Hindawi
Security and Communication Networks
Volume 2023, Article ID 5614241, 17 pages
https://doi.org/10.1155/2023/5614241

Review Article

Blockchain for Credibility in Educational Development: Key Technology, Application Potential, and Performance Evaluation

Yan Wang, Xin Cong, Lingling Zi, and Qiuyan Xiang

College of Computer and Information Science, Chongqing Normal University, Chongqing 401331, China

Correspondence should be addressed to Xin Cong; chongzi610@163.com

Received 10 November 2022; Revised 21 March 2023; Accepted 3 May 2023; Published 22 May 2023

Academic Editor: Yujue Wang

Blockchain proposes many innovative technologies to establish credible mechanisms in an open environment and therefore, it becomes a promising solution to the problem of credibility in educational development. To better understand the role of the blockchain, we aim to provide an extensive survey focusing on its key technology, application potential, and performance evaluation. First, from the perspective of blockchain characteristics, we summarize its application architecture in educational credibility. Next, we extensively discuss application potential of the blockchain, such as data storage, data sharing, achievement certification, and activity evaluation. Moreover, we investigate the performance evaluation, including basic performance metrics and specialized metrics for credibility. Finally, we analyze the challenges and research trends of blockchain in educational credibility and provide useful insights for future research.

1. Introduction

With ongoing educational reform, many researchers have focused on the issue of trust in the education field. Educational trust is a relationship of affirmative dependent on the educational system arising from the interaction between the trusting willingness of the educational subject and the trustworthy quality of the educational object [1]. Anwar et al. [2] pointed out that in the current educational environment, building trust in education is urgent. It is worth paying attention to the fact that the conventional educational paradigm can hardly adapt to the advancements in science and technology, as reflected in the following aspects. In the past, traditional educational trust relationships were usually based on geography and kinship, with emotional ties as the basic feature, and such relationships were vulnerable to artificial interference, not solid and strong enough, and not scientific enough, which has become a problem for credible educational development. The educational process is implicit and is not conducted under public scrutiny, there can be irregularities, and the results of such education can easily be questioned. In order to address such issues, the establishment of a credible mechanism for education seems extremely necessary. However, in this environment, it is very difficult to establish an open and transparent education credible system without reliable technical support. Considering the previous studies, decentralized technology such as blockchain is introduced to exclude human factors that affect the fairness of the education system and solve the trust crisis in education. Therefore, for educated people, they do not have the ability to assess information on their own and cannot actively choose educational environments and methods that interest them, thus lacking initiative. For teachers, they have no uniform criteria for assessing educated people as a whole, resulting in a reduction. Moreover, educational institutions are not transparent in the process of handling all educational data, and there is no supervisory body, leading to easy leakage of data privacy and reducing data authenticity. Therefore, it is essential to establish an educational credibility mechanism in order to ensure the fairness of the educational process and the effectiveness of the educational results.

Blockchain technology is seen as having great potential for applications in education, assisting in creating a more open and credible education system [3]. It proposes many frontier technologies to create trusted data transaction mechanisms in an open educational environment [4], such as smart contracts [5], asymmetric cryptography algorithms [6], consensus verification [7], and incentive mechanisms [8]. These technologies allow the blockchain to have characteristics such as distributed storage, decentralization, anonymity, and traceability [9, 10]. They break the traditional centralized structure and provide new technical solutions to solve the issue of credibility. However, considering the complexity of the education, the solution to this issue remains very challenging. So, the purpose of this paper is to explore how the blockchain can build a credible mechanism in an open educational environment.

The main contributions of this paper can be summarized as follows. (1) We summarize the application architecture of blockchain in educational credibility, including core technology and attributes. We highlight the core technologies, such as digital signature, consensus mechanism, encryption algorithms, and smart contracts. (2) On this application architecture, we demonstrate the application potential of blockchain in four aspects and for each aspect, we analyze current credibility issues in education and how blockchain can help address them. (3) To evaluate the performance of the blockchain-based systems, we provide basic performance metrics and specialized metrics. The former evaluates the important performance of the blockchain system itself, while the latter gives the unique evaluation method for assessing credibility.

The rest of the paper is structured as follows. Section 2 provides the architecture of the blockchain, Section 3 demonstrates educational application of the blockchain, Section 4 presents performance evaluation, and Section 5 is conclusions.

2. The Application Architecture of the Blockchain

Blockchain can be described as an immutable ledger that records data in a decentralized manner, which enables entities to interact without the presence of a centrally trusted third party [11], exploring the blockchain application architecture from a typical blockchain application in an educational environment. MOOCsChain [12] is the blockchain application on the MOOC platform, which consists of five main parts, registration authority (RA), MOOCs providers (MPs), end-users (EUs), blockchain (BC), and data storage servers (DSs). RA is mainly responsible for handling all platform registration requests and providing public and private keys for authorized users. EU is a port for users to use the platform and participate in the course. MP is a course content provider, and each MP is an independent entity that can communicate with the storage server. BC records key materials of learners using smart contracts and provides a decentralized storage environment. DS stores data through a distributed storage system to protect the limited storage capacity of BC. Publication Chain (PubChain) [13] mainly relies on the blockchain system and IPFS system. The blockchain runs a distributed consensus protocol to maintain the data on the chain, and participants interact with the blockchain when running activities on the PubChain.

Considering the particularity and complexity of application scenarios in education, the blockchain technology architecture can be divided into three parts, as shown in Figure 1. In the first circle, the disordered education data are added to the chain structure and stored according to the structure of Merkle tree; these nodes made up the bottom layer of the blockchain structure P2P network [14]. In the second circle, the core technology of the main applications of blockchain contains digital signature, consensus protocol, smart contract, and asymmetric encryption algorithm, which improves the legitimacy of the educational material [15]. In the third circle, benefiting from the core technology of the second circle, blockchain will have some attributes such as traceability [16], authenticity, anonymity, and security, which can be useful in educational scenarios such as certificate verification, online learning platforms, and lifelong learning records.

2.1. The Core Technology. The education filed mainly concentrates on the application of the core technology in blockchain, such as consensus verification, asymmetric cryptography algorithms [17], digital signature and smart contracts, which have their unique properties and complement each other to cooperate in educational scenarios. While ensuring the authenticity of the educational data, they help promote the construction of a credible system for education.

2.1.1. Smart Contract. A smart contract is a computer protocol designed to disseminate, validate, and enforce a contract in an informative manner, a piece of computer code that constitutes a program. It plays an important role in educational applications. In the first step, two or more users involved in educational activities agree to formulate their common opinion into a smart contract; in the second step, this smart contract is broadcast and stores to the block nodes in the framework through the blockchain network; in the third step, the successfully constructed smart contract waits for the conditions to be met and then automatically executes the contents of the contract. It is worth noting that not all blockchains have smart contracts, such as beacon chains. Blockchains that do not have smart contracts differ in the way they solve problems. Smart contracts are the unique existence of the blockchain technology that can convert the coding of data interactions into contracts and related documents in the traditional sense [18]. Smart contract provides a more fair and equitable method of transaction with transparent data, while minimizing interaction of parties in a decentralized manner [18]. These transaction data are traceable and irreversible and can be automatically executed according to the provided terms without the involvement of any third-party [19], enabling the sharing of data.

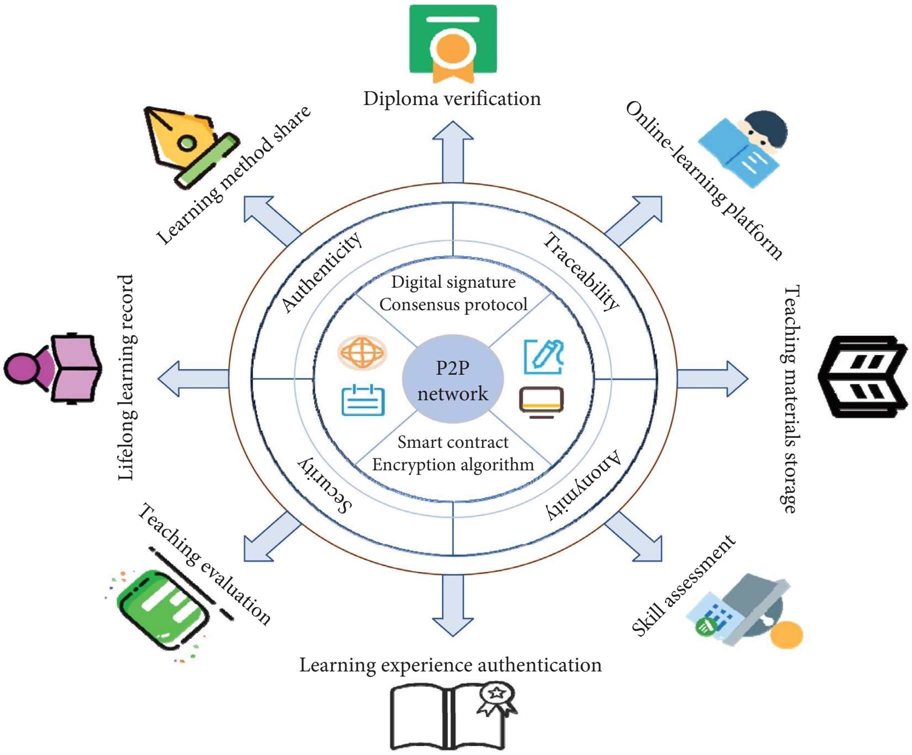

Figure 1: The application architecture of the blockchain in the educational credibility.

As can be seen from Figure 2, the education role inputs education data to the smart contract, which has a contract state, contract value, and contract code, and the contract is executed automatically after getting the input data. The corresponding output is obtained according to the contract content. There is no third-party involvement in the process, and the contract content will not be changed in the middle of the process to ensure the consistency of the result data. The execution of smart contracts has a huge impact on the blockchain technology [20], and all participants carry out contracts in accordance with the same standard to achieve maximum fairness and credibility.

2.1.2. Consensus Protocol. The main purpose of the consensus protocol is to enable decentralized network nodes to reach an agreement and complete the consensus verification. In a central and organizational body, all decisions are judged by selecting a highest-priority role [21], which is highly subjective and is unfair and lacking in credibility. However, the outcome is determined by all participating node and are subject to their interests in a distributed network. This process is known as consensus [22]. The specific consensus verification process is illustrated in Figure 3.

As can be seen from Figure 3, the main players in educational activities contain students, teachers, schools, and institutions who join together in a smart contract to choose the appropriate consensus protocol for their desired educational activities. For example, PubChain uses the PoA consensus protocol in federated chains and the PoW consensus protocol in public blockchains [23]. The consensus mechanism is that all nodes on the blockchain communicate consistently. When the educational data on a block change, all users will receive a notification and update their data status in time, solving the problem of synchronizing educational information data in an educational environment, and all its behaviors will be supervised [24]. The common consensus protocol is listed in Table 1.

2.1.3. Asymmetric Encryption Algorithms. Asymmetric encryption algorithms use key pairs, public and private keys to protect the information of users in the blockchain network [40]. The public key and the private key are generated simultaneously and play a decisive role in the subsequent creation, change, or view of the information in the block [41]. The user uses the public key to encrypt the data information, determining the authenticity of the information. Then, the only authorized user can use the private key to decrypt and access to obtain data. The execution flow of the asymmetric encryption algorithm is depicted in Figure 4.

As can be seen from Figure 4, students can encrypt their educational data and personal data using asymmetric encryption algorithms. If a teacher, school, or employer needs to access the student's data, it needs to be authenticated by the public key given by the student, and after the authentication, a series of educational activities can be carried out. Cryptography is one of the primary tools for ensuring data security [42], the most widely used asymmetric encryption algorithms, such as the RSA algorithms [43, 44], run slowly, have open methods, and encrypt data quickly, but the management of private keys is not secure enough. The DSA algorithm [45] has slow running speed and faster performance compared to RSA [46] algorithm, which is only

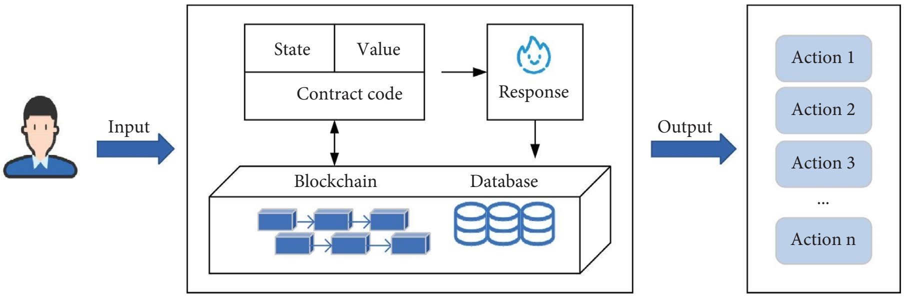

Figure 2: The process of executing contract in educational application.

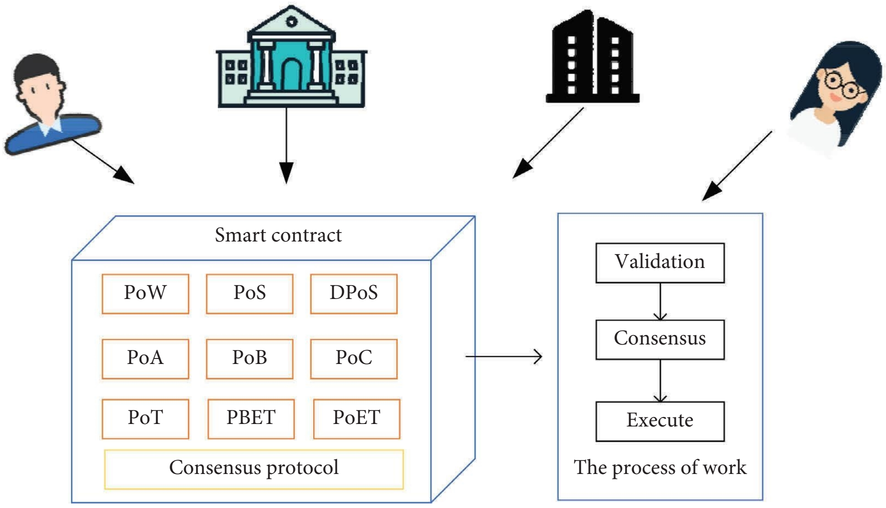

Figure 3: The process of consensus protocol in educational application.

capable of digital signatures, not for data encryption or decryption. Elliptic curve digital signature algorithm (ECC) [47, 48], runs fast, can use smaller keys, more efficient, but long operating times for encryption and decryption. The PTFT algorithm [49], fast running speed, high security, difficult to attack, but one-way strategy, and complex decryption process.

2.1.4. Digital Signature. A digital signature (also known as a public key digital signature) is a string of numbers that can only be generated by the sender of a message and cannot be forged by anyone else, and it is a valid proof of the authenticity of the message sent by the sender. It is an ordinary physical signature, similar to the one written on paper, but implemented using techniques in the field of public key cryptography, used to authenticate digital messages. A set of digital signatures usually defines two complementary operations, one for signing and the other for verification. Digital signatures are applications of asymmetric key cryptography. When educational data are stored, it is encrypted using asymmetric encryption algorithms, at which points a digital signature is used in an act similar to "stamping." The application of digital signatures mainly adds a layer of protection locks to educational data, verifies the user's identity information, traces the authenticity of the information source, prevents data from being tampered with and forged, increases the credibility of the information, and creates a more transparent and secure educational system.

2.2. The Attributes of Blockchain. The key attributes of blockchain applications in education filed are traceability, authenticity, anonymity, and security, which merge and complement each other and work together in establishing credible mechanisms.

2.2.1. Traceability. Traceability is due to the fact that all transactions on the block are sorted chronologically, and the previous block and the next block connected to itself can be found between blocks by index values. The index value on the block uses a one-way hash function, and there is no direct necessary connection between input and output. In other words, the input cannot be determined by just giving the output, so that the origin of the transaction data recorded in the block and the source of the data can be traced.

2.2.2. Authenticity. Blockchain is decentralized networks without the control of a central authority, and block nodes supervise each other to strictly prevent tampering attacks by malicious nodes. When a new node record is created, it is

Table 1: Consensus protocol.

Protocol name	Description	Advantages	Disadvantages
PoW [25–27]	Proof of work protocol, solving problems through miner mining [28]	Good performance against malicious node attacks	Takes a certain amount of energy [29]
PoS [30]	Proof of stake protocol, nodes with access to benefits to solve the problem [31]	Reaching consensus takes a short time	Hard forks are prone to occur
DPoS [32]	A special case of PoS, forming a consensus group to solve problems through the public interest	Propagation speed is fast Higher throughput	Elections are needed to determine the consensus group, and only a small number of nodes are elected
PoA [33]	Proof of authority protocol to publicly certify all document processes with trusted nodes	Small scale High credibility	Preventing node collusion requires user supervision
PoB [34]	Burn the proof protocol and select the final result through an algorithm	Fewer validators More efficient	Requires a lot of resources to test
PoC [35]	Capacity proof protocol with the hard disk as the consensus participant	Low cost addresses global trust and security	High energy consumption requires sacrificing node performance
PoT [36]	Proof of trust protocol, through the incentive mechanism, the node gives honest verification results	High throughput, low energy consumption	Nodes are likely to commit malicious behavior
PBFT [37]	Practical Byzantine fault tolerance algorithm, malicious nodes are not higher than 1/3 of the total	At the same time guarantee safety and activity	The node must be deterministic and must start execution from the same state
PoET [38]	The time it takes to prove consensus algorithms, typically used in permissioned blockchain networks, to determine mining rights on the network	The cost of participation is low, and more nodes can be easily joined	Requires specific hardware and is not suitable for large-scale applications
RAFT [39]	An algorithm that implements distributed consensus and is mainly used to manage the consistency of log replication	Easier to understand and apply to real systems	Only faulty nodes can be accommodated, not evil nodes

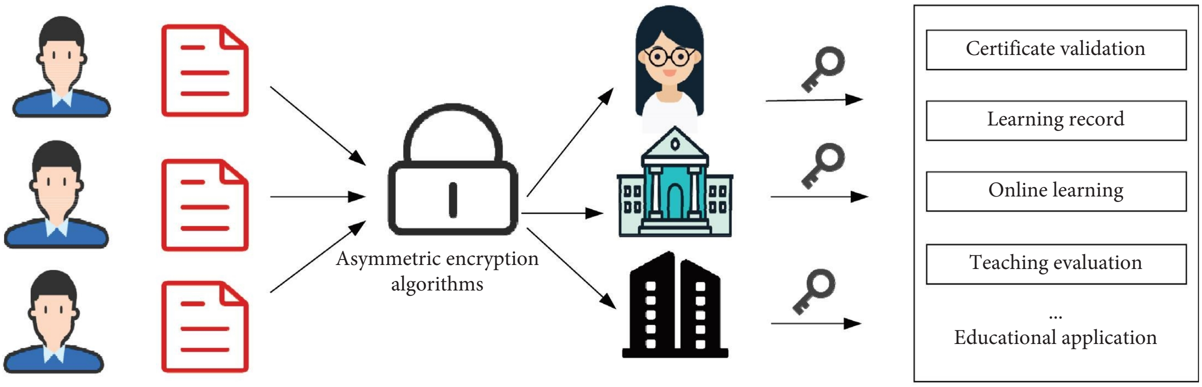

Figure 4: The process of encryption in educational application.

first verified by network nodes and then added to that chain. The data verified by the nodes will not be modified again and remain in its original data state.

2.2.3. Anonymity. The block nodes are all peer nodes with the same priority and structure in the network. On a technical level alone, the identity information of each block node does not need to be disclosed or verified, and information transfer can be done anonymously. The user access to the data is hidden and the information sharing process is also delivered anonymously and encrypted.

2.2.4. Security. The modification network cannot be controlled unless you have control over 51% of all data nodes, which makes the blockchain itself relatively secure from human subjective data changes. Only users with public keys can access and read the data because it is encrypted and stored using a highly secure asymmetric encryption process.

The previous attributes are the ones that education data will have when education applications are combined with the blockchain technology. For example, in the higher education certificate authentication system, the certificate data can be guaranteed to be real and safe after being processed by the blockchain technology and the source of that certificate data can be traced. The credibility of the certificate obtained through such an authentication process is greatly improved.

2.3. The Types of Blockchain. There are three types of blockchains, which are as follows:

(i) Public blockchain: each node on the public chain can freely join and exit the network and participate in the reading and writing of data on the chain, interconnecting with a flat topology when reading and writing, and there is no centralized server node in the network.

(ii) Private blockchain: the right access of each node in the private chain is controlled internally, while the read access can be opened to the public selectively on demand.

(iii) Consortium blockchain: each node of a federated chain usually has a corresponding physical institutional organization that is authorized to join and exit the network. Each institutional organization forms a stakeholder alliance to maintain the healthy operation of the blockchain.

The core difference between these three types is the degree of openness of access or decentralization. In general, the higher the decentralization is, the higher the trust and security and the lower the transaction efficiency. Usually, depending on the characteristics of the educational application itself, a type with a higher degree of adaptability is chosen based on the actual situation. In educational storage applications, the more decentralized type will be preferred, while educational assessment, authentication, and sharing applications will use the more efficient type.

3. Educational Application of the Blockchain

Blockchain technology has infinite possibilities for a wide range of application in the field of education [50]. Through a review of published papers, the application in educational credibility can be divided into four areas, including educational data storage, educational data sharing, educational achievement certification, and educational activity evaluation, as shown in Figure 5.

3.1. Educational Data Storage. In the field of education, various educational activities are emerging and more data are generated in the process of the activities. When traditional methods are used to handle data and manage process, there are problems in terms of efficiency and security of data storage. In terms of efficiency, since education is still largely controlled by institutions that provides quality, credibility, governance, and administrative functions [51]. However, many educated people have learning data at different stages of the educational process, thus these data are stored independently in different institutions, so this can affect the efficiency of querying the data. In terms of security, institutions generally store educated peoples' learning data in the form of a central database for unified management, which is singularly uncontrollable. Once there is a problem with the database, there is a great risk that the stored data will be tampered with or even lost. In addition, the lack of

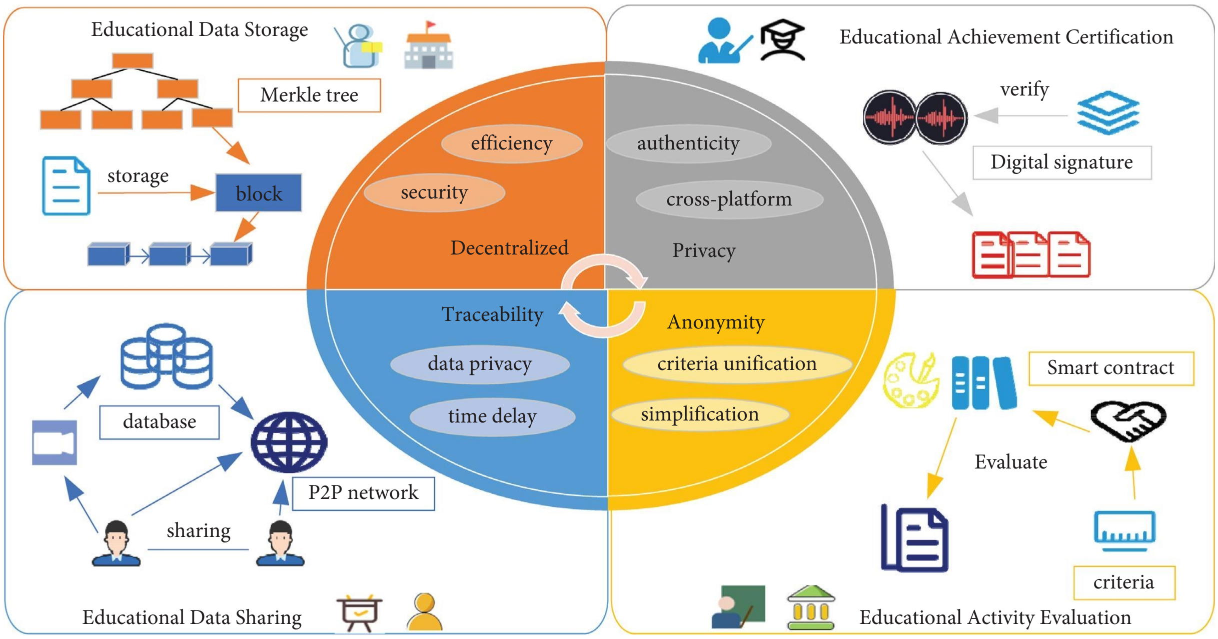

Figure 5: The application of the blockchain in educational credibility.

a supervisory and management body during the data storage process, and thus, the inability to guarantee data constancy, indicated that the privacy and security issues are of great concern. Therefore, how to store data in an efficient and secure way is a question we need to consider.

Blockchain offers a possible technology to solve the previous problems. For data storage efficiency, due to the limited block space, educational data updated by students are added to the blockchain in the form of blocks. The blocks store extremely important and effective educational information, such as students' basic personal information and educational data. Subsequent transactions can be made directly on the blockchain when educational activities are carried out, and the entire transaction process is guaranteed to be trusted. At this time, a hash index value is generated on the block, which can quickly locate where the block is located on the chain, and then efficiently query the data carried by the block, reducing the time cost of data query and analysis. For data security, educational data are stored using asymmetric encryption methods with digital signatures, and the generated key pairs can be accessed by authorized users who have public keys, thus avoiding abusive tampering of data by malicious nodes [52]. The decentralized nature of the blockchain technology allows the stored data to be free from the control of a central database, that is, distributed storage gives the students themselves full control over the management of the data. Since blocks are equivalent to peer nodes in the blockchain network, data interactions on blocks are always under the common and strict supervision of other blocks on the chain, ensuring the transparency of stored transactions and thus reducing the possibility of data privacy leakage.

Currently, researchers have applied the blockchain technology in data storage, such as student credit management [53], achievement management [54], and career data management in nonformal education [55]. Liang et al. implemented PDPChain [56] for secure storage of personal education data, and the blockchain network in the framework guaranteed the trusted storage of the private data by using a consortium chain. The encrypted ciphertext hashes are stored in a smart contract in the consortium blockchain, and transactions with consistent communication are sent to the network using the RAFT consensus mechanism. After the cryptographer verified the digital signature, the transactions are packaged, blocks are generated for sorting, and finally, the blocks are stored in the blockchain network intact. After this process, the personal education data stored in the blockchain network is safe and secure, and data transparency is truly achieved. Many scholars view the blockchain as the underlying architecture that stores all data transaction records in a ledger. Rooksby and Dimitrov [57] used the blockchain to register to determine ownership of intellectual property, preserve academic transcripts, and establish a more scientific storage model. Kosasi et al. [58] see blockchain as a digital system that offers tremendous potential for the storage of student educational records in the use of the higher education. Data privacy and security are ensured through unique asymmetric cryptography algorithms that ensure the storage of student records and credentials [59, 60]. The blockchain technology, with its unique advantage of data immutability, stores students' certificates of achievement that can accurately predict the future based on experience and helps students develop personal plans with the help of various algorithms [61]. Turkanovic et al. [62] proposed an ecosystem for managing digital micro-credentials (EduCTX), a global credit platform for higher education based on the blockchain technology. The main function of this platform is secure transfer and accumulation of credits. Students can store the credits they have earned during their studies in the system and when changing institution they do not have to worry about losing or tampering with their data. Ocheja et al. [63] presented a method to save learning records, and the scheme's is to securely store students' learning data. When learners switch to a new learning environment, they can take all of their learning records with them, ensuring the immutability and security of the educational data. Awaji et al. [64] proposed a secure system for achievement records, which attempts to store students' achievement records efficiently, encrypted in the form of blocks that can be easily located for queries and improved the efficiency of students' searches. Li and Han [65] developed the storage platform, a blockchain-based storage, and sharing scheme for educational records (EduRSS) to accomplish security and privacy protection of educational record storage.

Obviously, the blockchain technology can improve the efficiency of education data storage and create a more secure data storage environment, thus strengthening the trustworthiness of education data storage and ensuring the consistency and consistency of data in the storage process. Nevertheless, data overload is an issue we need to further study in an environment where data are highly trusted to grow rapidly.

3.2. Educational Data Sharing. In the environment of the Internet era, data sharing has become a major trend that can benefit multiple participants. In the field of education, we divide data sharing into two aspects: educational resource sharing and educational data sharing. Educational resources include various forms of resources, such as teaching software, teaching videos, and teaching environments. Educational data mainly refers to all data generated by educated people throughout their educational activities. Both are core components of educational activities. Traditional forms of data sharing are point-to-point transfers by data producers, which have high time delays in transmission and do not guarantee data privacy. Considering the time delay, in the context of modernization of education, information about educational resources and educated people is commonly shared among multiple parties in educational activities. Data producers provide the prepared data to the shared recipients, and the delivery process requires significant time costs. Moreover, in the case of sharing core educational data, the sharing process takes too long and is prone to security problems of data loss. In terms of data privacy, due to the wide application of artificial intelligence and big data technologies, data sharing transactions in education are becoming more and more frequent, and the issue of data privacy leakage is becoming more and more prominent. During the sharing process, the privacy and security of data can be damaged by a large number of users, and the availability of data can be greatly reduced. At present, vigorously promoting education data sharing has been a national strategy to promote the development of education information, and we need to reduce the sharing delay and improve data availability.

Blockchain network topology and anonymity protection technology can be used to solve the aforementioned issues. For time delay, the P2P network [66] topology contains a distributed structured topology (DHT) [67], which is a massive hash table maintained collectively by all nodes. This effectively reduces data latency. When users need to access data, they can directly query the hash index value for access, avoiding the intermediate transmission link, and the decentralized nature of the blockchain technology reduces the response time of access. For data privacy, data are encrypted and packaged in blocks, which is then connected in a chain to form a distributed ledger system. Also, anonymous technology can help to safeguard privacy [68]. Only authorized users have access to the private key for decryption, while educational data are keeping encrypted with public keys using asymmetric encryption methods. The original educational data are not shared directly on the blockchain, thus preventing the privacy of core data from being compromised and improving the security of sharing.

Currently, many scholars have developed a number of open-source platforms for data sharing. Gao [69] developed a platform of top-notch educational materials for universities and institutions. It compiles large number of educational resources that can be quickly accessed by the educated and used for self-study. PubChain, a decentralized distributed open access publishing platform based on blockchain and IPFS peer-to-peer file sharing system, was designed and implemented by Wang et al. [13] PubChain used the blockchain technology to confirm the registration of ownership of papers, track indexing, and be cited. When an author uploads his or her paper to PubChain, the paper was timestamped and registered as a permanent record. Compared to existing centralized publishing platforms, PubChain made papers freely available to everyone, eliminates the undesirable effects of information silos, and has the potential to become a unified database for sharing and recording papers globally. The sharing of smart education courses in institutions is an important way to improve the quality of individual students [70], and implements such an architecture for wireless communication requires prioritizing the blockchain technology that provides security and data transparency [71]. Using the blockchain technology to visualize student data to display learning outcomes addresses data transparency in the sharing of outcomes under the influence of teaching or administrative processes [72]. Various online education platforms provide a broad Internet environment for sharing multimedia learning resources, and the blockchain technology needs to be used to address the risk of decreasing trust in the process of resource sharing [73]. Gilda and Mehrotra [74] broke the conventional practice of sharing student data in paper form by using the blockchain technology to build a framework of trust and authorization to complete the overall assessment of students using the data obtained. Zhao et al. [75] proposed a sharing system for digital education resources, allowing educators and educational institutions to share teaching videos. Sharing records are not seen by others, and once a video is published in the system, it cannot be changed again, ensuring the accessibility and authenticity of digital resources. Han et al. [76] created a storage authentication structure that allows users to confirm the accuracy and integrity of outcomes from shared data using the blockchain technology. In addition, there are research results sharing platforms [77], skills sharing platforms [78], and school sharing online education platforms [79].

In summary, the sharing mechanism constructed by using the blockchain technology effectively reduces the time delay of data sharing, enhances the privacy and availability of shared data, and facilitates the establishment of a credible educational data sharing mechanism. However, in the process of data sharing, the confirmation of data resource ownership is the next step we should consider, which requires the support of multiple parties such as laws, policies, and standards.

3.3. Educational Achievement Certification. Certificates are the most reliable foundation for confirming students' own valuable capabilities in the wave of global education. It is a concise and direct reflection of the student's personal abilities through degree certification, learning record certification, skills certification, and results certification, and it is also a reference for corporate background checks during the job search process. Thus, verifying the authenticity of certificates such as diplomas or achievements can be a long and expensive process, and there is a risk of certificate forgery. Currently, students' learning experiences on different electronic platforms cannot yet be integrated or recognized, reducing students' motivation to learn online. In terms of authenticity, since certificates are usually paper-based, the data can be easily modified during storage and their privacy cannot be guaranteed. In addition, if the issue agency ceases to exist, the authenticity of the certificate will not be verified, which will lead to problems of diploma fraud and forge certificates. Therefore, educational certification is a matter of everyone's rights, and it is urgent to solve the related issues.

Thanks to the development of smart contracts and consensus protocol, tamper-proof and traceability features are considered as the best solution to the previous mentioning issues [80]. For cross-platform verification, learning platforms built with the blockchain technology can automatically issue digital certificates according to learning outcomes, and digital certificates are increasingly popular with the public because of their small size and easy preservation. Digital certificates integrate users' all cross-platform learning experiences and store them using the blockchain technology. Blockchain store user data in a distributed manner with decentralized features, uses smart contracts to incorporate users, enterprises, schools, and other roles into the platform, and adopts consensus protocols to form a multirole and certification platform. For data authenticity, educational data are packaged in blocks with encryption algorithms that will not be modified or deleted, and then, the blocks are added to the chain in chronological order to facilitate subsequent verification of the data by the employers or other departments to trace the authenticity of the data source.

There are some educational certification platforms based on the blockchain technology that provide users with one-stop certification solutions. Tian et al. [81] redesigned the expandable framework for validating the integrity and validity of educational digital evidence. The main execution process of the framework is that content providers submit educational digital evidence in their possession, and the framework records the documents in transactions, with multiple transactions stored on a block that contains the public key for preventing tampering with the evidence and tracking the corresponding documents. It uses the PBFT consensus mechanism to effectively guard against malicious and faulty nodes. When a new block is generated, the block is broadcast to other nodes. When each node receives the block, it verifies all transactions in the block by comparing the Merkle root in the block with the Merkle root in the node. It also verifies the authenticity and validity of the digital evidence of education and creates a fair and credible educational environment. Multimedia learning resources are becoming more and more abundant, and students are earning more and more certificates for studying on various online platforms [73]. The insecurity of digital education certificates makes students' abilities not well proven. By introducing blockchain, a technology that combines public and private chains using specific smart contracts, the verification of certificates on various platforms is realized [59]. Using certificate authorization services and transactions in the Hyper Ledger framework to achieve transparent information sharing between universities and enterprises, the information symmetry between students' skill achievement information and enterprises' recruitment demand is realized [82]. Sanni and Apriliasari [83] proposed a blockchain technology authentication system that can protect data rights from interference, and all data stored in the education system is secured. Due to the decentralized nature of the blockchain, the trust of parents, teachers, and other parties in the education system will be increased. Han et al. [84] suggested combining the blockchain technology and certification methods, using smart contract to integrate multiple players such as departments, colleges, universities, government agencies, and businesses to certify the formal educational achievements of educated people. Arenas and Fernandez [85] proposed Credence Ledger, a blockchain solution that decentralizes the authentication of academic credentials so that employers can quickly confirm the authenticity of this information. To create a student central approach to achievement certification in an open learning environment, Awaji and Ellis [86] developed a blockchain technology-based achievement certification system using the PoW consensus protocol for certification, which certifies grades that can be recognized by third-party entities. Bandara et al. [87] used a high trust level of the blockchain technology to build a distributed and secure collaborative certification database to verify the results of informal education in parallel with the university, partner institutions, and regulators. Alshahrani et al. [88] proposed a framework for higher education certificate certification based on the blockchain technology, in which education certificates are stored and the authenticity of higher certificates is verified using DPoS consensus protocol, and the certification process will become more convenient and credible. Similar educational certification precautions include credit certification [89], degree information certification [90, 91], and diploma certification [92].

In generally, the blockchain technology can rely on its own decentralized distributed storage management to achieve the authentication of cross-platform educational data. It can also guarantee the authenticity and validity of the educational data through immutability and data traceability. Meanwhile, it also can be used to create credible education achievement verification systems. The next issue we must address is how to construct a greater security consensus smart contract to enhance credibility because the authentication process requires the inclusion of multiple players such as schools, employers, and regulators.

3.4. Educational Activity Evaluation. In order to better improve the quality of education, when the educational activities are completed, they are evaluated accordingly. Students can evaluate the teacher's teaching, and teachers can also evaluate the students' abilities. On the one hand, the assessment behavior requires obtaining data from multiple parties and then synthesizing and processing the data. In general, this process is opaque and costly in terms of human and material resources. On the other hand, assessment criteria are usually defined by the high-priority roles involved in the assessment activities. However, the evaluated roles are largely passive [93]. In addition, the evaluation criteria vary from platform to platform, so the evaluation results are difficult to be recognized. In this case, it is very difficult to make an objective and comprehensive analysis for the educated people, therefore, a unified evaluation standard is needed due to the complexity of the evaluation process.

The blockchain technology includes consensus protocol and digital signature, which can provide new ideas and technical support for the problems in the educational activity evaluation process. In terms of process simplification, the roles involved in the evaluation of educational activities can clear know the educational data of all the evaluated objects on the chain, and can give the evaluation results directly through the educational data in a fair and open manner. During the evaluation process, the consensus protocol is equivalent to a broadcasting role. When the evaluation object gives the final result of the evaluated object, the blocks on the chain and all participants of this educational activity will be notified through the consensus protocol to ensure consistent communication information of all blocks. The entire process of evaluating educational activities is transparent, and the behavior of evaluation participants is monitored throughout. This simplifies the complex educational activity evaluation process, which originally requires multiple participants, upper-level discussions, and collective evaluation opinions, to the evaluation results given by the roles involved in the evaluation activity through a consensus protocol. In terms of standard unification, educated people can have different learning activities in multiple platforms, and different platforms have different criteria, and there is a lack of unified evaluation recognition criteria for the complete educational activities of the educated people. Evaluation can only be done by integrating the results of educational activities from different platforms, but such an evaluation behavior lacks real and completed data basis, and the obtained evaluation results do not have strict credibility. The consensus mechanism provides a powerful tool for the unification of evaluation criteria, which can objectively evaluate the results obtained by users after cross-platform educational activities. The data tracing function of the blockchain can record users' activity behaviors and enrich the details of the evaluation process, thus improving the reliability of assessment results.

There are several examples of the blockchain-based evaluation systems, such as Li et al. [94] developed a skills assessment system that enables teachers to assess student skills and teaching effectiveness based on the learning data in the system to create a fairer, healthier, and more open e-learning and online education environment. For any educational institution on the system can create and deploy course credit generation contracts on the blockchain, which contain information such as test scores, learning hours, and commenting behavior as a basis for automatically assessing users' specific course credits, simplifying the process and preventing data from being undisclosed and opaque. Lizcano et al. [95] see blockchain as the technology used to manage teaching content and student competencies by consensus among students, teachers, and employers, bridging the divide between academia and the world of work once and for all. The assessment of student learning and professional competencies [96] are performed automatically with the same criteria set by all parties involved in the assessment activity [97]. Widayanti et al. [98] showed that the assessment process using the blockchain technology as the underlying structure disrupts the traditional educational model and the results of automated assessment are more convincing. Zheng [99] created a learning assessment system that evaluates students in an anonymous way and the system is able to obtain the results quickly, ensuring that the results are objective and fair. Zhao et al. [100] proposed a blockchain technology-based student competency evaluation system that focuses on monitoring students' educational activities, analyzing learning data, and developing unified evaluation criteria through a PoA consensus protocol to objectively and comprehensively evaluate students' personal skills demonstrated in educational activities and give reference to students' future job search directions. Stepanova and Erins [101] proposed a career growth data evaluation model, which records the learning activity experience of an educated person in nonformal education and sets common criteria to assess the occupational competence of that user through a consensus protocol. Wu and Li [78] upgraded the personal skills competition model using the blockchain technology to analyze and unify the existing evaluation criteria and simplified the evaluation process. The assessment results were given directly through the students' skill operations on the operating system of digital education, which greatly improved the efficiency of activity evaluation and the accuracy of the results. Jirgensons and Kapenieks [102] discussed digital certificates and how the data traceability and decentralization of the blockchain technology can be used to develop unified recognition criteria to improve the credibility of the evaluation of educational activity certificates.

Generally speaking, the blockchain technology provides a solution to the current evaluation model with complex processes and lack of uniform criteria in educational activities. In addition, the traceability and authenticity of data enhances the credibility of evaluation results. Due to the complexity of the education field itself, most of the evaluation activities still require human intervention. How to use blockchain combined with artificial intelligence technology to train evaluation models and continuously optimize them is the next direction we need to study.

4. Performance Evaluation

Evaluation metrics are mainly used to measure the overall performance of the system application. Inspired by the software quality metrics, the evaluation metrics for studying and analyzing the blockchain technology in building a trustworthy mechanism in the education field from the perspective of expected target results should consider both the performance situation of the blockchain technology itself, the basic performance metrics; and the performance situation after application in the education field, the characteristic metrics. The basic performance metrics are response time, cost, throughput, efficiency, and reliability; the characteristic metrics are scalability, consistency, maintainability, real-time, and processability. We give the corresponding calculation formulas on different evaluation indexes, which are mainly derived from the common system performance evaluation criteria calculation rules, obtained after many practical studies. The performance of the system is accurately measured by mathematical methods. As the basis of [103], formula (1) similar to calculate of the latency time. According to the mathematical formulas, due to the same of underlying calculation logic, uses the cost required for a single block product the total number of blocks, getting formulas (2)–(4). Similarly, based on the [104], the calculation of efficiency, formulas (5)–(7) mainly uses response time division to the cost. The cost includes CPU, memory resource, and time.

4.1. Response Time. It refers to the time required from the start of a block transaction until the result is recorded on the blockchain after the transaction is closed. Define at the time of t_s transaction starts, at the t_e moment the transaction is recorded on the blockchain, in a period of time T, the total number of transactions is T_s, written as follows:

$$Ts = \sum_{te\in(0,T)\&(te-ts)\leq T} ts, \tag{1}$$

where t_s is the count value, and when the start time and end time meet the conditions, t_s is 1, otherwise 0. When education data are added to the chain in the form of block storage, the shorter the response time, the more efficient the storage is demonstrated. In data sharing, the shorter the response time, indicating that the user accesses the block data quickly, and the data sharing transaction is convenient and rapid.

4.2. Cost. It refers to the consumption of the blockchain in the process of executing the application. Public chains generally encourage nodes to synchronize information and ensure data security through a token mechanism. This way of storing data will make the cost of educational applications using public chains increase, but this increase is acceptable relative to the benefits it brings. Other types of resource cost consumption are similar for the three types of blockchains. There is a certain amount of loss in the process of generating a block's transaction, and different cost types consume in different ways. When the consumption is a resource, assuming that the energy cost per unit consumed is E_s, the time consumed by a single transaction is T, and a single transaction refers to the time that the block lasts from generation to being added to the blockchain. Thus, the cost E calculation can be focused on the use of the central processing unit (CPU), written as follows:

$$E = Nn \cdot Es \cdot \int_0^T CPU(t)\mathrm{d}t, \tag{2}$$

where N_n represents the number of CPU and CPU(t) represents the usage rate of the CPU at the t moment. When the consumption is time, each transaction generated consumes a corresponding amount of time, written as follows:

$$T = Nt, \tag{3}$$

where T is total time, N is the number of transaction, and t is the time of per transaction. When the consumption is human resources, depending on the educational application, human resources will change as well. The larger an application project, the more manpower is required, and the more costly it is for different manpower to perform their respective roles in the application. When the consumption is memory resource, every time a block is added, the corresponding memory resource is consumed, written as follows:

$$M = Bb, \tag{4}$$

where M is the cost of memory resource, B is the memory size of block, b is the number of new block added. Compared with the traditional data sharing and certificate certification costs, after using the blockchain technology, it is not necessary to separate the ultra-large capacity central database for data storage, do not need to spend a lot of paper resources for certificate issuance, and do not need to hire third-party irrelevant personnel for supervision and management, which greatly reduces the cost of manpower and material resources.

4.3. Throughput. It refers to the number of transactions made per unit time for blocks with transactions on the blockchain, and the data interaction within blocks without transactions. Block transaction data can be used to gauge the system's throughput during the real application process. For instance, in a blockchain-based credit transfer framework, the faster the system responds to an application confirmation when multiple users submit credit transfer requests, the better the system throughput. Similarly, in a data-sharing framework, the faster the system throughput is, the more users are permitted to access shared resources.

4.4. Efficiency. It refers to the number of transactions that can be processed per unit of resource on the blockchain. This unit resource can be a memory resource, it can be a CPU resource, also can be a time resource, assuming that the efficiency is P, the number of nodes in the blockchain is N, the node ID is i, and different resource types are calculated differently. When the unit resource is a memory resource, the following expression is obtained:

$$P = \frac{T_s}{\sum_{i=1}^{N} \int_{ts}^{te} (Ai(t) + Bi(t))\mathrm{d}t}, \tag{5}$$

where $A_i(t)$ and $B_i(t)$ are represented as the occupied memory and running memory of node i at t moment, respectively. When the unit resource is a CPU resource, the following expression is obtained:

$$P = \frac{Ts}{\sum_{i=1}^{N} Nn \bullet \int_{ts}^{te} CPU_i(t)\mathrm{d}t}. \tag{6}$$

When the unit resource is a time resource:

$$P = \frac{Ts}{S}, \tag{7}$$

where S represents the total number of blocks.

4.5. Reliability. Reliability mostly pertains to the maximum number of malicious nodes that can exist, as there will unavoidably be malicious nodes on the blockchain. The ratio of the maximum number of malicious nodes to the total number of nodes can be accommodated when the blockchain is functioning smoothly. General data storage systems and data sharing platforms will fall collectively as a result of security threats, exposing the user's data. Following the development of the blockchain technology, every block in the chain is now interdependent and mutually contained, and data are saved using encryption techniques. If the node is attacked by a malicious party, this node is invalid, and the data of all other nodes are not impacted in any way.

4.6. Scalability. It refers to storage capacity and usage scenarios. Due to the restricted storage capacity of paper certificates and the use of a single storage technique, the record information that can be saved will be significantly constrained, raising doubts about the validity of the certificate. After the blockchain is combined, information can be saved through block nodes, a variety of smart contracts can be introduced; students, schools, governments, and employers can be included in the contract, multiparty authentication can be improved, and the credibility of data information can be increased. The ensuing contract can also be modified in accordance with various educational scenarios, and the scalability is relatively high.

4.7. Consistency. It refers to information that does not change over time. To prevent tampering with the data saved in the blockchain, decentralized distributed storage is used. The longer block data are kept unmodified, the higher the degree of authentication of the accessed data, the more robust the consistency. For instance, in the blockchain-based higher education transcript storage system proposed by Arndt and Guercio [105], the grade information of educated peoples after receiving higher education is stored in the system, and after a few years, the information queried by authorized users will not change. The more stable the system is, the better the performance will be.

4.8. Maintainability. It refers to problems that arise later and consume low cost. The blockchain is in a peer-to-peer network, there is no third-party control, and the blocks are equal nodes, avoiding a single point of failure and effectively lowering the risk of the system failing as a whole due to a small attack. This is in contrast to the centralized network of the traditional education system. The credibility and usefulness of a blockchain-based education system increase once it is put into operation because nodes watch out for one another, lowering error rates and maintenance costs down the road.

4.9. Real Time. It refers to calculate the time required to collect the data. The quicker the time, the more accurate the data are proven to be. The block of stored data will be stamped with a time stamp after it is added to the blockchain; this ensures that the data cannot be tampered with. The block of stored data will then be encrypted and saved. For instance, in the use of the graduate diploma storage system suggested by Schr and Mösli [106], when the educated people's graduation information is kept on the blockchain, the record is permanently maintained and no alteration is allowed, avoiding the issue of certificate fraud.

4.10. Processability. In the education process, many intermediate data are generated, which must all be recorded and saved. The block timestamp is verified for subsequent authentication and traces the authenticity of the data source. The blockchain technology can record users' learning data of formal education, learning data of nonformal education, cross-platform learning experiences and learning outcomes in a timely manner, and record index values are encrypted in a public key manner.

The abovementioned evaluation metrics are reflected in the construction of a credible system in educational application scenarios. The basic indicators are the characteristics that every educational application system must have, and the basic performance of the system is reflected by the final results of these evaluation indicators. The evaluation of characteristic indicators is also involved in the existing applications. For example, scalability and consistency are reflected in [54, 76], process and real-time are reflected in [59, 74], and maintainability is reflected in [52, 57]. These evaluation metrics side-by-sides reflect that the blockchain technology plays a necessary role in building credible educational applications.

5. Conclusions

Establishing credibility in education is an urgent need to solve the optimization problem in education field at present. In this process, the blockchain technology shows its unique performance attributes, demonstrating its necessity for establishing credible applications in the education field. This paper focuses on the use of decentralized storage, privacy protection, and secure authentication of the blockchain technology to enhance trustworthiness and gives performance evaluation criteria for blockchain educational applications. They improve the privacy of education data storage, enhance the traceability of education data sharing, maintain the authenticity of education result authentication, ensure the fairness of education activity evaluation, and help build a credible system in the education field. However, considering the special nature of the education field itself, which involves many factors such as education environment, teaching methods, learning outcomes, and evaluation standards, the establishment of a credible system of the blockchain technology in the education field will face many challenges, such as limited storage space for education data, difficulties in authentication of education resources, and security issues of the blockchain technology itself.

5.1. Limited Storage Space. Rapid growth of education data, the limited storage space make it difficult to store all the education process data, which increases the difficulty of data traceability, reduces the authenticity of data sources and weakens the credibility of results. With the mature application of big data technology in the field of education, the data generated in educational activities has jetted up so much that the blocks in the blockchain need to carry more and more data, and the demand for storage space has become higher and higher. The data volume of educator information, educated person information, learning records, and certificate information is getting larger and larger, which will lead to serious limitation of data storage space, affecting the speed of storage and update of education data information, and also reducing the efficiency of user access to data. It is suggested to combine cloud storage, put a large amount of user information on the cloud, and store index values on the blockchain, which improves storage efficiency, ensures data authenticity and security, and also reduces the storage pressure of the blockchain.

5.2. Ambiguous Resource Rights. Data property rights are disputed, educational data are virtual, the authenticity of data sources cannot be confirmed nor can they be used as a basis for evaluation of educational activities, and the validity of evaluation results can be questioned. Compared with the real existence of data in the real world, the virtual nature of data on blockchain networks has become problematic. The relevant authorities should formulate corresponding regulations to clarify the ownership of data in order to confirm the rights of virtual data on the blockchain network. The data producer owns all the rights to the data, and any user who wants to use the data must get permission from the producer and provide something of value in exchange. The results obtained by the user through data analysis should be reasonably shared with the data producer by reaching a corresponding agreement.

5.3. Issue of Blockchain. The security of the blockchain itself still needs to be strengthened, and the construction of a credible system for educational application scenarios will also face security challenges. The development and use of blockchain's anonymity protection technology are not mature enough, and the management of keys is still at an early stage of development. With the development of cryptography and other technologies, whether the key will be cracked and whether it will cause information leakage afterwards, leading to a crisis of trust in education data. Consider multiple collaborative protection of the blockchain in time, space, technology, and other dimensions to better maintain the security of the blockchain.

While there are many issues that need to be explored in depth, this research opens a window of opportunity to better address trust relationships in education. As blockchain continues to develop, future applications in education will become more widespread and deeper, taking a research step in the direction of building a trustworthy system for education exploratory step.

Data Availability

The data supporting this review are from previously reported studies and datasets, which have been cited.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Key Program of Chongqing Education Science Planning Project (K22YE205098) and the Doctoral Research Foundation of Chongqing Normal University (Nos. 21XLB030, and 21XLB029).

References

[1] J. Fan and X. Li, "Educational trust: the key to enhance the credibility of ideological and political education," *Journal of Henan Normal University (Natural Science)*, vol. 49, pp. 144–150, 2022.

[2] A. S. Anwar, U. Rahardja, A. G. Prawiyogi, N. P. L. Santoso, and S. Maulana, "iLearning model approach in creating blockchain based higher education trust," *International Journal of Artificial Intelligence*, vol. 6, no. 1, 2021.

[3] Q. Li and X. Zhang, "Blockchain:A technology to win open and trust in education," *The Journal of Distance Education*, vol. 35, no. 1, pp. 36–44, 2017.

[4] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, Article ID 117134, 117151 pages, 2019.

[5] L. Ouyang, "Smart contracts: architecture and research progresses," *Acta Automatica Sinica*, vol. 45, no. 3, pp. 445–457, 2019.

[6] S. Nithya and E. G. D. P. Raj, "Survey on asymmetric key cryptography algorithms," *Journal of Advanced Computing and Communication Technology*, vol. 2, no. 1, pp. 1–4, 2014.

[7] W. Ren, J. Hu, T. Zhu, Y. Ren, and K. K. R. Choo, "A flexible method to defend against computationally resourceful miners in blockchain proof of work," *Information Sciences*, vol. 507, pp. 161–171, 2020.

[8] Q. Zhang, "Incentive mechanism for federated learning based on blockchain and Bayesian game," *Scientia Sinica*, vol. 52, no. 6, pp. 971–991, 2022.

[9] W. Li, M. He, and H. Sang, "An overview of blockchain technology: applications, challenges and future trends," in *Proceedings of the 2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, Beijing, China, June 2021.

[10] A. Firdaus, M. F. A. Razak, A. Feizollah, I. A. T. Hashem, M. Hazim, and N. B. Anuar, "The rise of "blockchain": bibliometric analysis of blockchain study," *Scientometrics*, vol. 120, pp. 1289–1331, 2019.

[11] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, "Blockchain in healthcare and health sciences—a scoping review," *International Journal of Medical Informatics*, vol. 134, Article ID 104040, 2020.

[12] D. Li, D. Han, Z. Zheng et al., "MOOCsChain: a blockchain-based secure storage and sharing scheme for MOOCs learning," *Computer Standards & Interfaces*, vol. 81, no. 2022, Article ID 103597, 2022.

[13] T. Wang, S. Chang Liew, and S. Zhang, "Pubchain: a decentralized open-access publication platform with participants incentivized by blockchain technology," in *Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC)*, IEEE, Montreal, QC, Canada, October 2020.

[14] S. Kwak and J. Lee, "Implementation of blockchain based P2P energy trading platform," in *Proceedings of the 2021 International Conference on Information Networking (ICOIN)*, IEEE, Jeju Island, South Korea, January 2021.

[15] H. Xu, "Trusted sharing platform of online education resources based on blockchain," *Wireless Internet Technology*, vol. 19, no. 13, pp. 63–65, 2022.

[16] S. Ølnes, J. Ubacht, M. Janssen, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," *Government Information Quarterly*, vol. 34, no. 3, pp. 355–364, 2017.

[17] Z. Meng and Y. Wang, "Asymmetric encryption algorithms: primitives and applications," in *Proceedings of the 2022 IEEE 2nd International Conference on Electronic Technology, Communication and Information (ICETCI)*, IEEE, Changchun, China, May 2022.

[18] A. Anjum, M. Sporny, and A. Sill, "Blockchain standards for compliance and trust," *IEEE Cloud Computing*, vol. 4, no. 4, pp. 84–90, 2017.

[19] V. Buterin, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, pp. 2–1, 2014.

[20] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Decentralized Business Review*, Article ID 21260, 2008.

[21] R. Sujeetha and C. A. S. Deiva Preetha, "A literature survey on smart contract testing and analysis for smart contract based blockchain application development," in *Proceedings of the 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, IEEE, Trichy, India, October 2021.

[22] J. Jayabalan and N. Jeyanthi, "A study on distributed consensus protocols and algorithms: the backbone of blockchain networks," in *Proceedings of the 2021 International Conference on Computer Communication and Informatics (ICCCI)*, IEEE, Coimbatore, India, January 2021.

[23] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: its promise, components, processes, and problems," *IEEE Consumer Electronics Magazine*, vol. 7, pp. 6–14, 2018.

[24] M. Dotan, Y. A. Pignolet, S. Schmid, S. Tochner, and A. Zohar, "Survey on blockchain networking: context, state-of-the-art, challenges," *ACM Computing Surveys*, vol. 54, no. 5, pp. 1–34, 2021.

[25] J. Pan, Z. Song, and H. Wangze, "Development in consensus protocols: from PoW to PoS to DPoS," in *Proceedings of the 2021 2nd International Conference on Computer Communication and Network Security (CCNS)*, IEEE, Xining, China, July 2021.

[26] T. P. Keenan, "Alice in blockchains: surprising security pitfalls in PoW and PoS blockchain systems," in *Proceedings of the 2017 15th Annual Conference on Privacy, Security and Trust (PST)*, IEEE, Calgary, AB, Canada, August 2017.

[27] N. Lasla, L. Al-Sahan, M. Abdallah, and M. Younis, "Green-PoW: an energy-efficient blockchain proof-of-work consensus algorithm," *Computer Networks*, vol. 214, Article ID 109118, 2022.

[28] M. Alzayat, J. Messias, B. Chandrasekaran, K. P. Gummadi, and P. Loiseau, "Modeling coordinated vs. P2P mining: an analysis of inefficiency and inequality in proof-of-work blockchains," 2021, https://arxiv.org/abs/2106.02970.

[29] S. . E. Thomsen and B. Spitters, "Formalizing nakamoto-style proof of stake," in *Proceedings of the 2021 IEEE 34th Computer Security Foundations Symposium (CSF)*, IEEE, Dubrovnik, Croatia, June 2021.

[30] K. Chen, "A formal analysis method of PoS consensus protocol based on byzantine fault tolerance," *Netinfo Security*, vol. 21, no. 8, pp. 35–42, 2021.

[31] J. Neu, S. Sridhar, L. Yang, D. Tse, and M. Alizadeh, "Securing proof-of-stake nakamoto consensus under bandwidth constraint," 2021, https://arxiv.org/abs/2111.12332.

[32] H. Xu, "Consensus protocol based on DPOS and aggregate signature," in *Proceedings of the 2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and*

Applications (CVIDL & ICCEA), IEEE, Changchun, China, May 2022.

[33] A. C. An, P. T. X. Diem, L. T. T. Lan, T. V. Toi, and L. D. Binh, "Building a product origins tracking system based on blockchain and PoA consensus protocol," in *Proceedings of the 2019 International Conference on Advanced Computing and Applications (ACOMP)*, IEEE, Nha Trang, Vietnam, November 2019.

[34] A. Ahmad, "Performance evaluation of consensus protocols in blockchain-based audit systems," in *Proceedings of the 2021 International Conference on Information Networking (ICOIN)*, IEEE, Jeju Island, Korea, January 2021.

[35] R. Ezzine, "A rigorous proof of the capacity of MIMO gauss-Markov Rayleigh fading channels," in *Proceedings of the 2022 IEEE International Symposium on Information Theory (ISIT)*, IEEE, Espoo, Finland, June 2022.

[36] X. Zhu, Y. Li, L. Fang, and P. Chen, "An improved proof-of-trust consensus algorithm for credible crowdsourcing blockchain services," *IEEE Access*, vol. 8, Article ID 102177, 102187 pages, 2020.

[37] J. Zhang, R. Tian, Y. Cao et al., "A hybrid model for central bank digital currency based on blockchain," *IEEE Access*, vol. 9, Article ID 53589, 53601 pages, 2021.

[38] A. Pal and K. Kant, "DC-PoET: proof-of-elapsed-time consensus with distributed coordination for blockchain networks," in *Proceedings of the 2021 IFIP Networking Conference (IFIP Networking)*, IEEE, Espoo, Finland, June 2021.

[39] D. Huang, X. Ma, and S. Zhang, "Performance analysis of the raft consensus algorithm for private blockchains," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 172–181, 2020.

[40] A. S. Sharifovich, H. X. Maxmudovich, and B. M. Mansurovich, "Protocol for electronic digital signature of asymmetric encryption algorithm, based on asymmetric encryption algorithm based on the complexity of prime decomposition of a sufficiently large natural number," *Texas Journal of Multidisciplinary Studies*, vol. 7, pp. 238–241, 2022.

[41] C. Sullivan and E. Burger, "E-residency and blockchain," *Computer Law & Security Report*, vol. 33, pp. 470–481, 2017.

[42] G. Verma, M. Liao, D. Lu, W. He, X. Peng, and A. Sinha, "An optical asymmetric encryption scheme with biometric keys," *Optics and Lasers in Engineering*, vol. 116, pp. 32–40, 2019.

[43] X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption," in *Proceedings of the 2011 6th international forum on strategic technology*, IEEE, Harbin, Heilongjiang, August 2011.

[44] Y. Song, "Research on security communication and application based on RSA algorithm," *Electronics Test*, vol. 16, pp. 33–36, 2021.

[45] L. X. Van and D. Hong, "Constructing a digital signature algorithm based on the difficulty of some expanded root problems," in *Proceedings of the 2019 6th NAFOSTED Conference on Information and Computer Science (NICS)*, IEEE, Hanoi, Vietnam, December 2019.

[46] F. J. Aufa and A. Affandi, "Security system analysis in combination method: RSA encryption and digital signature algorithm," in *Proceedings of the 2018 4th International Conference on Science and Technology (ICST)*, IEEE, Yogyakarta, Indonesia, August 2018.

[47] F. Liu, "Research on random encryption scheme of RSA algorithm and ECC algorithm," *Journal of Fujian Computer*, vol. 37, no. 8, pp. 4–7, 2021.

[48] L. Gong, "Design of network information security encryption system based on improved ECC algorithm," *China Computer & Communication*, vol. 34, no. 3, pp. 227–229, 2022.

[49] A. Alarifi, M. Amoon, M. H. Aly, and W. El-Shafai, "Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system," *IEEE Access*, vol. 8, Article ID 221246, 221268 pages, 2020.

[50] C. Turcu, C. Turcu, and I. Chiuchisan, "Blockchain and its potential in education," 2019, https://arxiv.org/abs/1903.09300.

[51] A. Mikroyannidis, J. Domingue, M. Bachler, and K. Quick, "A learner-centred approach for lifelong learning powered by the blockchain," *EdMedia+ Innovate Learning*, Association for the Advancement of Computing in Education (AACE), Chesapeake, VA, USA, 2018.

[52] H. Shen and Y. Xiao, "Research on online quiz scheme based on double-layer consortium blockchain," in *Proceedings of the 2018 9th International Conference on Information Technology in Medicine and Education (ITME)*, IEEE, Hangzhou, China, October 2018.

[53] G. Zou, "Designing a credit bank model based on blockchain technology," *Scientific and Social Research*, vol. 4, pp. 42–49, 2022.

[54] A. Rajalakshmi, K. Lakshmy, M. Sindhu, and P. Amritha, "A blockchain and ipfs based framework for secure research record keeping," *International Journal of Pure and Applied Mathematics*, vol. 15, pp. 1437–1442, 2018.

[55] L. Liu and S. Li, "Investigating the Impact of Bank Housing Credit Risk Control Strategy by Blockchain Technology on the Household Consumption Plan," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 7021384, 12 pages, 2022.

[56] W. Liang, Y. Yang, C. Yang, Y. Hu, S. Xie, and K. C. Li, "PDPChain: A Consortium Blockchain-Based Privacy protection Scheme for Personal Data," *IEEE Transactions on Reliability*, pp. 1–13, 2022.

[57] J. Rooksby and K. Dimitrov, "Trustless education? A blockchain system for university grades," *Ubiquity: The Journal of Pervasive Media*, vol. 6, no. 1, pp. 83–88, 2019.

[58] S. Kosasi, U. Rahardja, N. Lutfiani, E. P. Harahap, and S. N. Sari, "Blockchain technology-emerging research themes opportunities in higher education," in *Proceedings of the 2022 International Conference on Science and Technology (ICOSTECH)*, IEEE, Batam City, Indonesia, February 2022.

[59] H. Al, F. A. Shuhaimi, and K. K. J. Al Ismaily, "The upcoming Blockchain adoption in Higher-education: requirements and process," in *Proceedings of the 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC)*, IEEE, Muscat, Oman, Janauary 2019.

[60] D. Shah, D. Patel, J. Adesara, P. Hingu, and M. Shah, "Exploiting the capabilities of blockchain and machine learning in education," *Augmented Human Research*, vol. 6, no. 1, pp. 1–14, 2021.

[61] M. Mulyati, I. Ilamsyah, A. Aris, I. Gunawan, and M. Suzaki Zahran, "Blockchain technology: can data security change higher education much better?" *International Journal of Cyber and IT Service Management*, vol. 1, no. 1, pp. 121–135, 2021.

[62] M. Turkanović, M. Holbl, K. Kosic, M. Hericko, A. Kamisalic, and A. Kamišalić, "EduCTX: A EduCTX: A Blockchain-Based Higher Education Credit Platformlockchain-Based Higher Education Credit Platform," *IEEE access*, vol. 6, pp. 5112–5127, 2018.

[63] P. Ocheja, B. Flanagan, and H. Ogata, "Connecting decentralized learning records: a blockchain based learning analytics platform," in *Proceedings of the 8th International Conference on Learning Analytics and Knowledge*, Sydney, Australia, March 2018.

[64] B. Awaji, S. Ellis, and L. Marshall, "Investigating the requirements for building a blockchain-based achievement record system," in *Proceedings of the 5th International Conference on Information and Education Innovations*, London, United Kingdom, August 2020.

[65] H. Li and D. Han, "EduRSS: a blockchain-based educational records secure storage and sharing scheme," *IEEE Access*, vol. 7, Article ID 179273, 179289 pages, 2019.

[66] F. Liu, "Research on the educational resources sharing framework based on blockchain," *Modern Educational Technology*, vol. 28, no. 11, pp. 114–120, 2018.

[67] E. Daniel and F. Tschorsch, "IPFS and friends: a qualitative comparison of next generation peer-to-peer data networks," *IEEE Communications Surveys & Tutorials*, vol. 24, pp. 31–52, 2022.

[68] X. Wang, "Design of educational data sharing platform based on blockchain technology," *Industrial Technology Innovation*, vol. 8, no. 2, pp. 31–36, 2021.

[69] F. Gao, "Study on construction of high-quality education resources platform framework based on blockchain," *Plateau Science Research*, vol. 5, no. 2, pp. 117–124, 2021.

[70] F. P. Oganda, N. Lutfiani, Q. Aini, U. Rahardja, and A. Faturahman, "Blockchain education smart courses of massive online open course using business model canvas," in *Proceedings of the 2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, IEEE, Manado, Indonesia, October 2020.

[71] H. Nusantoro, P. A. Sunarya, N. P. L. Santoso, and S. Maulana, "Generation smart education learning process of blockchain-based in universities," *Blockchain Frontier Technology*, vol. 1, no. 1, pp. 21–34, 2021.

[72] P. Ocheja, B. Flanagan, H. Ogata, and S. S. Oyelere, "Visualization of education blockchain data: trends and challenges," *Interactive Learning Environments*, pp. 1–25, 2022.

[73] T. Alam, M. Benaida, and B. Mohamed, "Blockchain and internet of things in higher education," *Universal Journal of Educational Research*, vol. 8, no. 5, pp. 2164–2174, 2020.

[74] S. Gilda and M. Mehrotra, "Blockchain for student data privacy and consent," in *Proceedings of the 2018 International Conference on Computer Communication and Informatics (ICCCI)*, IEEE, Coimbatore, India, January 2018.

[75] G. Zhao, H. Hui, and D. Bingbing, "Design and implementation of the digital education resources authentication system based on blockchain," in *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*, Nanjing China, January 2020.

[76] C. H. Han, G. J. K. Han, O. A. Gwang-Jun Kim, A. T. Osama Alfarraj, and Y. R. Amr Tolba, "ZT-BDS: a secure blockchain-based zero-trust data storage scheme in 6G edge IoT," *Journal of Internet Technology*, vol. 23, pp. 289–295, 2022.

[77] A. A. Gde, H. Nugroho, and R. Hendriyanto, "A blockchain-based halal certificate recording and verification prototype," *JOIV: International Journal on Informatics Visualization*, vol. 6, no. 2, pp. 364–370, 2022.

[78] B. Wu and Y. Li, "Design of evaluation system for digital education operational skill competition based on blockchain," in *Proceedings of the 2018 IEEE 15th International Conference on E-Business Engineering (ICEBE)*, IEEE, Xi'an, China, October 2018.

[79] X. Chen, "Blockchain simulation: a web application for it education," in *Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, Las Vegas, NV, USA, January 2021.

[80] R. Q. Castro and M. Au-Yong-Oliveira, "Blockchain and higher education diplomas," *European Journal of Investigation in Health, Psychology and Education*, vol. 11, pp. 154–167, 2021.

[81] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: a secure digital evidence framework using blockchain," *Information Sciences*, vol. 491, pp. 151–165, 2019.

[82] Q. Liu, Q. Guan, X. Yang, H. Zhu, G. Green, and S. Yin, "Education-industry cooperative system based on blockchain," in *Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, IEEE, Shenzhen, China, August 2018.

[83] M. Sanni and D. Apriliasari, "Blockchain technology application: authentication system in digital education," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 3, no. 2, pp. 151–163, 2021.

[84] M. Han, Z. Li, J. He, D. Wu, Y. Xie, and A. Baba, "A novel blockchain-based education records verification solution," in *Proceedings of the 19th Annual SIG Conference on Information Technology Education*, Fort Lauderdale, FL, USA, September 2018.

[85] R. Arenas and P. Fernandez, "CredenceLedger: a permissioned blockchain for verifiable academic credentials," in *Proceedings of the 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, IEEE, Stuttgart, Germany, June 2018.

[86] B. Awaji and S. Ellis, "Design, implementation, and evaluation of blockchain-based trusted achievement record system for students in higher education," 2022, https://arxiv.org/abs/2204.12547.

[87] I. B. Bandara, F. Ioras, and M. P. Arraiza, "The emerging trend of blockchain for validating degree apprenticeship certification in cybersecurity education," in *INTED2018 Proceedings*, pp. 7677–7683, 2018.

[88] M. Alshahrani, N. Beloff, and M. White, "Revolutionising higher education by adopting Blockchain technology in the certification process," in *Proceedings of the 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, IEEE, Piscataway, NJ, USA, December 2020.

[89] J. Woo, R. Fatima, C. J. Kibert, R. E. Newman, Y. Tian, and R. S. Srinivasan, "Applying blockchain technology for building energy performance measurement, reporting, and verification (MRV) and the carbon credit market: a review of the literature," *Building and Environment*, vol. 205, Article ID 108199, 2021.

[90] Z. A. Shaikh, A. A. Khan, L. Baitenova et al., "Blockchain hyperledger with non-linear machine learning: a novel and secure educational accreditation registration and distributed ledger preservation architecture," *Applied Sciences*, vol. 12, no. 5, Article ID 2534, 2022.

[91] M. A. Kusuma, P. Sukarno, and A. Aulia, *Security System for Digital Land Certificate Based on Blockchain and QR Code Validation in Indonesia*, EasyChair, Indonesia, 2022.

[92] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere, and B. Stiller, "The proposal of a blockchain-based architecture for transparent certificate handling," in *Proceedings of the*

International Conference on Business Information Systems, Springer, Amsterdam, Switzerland, 2018.

[93] T.-T. Kuo, "The anatomy of a distributed predictive modeling framework: online learning, blockchain network, and consensus algorithm," *JAMIA Open*, vol. 3, no. 2, pp. 201–208, 2020.

[94] C. Li, J. Guo, G. Zhang, Y. Wang, Y. Sun, and R. Bie, "A blockchain system for E-learning assessment and certification," in *Proceedings of the 2019 IEEE International Conference on Smart Internet of Things (SmartIoT)*, IEEE, Tianjin, China, August 2019.

[95] D. Lizcano, J. A. Lara, B. White, and S. Aljawarneh, "Blockchain-based approach to create a model of trust in open and ubiquitous higher education," *Journal of Computing in Higher Education*, vol. 32, no. 1, pp. 109–134, 2020.

[96] S. Solomon, "Blockchain Technology and Gamification-Conditions and Opportunities for education," in *Proceedings of the 8th International Adult Education 2018-Transformation In the Era Of Digitization And Artificial Intelligence*, Prague, Castle, March 2019.

[97] R. Bucea-Manea-Ţoniş, O. M. D. Martins, R. Bucea-Manea-Ţoniş et al., "Blockchain technology enhances sustainable higher education," *Sustainability*, vol. 13, no. 22, Article ID 12347, 12347 pages, 2021.

[98] R. Widayanti, E. P. Harahap, N. Lutfiani, F. P. Oganda, and I. S. P. Manik, "The impact of blockchain technology in higher education quality improvement," *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, vol. 7, no. 2, pp. 207–216, 2021.

[99] Y. Zheng, "Design of a blockchain-based e-portfolio evaluation system to assess the education and teaching process," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 16, no. 5, pp. 261–280, 2021.

[100] W. Zhao, K. Liu, K. Ma, and K. Ma, "Design of student capability evaluation system merging blockchain technology," *Journal of Physics: Conference Series*, vol. 1168, no. 3, p. 032123, 2019.

[101] V. Stepanova and I. Erins, "Assessment of blockchain-based professional growth data processing model," in *Proceedings of the 2020 the 4th International Conference on Business and Information Management*, Rome Italy, August 2020.

[102] M. Jirgensons and J. Kapenieks, "Blockchain and the future of digital learning credential assessment and management," *Journal of Teacher Education for Sustainability*, vol. 20, pp. 145–156, 2018.

[103] J. Xia and W. Zhang, "An overview of blockchain-based educational application systems," *Heilongjiang Science*, vol. 13, pp. 39–42, 2022.

[104] X. Lingling, "Blockchain technology research and application," *Chinese Journal of Scientific Instrument*, vol. 41, pp. 43–53, 2020.

[105] T. Arndt and A. Guercio, "Blockchain-based transcripts for mobile higher-education," *International Journal of Information and Education Technology*, vol. 10, pp. 84–89, 2020.

[106] F. Schär and F. Mösli, "Blockchain diplomas: using smart contracts to secure academic credentials," *Journal of Higher Education Research*, vol. 41, no. 3, pp. 48–58, 2019.