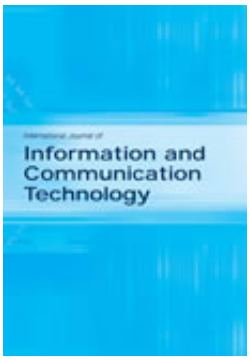
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of Information and Communication Technology

ISSN online: 1741-8070 - ISSN print: 1466-6642
https://www.inderscience.com/ijict

Blockchain-enabled secure distance learning platforms for higher education

Jianmin Chen, Xue Chang

DOI: 10.1504/IJICT.2026.10078368

Article History:

Received:	06 January 2026
Last revised:	16 February 2026
Accepted:	17 February 2026
Published online:	29 May 2026

Blockchain-enabled secure distance learning platforms for higher education

Jianmin Chen and Xue Chang*

Faculty of Education,
Changchun Guanghua University,
130033, Changchun China
and
Shenzhen City Polytechnic (Shenzhen Institute of Technology),
Guangdong, 518045, China
Email: jianmin346@foxmail.com
Email: xuechang50@gmail.com
Email: 350471682@qq.com
*Corresponding author

Abstract: Some people are concerned about the protection of students' privacy, the authenticity of the materials used in the courses, and the safety of students communicating with one another in virtual learning settings. The growing number of educational institutions offers online degree programs. There is a single point of failure in older systems, which could be exploited to alter academic records, gain unauthorised access to systems, and cause problems. It is caused by the fact that earlier systems were designed to function well with centralised architecture. BESDL, which stands for blockchain-enabled secure distance learning, is one approach that could address these issues. The blockchain technology's permanent record and decentralised consensus make data more trustworthy, open, and dependable than it would otherwise be. The three primary components of this system are the secure content-based access control (SCBAC), the decentralised identity management (DIM), and the encrypted content delivery (ECD) protocols, which collaborate to safeguard educational resources. According to the test findings, BESDL enhances system security, maintains examinable academic records, and accelerates the checking process. To summarise, BESDL is not only dependable but also flexible, making it an excellent option for future higher education institutions that will combine online learning.

Keywords: blockchain; distance learning; higher education; smart contracts; secure authentication.

Reference to this paper should be made as follows: Chen, J. and Chang, X. (2026) 'Blockchain-enabled secure distance learning platforms for higher education', *Int. J. Information and Communication Technology*, Vol. 27, No. 56, pp.1–31.

Biographical notes: Jianmin Chen is a graduate of Harbin Normal University. She is a researcher specialising in education. Her research interests include teacher education and teaching management, and digital teaching reform. She has published several academic papers in peer-reviewed journals such as (*Education and Teaching Forum*), and actively participates in interdisciplinary research. Her current research focuses on the reform of higher education in the context of digital transformation, as well as the campus dissemination and practice of intangible cultural heritage.

Xue Chang is a Doctor of Faculty of Business in Shenzhen City Polytechnic (Shenzhen Institute of technology). Her research interest includes corporate governance, finance, and accounting. She used to publish a paper named 'Research on various problems of commercial banks in China' in the (business accounting).

1 Introduction

One primary reason why online and remote learning solutions are becoming more popular is that schools are quickly embracing digital learning. The COVID-19 pandemic and other significant global events have further elucidated this pattern. The platforms are helpful because they enable individuals to continue studying. Still, it is very challenging to ensure data accuracy, develop confidence in academic records, and prevent fraud in degree verification. Certificates gained via remote learning would not be as trustworthy as those earned through conventional means. This is because the most common ways to store student data and certificates have security holes (Chinnasamy et al., 2025; Rakha and Alzubi, 2025). Credential tampering and the issues with the current verification mechanisms have led many people to lose faith in colleges and institutions (Cardenas-Quispe and Pacheco, 2025; Leka and Selimi, 2021).

This firm could undergo significant changes in immutable, decentralised, and straightforward records data. Some studies suggest that blockchain technology could improve document management, enhance the security of certification procedures, and promote academic integrity by enabling remote verification (Berrios Moya et al., 2025). One can build new educational systems that are secure, scalable, and maintain students' privacy by using blockchain technology alongside other technologies such as deep learning, Merkle structures, and zero-knowledge proofs (ZKPs) (Delgado-von-Eitzen et al., 2021). The pace of blockchain research and development is rising across many areas, including data protection laws such as GDPR (Molina et al., 2020), online privacy and security (Ayub Khan et al., 2021), and the long-term survival of businesses (Bidry et al., 2023).

It is important to emphasise that significant deficiencies persist in the current literature on this topic, notwithstanding these amendments. So far, most blockchain-based educational systems have focused on verifying credentials. However, there are still many more secure places to study from home that have not been explored. These include identity management, knowledge dissemination, and the dynamic interactions between educators and learners (Ariffin et al., 2025; Bucea-Manea-Ţoniş et al., 2021). Additionally, the various methods for verifying academic credentials are neither interoperable nor scalable, complicating their use by large corporations (Zhao et al., 2023; Nassani et al., 2023). A lot of research has also said that using blockchain technology in schools is a bad idea. People are worried that the technology will not work with easy-to-use solutions, that it will be too expensive to operate, and that it will not work with environmentally friendly practices (Chen et al., 2025). Lastly, the rise of immersive technologies like the metaverse has led to new techniques for certification and assessment. But these models require trust mechanisms that blockchain technology can provide, as noted by Razzaq et al. (2025) and Krishnan et al. (2025).

It needs solutions that are secure, reliable, and can evolve with us to make learning online easier. These systems must identify students, keep their information confidential, and transfer information in a manner that is difficult to detect. This paper proposes a method for utilising the inherent decentralised trust structure. The system is called blockchain-enabled secure distance learning (BESDL). One idea is to employ smart contracts to support decentralised identity management (DIM), the sharing of encrypted content, and restricting access to specific areas. The BESDL is making sure that students are equipped for college in the new digital age by addressing potential issues before they arise.

Although there is a growing trend of using blockchain to verify academic credentials and manage certificates, existing blockchain-based education systems are mostly confined to post-learning record verification and do not meet the operational needs of safe distance learning. Specifically, current solutions primarily rely on immutable credential stores. In contrast, they lack three important features of the requirements of real-time learning:

1 access control of learning resources and assessment with fine-grained controls

2 decentralised and privacy-preserving identity management that does not create institutional identity silos

3 secure and verifiable delivery of instructional content at every stage of the learning lifecycle.

Additionally, the majority of current frameworks are based on partially centralised identity providers, do not support dynamic authorisation for heterogeneous academic roles, and provide a low level of protection against insider abuse and the dissemination of unauthorised content. Moreover, interoperability and scalability issues have not yet been addressed, so the existing blockchain-based learning systems are not applicable to large-scale, multi-institutional implementations. As a solution to such limitations, a framework, the BESDL, that expands the applications of blockchain past credential validation is proposed in this paper, combining smart contract-based access control (SCBAC), DIM, and encrypted content delivery (ECD) into a single framework. Compared with current solutions, BESDL establishes end-to-end security for authentication, authorisation, content sharing, and credential verification on a decentralised platform, providing reliable, secure, and efficient distance learning in higher education.

The main contribution of the paper is as follows:

- This method implements BESDL. By using smart contracts to govern access, DIM, and ECD, this architecture safeguards higher education from the very beginning to the very end.
- By using procedures that do not require evidence of knowledge and record-keeping that cannot be modified, this approach ensures that academic degree verification is both transparent and unchangeable. This is made possible by the utilisation of blockchain technology.
- The confidentiality of students' information would be maintained through decentralised identification systems and rapid consensus procedures. Moreover, the architecture makes it easy for a large number of educational institutions to utilise.

- The outcomes of the experiment show that this method is superior to the centralised distance learning systems now in use in terms of data security, the speed of authentication, and overall safety.

The remainder of this paper is structured as follows: Section 2 presents the related work. In Section 3, the proposed method is explained. In Section 4, the paper's results are discussed and analysed. Finally, in Section 5, the paper concludes with a discussion of future work.

2 Related survey

A recent study finds that blockchain technology has the potential to be used in higher education to safeguard credentials, verify certificates, and enhance the transparency of evaluations. Table 1 presents the related literature and compares their work. On the other hand, the majority of these solutions are difficult to scale up, generate significant revenue, do not integrate with other systems, and are not suitable for widespread use. By leveraging smart contracts for access control, DIM, ECD, and remote schooling, our system has the potential to expand and ensure all three.

Despite the rapid growth of online learning systems, current systems remain inherently constrained. Centralised LMSs have disadvantages, including single points of failure, changeable academic records, a lack of transparency, and the potential for credential fraud. On the contrary, existing blockchain-based learning applications, though providing immutability and decentralisation, tend to be highly limited in scope (only certificate checking), struggle with scalability and interoperability, and are characterised by latency and complexity. Thus, the fundamental issue in the context of the current paper is the absence of an integrated, scalable, and secure architecture that would ensure decentralised identity control, tamper-resistant access control, ECD, and efficient credential verification in higher education distance learning.

The current education systems cannot sustain secure end-to-end learning processes because centralised LMS platforms rely on changing databases, fragmented modules, and institutional trust, which create risks of data modification, single points of failure, and delayed credentialing. Although blockchain-based systems enhance immutability and transparency, most focus primarily on certificate validation and lack thorough integration with identity management, secure content delivery, extensible access control, and full automation of the academic lifecycle. As a result, both fail to offer a single, safe, and scalable system for handling all aspects of the learning process, from enrolment to certification.

According to the gaps that have been presented in the associated work, especially the excessive focus on credential validation, the lack of strong integration between identity and access control, and the lack of secure content dissemination, the suggested methodology will offer an end-to-end security paradigm to the full distance-learning lifecycle. In this regard, BESDL uses a layered design that integrates SCBAC, DIM, ECD, and immutable credential verification (ICV) within a single blockchain-based application. These design decisions focus squarely on the functional and architectural shortcomings identified by current blockchain-based education systems.

Table 1 Comparison of existing literature

Author name	*Methodology*	*Purpose*	*Results*	*Advantages*	*Limitations*
Paul et al. (2022)	Blockchain technology (BCT) as a digital ledger system (DLS)	Ensure transparent, immutable storage and transactions for online education and asset management.	Growing adoption of digital currency and online education.	Secure, transparent, immutable records.	High-tech reliance, poor infrastructure compatibility, and scalability issues.
Rahardja (2022)	Blockchain-integrated educational framework (BIEF) with IoT and big data	Decentralise higher education and break the central authority in the academic value chain.	Better openness and decentralisation.	Enhances knowledge exchange, reduces central dependency.	Resistance to adoption, governance challenges.
Cheriguene et al. (2022)	Novel online teaching and assessment (NOTA)	Ensure fair exams and motivate teachers/students during COVID-19.	90%+ satisfaction in pandemic trials.	Transparent, fair, incentivised participation.	Limited large-scale testing, not validated outside emergencies.
Alangari et al. (2022)	Blockchain-based academic verification model (BBAVM)	Provide secure, transparent academic document verification (Saudi Vision 2030).	Faster and more reliable verification.	Fraud prevention, high trust in certification.	High infrastructure cost, low readiness, and institutional resistance.
Bjelobaba et al. (2023)	Collaborative learning and student work evaluation (CLSW) with VFN	Simplify certification, safeguard student work, and identify employable skills.	Lecturers willing to adopt BCT.	Supports peer review, protects student data.	Institutional unpreparedness and unclear certification criteria.
Rahardja et al. (2021)	Blockchain-based e-learning platform (BBELP)	Address security, privacy, and sustainability in e-learning during COVID-19.	Improved taxonomy and data protection.	Strong privacy, secure environment.	Pandemic-specific validation, system complexity, and institutional dependency.
Mainetti et al. (2022)	Digital brick platform (DBP) with SCORM, ML, and blockchain	Enable digital badges, secure certifications, and personalised learning.	Transparent, validated, secure platform.	Personalised learning, robust certification.	Scalability limits, badge regulation dependency, and pilot-only validation.
Dias and Silva (2023)	Blockchain-based remote assessment framework (BRAAF)	Mitigate cheating and plagiarism in online classes.	Increased trustworthiness in online assessments.	Secure, reliable, plagiarism-resistant.	High setup cost, technical complexity, and training needs.
AlShamsi et al. (2024)	Blockchain sustainability model (BSM) via SEM-ANN (PMT + ECM)	Identify determinants of blockchain sustainability in higher education.	Satisfaction & usefulness are most influential.	Provides deep behavioural insights.	Limited to student datasets, culturally dependent.
Kontzinos et al. (2024)	Blockchain-powered higher education platform (BPHEP)	Simplify certificate and micro-accreditation verification (smart badges).	Strong stakeholder support, positive pilot.	Valid badges, trust in accreditation.	Small-scale test, uncertain long-term impact, policy alignment needed.
Dash et al. (2025)	Certification verification system (CVS) with hyperledger fabric (HLF)	Decentralise academic credential verification securely.	HLF outperformed Ethereum in TPS and scalability.	Permissioned, secure, enterprise-ready.	Limited to permissioned networks, poor interoperability, and domain-specific use.
Balobaid et al. (2023)	Merkle tree-based blockchain framework (MTBF) + DNA-based chaotic cryptosystem (DNACC)	Strengthen cryptography for student records and secure audit trails.	Resistant to collisions and attacks.	High cryptographic robustness, improved security.	Computationally expensive, untested scalability across multiple institutions.
Saadati et al. (2023)	Blockchain learning management system (BLMS) with adaptive self-regulated learning intervention (ASRLI)	Improve planning, reflection, ZPD, and self-awareness in higher education.	ELT MA students showed strong SRL skills.	Improves collaboration, reflection, and self-regulation.	Small sample size, insufficient cross-validation.

3 Proposed methodology

As the number of individuals using remote learning systems continues to increase, the need for them is growing. It is becoming increasingly important to ensure that these systems are safe, user-friendly, and reliable. Individuals lack trust in online education due to difficulties experienced with previous versions, and they struggle to keep pace with technological advancements over time. Centralised management, data manipulation, the fabrication of fake credentials, breaches of privacy regulations, and a loss of trust are some of the potential problems that could occur. Other possible issues include the failure to maintain confidence.

A BESDL system is presented in this study as a potential solution to the challenges identified there. Figure 1 shows the layered architecture of the BESDL framework. To function correctly, this system leverages the trustless consensus mechanisms, decentralisation, and immutability that are intrinsic to blockchain technology. A learning environment that is not only incredibly efficient but also highly safe and very adaptable is created when the four components of the system – user interaction, application service, blockchain, and security and data management – are brought together. This environment results from the combination of these four components. The BESDL architecture integrates a DIM system, encrypted content distribution, and smart contracts to ensure that all aspects are authentic, responsible, and compliant with the law, creating a secure environment for higher education throughout its entire lifecycle. It is done to ensure that everything is genuine, responsible, and in compliance with the law.

BESDL has been incorporated into existing learning management systems via a thin outermost layer that exposes RESTful APIs and event webhooks, enabling the LMS to invoke blockchain services to verify identity and control access, register content, and validate credentials without altering the underlying LMS. It assumes and implements interoperability based on the learning tools interoperability (LTI) and experience API (xAPI) specifications developed by the 1EdTech Consortium, allowing BESDL to serve as an external, trusted service for authentication, authorisation, and credential anchoring, with the regular components of an LMS controlling course delivery and user interfaces. The design enables the BESDL to be integrated into heterogeneous LMS systems via standard API connectors, OAuth-based authentication, and event-driven synchronisation, providing compatibility with the multi-institution environment.

User interaction layer

The BESDL platform is open to everyone, including students, instructors, and administrators. This is because the user interaction layer is where decentralised applications (DApps) enable individuals to interact with each other. This layer facilitates direct communication among stakeholders, eliminating the need for intermediaries and ensuring everyone can access the information. Professors are responsible for delivering tests, assessing students' work, and disseminating course materials. Students, on the other hand, are expected to turn in original work and participate in class debates. Administrators are responsible for ensuring that credentialing, certification, and policy

implementation are implemented effectively. People can interact without a trustworthy third party, thanks to distributed application programming (DApps). This makes a decentralised system possible. This layer is crucial for making remote learning scalable because it ensures the design is user-friendly, the software is simple to use, and it works on various platforms.

Application service layer

The application service layer is a key component of the BESDL architecture. There are many aspects to it, such as online classrooms, assessment modules, places to share information, and various learning management systems. This layer makes it easy for users to find all examinations, course materials, and feedback mechanisms accessible to them. This means it uses blockchain technology to verify the authenticity of academic work. This makes sure that no one cheats on exams or in school. Adding recommendation algorithms and adaptive learning engines to this layer could make the education even more personalised. Because this layer is modular, it is possible to add new services without modifying the architecture below. This makes it easier to scale up in the long run.

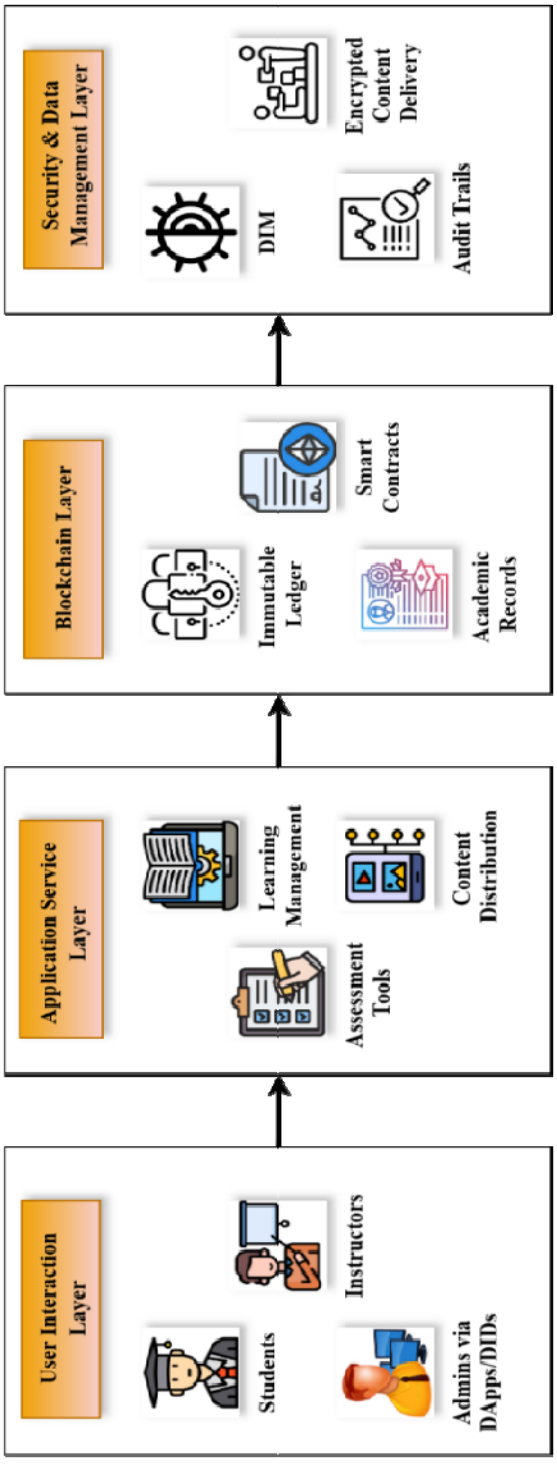
Blockchain layer

The Blockchain Layer is both immutable and secure, which is why the BESDL design requires it to work. Distributed ledgers keep track of all academic transactions, such as signing up for a class, completing a course, obtaining exam results, and earning certifications. Because of human mistakes, smart contracts make things clearer and less likely to go wrong. This could be useful in various areas, such as automated grading, certificate verification, and fee payment. Schools and companies would now examine each student's credentials since blockchain technology cannot be modified. Because of this, it is not easy to edit or make up school records. Techniques that require individuals to agree demonstrate that the system is not dependent on trust, thereby protecting it from breakdowns when one component fails. Proof-of-stake and proof-of-authority (PoA) are two methods that ensure many nodes review all activities recorded on the blockchain.

Security and data management layer

The security and data management layer encompasses a range of responsibilities, including ensuring compliance with institutional and legal requirements and safeguarding users' privacy. DIM enables everyone, including students and instructors, to maintain their digital identities safely and privately. This helps people protect their online identities. ECD keeps students' private information and crucial academic materials safe while they are being sent over a network. Audit trails based on blockchain could help uncover relationships between research papers. This implies that open monitoring would be conducted in compliance with privacy laws such as the GDPR. This layer protects against cyberattacks, data breaches, and unauthorised access while simultaneously fostering a learning environment built on trust.

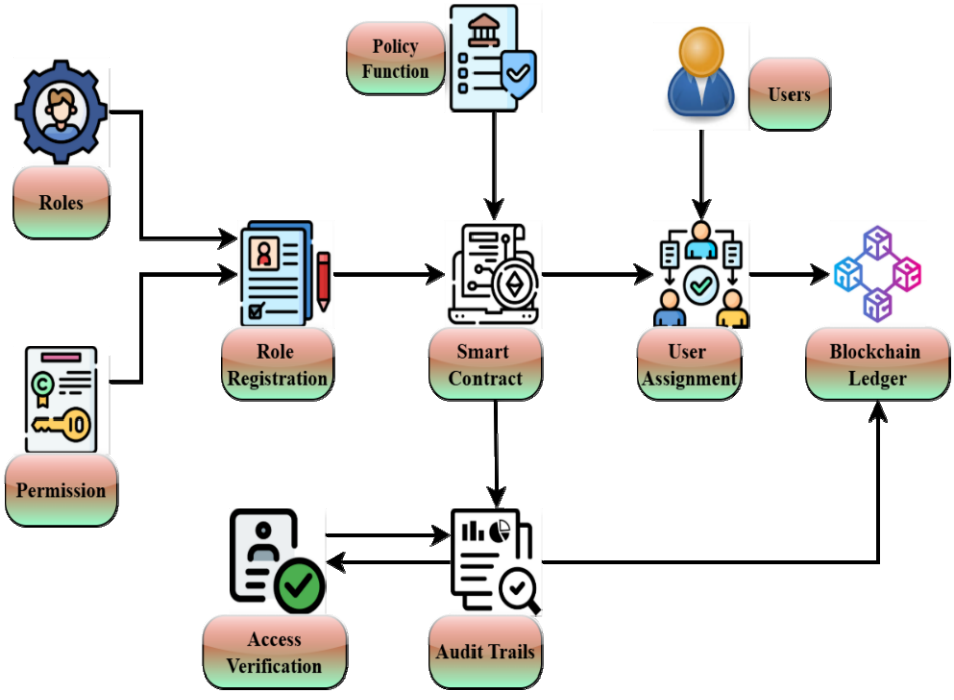
Figure 1 Layered architecture of BESDL framework (see online version for colours)



3.1 Smart contact-based access control

Figure 2 shows the role-based access via smart contracts (SCBAC). Access control is a crucial aspect of BESDL, as it demonstrates how various user types access course materials, resources, tests, and credentials. RBAC and ABAC are two examples of classic access control systems that often have issues with data manipulation, unauthorised privilege escalation, and single-point failures. This is because these systems require a central server or a third-party authority to operate. SCBAC was a way to get past these constraints. It exploits the fact that blockchain technology cannot be modified, that smart contracts can be automated, and that blockchain technology is decentralised to create clear, lasting access controls. Because SCBAC's access rules are cryptographically validated and self-executing, it is possible to audit the behaviour of every user in the learning environment without the need for intermediaries.

Figure 2 Role-based access via smart contracts (SCBAC) (see online version for colours)



Let us imagine there is a system where the number of users is not known for this explanation:

$$U = \{u_1, u_2, ..., u_n\} \tag{1}$$

Equation (1) shows that with every single element u_i refers to individuals involved in the BESDL ecosystem, including students, teachers, or assessors participating in the process. It would also present the list of promises like equation (2):

$$R = \{r_1, r_2, ..., r_m\} \tag{2}$$

when the r_j gives the user a list of permissions that tell them what they can and cannot do. For example, take the inequality r_1. It is supposed to make a point using the pupil's r_2 squared as an example to make an analogy. When the investigator's point of view r_3. Each job has a list of rights that lets them examine exams, send new assignments, and view course materials. Also, every work could produce new tasks.

The mapping function is one of the most important components of SCBAC's access policy, using equation (3):

$$P(u_i, r_j) = \begin{cases} 1, & \text{if } u_i \in R_j \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

It needs to get a user u_i first, before it can utilise this method. They can only use the tools they need to complete their duties r_j. The user will not be allowed in until they can prove they meet the job qualifications. $P(u_i, r_j)$ will always return this value, no matter whether it is true or false. For automated programs using blockchain, it is crucial to ensure that permissions are both trustworthy and easily verifiable.

Another technique to make the model better is to include additional things that are authorised in a permission set Ω. These jobs involve acquiring supplies, turning in work, grading exams, and even handing out diplomas. If it takes all of r_j, obtains a connection to a section of the access $\Omega_j \subseteq \Omega$ that is allowed. So, this implies that for one user u_i, taking up the role r_j of that, the following permissions are now in effect using equation (4):

$$Perm(u_i) = \Omega_j \quad \text{if } P(u_i, r_j) = 1 \tag{4}$$

The mapping enables the construction of a flexible and rule-based access control system by ensuring that permissions align with the provided duties. The person is an example of a customer who is learning. At the coordinates r_1 one will be able to find the necessary supplies and complete the required paperwork to submit the work. The equation that has the variables $Perm(u_s) = \{view\ content, submit\ assignment\}$ the instructor u_t goes over what would've learnt in one turn in the work. Provided to the vector that r_2 shows $Perm(u_s) = \{upload\ content, grade\ assignment\}$.

3.1.1 Putting SCBAC into action with smart contracts

People use the policy function $P(u_i, r_j)$. This is feasible because of smart contracts, which are essentially small pieces of code that operate on the blockchain. It is challenging to update smart contracts because they make it difficult for those who are not intended to change the restrictions on who can access them. To create a basic SCBAC smart contract, one would need the following.

Not only does registering roles create new employment, but it also makes it easier to improve the rights of those who already have work. So, it has equation (5):

$$Register\ role(r_j, \Omega_j) \tag{5}$$

r_j provides the option to play a different part as long as their formal authority allows them to employ the coefficients of Ω_j.

The process that allows users access to resources is called 'user assignment'. It involves defining the user's assigned role and its associated permissions. Look at this equation (6):

$$AssignUser\left(u_i, r_j\right) \tag{6}$$

assures that the user u_i is genuine, makes sure that the rights that r_j provide are preserved. The smart contract verifies before anything happens using equation (7):

$$VerifyAccess\left(u_i, action\right) = \begin{cases} \text{True}, & \text{if } action \in \Omega_j \text{ and } P\left(u_i, r_j\right) = 1 \\ \text{False}, & \text{Otherwise} \end{cases} \tag{7}$$

Only a select group of approved users will be allowed to accomplish certain things from now on. The blockchain maintains a record of all access requests, including those that are not authorised. This makes a record of the audit using equation (8):

$$Log\left(u_i, r_j, action, status, timestamp\right) \tag{8}$$

One can determine if an item can be brought inside by its state. This enables unambiguous accountability in the event of a dispute or forensic inquiry.

Math-based safety guarantees

It conducts an analytical study of SCBAC's features to better understand its strengths. For permission to be complete, every action must be connected to a valid function. Since equation (9) shows this:

$$\forall action \in \Omega, \exists r_j \in R : action \in \Omega_j \tag{9}$$

It wants to check in with everyone to make sure they can stay focused. The blockchain record cannot be amended; therefore, it cannot be revoked, meaning users cannot contest the submission of an access request. The reason for this is that the blockchain record cannot be changed. The fact that blockchain technology cannot be modified implies that equation (10) shows:

$$Log\left(u_i, r_j, action, status, timestamp\right) \notin M \tag{10}$$

The letter M stands for the set of entries that would be changed. This set is empty since everyone agrees on the blockchain. Once an access control policy has been added to a smart contract, these are the procedures to make sure it stays real with equation (11):

$$f_{policy}(t) = f_{policy}(t+1) \tag{11}$$

When someone has to deal with it, they ensure things stay moving by determining who can get in. It put the principle of 'least privilege' into practice by granting each user access to only the resources they need to do their job, as defined by equation (12).

$$Perm\left(u_i\right) \subseteq \Omega \ \ \forall u_i \in U \tag{12}$$

Do not give someone too much authority or power that is not founded on anything. The contract makes it very clear that the student must get the teacher's permission before taking the exam. The blockchain ledger simultaneously tracks the attempt, time, and

outcome. The system maintains records of even unlawful actions to ensure fairness and honesty. The system verifies that only the grader linked to the utilised one is awarded a mark. Obtain the necessary authority to administer the exam that awards those grades. One can protect against impersonation and role abuse by ensuring that only authorised individuals can authorise tests. The SCBAC notion is significantly better than earlier, more centralised access control methods, as it is decentralised, tamper-resistant, and automated. In the BESDL environment, SCBAC uses math to define users, roles, privileges, and access limits in a legally compliant manner. Then, smart contracts make sure that these rules are obeyed. This ensures that only authorised individuals can perform specific tasks at work. It is crucial to include SCBAC in the process of creating safe remote learning systems for future generations. Because blockchain technology cannot be modified and is available to everyone, it is more reliable, accountable, and compliant.

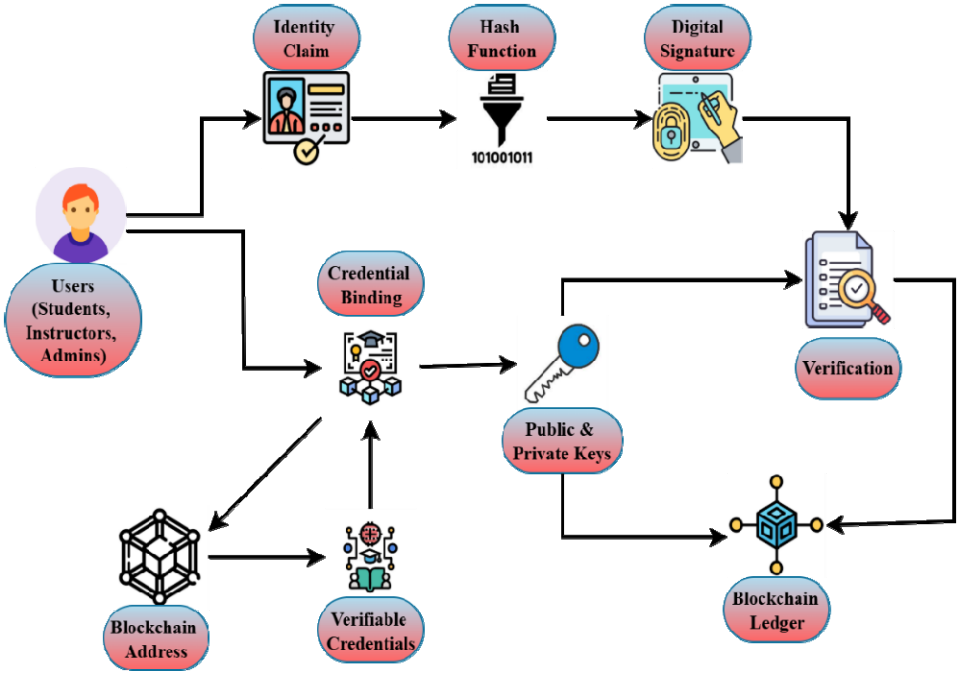
3.2 Decentralised identity management

In distance learning, centralised identity management is common because authentication techniques often rely on institutional servers or third-party identity providers. People are aware that centralised systems have several drawbacks, including making customers less secure and facilitating easier access for hackers to steal or leak their private information. The DIM component of the BESDL system enables individuals to verify each other's identities and complete schoolwork without relying on a central authority. A blockchain address cryptographically linked to verified credentials identifies each user. This ensures the user's identity is both authentic and confidential. Figure 3 shows the BESDL identity management using blockchain (DIM).

The core notion underpinning DIM is that identities are independent of one another at their most basic level. The public-private key pair (*pk*, *sk*) is what identifies each user, not their true name, which is recorded in institutional databases. This is done to prevent unauthorised individuals from accessing the system. The user's private key, which is displayed by the symbol (*sk*), is concealed. The user's public key, denoted by the symbol *pk*, is visible to all nodes on the blockchain. Digital signatures would be used to ensure that statements about someone's identification are authentic, legitimate, and cannot be altered.

The BESDL system presupposes a semi-permissioned blockchain with validator nodes being trusted academic institutions with a PoA consensus model, and most of them being honest. The attack threat is an external attack like impersonation, replay attack, unauthorised access and credential forgery, but not large-scale collusion of validators or majority attack. Students and instructors are subjected to the system but not considered validating nodes and the users are expected to protect their own private keys. In terms of cost and complexity, smart contract execution has transaction (gas) fees on state-changing operations such as assign roles and issuance of credentials and verification functions need only a small amount of cost. The complexity of most contract operations is constant or linear to the number of roles or permissions and by hashing the content and storing hashes on-chain and all the content off-chain, the system has lower storage costs and guarantees lower operational costs compared to all on-chain implementations.

Figure 3 BESDL identity management using blockchain (DIM) (see online version for colours)



3.2.1 Authentication

m is a means to show the identity claim. In BESDL, the letter m could mean a variety of different things, such as a student's enrolment ID, a teacher's authorisation to teach a class, or a grading authority. A digital signature made by the user using their private key could show that this statement is true, as shown in equation (13):

$$\sigma = Sign_{sk}\left(H(m)\right) \tag{13}$$

The identity claim *m* has a cryptographic hash called $H(m)$. The hash function must transform the claim into a digest of a fixed size that cannot be tampered with. This makes it impossible for two emails to have the same hash. The $Sign_{sk}(\cdot)$ is made up of the signing function, which will create a signature called σ by combining the hash value with the user's private key. It will use the user's public key to verify the signature based on equation (14):

$$Verify_{pk}\left(\sigma, H(m)\right) = 1 \tag{14}$$

Authentication is granted only when the signature is verified as genuine and the associated name matches the individual's true identity. If the verification technique returns a value of 0, it means the claim or signature is not genuine. This method reduces the risk of identity theft and impersonation by only allowing authorised individuals to authenticate their identities.

3.2.2 Identity as a blockchain address

The blockchain can determine who a DIM user is by looking at their public key, which is connected to the address below in equation (15):

$$Addr = f(pk) \tag{15}$$

For example, Ethereum utilises the deterministic function $f(\cdot)$. SHA-256 and RIPEMD-160 are two further examples of hash-based transformations. The person's unique blockchain address is akin to a digital passport when compared to anything else. When keys are cryptographically connected to addresses, it ensures that the addresses are unique. This also makes the addresses unchangeable and prohibits anybody from replicating them.

Also, many blockchain addresses contain verifiable credentials, or VCs for short. Credentials can be used to verify a student's class attendance, enable teachers to upload course materials, and allow examiners to provide assessments. One would keep these credentials off-chain by using pointers that reference the blockchain. This makes them safe and impossible to modify. One would store them on the blockchain; however, if one wants to be honest and upfront about everything. Digital signatures ensure that credentials remain valid. These signatures could originate from trustworthy organisations or be checked via a decentralised consensus mechanism. The confirmation of access via proper channels to make it easier for DIM checks to access, the tuple could be seen in a different way based on equation (16):

$$Identity(u_i) = (Addr_i, VC_i, pk_i, sk_i) \tag{16}$$

The user's blockchain address $Addr_i$ shows the times the values of u_i. VC_i a symbol of truth that connects us both as new students at this school. There is a math portion in the sentence somewhere, involving the public and private keys pk_i, sk_i that says when a user u_i performs anything, like attempting to get to test materials, the system does this:

$$AccessGranted(u_i, action) = \begin{cases} 1, & \text{if } Verify_{pk_i}\left(Sign_{sk}\left(H(m)\right), \left(H(m)\right) = 1 \wedge VC_i\right) \vDash action \\ 0, & \text{Otherwise} \end{cases} \tag{17}$$

In equation (17), the $\vDash$ symbol indicates that the validated credential grants permission for the action in question. Access is not allowed until the user's identification and permission have been validated with the relevant authorities for safety concerns.

DIM is the ideal security choice for BESDL because it offers many outstanding features, such as: it is mathematically certain that each claim of identity is valid, since a private key is used to verify them. A hacker can forge signatures if they have the user's secret key. Because hash functions check that the signature is valid for integrity, any modification to the identity claim would make the signature meaningless. As suggested in equation (18),

$$H(m_1) \neq H(m_2) \quad \forall m_1 \neq m_2 \tag{18}$$

Non-repudiation makes it harder for a user to later deny involvement in a claim by linking their signature to their private key. The fact that no single person controls the authentication process makes it decentralised. Blockchain nodes, on the other hand, work

together to validate identities and signatures, which fixes these types of problems. Users can maintain their privacy by making the right claims, thereby keeping their identity hidden. Using ZKPs is one way to improve DIM. ZKPs would enable users to validate their registrations without providing any personal information.

3.2.3 Example scenario in distance learning

Imagine being a student trying to submit an assignment. Imagine one of them. The student should use their private key to sign a claim that states, "I am enrolled in course X". Ensure the signature is directly linked to the work. The blockchain-based system would use the student's public key to determine whether the credential VC_i is legitimate. One does not have to join the X-class. There is no way that the assignment will be accepted until both of these conditions are met. If it does not happen, the contract will be void. If one does it this way, phony students or those pretending to be students will not be able to turn in their work.

In the same manner, teachers must provide documentation that they are qualified to grade a test. One needs to confirm someone's credentials and signature before allowing them into the grading system. Role-based authentication is how DIM makes sure that rules are followed.

3.2.4 Adding mathematical factors to credential verification

One way to describe the link between identity and credentials is as follows in equation (19):

$$Bind\left(VC_i, Addr_i\right) = Sign_{sk_{auth}}\left(H\left(VC_i \parallel Addr_i\right)\right) \tag{19}$$

where the sk_{auth} a system, owned by an organisation (such as a university), retains the secret code. This keeps credentials secure by associating them with the correct blockchain address. The system will verify all of the following while it is running using equation (20):

$$Verify_{pk_{auth}} Bind\left(VC_i, Addr_i\right), H\left(VC_i \parallel Addr_i\right) = 1 \tag{20}$$

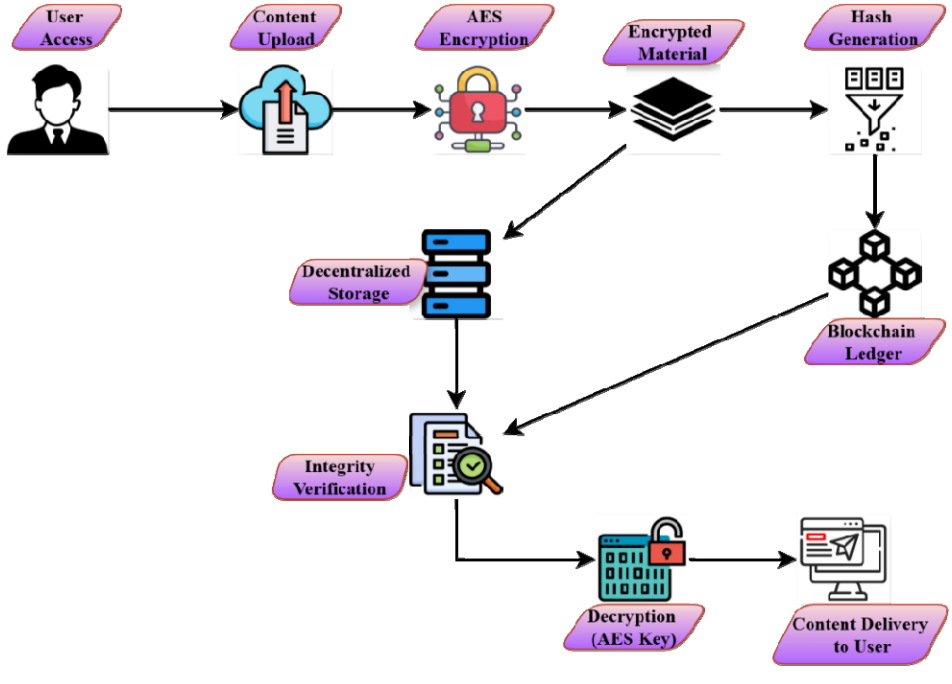
This must be done correctly for the system to recognise the credential. Because of this, evil individuals cannot create new credentials or reuse old ones.

BESDL's DIM solution provides a safe and mathematically sound approach to managing user IDs. The DIM keeps users' identities safe by assigning each user a unique blockchain address linked to their validated credentials. It does this by employing public-key cryptography and digital signatures. As an example, the equations $\sigma = Sign_{sk}(H(m))$ and $Verify_{pk}(\sigma, H(m)) = 1$ provides the authentication process, which becomes official. This ensures authenticity, integrity and non-repudiation are maintained. Credential binding and decentralised verification are two strategies that give individuals greater control over their digital identities and reduce the risks of issues arising from centralised verification. The DIM ensures that everyone respects regulations when online, protects children's privacy, and prevents impersonation.

3.3 Encrypted content delivery

When using blockchain technology in virtual classrooms, it is crucial to ensure that all teaching resources, such as homework, exams, and course materials, are authentic, private, and secure. Figure 4 shows the safe delivery of learning content. Centralised storage mechanisms that have been around for a long time can pose problems because they can be modified, accessed without authorisation, or fail in a single location. The ECD protocol is one approach to delivering significant academic articles across decentralised storage networks. Blockchain hashing ensures authenticity, and symmetric encryption preserves privacy. BESDL combines the latest encryption technologies, decentralised storage systems (such as IPFS), and blockchain technology to transmit crucial academic information securely.

Figure 4 Secure delivery of learning content (ECD) (see online version for colours)



Providing educational materials to keep children safe is a significant aspect of early childhood development (ECD). An increasing number of individuals are embracing decentralised networks like IPFS to keep their data secure. These networks are becoming so fast that it is unnecessary to have a central server. IPFS is a file system that is distributed across many machines. It generates a unique identifier (CID) by hashing the contents of each file. After that, this information is used to determine the purpose of each file. One technique to ensure that files cannot be modified is to address them by their content rather than their location. The hash of a file, and hence, its CID, changes every time the file is updated, making it easy to identify any traces of manipulation.

There will be a methodical approach to ascertain the hash for each F file, including study guides or examinations based on equation (21).

$$CID = H(F) \tag{21}$$

$H(\cdot)$ employs a hash algorithm that cannot be broken, like SHA-256. The graphic above shows the method as IPFS finds the proper file by comparing the *CID* to the information when a teacher or student requests it. IPFS is immune to censorship, redundant, and always accessible because information is distributed across a network. Blockchain technology retains hash values as permanent linkages to the content.

3.3.1 Encrypt data via the advanced encryption standard

The internet protocol file system (IPFS) does not automatically protect privacy, as anyone can view the files it stores. But it ensures that distribution is decentralised. Before it is saved, the advanced encryption standard (AES) safeguards all the course information. The AES uses a secret key to encrypt data in blocks of a fixed size, typically 128 bits. The initial phase in this process is the plaintext data. If it is assumed that the initial piece of information is a plaintext message M, it can be said that the encryption process works like equation (22):

$$C = Enc_k(M) \tag{22}$$

With C being the ciphertext stored in IPFS and k being the shared secret key. To read the message, all allowed users must use the same secret key in equation (23):

$$M = Dec_k(C) \tag{23}$$

This symmetric architecture is ideal for encrypting large multimedia files, such as scanned exam papers, instructional videos, and electronic books. When it comes to that, it truly shines. The key management method is highly significant, as only approved students, teachers, or examiners should have access to the key to decode the data.

3.3.2 Key management in ECD

One has to be extremely cautious when working with keys in ECD. It is vitally crucial that AES keys not be disclosed to the public, as they are used to encrypt and decrypt data. One approach to fix this issue is to use hybrid cryptography, which means encrypting the AES key with asymmetric cryptography. Any authorised user would encrypt a public-private key pair (pk, sk) that has the AES key k in the following way in equation (24):

$$k' = Enc_{pk}(k) \tag{24}$$

To decode the message, one needs the right private key sk in equation (25).

$$k = Dec_{sk}(k') \tag{25}$$

This strategy ensures that only those with permission can access the encryption key, regardless of the data's encryption method. BESDL can provide role-based authentication since it can encrypt and decrypt data. This is possible because of SCBAC and DIM.

3.3.3 Blockchain-based Integrity verification

It is also crucial to keep the data confidential and ensure it remains unchanged. A blockchain is a distributed ledger that cannot be updated. It would also keep track of the

hash values of encrypted data. IPFS keeps the ciphertext C, and every time a teacher uploads course material, a smart contract writes the hash to the blockchain. When a student obtains the ciphertext using IPFS, the hash value $H(C)$ is recalculated throughout the system, which makes it easier to retrieve back using equation (26):

$$H'(C) = H\left(C_{retrieved}\right) \tag{26}$$

If one wants to be sure that the file has not been altered after it was uploaded, one would check the system to verify whether $H'(C) = H(C)$. This prevents malicious actors on the IPFS network from secretly altering or adding to valuable content. The first hash values are always right since the data on a blockchain cannot be modified.

When it comes to BESDL, ECD's key role is to make sure that significant intellectual information is shared. For example, AES could be used to encrypt a document intended for an exam before it is uploaded to IPFS. The blockchain contains a list of addresses for the people who can receive the message, along with the corresponding hash. They will only be able to view the ciphertext and the AES key they produced themselves when they attempt to read the document. The hash of the ciphertext must be compared to the record on the blockchain before the decryption process can begin. This is done to make sure that the ciphertext has not been modified in any way. Strong cryptographic assurances of privacy and security would also be helpful for both students and professors when sharing course materials such as session recordings, certification papers, and lecture notes.

The ECD approach employs decentralised storage, symmetric encryption, and blockchain verification to ensure the security of distributing instructional content within the BESDL framework. One can be sure that all course materials and exams are legitimate by verifying their hashes against those stored on the blockchain. IPFS is used to exchange these files in a way that prevents control by a single person, and AES is used to protect them. ECD is a key aspect of making blockchain-based remote learning secure, as it is built on sound principles.

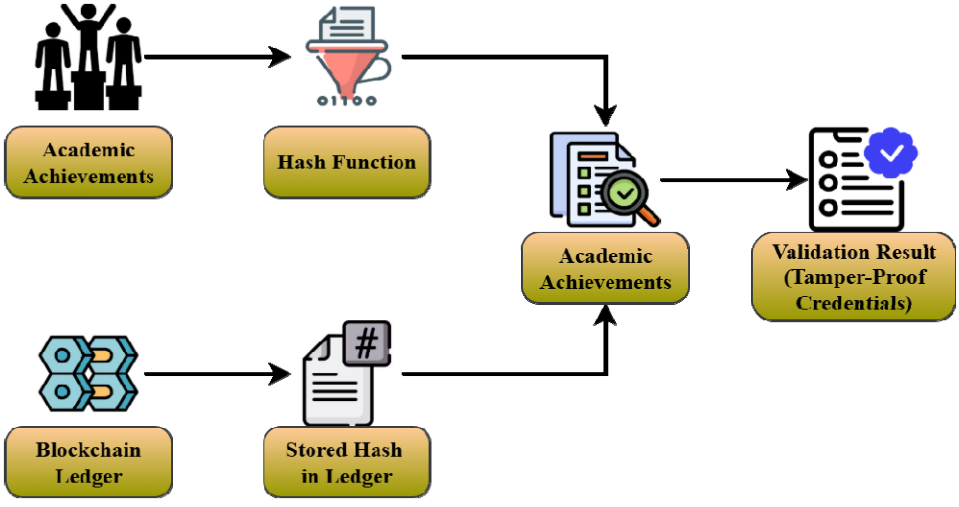
BESDL considers external attackers, malicious insiders (students, instructors, or administrators), and leaked platform components as potential opponents, and identifies smart contracts, decentralised identity authentication, ECD, and on-chain credential management as key attack surfaces. The security requirements include strong authentication, tamper-resistant access control, confidentiality and integrity of learning materials, and unchangeable, verifiable academic credentials, with the assumptions that blockchain consensus is correct and that cryptographic primitives are secure.

3.4 Immutable credential verification

The ICV technique is founded on the premise that academic achievements, such as degrees, certificates, and test scores, should be stored in a manner that makes them impossible to fabricate or manipulate. Figure 5 shows the blockchain-powered credential validation (ICV). The older centralised systems that store credentials are at risk of several threats, including data breaches, document forgeries, and unauthorised changes. Because blockchain technology uses an append-only ledger, it is hard to modify data recorded on the network without the approval of all nodes. One technique that is seen to be formal is to digitise the credential record C and then add it to the blockchain as a transaction. There is a lot of information about this item, such as the issuer's name, the date, the course IDs, and cryptographic hashes, to mention a few. To ensure that no single individual can alter

the ledger, blockchains employ consensus methods such as proof of work and proof of stake. So, C_{record} is the one that keeps a permanent electronic record of the student's academic progress in the correct location.

Figure 5 Blockchain-powered credential validation (ICV) (see online version for colours)



3.4.1 Credential hashing

There are privacy and verification issues that prevent the blockchain from storing raw credentials directly. $H(\cdot)$ is a cryptographic function that would also be used to hash information regarding credentials. Hash functions are challenging to understand because they convert inputs of varying lengths into outputs of fixed length. $H(C_{record})$ refers to both the hash value and the record, which stands for the digital fingerprint of the credential it speaks about. This is the math model that would be used in equation (27).

$$H : \{0,1\}^{*} \rightarrow \{0,1\}^{n} \tag{27}$$

A lot of people utilise SHA-256 algorithms, where n needs 256 bits of data. This method protects the data by storing it in a form that does not depend on the blockchain $H(C_{record})$. The hash will be considerably different from the original if one updates the original credential C in any manner. One would establish a connection between a credential document stored off-chain and its on-chain reference, which cannot be altered using a hash.

3.4.2 Distributed ledger technology

There is a way to keep track of credentials that is like a blockchain ledger. This strategy is termed the commitment mechanism. The issuing institution must write the credential's hash on the blockchain as part of the deal. C_{ledger} will be the formal accounting record. One needs to go down the entry in the ledger. The verification function checks whether the credential is valid by comparing the recomputed hash with the one stored on the blockchain. The equation (28) looks like this more formally:

$$V(C) = H\left(C_{record}\right) \stackrel{?}{=} H\left(C_{ledger}\right) \tag{28}$$

$V(C)$ is a verification method that incorporates an equivalency check. This check compares the provided credential with the commitment recorded in the ledger. Because the credential is binding, no one trying to do anything wrong will be able to change it, duplicate it, or create a new one without being discovered. For a blockchain network to be genuine, all nodes must agree, not just a central authority.

3.4.3 Verification function

When someone outside the organisation, such as an employer, accrediting body, or school, requests that a certification be examined, the verification process begins. It is common not to ask whether a certificate C_{record} is valid since it is the number on the record. The verifier needs to figure out its hash value by the entry looks like this $H(C_{record})$. The next step is to check this value against the one that is stored on the blockchain. This is particularly true for $H(C_{ledger})$ when they are together. If the two numbers are the same, the credential stays the same. When it comes to the normal use of equation (29):

$$V(C) = \begin{cases} 1 & \text{if } H\left(C_{record}\right) = H\left(C_{ledger}\right) \\ 0 & \text{otherwise} \end{cases} \tag{29}$$

This binary verification function provides deterministic validation; thus, the result is precise and cannot be read any other way. A cryptographic guarantee will prevent forgery by producing a new hash even if the data changes by a tiny amount (such as a student's name or grade).

3.4.4 Tamper-resistance

A credential that cannot be changed: There is broad consensus on verification, and it cannot be altered by cryptography; therefore, it is hard to tamper with. Updating old blocks would require significant labour; the blockchain cannot be updated. This is because hashes connect blocks in a specific manner. If an adversary wants to modify $H(C_{ledger})$, they would do it by changing the blockchain. Because the blockchain is so robust, it will be very hard for them to out-consensus the network and recalculate all the hashes for the following block. In principle, this implies that one cannot fabricate credentials using this method. Verification of academic credentials helps colleges worldwide maintain their trustworthiness by combating degree fraud, fraudulent degrees, and phony transcripts using tamper-proof materials.

One would want to consider probability constraints when attempting to demonstrate the accuracy of credential verification. When one employs SHA-256 or a similar strong cryptographic hash algorithm, the chances of two separate credentials, $C_1 \neq C_2$. The risk of a collision hash value is very low based on equation (30):

$$P\left[H\left(C_1\right) = H\left(C_2\right)\right] \approx \frac{1}{2^n} \tag{30}$$

where $n = 256$. This means that there is a 1 in 2^{256} chance that an opponent will produce a credential that matches an existing ledger hash. The system examines credentials to ensure they are legitimate and not compromised. This is done to verify the math.

3.4.5 Decentralised trust model

In the past, the authority that issued credentials was responsible for maintaining centralised repositories that were up to date so that anyone could verify them. ICV enables decentralised trust, eliminating this need. Consensus solutions for blockchain technology allow multiple nodes to verify transactions, eliminating the risk of bias and failure points in institutions. Each certificate is verified using cryptographic proofs rather than relying on institutional approval. This means that people all across the globe can see and appreciate achievements. If institutions and organisations worldwide can verify credentials without contacting the issuer, they could achieve faster verification, greater openness, and greater trust. ICV is based on aspects unrelated to encryption, such as trust frameworks and educational institutions, in principle. Schools would protect their students' academic records by integrating blockchain technology into their credentials. This way, the data cannot be edited or destroyed. Its immutability safeguards both its integrity and the preservation of its historical records, as it is hard to revoke or change a credential after the fact without following specific revocation procedures. If students had access to self-sovereign education records that worked better together across the academic, political, and corporate worlds, they could verify their credentials anywhere in the world.

4 Results and discussion

To test the new BESDL system, it used the Kaggle Student Academic Performance Dataset (https://www.kaggle.com/datasets/aljarah/xAPI-Edu-Data/data). This dataset includes students attending colleges and universities and provides information on their demographics, study methods, grades, and final grades. To evaluate circumstances in which verifying students' identities, limiting access, and checking credentials for online learning are necessary, this dataset would be used. Nearly 600 data samples are available, including information on the number of attendees, their exam performance, and participation in online classes. IPFS was used to store data across a large number of computers, solidity was used to write smart contracts, and Ethereum (Ganache) was used to run the blockchain. The BESDL architecture was constructed using these three components. It is possible to link the learning management system (LMS) to the blockchain by using Node.js. An Intel Core i7 processor, 32 gigabytes of random access memory (RAM), and a desktop computer running Ubuntu 22.04 were used for the experiment. To assess its effectiveness, development potential, and security, it was compared to more traditional, centralised systems for remote learning.

In our experiments, the student academic performance dataset retrieved in the Kaggle is considered only as an off-chain data source to simulate learners, roles, activities, and outcomes: each student record is encoded as a blockchain identity to be authenticated by the DIM, activity and role attributes are encoded as SCBAC permissions to be accessed with, and the ultimate performance fields are coded as credential objects with their hashes anchored on the blockchain to reflect the credential issuance and verification.

The prototype deploys an Ethereum-based private blockchain and uses IPFS as the decentralised storage layer, with the blockchain network configured using the PoA consensus mechanism to provide low-latency validation in an academic deployment environment. The SCBAC, DIM, ECD, and ICV constitute the proposed BESDL architecture in this paper, and the Ethereum-IPFS-PoA stack is the evaluation and implementation stack used to test the viability and performance of the proposed architecture, rather than an obligatory or binding deployment decision.

Kaggle Student Academic Performance is an appropriate dataset to evaluate security since it contains realistic academic data like enrolment data, assessments and grades and thus can be used to test security authentication, access control, data integrity and credential verification procedures in a realistic environment. To analyse scalability, it is important to explicitly define system parameters to guarantee reproducibility. In addition, the summary of the results must be presented in a comparative performance table, in which the percentage changes in performance between centralised systems and the new system should be identified in the key metrics of the purpose, which include accuracy of authentication, latency, throughput, scalability, and speed of verification.

4.1 Authentication accuracy vs. transaction latency

One approach to assessing a system's authentication reliability is to evaluate how effectively it confirms the identities of authorised users and blocks unauthorised access. Figure 6(a) shows the authentication accuracy. When people use older, centralised e-learning systems, their passwords and institutional credentials are at risk of being stolen through phishing and other methods. The BESDL system, on the other hand, leverages blockchain-based digital signatures and DIM to improve the link between user credentials and stored documents. During the tests, BESDL achieved a far higher authentication accuracy of 98.5% than centralised solutions, which achieved an overall accuracy of 91.3%. This new notion indicates that using cryptography to verify the blockchain makes it harder for anyone to impersonate another user. This makes remote learning environments more reliable.

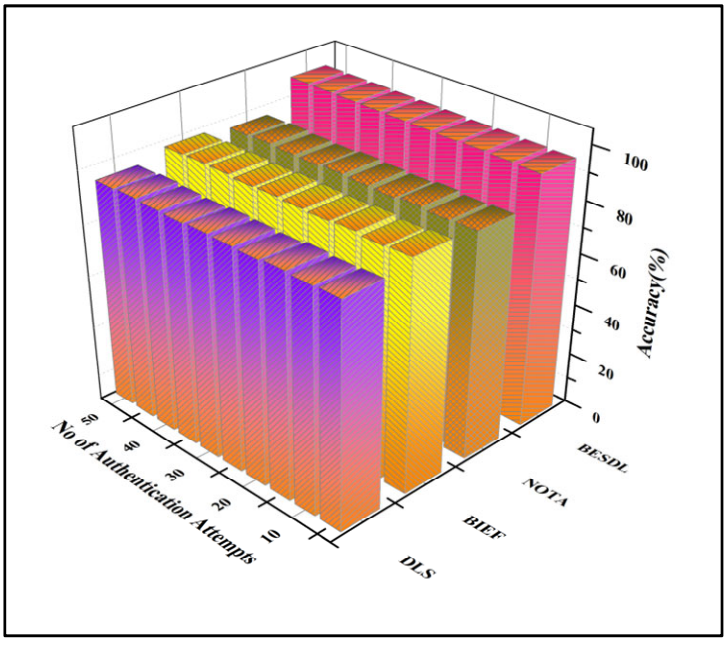
Transaction latency occurs when it takes a lengthy time to record and verify academic activity, such as handing in an assignment or revising a grade. Figure 6(b) shows the transaction latency. The centralised servers used in prior systems start to slow down under heavy demand. BESDL is responsible for verifying every transaction on the Ethereum blockchain via distributed consensus. Using PoA consensus to speed things up reduced the time to process a transaction to 2.7 seconds. Centralised systems, on the other hand, experienced an average delay of 1.9 seconds and surges exceeding 4 seconds at peak demand. The extra time it takes for blockchain-based consensus to reach agreement is not particularly long compared to updating databases directly.

4.2 Throughput vs. scalability index

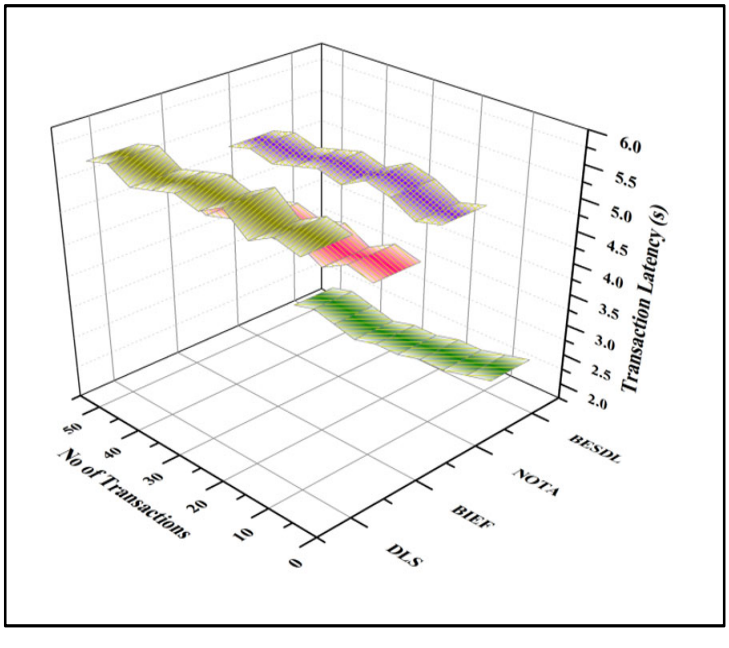
Throughput is the rate at which transactions can be processed by a computer system. Figure 7(a) shows the throughput. A server becomes congested when many people use it, and centralised solutions cannot handle the increased load. BESDL can monitor pupil behaviour in real time, thanks to smart contract automation and distributed nodes. BESDL outperformed central models when 10,000 users were simultaneously involved. It had 320 TPS, far more than the 190 TPS central models achieved. Using off-chain

storage via IPFS and parallel verification techniques can make it easier to manage large-scale, distributed learning activities.

Figure 6 (a) Authentication accuracy (b) Transaction latency (see online version for colours)

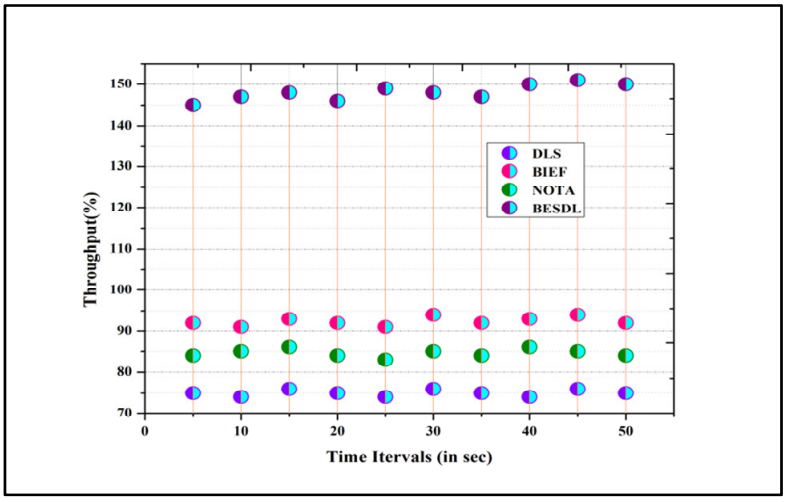


(a)

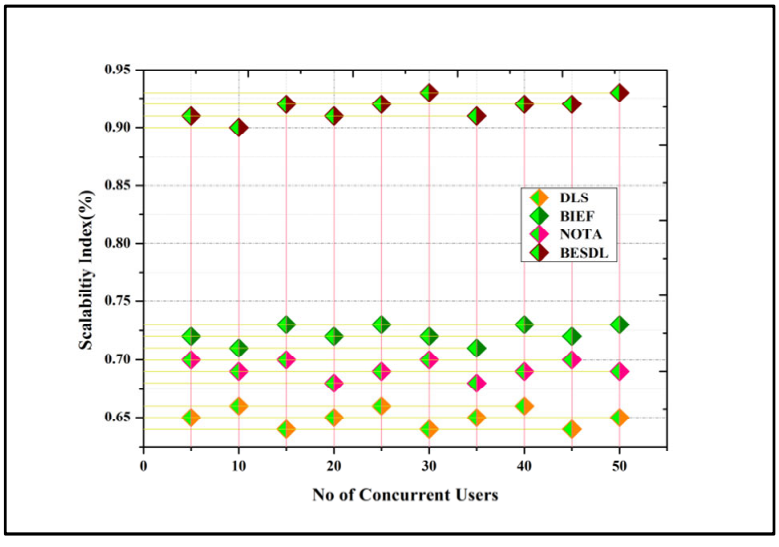


(b)

Figure 7 (a) Throughput (b) Scalability index (see online version for colours)



(a)



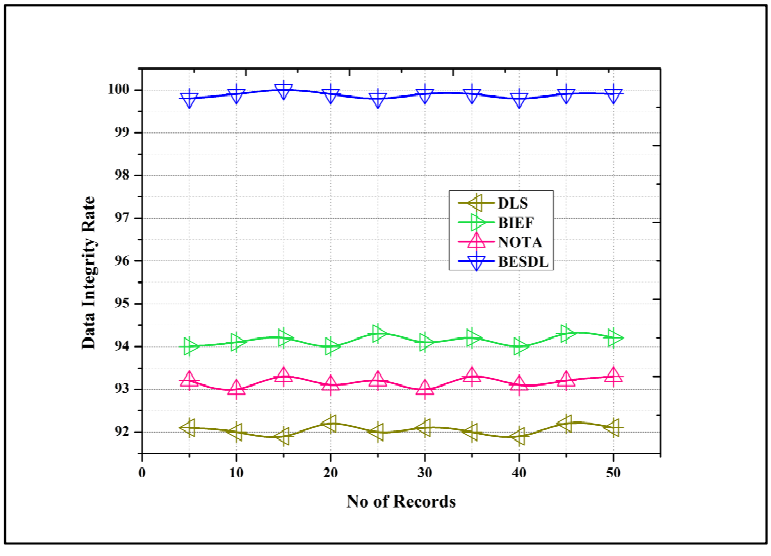
(b)

A framework is scalable if it can accommodate additional users without becoming slower. Because they only use a limited number of centralised servers, traditional systems cannot grow. Figure 7(b) shows the scalability index. BESDL can still grow horizontally, which means it could add new schools or students. It is possible because of blockchain nodes and a distributed storage mechanism. It did not seem like the performance changed significantly as the number of users at the same time rose from 1,000 to 10,000 (our estimates indicate a loss of efficiency of less than 6%). Centralised systems, on the other hand, saw a decline of around 28%. In higher education, decentralisation with blockchain technology appears to be the most effective approach for growing ecosystems.

4.3 Data integrity rate

The safety and verifiability of academic records heavily depend on the precision of the data. Some hazards of centralised systems include the potential for database hacking, unauthorised changes to records, and unauthorised system modifications. Figure 8 illustrates the data integrity rate. BESDL employs cryptographic hashing to store credentials and transactions on the blockchain in a way that cannot be changed. This helps make the blockchain safer. BESDL maintained data integrity at 100% throughout the simulated insider attacks, preventing any alterations exceeding 3.5%. The fact that blockchain technology cannot be modified helps maintain the honesty of academic approaches.

Figure 8 Data integrity rate (see online version for colours)



4.4 Access control efficiency

One way to assess the effectiveness of access control is by measuring how well it prevents unauthorised entry. Figure 9 shows the access control efficiency. Centralised system access methods based on roles could lead to privilege escalation and bad session management. BESDL employs smart contract-based dynamic access restrictions to prevent unauthorised access to sensitive information by administrators, students, and instructors. BESDL works 99.2% of the time, whereas centralised techniques can only stop 92.6% of fake attempts. This occurred because the setup process was broken or there were not enough authentication requirements. Because of this, BESDL makes sure that the access control system is automated, accurate, and robust.

Figure 9 Access control efficiency (see online version for colours)

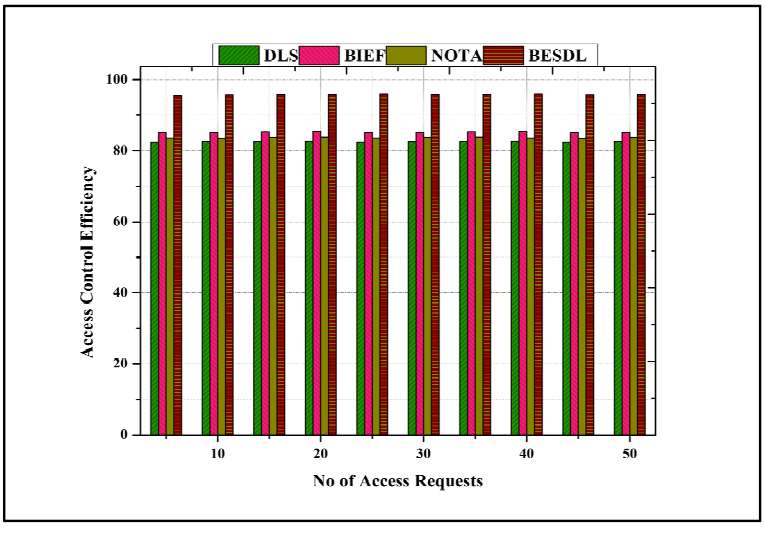
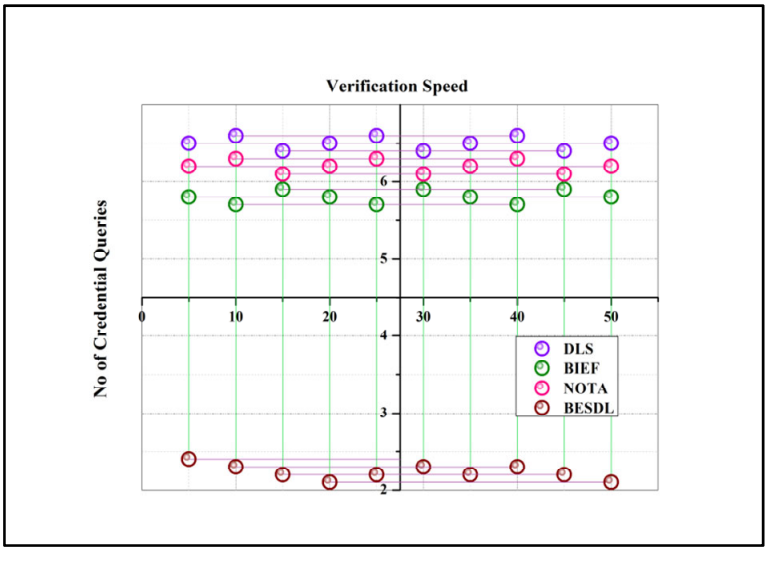


Figure 10 Credential verification speed (see online version for colours)



4.5 Credential verification speed

Figure 10 shows the credential verification speed. The speed of credential verification refers to how quickly a student's record or certificate is examined during the verification process. Old techniques waste time because they require verification or depend on others. The BESDL platform makes it easy to check the blockchain directly; thus, there is no need for intermediaries anymore. Centralised systems required an average of 12.4 seconds to verify credentials through database queries and cross-validation. BESDL

only needed 2.1 seconds, significantly less time than the other methods. BESDL is a wonderful option for job applications, student transfers, and online tests that require immediate verification, as it processes data so rapidly.

4.6 Storage overhead

Storage overhead is the extra space required to store both the transactions recorded on the blockchain and those that are not. Table 2 gives the values of storage overhead. Centralised systems could save money and improve clarity by adopting compression-tuned relational databases. BESDL uses IPFS for large amounts of data and blockchain for large hashes, which makes storage considerably more expensive than it would be with other methods. The findings indicated a 15% increase in storage use relative to centralised systems. Decentralised databases are superior to central databases because they offer several benefits, including immutability, openness, and verifiability.

Table 2 Storage overhead

Blockchain data size (in GB)	*DLS*	*BIEF*	*NOTA*	*BESDL*
5	520	490	505	310
10	518	488	507	312
15	522	492	506	311
20	521	491	508	309
25	520	489	505	308
30	519	490	506	307
35	522	492	507	309
40	518	491	505	310
45	521	489	508	311
50	520	490	507	308

4.7 Security resilience

Replay attacks, denial-of-service attacks, and credential forgery are all types of attacks that could compromise a framework's security. Table 3 illustrates the security resilience. Another bad attack is making fake credentials. Databases and single-point failures are more likely to happen in centralised systems. BESDL is hard to attack because it uses cryptography to reach consensus and is not controlled by any single person or group. Experimental stress testing showed that BESDL was able to successfully stop 97.8% of assault circumstances, which is far better than centralised infrastructures. BESDL helps protect academic integrity by making it hard to fabricate credentials. This is because it saves information in a ledger that cannot be changed.

The BESDL testbed simulated attack scenarios by intentionally introducing malicious transactions and behaviours, such as identity-spoofing attacks using invalid key pairs, repeated (replay) access attempts, unauthorised role/permission requests to trigger privilege-escalation checks in SCBAC, tampering with off-chain content hashes during retrieval, and forged credential records during verification. External attackers attempting impersonation and unauthorised access, malicious insiders using legitimate credentials, and compromised client or storage nodes attempting to alter learning content or

credentials were therefore the threat models considered in the security-resilience evaluation; no large-scale network-level denial-of-service attacks were considered.

Table 3 Security resilience

No. of attack scenarios	*DLS*	*BIEF*	*NOTA*	*BESDL*
5	87	89.2	88	96.7
10	86.9	89.1	88.1	96.9
15	87.1	89.3	88.2	97
20	87	89.4	88	97.1
25	86.9	89.2	88.1	97.2
30	87.1	89.3	88.2	97
35	87	89.4	88	97.1
40	87.1	89.2	88.2	97.2
45	86.9	89.3	88.1	97.1
50	87	89.4	88	97.3

4.8 User satisfaction score

It used platform confidence as one of the factors in our fake surveys to gauge users' happiness. Other things that mattered were how simple it was to use and how open it was. Table 4 gives the user satisfaction score. People are cautious about sharing their personal information with centralised platforms because they lack trust in them and feel insecure about using them. Customers were very happy with BESDL's automated verification and clear blockchain records, giving them an average rating of 4.6 out of 5. This is far better than the rating for centralised approaches. The administrators appreciated the reduced paperwork and the system's increased reliability. The students loved how quickly the certificate verification was completed. The findings reveal that blockchain technology aids remote learners in more ways than just with their technical abilities. It also makes them feel safer and more confident.

Table 4 User satisfaction score

No. of users surveyed	*DLS*	*BIEF*	*NOTA*	*BESDL*
5	78.2	81.3	79.5	91
10	78	81.1	79.6	91.2
15	78.1	81.4	79.4	91.3
20	78.3	81.2	79.7	91.4
25	78	81.3	79.6	91.5
30	78.2	81.1	79.5	91.6
35	78.1	81.4	79.4	91.5
40	78.3	81.2	79.7	91.6
45	78	81.3	79.6	91.7
50	78.2	81.1	79.5	91.8

There were several ways in which the BESDL architecture surpassed straightforward centralised systems. For instance, it was more accurate in validating identities (98.5%), protected data from tampering (storage that was 100% tamper-proof), and validated credentials in under 2.1 seconds. During scalability testing, the framework demonstrated the ability to handle more than 10,000 transactions simultaneously without slowing. Surveys of satisfied customers have shown that blockchain technology is useful for online college programs. The results of these studies also showed that individuals have faith in it and consider it to be beneficial.

The BESDL system is estimated using the consumption of the validator node resources over the mining power as the energy consumption due to the fact that the system is run using a PoA consensus system. Energy is based on observing the average amount of power used (CPU utilisation-based wattage) by validator nodes in processing a transaction and multiplication by the execution time in the formula Energy = Power × Time. Since PoA has no computational-intensive mining, BESDL has much lower energy consumption than proof-of-work systems, and its efficiency can be measured by the number of transactions per watt to prove that it is low-energy consumption.

5 Conclusions

BESDL is the only educational system built on blockchain that offers a complete end-to-end, lifecycle-driven security architecture comprising smart contract-based access control, DIM, ECD, and ICV within a single framework. This close integration enables real-time authentication, fine-grained authorisation, secure dissemination of learning content, and reliable assessment, making BESDL significantly more appropriate for large-scale, multi-institution distance learning systems than existing certificate-based systems. Considering that it can handle a large number of students at the same time without slowing down, this technology is ideal for use in virtual classrooms. A secure, user-friendly platform that promotes transparency, responsibility, and inclusivity is what schools, students, and instructors all want. This is what the BESDL model gives us. As a result, this contributes to the development of future initiatives that enhance the accessibility of technology for academics.

5.1 Limitations and future works

One issue with the current method is that it consumes excessive energy, takes too long to process, and does not integrate well with other learning management systems. The focus of future research will be on lightweight consensus methods, cross-chain interoperability, and AI-driven adaptive security protocols. These are all aimed at enhancing sustainability, efficiency, and universal acceptance.

Acknowledgements

The research presented in this manuscript was partially funded by the Doctoral Startup Grant from Shenzhen City Polytechnic (id: BS22024003). Scientific Research Project of the Department of Education of Jilin Province JJKH20261029SK.

Declarations

Author contributions: Methodology: Jianmin Chen; Investigation: Xue Chang. All authors have read and agreed to the published version of the manuscript.

The dataset is obtained from https://www.kaggle.com/datasets/aljarah/xAPI-Edu-Data/data. Dataset name: Students' Academic Performance Dataset.

The authors did not have any conflict of interest.

References

Alangari, S., Alshahrani, S.M., Khan, N.A., Alghamdi, A.A., Almalki, J. and Al Shehri, W. (2022) 'Developing a blockchain-based digitally secured model for the educational sector in Saudi Arabia toward digital transformation', *PeerJ Computer Science*, Vol. 8, No. 2, p.e1120.

AlShamsi, M., Al-Emran, M., Daim, T., Al-Sharafi, M.A., Bolatan, G.I.S. and Shaalan, K. (2024) 'Uncovering the critical drivers of blockchain sustainability in higher education using a deep learning-based hybrid SEM-ANN approach', *IEEE Transactions on Engineering Management*, Vol. 71, No. 2, pp.8192–8208.

Ariffin, N.H.M., Zulkefli, N.A.M. and Nasruddin, Z.A. (2025) 'Challenges of blockchain technology and its relationships to sustainable education: an analysis using AI-based literature review', *Journal of Advanced Research Design*, Vol. 127, No. 1, pp.173–188.

Ayub Khan, A., Laghari, A.A., Shaikh, A.A., Bourouis, S., Mamlouk, A.M. and Alshazly, H. (2021) 'Educational blockchain: a secure degree attestation and verification traceability architecture for higher education commission', *Applied Sciences*, Vol. 11, No. 22, p.10917.

Balobaid, A.S., Alagrash, Y.H., Fadel, A.H. and Hasoon, J.N. (2023) 'Modeling of blockchain with encryption based secure education record management system', *Egyptian Informatics Journal*, Vol. 24, No. 4, p.100411.

Berrios Moya, J.A., Ayoade, J. and Uddin, M.A. (2025) 'A zero-knowledge proof-enabled blockchain-based academic record verification system', *Sensors*, Vol. 25, No. 11, p.3450.

Bidry, M., Ouaguid, A. and Hanine, M. (2023) 'Enhancing e-learning with blockchain: characteristics, projects, and emerging trends', *Future Internet*, Vol. 15, No. 9, p.293.

Bjelobaba, G., Savić, A., Tošić, T., Stefanović, I. and Kocić, B. (2023) 'Collaborative learning supported by blockchain technology as a model for improving the educational process', *Sustainability*, Vol. 15, No. 6, p.4780.

Bucea-Manea-Țoniș, R., Martins, O.M., Bucea-Manea-Țoniș, R., Gheorghiță, C., Kuleto, V., Ilić, M.P. and Simion, V.E. (2021) 'Blockchain technology enhances sustainable higher education', *Sustainability*, Vol. 13, No. 22, p.12347.

Cardenas-Quispe, M.A. and Pacheco, A. (2025) 'Blockchain ensuring academic integrity with a degree verification prototype', *Scientific Reports*, Vol. 15, No. 1, p.9281.

Chen, C.L., Zeng, K.W., Chen, H.C., Deng, Y.Y., Lee, C.F., Huang, D.C. and Liu, L.C. (2025) 'Secure and efficient graduate employment: a consortium blockchain framework with InterPlanetary file system for privacy-preserving resume management and efficient talent-employer matching', *PLoS One*, Vol. 20, No. 8, p.e0315277.

Cheriguene, A., Kabache, T., Kerrache, C.A., Calafate, C.T. and Cano, J.C. (2022) 'NOTA: a novel online teaching and assessment scheme using blockchain for emergency cases', *Education and Information Technologies*, Vol. 27, No. 1, pp.115–132.

Chinnasamy, P., Subashini, B., Ayyasamy, R.K., Kiran, A., Pandey, B.K., Pandey, D. and Lelisho, M.E. (2025) 'Blockchain based electronic educational document management with role-based access control using machine learning model', *Scientific Reports*, Vol. 15, No. 1, p.18828.

Dash, S.P., Jena, A.K. and Murala, D.K. (2025) 'A hyperledger-based secure framework for academic certificate authentication using blockchain', *International Journal of Safety & Security Engineering*, Vol. 15, No. 6, p.1185.

Delgado-von-Eitzen, C., Anido-Rifón, L. and Fernández-Iglesias, M.J. (2021) 'Blockchain applications in education: a systematic literature review', *Applied Sciences*, Vol. 11, No. 24, p.11811.

Dias, P.V. and Silva, F. (2023) 'Blockchain and digital signature supporting remote assessment systems: a solution approach applied to higher education institutions scope', in *Advances in Tourism, Technology and Systems: Selected Papers from ICOTTS 2022*, Vol. 2, pp.775–784.

Kontzinos, C., Karakolis, E., Kokkinakos, P., Skalidakis, S., Askounis, D. and Psarras, J. (2024) 'Application and evaluation of a blockchain-centric platform for smart badge accreditation in higher education institutions', *Applied Sciences*, Vol. 14, No. 12, p.5191.

Krishnan, S., Rajendran, S. and Zakariah, M. (2025) 'A secured accreditation and equivalency certification using Merkle mountain range and transformer based deep learning model for the education ecosystem', *Scientific Reports*, Vol. 15, No. 1, p.22511.

Leka, E. and Selimi, B. (2021) 'Development and evaluation of blockchain based secure application for verification and validation of academic certificates', *Annals of Emerging Technologies in Computing (AETiC)*, Vol. 5, No. 2, pp.22–36.

Mainetti, L., Paiano, R., Pedone, M., Quarta, M. and Dervishi, E. (2022) 'Digital brick: enhancing the student experience using blockchain, open badges and recommendations', *Education Sciences*, Vol. 12, No. 8, p.567.

Molina, F., Betarte, G. and Luna, C. (2020) 'A blockchain based and GDPR-compliant design of a system for digital education certificates', *CLEI Electronic Journal*, Vol. 26, No. 1, pp.1–17.

Nassani, A.A., Grigorescu, A., Yousaf, Z., Trandafir, R.A., Javed, A. and Haffar, M. (2023) 'Leading role of e-learning and blockchain towards privacy and security management: a study of electronics manufacturing firms', *Electronics*, Vol. 12, No. 7, p.1579.

Paul, P., Aithal, P.S. and Saavedra, M.R. (2022) 'Blockchain in educational development: potentialities and issues – towards sophisticated digital education systems', *International Journal of Applied Science and Engineering (IJASE)*, Vol. 11, No. 2, pp.1–12.

Rahardja, U. (2022) 'Blockchain education: as a challenge in the academic digitalization of higher education', *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, Vol. 4, No. 1, pp.62–69.

Rahardja, U., Aini, Q., Oganda, F.P. and Devana, V.T. (2021) 'Secure framework based on blockchain for e-learning during COVID-19', in *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, pp.1–7.

Rakha, A. and Alzubi, A. (2025) 'A blockchain-based deep learning approach for student course recommendation and secure digital certification', *Scientific Reports*, Vol. 15, No. 1, p.29203.

Razzaq, A., Altamimi, A.B., Khan, W., Alsaffar, M., Alfaisal, F.F., Ahmed, S. and Zhang, T. (2025) 'A metaverse-based virtual reality platform for online certification using Web3', *PLoS One*, Vol. 20, No. 8, p.e0328620.

Saadati, Z., Zeki, C.P. and Vatankhah Barenji, R. (2023) 'On the development of blockchain-based learning management system as a metacognitive tool to support self-regulation learning in online higher education', *Interactive Learning Environments*, Vol. 31, No. 5, pp.3148–3171.

Zhao, M., Liu, W., Saif, A.N.M., Wang, B., Rupa, R.A., Islam, K.A., Rahman, S.M., Hafiz, N., Mostafa, R. and Rahman, M.A. (2023) 'Blockchain in online learning: a systematic review and bibliographic visualization', *Sustainability*, Vol. 15, No. 2, p.1470.

Websites

https://www.kaggle.com/datasets/aljarah/xAPI-Edu-Data/data.