performance of an algorithm is the number of communications, and an excellent number of communications can enhance the efficiency of the algorithm.

In this section, the efficiency of NCG-PBFT algorithm is verified by comparing the number of communications in different situations between NCG-PBFT and PBFT, SPBFT and VPBFT consensus algorithms. The experiment first analyzes the number of communications between PBFT and NCG-PBFT algorithms in different situations.

1) Analysis of communication counts of PBFT consensus algorithm. In the consistency protocol of PBFT consensus algorithm, the master node broadcasts the client's message to other replica nodes in the pre-prepare phase for (n-1) times, the nodes in the prepare phase interact with each other for $(n-1)^2$ time, and each node in the commit phase responds to and sends the message to the nodes other than its own for $n(n-1)$ times. So the number of communication to complete the consistency protocol is as in Eq:

$$C = 2n(n-1) \tag{9}$$

If the master node is down or error occurs in the consensus, the number of communication is given in the following equation assuming that the probability of view switching protocol occurs is $p(0 < p < 1)$:

$$M = pn(n-1) \tag{10}$$

So the total number of communications of PBFT is given in Eq:

$$S = 2n(n-1) + pn(n-1) \tag{11}$$

2) NCG-PBFT consensus algorithm communication number analysis. There are only two phases in NCG-PBFT consensus algorithm, proposal and accept, so the number of communications in the process of consistency agreement is shown in Eq:

$$C^{'} = n(n-1) \tag{12}$$

In NCG-PBFT algorithm, it is assumed that the probability of the view switching protocol appearing is $v(v < p)$. The reliability of the master node is guaranteed due to the setup of the reputation ratio based master node decision group and the master node selection method in the No. method. The number of verification nodes is generally set to $(n-1)/6$, so the number of communications is as in Eq:

$$M^{'} = v\{[(n-1)/6]-1\}^2 \tag{13}$$

So the total number of communications of the NCG-PBFT algorithm is given in Eq:

$$S^{'} = n(n-1) + v[(n-7)/6]^2 \tag{14}$$

3) Ratio of the number of communications between the two algorithms. Without view switching protocol as in Eq:

$$T = \frac{2n(n-1)}{n(n-1)} \tag{15}$$

As shown in Eq. The number of communications of the PBFT consensus algorithm without view switching protocol is always greater than the NCG-PBFT No. 1 method and twice as many as the NCG-PBFT algorithm.

The case of view switching protocol occurs as shown in Eq:

$$T^{'} = \frac{2n(n01) + pn(n01)}{n(n01) + v[(n07)/6]^2} \tag{16}$$

In the NCG-PBFT algorithm, because the reliability of the master node selection is guaranteed at the beginning, although the number of communication times of both algorithms increases as the number of nodes increases, it can be seen that the number of communication times of the NCG-PBFT algorithm is much smaller than that of the PBFT algorithm through Equation (16).

The NCG-PBFT algorithm is compared with the other three algorithms for the communication number experiments, and the experimental results are shown in Fig. 6. The PBFT consensus algorithm communicates much more than the other three algorithms at a node count of 28, with a maximum value of 1700. In all four consensus algorithms, the number of communications increases with the number of nodes. However, the NCG-PBFT algorithm has the slowest growth rate, which is significantly lower than the remaining three consensus algorithms. It indicates that the reliable master node election mechanism and the optimization of the communication process effectively reduce the system communication overhead.

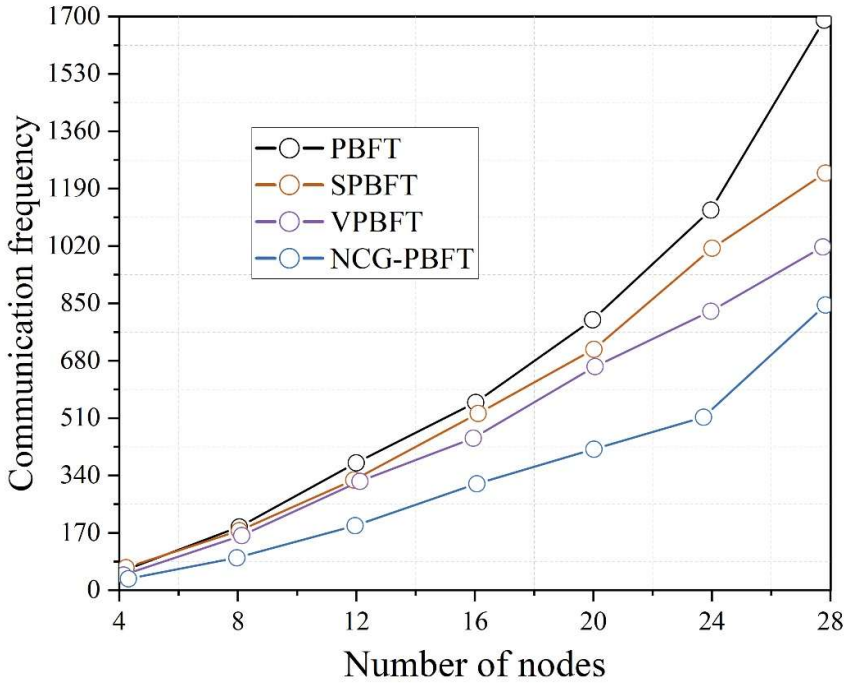

Fig. 6. Experimental results

4.2. Design of educational evaluation platform based on blockchain technology

4.2.1. Framework design. The overall framework structure of the comprehensive education quality evaluation platform is shown in Figure 7.

From the bottom up, the bottom layer is the infrastructure layer, which contains 5G high-speed network, education cloud server, artificial intelligence engine, cluster management, etc., providing basic services to realize real-time collection and high-speed transmission of data.

The second layer is the management layer, where all parties join the blockchain network in the form of nodes. For example, students, colleges and universities, learning institutions and organizations, through the public key infrastructure (PKI) and consensus mechanism to jointly complete the identity authentication management, the authentication of the nodes through the message interoperability between the nodes to ensure the consistency of the data. A small number of public service departments representing the government join as trust service nodes for supervision to prevent 51% arithmetic attacks from causing leakage or illegal modification of records.

The third layer is the data layer, which utilizes distributed ledger technology to integrate various educational and teaching activities and student learning activities data records. Through timestamp

sorting, it forms a perfect historical chain of educational big data and carries out distributed storage of educational big data, which provides the basis for the evaluation of talent training quality and discipline assessment work in the later stage.

The fourth layer is the service layer, which utilizes blockchain key technology to provide various application services. For example, smart contracts and timestamps are utilized to provide a secure and efficient learning environment to ensure the authenticity and non-tamperability of data. Asymmetric cryptographic algorithms are utilized to provide security for data storage, transmission and shared use, and to prevent leakage of sensitive and secret data, so as to ensure the confidentiality and integrity of data. Digital signatures are utilized to achieve identity auditing of all parties' subjects and prevent overstepping access to ensure data security. The highest layer is the application layer, which provides various kinds of applications for specific scenarios, such as comprehensive quality evaluation and learning achievement authentication.

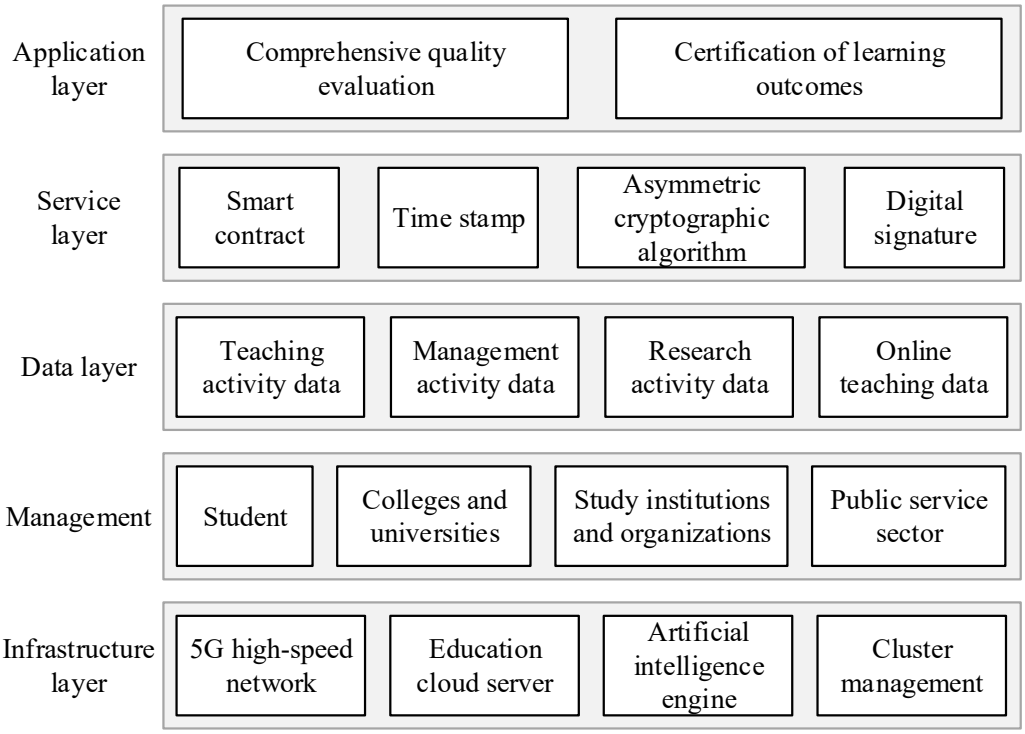

Fig. 7. The overall framework of the comprehensive quality evaluation platform

4.2.2. Platform testing. In order to verify whether the improved algorithm NCG-PBFT algorithm meets the performance and stability requirements of the comprehensive education quality evaluation system, the system needs to be stress-tested accordingly.

This test uses the Caliper tool to test the runtime throughput of the system, which is a blockchain performance benchmarking framework that allows users to test different blockchain solutions with customized use cases. Caliper is installed and configured for network connectivity, and the system's runtime throughput is stress tested using the npx caliper launch manager --caliper-workspace command.

The results of the system runtime throughput test are shown in Figure 8, where it can be seen that the request frequency reaches 350tx/s and stabilizes afterwards. Compared to the PBFT algorithm, the runtime throughput of the stabilized system is improved by 74.54%. Compared to the C-PBFT algorithm, the runtime throughput of the stabilized system is improved by 45.45%. The test results prove that the runtime throughput of the NCG-PBFT system has been significantly improved, which meets the performance and stability requirements of the comprehensive education quality evaluation system.

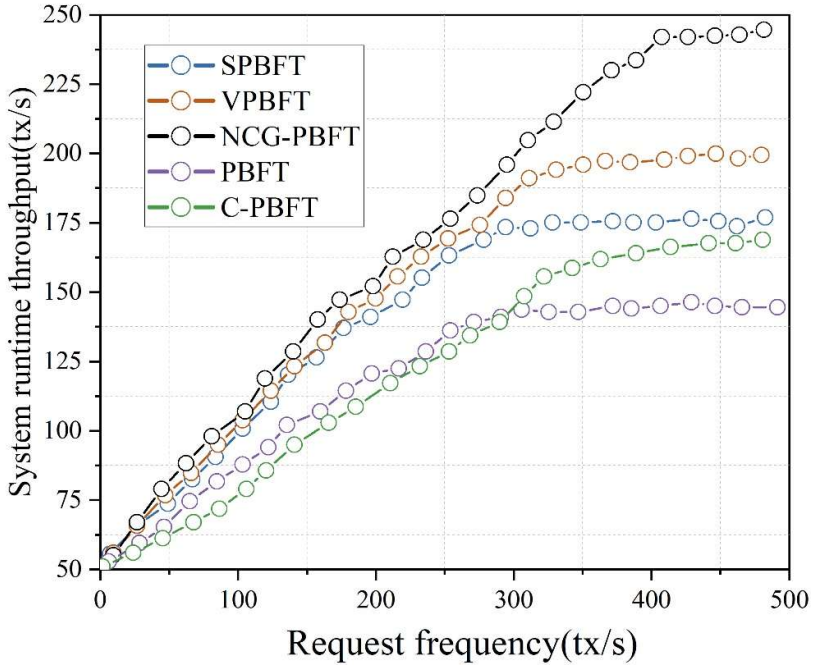

Fig. 8. System runtime throughput test results

5. Conclusion

This paper analyzes the advantages of blockchain technology in processing education data and its benefits in education evaluation jointly with big data. It proposes and improves the PBFT consensus algorithm, applies the NCG-PBFT consensus algorithm to the comprehensive educational quality evaluation system, and tests the operational performance of the comprehensive educational quality evaluation system.

1) When improving the NCG-PBFT consensus algorithm for node honest behavior testing, the algorithm node credit value grows with the increase of credit score reward Rsr. When the credit threshold of advanced nodes is reached, the growth rate becomes slower, showing a trend of first fast and then slow. Similarly get the higher the credit score penalty Rsp, the faster the credit value decreases.

2) Under the same conditions, NCG-PBFT consensus algorithm has more throughput than the traditional PBFT consensus algorithm, and the throughput is increased by about 9% overall.NCG-PBFT consensus algorithm has a shorter processing delay in the normal block out delay scenario. The shorter the normal block out delay of the consensus algorithm, the faster the transaction processing speed of the whole blockchain network will be.

3) Comparing the four algorithms for the number of communications under different scenarios, the NCG-PBFT algorithm has the slowest growth in the curve of the number of communications, which is significantly lower than the remaining three consensus algorithms. It shows that the use of Fibonacci function characteristics to select consensus nodes can reduce the number of communications of the NCG-PBFT consensus algorithm.

4) Establish a five-layer integrated education comprehensive quality evaluation platform with infrastructure layer, management layer, data layer, service layer and application layer, and bring the improved NCG-PBFT consensus algorithm into the education comprehensive quality evaluation platform. The system performance test obtained that compared with the PBFT algorithm, the throughput of the system utilizing the NCG-PBFT algorithm is increased by 74.54% during stable operation, which meets the requirements of the comprehensive quality evaluation system for education.

Acknowledgements

1) Shandong Province Education science "14th Five-Year Plan" project: Research and practice of applying blockchain technology to improve ideological and political education and teaching in secondary vocational schools (Project number: 2021ZC191).
2) Shandong Province 2021 vocational education teaching reform research project: Innovation and practice of teaching mode of ideological and political course in secondary vocational schools based on blockchain (Item number: 2021301).

References

[1] Zheng, Y. (2021). Design of a blockchain-based e-portfolio evaluation system to assess the education and teaching process. International Journal of Emerging Technologies in Learning (iJET), 16(5), 261-280.

[2] Chen, G., Xu, B., Lu, M., & Chen, N. S. (2018). Exploring blockchain technology and its potential applications for education. Smart Learning Environments, 5(1), 1-10.

[3] Min, L., & Bin, G. (2022). Online teaching research in universities based on blockchain. Education and Information Technologies, 27(5), 6459-6482.

[4] Shukla, A., Patel, N., Tanwar, S., Sadoun, B., & Obaidat, M. S. (2020, October). BDoTs: Blockchain-based evaluation scheme for online teaching under COVID-19 environment. In 2020 International Conference on Computer, Information and Telecommunication Systems (CITS) (pp. 1-5). IEEE.

[5] Bjelobaba, G., Paunovic, M., Savic, A., Stefanovic, H., Doganjic, J., & Miladinovic Bogavac, Z. (2022). Blockchain technologies and digitalization in function of student work evaluation. Sustainability, 14(9), 5333.

[6] Liu, J., & Zhu, T. (2021). Application of blockchain technology in cultural and creative design and education. International Journal of Emerging Technologies in Learning (iJET), 16(4), 228-239.

[7] Duan, B., Zhong, Y., & Liu, D. (2017, December). Education application of blockchain technology: Learning outcome and meta-diploma. In 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS) (pp. 814-817). IEEE.

[8] Bjelobaba, G., Savić, A., Tošić, T., Stefanović, I., & Kocić, B. (2023). Collaborative learning supported by Blockchain Technology as a model for improving the Educational process. Sustainability, 15(6), 4780.

[9] Bucea-Manea-Ţoniş, R., Martins, O. M., Bucea-Manea-Ţoniş, R., Gheorghiţă, C., Kuleto, V., Ilić, M. P., & Simion, V. E. (2021). Blockchain technology enhances sustainable higher education. Sustainability, 13(22), 12347.

[10] Tsai, C. T., Wu, J. L., Lin, Y. T., & Yeh, M. K. C. (2022). Design and development of a Blockchain-based secure scoring mechanism for online learning. Educational Technology & Society, 25(3), 105-121.

[11] Wu, B., & Li, Y. (2018, October). Design of evaluation system for digital education operational skill competition based on blockchain. In 2018 IEEE 15th international conference on e-business engineering (ICEBE) (pp. 102-109). IEEE.

[12] Atienza-Mendez, C., & Bayyou, D. G. (2019). Blockchain technology applications in education. International Journal of Computing and Technology, 6(11), 68-74.

[13] Ayasrah, F. T. M., Shdouh, A., & Al-Said, K. (2023). Blockchain-based student assessment and evaluation: a secure and transparent approach in jordan's tertiary institutions. Kurdish Studies, 11(2), 2036-2049.

[14] Alshahrani, M. Y. (2021). Implementation of a blockchain system using improved elliptic curve cryptography algorithm for the performance assessment of the students in the e-learning platform.

Applied Sciences, 12(1), 74.

[15] Zhao, W., Liu, K., & Ma, K. (2019, February). Design of student capability evaluation system merging blockchain technology. In Journal of Physics: Conference Series (Vol. 1168, No. 3, p. 032123). IOP Publishing.

[16] Li, T., Duan, B., Liu, D., & Fu, Z. (2018). Design of outcome-based education blockchain. International Journal of Performability Engineering, 14(10), 2403.

[17] Lam, T. Y., & Dongol, B. (2022). A blockchain-enabled e-learning platform. Interactive learning environments, 30(7), 1229-1251.

[18] Sun, X., Zou, J., Li, L., & Luo, M. (2021). A blockchain-based online language learning system. Telecommunication Systems, 76(2), 155-166.

[19] Md. Habibur Rahman,Brenno Castrillon Menezes & Roberto Baldacci. (2024). Exploring the role of blockchain technology, warehouse automation, smart routing, and cloud computing in logistics performance. Production & Manufacturing Research(1).

[20] Olha Prokopenko,Artem Koldovskiy,Marina Khalilova,Aigul Orazbayeva & José Machado. (2024). Development of Blockchain Technology in Financial Accounting. Computation(12),250-250.

[21] Bogdanov ,N. Shchegoleva ,V. Khvatov ,J. Kiyamov& A. Dik. (2024). Combining PBFT and Raft for Scalable and Fault-Tolerant Distributed Consensus. Physics of Particles and Nuclei(3),418-420.