applied sciences

MDPI

Article

Blockchain Hyperledger with Non-Linear Machine Learning: A Novel and Secure Educational Accreditation Registration and Distributed Ledger Preservation Architecture

Zaffar Ahmed Shaikh [1], Abdullah Ayub Khan [1,2,*], Laura Baitenova [3], Gulmira Zambinova [4], Natalia Yegina [5], Natalia Ivolgina [6], Asif Ali Laghari [2,*] and Sergey Evgenievich Barykin [7]

1 Faculty of Computing Science and Information Technology, Benazir Bhutto Shaheed University Lyari, Karachi 75660, Sindh, Pakistan; zashaikh@bbsul.edu.pk
2 Department of Computer Science, Sindh Madressatul Islam University, Karachi 74000, Sindh, Pakistan
3 Almaty University of Power Engineering and Telecommunications (AUPET) Named after G.Daukeev, Almaty 050013, Kazakhstan; baitenova_laura@mail.ru
4 Kazakh University of Economics, Finance and International Trade, Nur-Sultan 010005, Kazakhstan; gulmira_6969@mail.ru
5 Department of Economics, Ogarev Mordovia State University, 430005 Saransk, Russia; avantacom@mail.ru
6 Plekhanov Russian University of Economics, 115903 Moscow, Russia; nataly55550@yandex.ru
7 Graduate School of Service and Trade, Peter the Great St. Petersburg Polytechnic University, 195251 St. Petersburg, Russia; sbe@list.ru
* Correspondence: abdullah.ayub@bbsul.edu.pk (A.A.K.); asif.laghari@smiu.edu.pk (A.A.L.)

Abstract: This paper proposes a novel and secure blockchain hyperledger sawtooth-enabled consortium analytical model for smart educational accreditation credential evaluation. Indeed, candidate academic credentials are generated, verified, and validated by the universities and transmitted to the Higher Education Department (HED). The objective is to enable the procedure of credential verification and analyze tamper-proof forged records before validation. For this reason, we designed and created an accreditation analytical model to investigate individual collected credentials from universities and examine candidates' records of credibility using machine learning techniques and maintain all these aspects of analysis and addresses in the distributed storage with a secure hash-encryption (SHA-256) blockchain consortium network, which runs on a peer-to-peer (P2P) structure. In this proposed analytical model, we deployed a blockchain distributed mechanism to investigate the examiner and analyst processes of accreditation credential protection and storage criteria, which are referred to as chaincodes or smart contracts. These chaincodes automate the distributed credential schedule, generation, verification, validation, and monitoring of the overall model nodes' transactions. The chaincodes include candidate registration with the associated university (candidateReg()), certificate-related accreditation credentials update (CIssuanceTrans()), and every node's transactions preservation in the immutable storage (ULedgerAV()) for further investigations. This model simulates the educational benchmark dataset. The result shows the merit of our model. Through extensive simulations, the blockchain-enabled analytical model provides robust performance in terms of credential management and accreditation credibility problems.

Keywords: blockchain; hyperledger sawtooth; machine learning; artificial neural network; consortium network; certificate credentials accreditation

check for updates

Citation: Shaikh, Z.A.; Khan, A.A.; Baitenova, L.; Zambinova, G.; Yegina, N.; Ivolgina, N.; Laghari, A.A.; Barykin, S.E. Blockchain Hyperledger with Non-Linear Machine Learning: A Novel and Secure Educational Accreditation Registration and Distributed Ledger Preservation Architecture. *Appl. Sci.* **2022**, *12*, 2534. https://doi.org/10.3390/app12052534

Academic Editor: Pericle Perazzo

Received: 28 January 2022
Accepted: 26 February 2022
Published: 28 February 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

Certificate issuance and pre-verification by Higher Education Department (HED) recognized universities play a vital role in developing a platform and opportunities to pre-verify issued certificates through the e-portal mechanism. This scenario uplifts the educational turnaround, which directly impacts the economy and a skilled workforce with social mobility to promote and achieve the well-being of educationalists around the

world [1]. Issuance of certificate credential accreditation by the HED and universities significantly impacts academic record attestation and verification, which is very essential for further higher studies and international educational processing applications [2]. The primary stakeholders involved in the process are candidates (students), universities, private recruitment organizations, government job providers and agencies, and semi-governmental departments. The university issuance certificate is the only verified document that is considered as a professional credential completion proof of higher education requirements [3,4].

The Higher Education Department faces a wide range of fraud identification problems and must detect prevailing limitations that damage the authenticity of the accreditation process and have detrimental effects, as shown in Figure 1 [5]. This kind of issue is widespread mostly in countries that are in the developing phases. The existing system is running for the certificate issuance process and accreditation, which is one of the main concerns towards pervasive and systemic concerns such as tampering and forgeries [6,7]. It leads to the emerging problems of certificate duplication fraud, including document forgery, misrepresentation of credentials, a slight alteration in the cumulative percentage, and so on. The HED-recognized universities that provide academic completion certificates need to pre-verify and attest first, then record all the ledgers in immutable storage that will never compromise the services of accreditation of the HED [8].

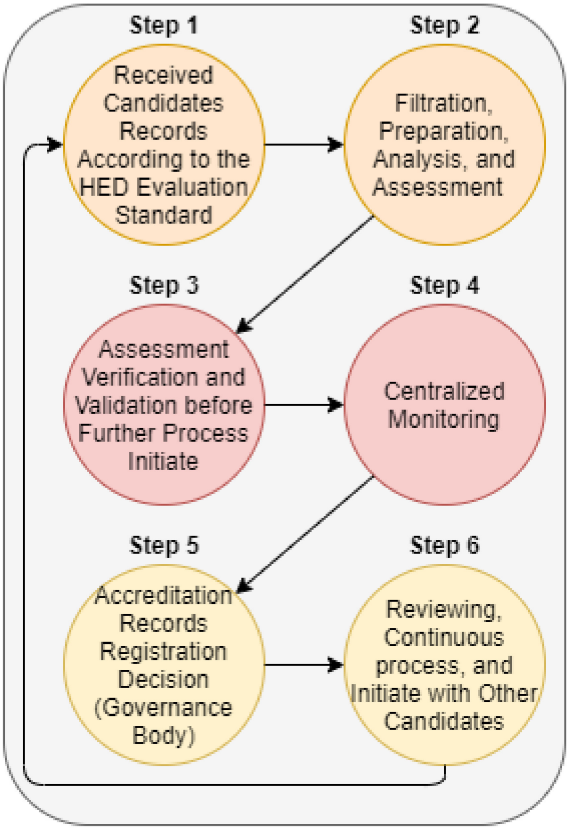

Figure 1. Current process of candidate credential accreditation.

The tampered credential issuance certificate cases are registered and reported in the higher education degree verification and traceability department [9]. As the HED survey reported, over one-fourth of submitted applications admit that there is no pre-verified work done by the university before submitting them to HED for attestation and verification. Every year, more than 150,000 forged certificates are issued [10,11]. These misrepresented applications outperform their peers in the market for seeking jobs in highly competitive environments. Fake credential registration enables candidates to get a free position by misusing forged credentials or university certificates.

The system in developing countries uses one-to-one channels for the issuance of certificates, accreditation registration, credential verification, and traceability mechanisms between the HED and universities [12]. Still, the process of issuing certificates and accreditation candidate credentials is based on a semiautomatic structure, which is slower, hard to access, time-consuming, less efficient, insecure, and costly. Hence, that is the reason for credential forgery and the process of accreditation to tamper with certificates, illegitimately issued through the current system.

During the current pandemic situation, the method of teaching and learning moved towards the pervasive environment, and people widely adopted the method of online studies and examinations. It also transforms the existing academic systems, including university pre-verification, a two-way process of certificate credential verification between universities and HED for accreditation (still semiautomatic), and certificate verification and attestation in developing countries. In this overall scenario, the semiautomatic system has no proper technique to secure centralized records, no availability of immutable storage, system provenance, or fulfilling the requirements of candidates' educational needs. As a result, a decentralized architecture is essential to provide ledger integrity, transparency, fully automated and online process mechanisms, communication node connectivity (P2P), and a completely traceable and secure infrastructure. However, the involvement of root stakeholders in the process of certificate issuance and accreditation includes (i) the Federal Education Ministry (FEM), (ii) the HED, (iii) registered universities, (iv) the accreditation department, and (v) candidates.

Candidate credential verification and a quick accreditation process are two examples of how blockchain distributed ledger technology can help with online learning, development, and management, including easy and secure verification [13]. The blockchain also allows for tamper-proof examination of registered accreditation versions of records. This process guarantees the privacy and protection of the recorded credentials of the marked certificate. Further, the system does not charge the extra cost of availability, security, and maintenance level of provenance pertinent to storing the accreditation details with addresses [14]. With the collaboration of machine learning, especially artificial neural networks with blockchain technology, the mechanism of credential classification and verification will be more robust.

For example, hyperledger sawtooth has provided a modular enterprise infrastructure that acts on a consortium network architecture for intelligent public–private communication and connectivity [15]. Through the edge devices, the HED engineer handles a diverse range of accreditation scheduling, monitoring, and maintenance of delivery and preservation protocols and automates a configurable customized structure that enables optimization, versatility, and innovation as well [15]. For ledger protection, SHA-256 hash-based encryption mechanisms support chaincodes that are designed and implemented using the distributed general-purpose language (Go/Java). A consortium network design includes the trustworthy execution of educational node transactions and a pluggable consensus protocol with efficient pre-defined fault tolerance.

However, the main concern of this paper is to address the limitations and issues of accreditation credential evaluation and verification using blockchain–machine learning collaborative technology. This paper proposes a novel collaborative model of machine learning and blockchain hyperledger sawtooth-enabled secure accreditation analysis procedure for investigating if a certificate credential is tamper-proof and verifying process credibility for the Higher Education Department. In this process, a ministry of education is responsible for managing the process of higher education accreditation for efficient certificate credentials verification and issuing by affiliated HED-recognized universities. The proposed modular solution used hyperledger sawtooth (a consortium structure) to design and deploy a hybrid hyperledger network, which is based on public (for candidate application scenario) and private (to maintain ledger privacy between stakeholders) networks. Several participating members are analyzed and registered to the consortium network, to achieve integrity, confidentiality, privacy, secrecy, and provenance. Moreover, this solution also covers the ledger protection scenario, such as hash-encrypted (SHA-256) based distributed ledger

storage in the immutable preservation (IPFS) performed on the network in a chronological form. The main contribution of the paper is as follows:

- In this paper, a secure process of accreditation/credential verification and investigation of the certificate credibility is presented. An analysis of the forge proof and tampering aspects of the issuance certificate is presented.
- A secure analytical model is proposed for accreditation credential analysis, such as matching the content of the original issuance certificate with the verifiable one by using machine learning techniques, especially artificial neural networks (ANNs).
- Blockchain ledger technology is used to design and deploy smart contracts/chaincodes. It automates events of educational nodes' transactions (credentials verification) execution with defined consensus policies in a consortium or hybrid hyperledger sawtooth network.
- Because of an efficient modular structure and open-source in nature, we select hyperledger sawtooth for educational accreditation credential process security and simulate the working operations through the use-case diagram. Finally, we examine and evaluate emerging challenges and issues in the current distributed architecture and also discuss the open research areas of educational-blockchain technology with future directions.

The rest of the paper is organized as follows. Section 1 discusses the current accreditation credential evaluation process for higher education degree issuance and attestation involving centralized storage mechanism and blockchain hyperledger technology. In Section 2, we studied several proposed systems for the secure procedure of accreditation analysis and degree verification attestation-related articles and requirements. Section 3 discusses the higher education accreditation credential analysis procedure and the role of blockchain distributed applications with hyperledger sawtooth-enabled consortium networks for ledger privacy and protection. In Section 4, we proposed a model for the HED to investigate a secure analytical process of degree credential verification. Further, smart contracts are designed and deployed to automate verification and analysis processes. Finally, we conclude this paper in Section 5.

2. Related Literature

Accredited record preservation is the primary concern of this research, followed by privacy protection of ledgers, pre-verification, and forged proof of credential analysis. Data classification is a component of machine learning algorithms that detects every aspect, recognizes patterns, retrieves knowledge, and classifies published credentials issued by universities via certificates [16]. So, the blockchain has been hosted on decentralized distributed networks with P2P connectivity, and distributed records are safe because of cryptographic hash-encryption. By this act, all the accredited records are stored in an immutable preservation structure that is almost impossible to update. Not only this, even the stored records cannot be damaged in any way on the distributed network because all the current preserved records are handled through a group of educational nodes, not owned by one entity.

Every transaction is initiated by the node that is bound to other connected participant nodes so that it allows verification and digital signature among stakeholders before publishing record updates [17]. The individual node contains distinct transactions and is inspected by almost half the nodes on the hyperledger sawtooth consortium network for validation. After the verification and validation, the nodes take part in the chain that has previously been achieved by the chronological architecture.

The category of blockchain is distributed into three parts: (i) allowed blockchain, (ii) not permitted blockchain, and (iii) hybrid blockchain. For educational credential evaluation analysis, we have examined and evaluated various related articles, and their implementation limitations are as follows (as shown in Table 1):

Table 1. Related literature.

Research Method	Research Description	Limitation/Issues	Similarity/Differences
Blockchain-based education project [18]	The authors of this paper discussed the blockchain-enabled educational project, which mainly focuses on the systematic protocols for secure execution of educational node transactions in the distributed network, and improves the communication implementation of technology in the field of education by using Ethereum.	• Token system • Cooperative learning • E-certificate preservation • Data redundancy • Complex authentication	• Public network • Permissionless network architecture • Pre-define consensus policy • Blockchain customized protocol used
A blockchain-based intact education system for thepost-COVID-19 era [19]	The authors of this paper proposed a method that provides learning content and results that can be preserved in blockchain distributed storage. Design and implement the security mechanism for the storage of certificate credentials that records provenance, integrity, and transparency in a chain-like structure.	• Learning data protection • Weak prevention • Behavior analysis • No hyperledger used • Ethereum architecture	• Public permissionless network • Customized blockchain consensus policy design • Used simple blockchain network protocol
A blockchain-based framework for securing students' educational data [20]	In this paper, the authors proposed a method to protect students' sensitive records using blockchain hash-encryption. This technology ensures the privacy preservation of digital ledgers in immutable storage.	• SHA-256 • Complex record-keeping strategy • Customized consensus • Complex registration of participating stakeholders • Data scope and scalability	• Ethereum network • Cross-chaining issue • Two-way authentication • Complex architecture while exchange records
Blockchain in Indonesia university: A design view-board of digital technology education [21]	The authors of this paper presented the Edu-blocs project to simplify the process of educational record-keeping and exchange active results using a public peer-to-peer network structure to ensure the privacy and protection of candidate credentials and data security.	• Regionally specific, only for Indonesian universities • Hash-encryption used • Complex method for ledger preservation • Record scalability issue • Digital signature	• One-to-one process • Economic costs • Provide a platform for learning certification and information recovery • Pre-define node/block size

Table 1. *Cont.*

Research Method	Research Description	Limitation/Issues	Similarity/Differences
Blockchain-enabled digital rights management for multimedia resources of online education [22]	This paper discussed the blockchain-enabled digital rights management architecture for sharing and managing multimedia resources for pervasive learning using a hybrid network structure.	• Infringement of digital copyrights • Multi-chain pattern • Life-long learning support • SHA-256 for ledger security • Streamline automation	• Combination of public and private blockchain • High security • Low latency • Transaction of multimedia digital works
Blockchain technology for higher education system: A mirror review [23]	The survey paper discussed the role of blockchain distributed technology and highlighted a few of the many models designed to support educational organizations.	• Connected pool of high education bodies • Transaction transmission speed, delivery, and scalability limitations • Data sharing security • Scope of data preservation and privacy	• Secure architecture • Complex devilry strategy • Data recurring • Weak data protection • Permissioned ledger

3. Blockchain Applications and Higher Education Accreditation Analysis

The blockchain distributed ledger technology makes bitcoin and other cryptocurrencies work as financial assets. The secure nature of blockchain and safe integral features provide a new way in a pervasive learning environment [24]. There are several benefits to using blockchain in the education industry. One of these technological advantages is to transform the record-keeping of candidate certificates credentials and personal details and preserve them in the distributed storage. In this whole scenario, there is no need for intermediary verification, no additional paper-based validations or authority certificates and signatures are needed. That is the reason it helps secure the accreditation process from data collection to credentials preservation, shown in Figure 2.

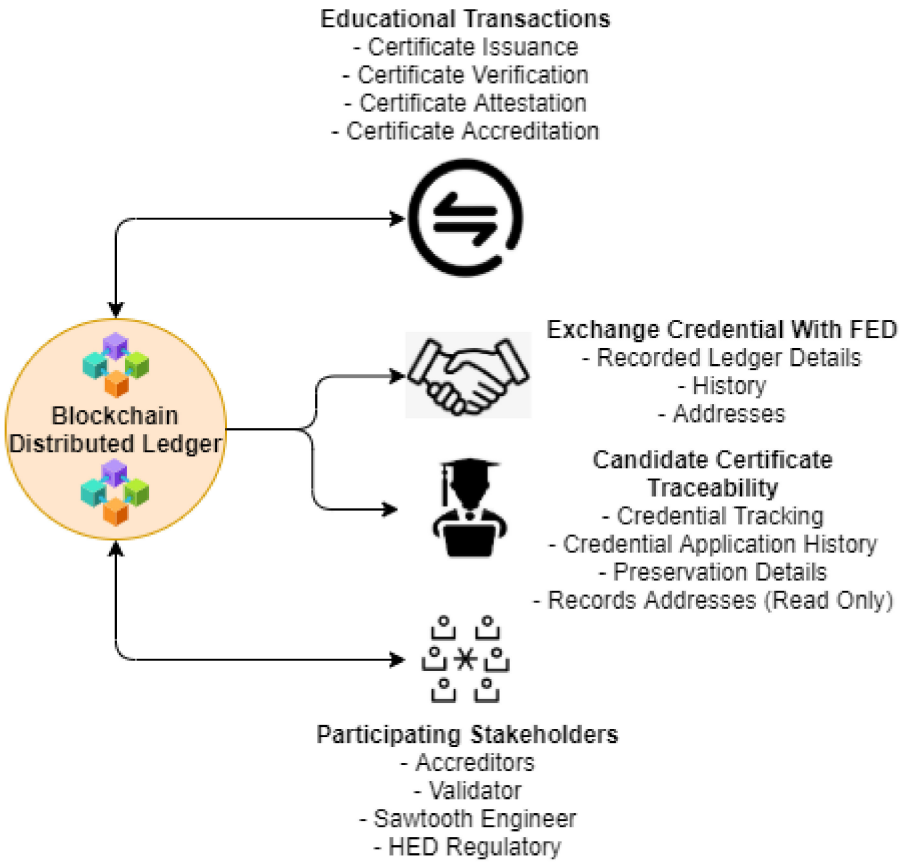

Figure 2. Blockchain educational distributed application.

At the current stage, the education industry is one of the systems most affected by fraud, forged, and hacked systems. The manipulation and alteration of the information by a malicious attacker from the education system is another challenging aspect. To overcome this situation, blockchain distributed technology is introduced that ensures a consistent and integrated ledger for all academic qualifications [25]. The records of university candidates are preserved on the online ledger, which is not changed directly. A digital signature and consensus permission are needed to change the state of the permissioned ledger. The blockchain private network is used to protect educational information secrecy that cannot be manipulated through transmission. Moreover, universities in developing countries need to develop a ledger with a custom blockchain protocol to prevent records and detailed addresses from being altered. This platform is vital for issuing candidate certificates; not only that, but it also allows secure transactions for the process of accreditation and preservation.

3.1. Role of Hyperledger Sawtooth

Hyperledger sawtooth is a modular enterprise blockchain infrastructure for developing, deploying, and executing distributed ledgers [15,26]. In the education environment, the design philosophy targets keeping candidate certificate-related ledgers distributed and creating programable smart contracts through safety, transparency, immutability, and availability, each for educational use [27]. It provides a novel consensus where certificate-related credentials analysis reports can be submitted for verification, validation, and approval, and stores approved ledger details in distributed storage using Proof of Elapsed Time (PoET). This algorithm targets huge distributed validator populations with a small number of resources required [28]. No additional source of hardware, cost, or human ability is required to execute hyperledger sawtooth. It includes a distributed application (DApp) for candidate certificate's credentials verification and attestation, which is based on a web app (frontend), a transaction processor (for executing business logic and chaincode), and a customized REST API for secure communication.

3.2. Features of Consortium Blockchain

In this context, a consortium blockchain network is designed instead of only a single HED (all departments in one domain); multiple departments of higher education govern the infrastructure for the process of certificate issuance, credentials verification, validation, and accreditation of educational qualifications in the ledger [29–31]. This network behaves like a hybrid architecture, neither public nor permissioned. There is no single authority over the network; all the connected stakeholders can come together on the same platform and work on the same issues. Stakeholders contribute to the network and get proof-of-work and feature ability. This collaborative infrastructure provides more exposure and innovation in the fields of certificate issuance, validation, accreditation, and preservation. The applicational features of consortium blockchain are different as compared to public or private blockchain networks and are as follows:

1. It provides a more efficient and fast response to the delivery of certificate credentials for registration, issuance, verification, validation, and accreditation.
2. It consumes low transactional costs and energy as compared to public architecture.
3. It resolves scalability-related issues, regulatory problems, and accessibility challenges.
4. Handling of data and immutable preservation are the main advantages of this network.

4. Proposed Model

In the proposed analytical model, we design and create a classification mechanism that analyzes the candidate certificate and retrieves the exact/original credentials during the process of pre-verification. This process helps universities pre-verify candidate certificates before submitting them to the Higher Education Department for further verification, validation, and attestation.

For this purpose, we implement an accreditation analytical model, which is considered a breakthrough as it solves the originality problem through an artificial neural network. We identify various classification loopholes, detection-related issues, and unstable recognition in the dynamic time for a large number of candidate certificate evaluations. In this paper, we construct a good certificate credential identification, pattern extraction, detection, recognition, and classification task with the original (system ledger) and issue a certificate for pre-verification purposes. We use an artificial neural network with self-correlation and schedule to minimize structural risk with high-dimensional space classification.

The notations of artificial neural networks with respect to the process of classification are discussed as follows: (i) weight (w), (ii) bias (b), (iii) input neurons (a), (iv) counter (i), (v) number of total inputs in a single layer (n), (vi) threshold (t), (vii) output neurons (z), and activation function (σ).

In the process of certificate pre-verification, the weight is the connection between the connected neurons in the artificial neural network structure. An individual neuron holds a

certain number of credentials or values. Each neuron assigns a label, then the input values are a_1, a_2, a_3, and a_n, with the corresponding weight w_1, w_2, w_3, and w_n, respectively. The sum of inputs and weights, demonstrating the level of excitation, is as follows:

$$\text{Level of excitation} = \sum_{i-1}^{n} wi * ai \tag{1}$$

If the threshold range of the threshold increases in this proposed nonlinear analytical model, where the output neuron (z) = total (level of excitation), the expression is expressed as follows:

$$\sigma = \begin{cases} 1 \; if \; total \; of \; input \; and \; weight \geq t \\ 0 \; if \; total \; of \; input \; and \; weight < t \end{cases} \tag{2}$$

The activation function is performed nonlinearly, so when the threshold value = '0', the threshold falls towards the negative (−) side. There is a need to schedule parameters, such as bias and weight, w0 = −t. For example, if a constant unit is added to maintain nonlinear high-dimensional classification, for example, if a value of a = 1 with formal inputs, then the output (z) equation shows as:

$$z = \begin{cases} 1 \; if \; total \; of \; input \; and \; weight \geq t \\ 0 \; if \; total \; of \; input \; and \; weight < t \end{cases} \tag{3}$$

The proposed conceptual framework is categorized into two distinct folds: credential pre-verification before accreditation and attestation through the process of the HED, and maintaining secure events of node transactions and records preserved in distributed immutable storage, as shown in Figure 3.

- The first step is the pre-verification phase, which is performed by universities when a candidate gets to validate and attest his/her certificate from the HED. This initial step reduces the additional time and cost of communication, for example, the process of one-to-one communication between HED and universities for credential verification via courier or electronic mail, etc.
- In the second step, these verifiable records are accredited in the HED ledger without requiring any manual process of editing to submissions. The list of sequences is elaborated as follows:
  - i. Pre-verification record collection
  - ii. Align records for processing
  - iii. Check the ledger before adding new transactions
  - iv. Add records
  - v. Exchange details of the updated ledger among connected stakeholders
- In the final step, blockchain hyperledger sawtooth is used to protect individual node transactions with a hash-based (SHA-256) encryption mechanism. Secure delivery of educational records on the consortium network along the customized blockchain consensus protocols is proposed. So, it preserves the overall records in the distributed storage system, which is the InterPlanetary file system (third-party preservation requires a small piece of cost), shown in Figure 3.

As shown in the smart contract (Appendix A), it initiates with the candidate's registration and schedules the distributed accreditation process after the pre-verification of individual certificates' credentials by universities, mentioned in the contract (candidateReg()). The system engineer (HED expert) is the person responsible for initiating and creating the event of registration transactions and recording addresses. As a result, the new accreditation ledger transactions schedule, which is managed by the HED accreditation engineer, is mentioned in the contract (CIssuanceTrans()). This function is automated to add and update the ledger with newly collected records of candidates from different universities. The automated validation of individual records is performed in the updated ledger (ULedgerAV()), as shown in Figure 4. The smart contract also records additional details of the accreditation process, such as get records (gRecords()), update

ledger (uLedger()), secure preservation (sPreserve()), manage chain (mChain()), blockchain hyperledger sawtooth timestamp [execute], and dynamic activities.

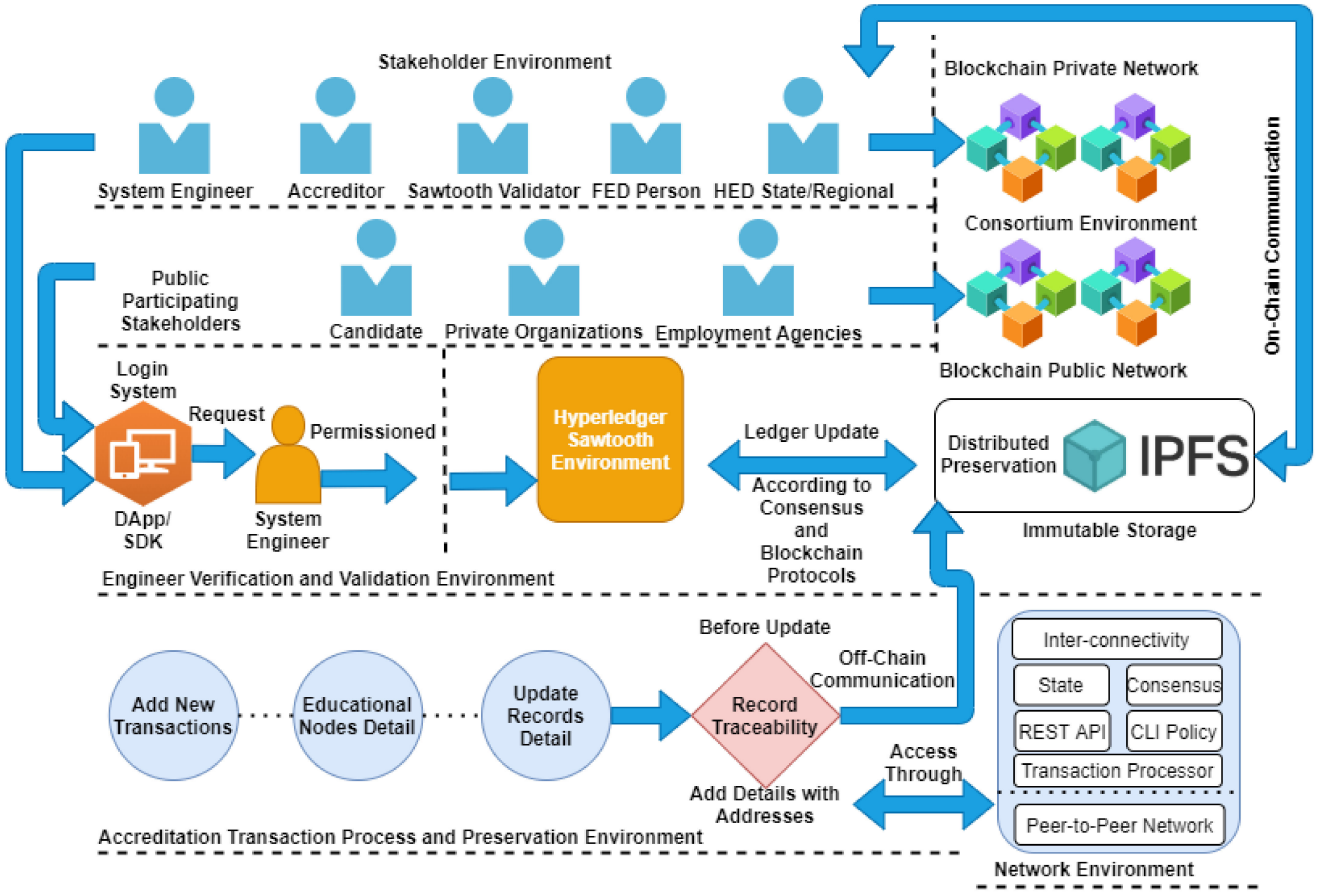

Figure 3. Blockchain hyperledger sawtooth-enabled certificate credentials verification and accreditation architecture for HED.

4.1. Simulation Results and Discussion

In this context, the simulation results are compared with the state-of-the-art methods to check the validity and robustness of the proposed analytical accreditation model in terms of certificate credential identification, pattern extraction, detection, recognition, and classification for verification of certificate credential and management. We simulate our proposed model on the sample dataset (collected from distinct open-source platforms) of certificates. The artificial neural network is applied to the collected dataset for the purpose of training the network, this whole scenario is designed to identify tamper or forged credentials and pre-verify certificate credentials before attestation, as already discussed in the above sections.

In the artificial neural network used to analyze the high-dimensional classification, the process of analysis is as follows: (i) distribute individual aspects of the certificate, (ii) identify rate of originality/tamper or forged proof, (iii) extract pattern, (iv) detection, (v) recognition, and (vi) classification, as shown in Figure 5.

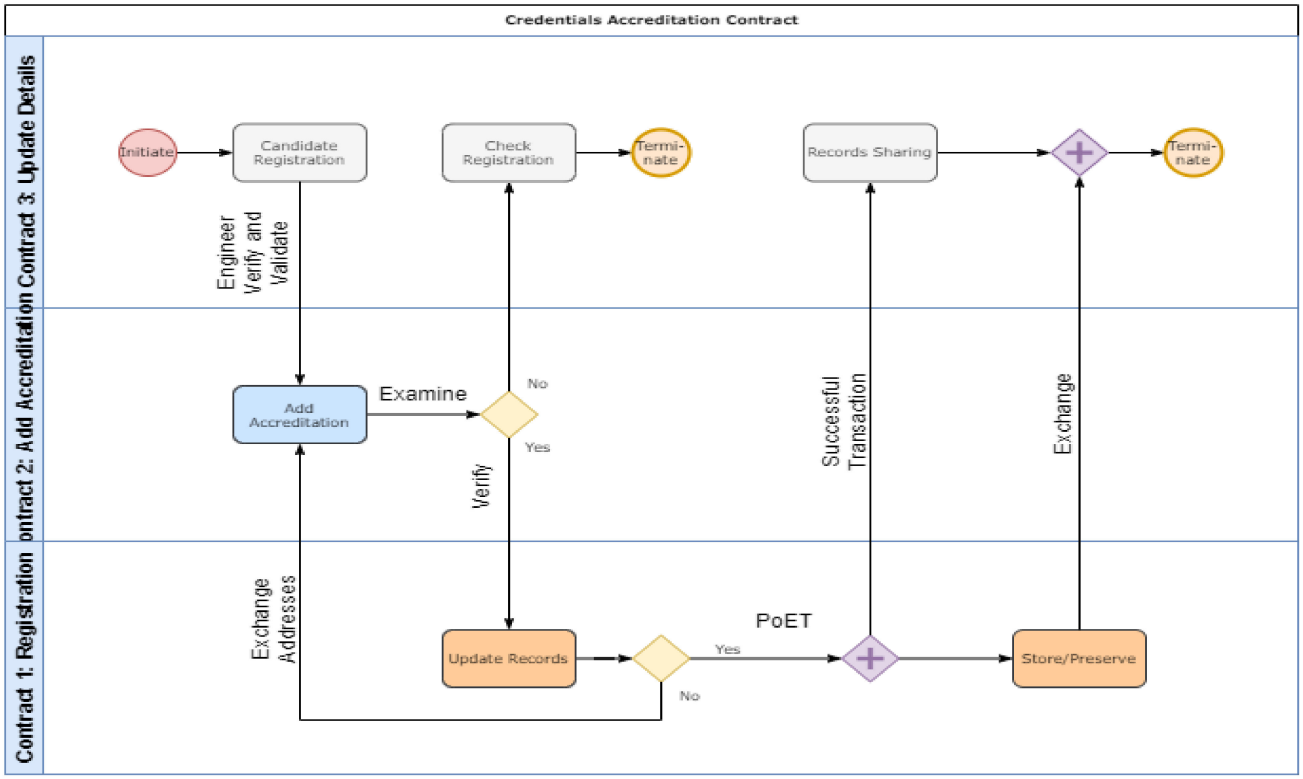

Figure 4. Events of education-accreditation node transactions.

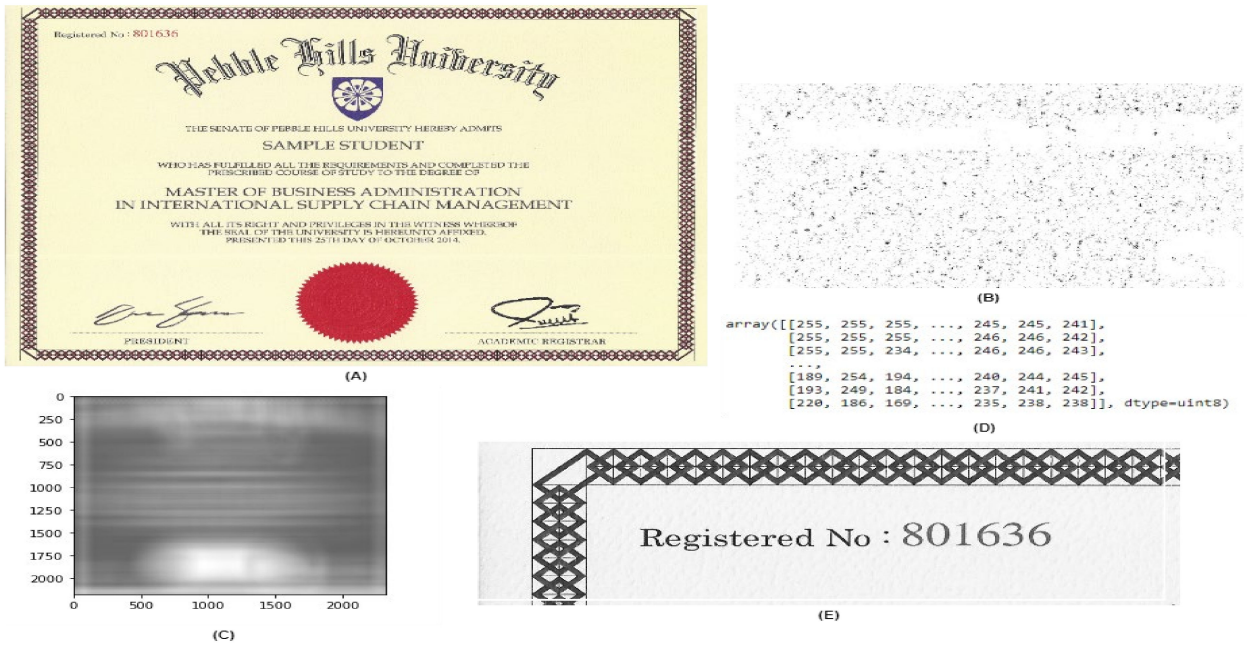

Figure 5. Simulation results of the proposed accreditation model. (**A**) Input image, (**B**) encode to identify tampering, (**C**) convert into grayscale to fine trace, (**D**) image matrix, and (**E**) output to check individual aspects.

According to the process of pre-verification, we evaluate the detection and classification of originality and tampering of certificate credentials through the number of recognition items and rate of error generation. By this act, we get the frequency of credential originality classification, shown in Figure 6. The evaluation matric of the proposed process is

defined as follows: (i) evaluation of pattern for classification, (ii) validation, and (iii) rate of detection, shown in Figure 7.

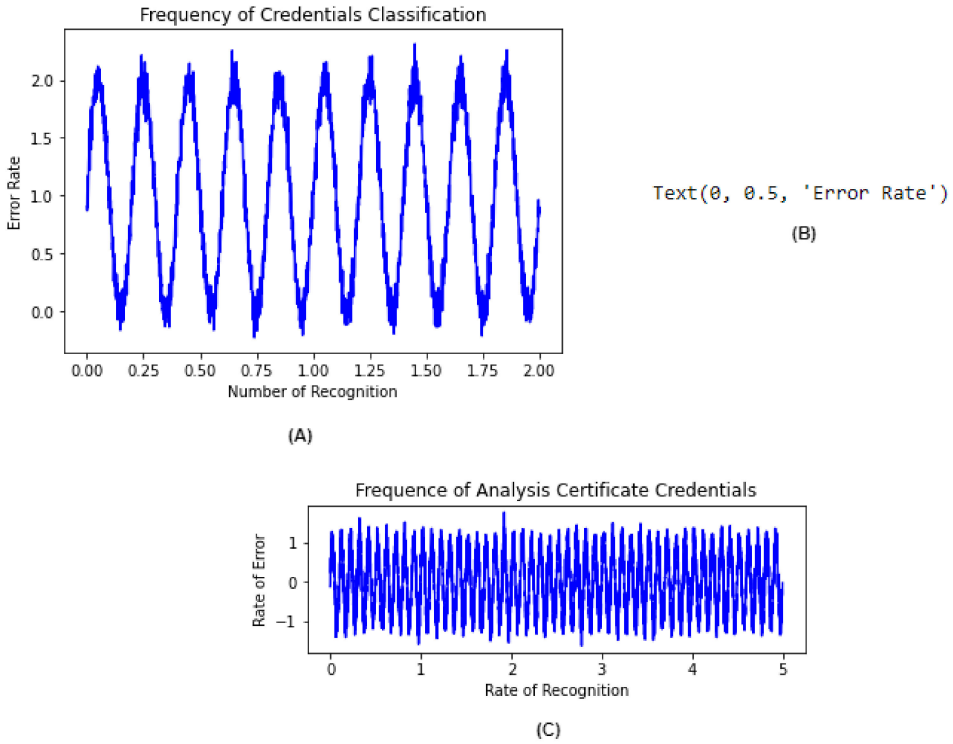

Figure 6. Certificate pre-verification/classification. (**A**) Calculate frequency of credential classification, (**B**) error rate, and (**C**) calculate frequency of analysis.

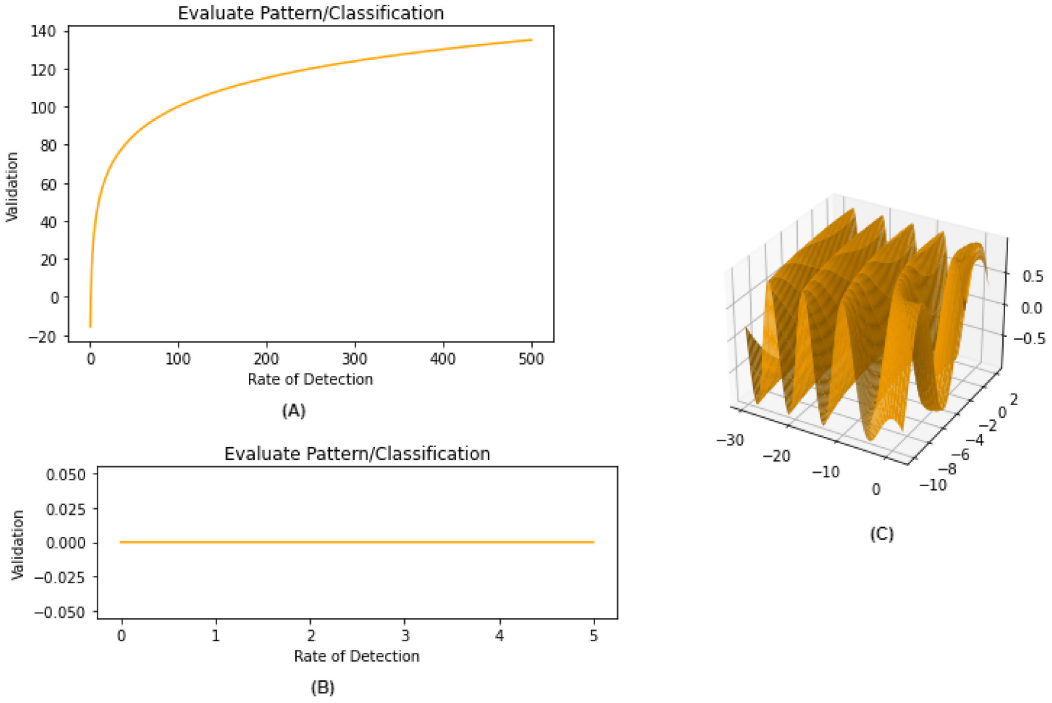

Figure 7. Rate of certificate credentials detection. (**A**) Evaluate pattern for classification, (**B**) rate of validation, and (**C**) pattern classification evaluation through a 3D model.

Another simulation is applied on the same dataset to find a trace of a different portion of certificate credentials for the purpose of analyzing forged proof accurately. Figure 8

presents the result of the proposed accreditation model for pre-verification/classification of distinct aspects, where we provide an input image of the certificate to trace credential credibility. Initially, the model encodes images to identify tampering/originality, then it moves towards the conversion of grayscale to fine traces. After the completion of the tracing process, the image matrixes calculate bit-by-bit to analyze alteration through the bits of the image. Finally, we get the output of the image with a detailed description, as shown in Figure 8.

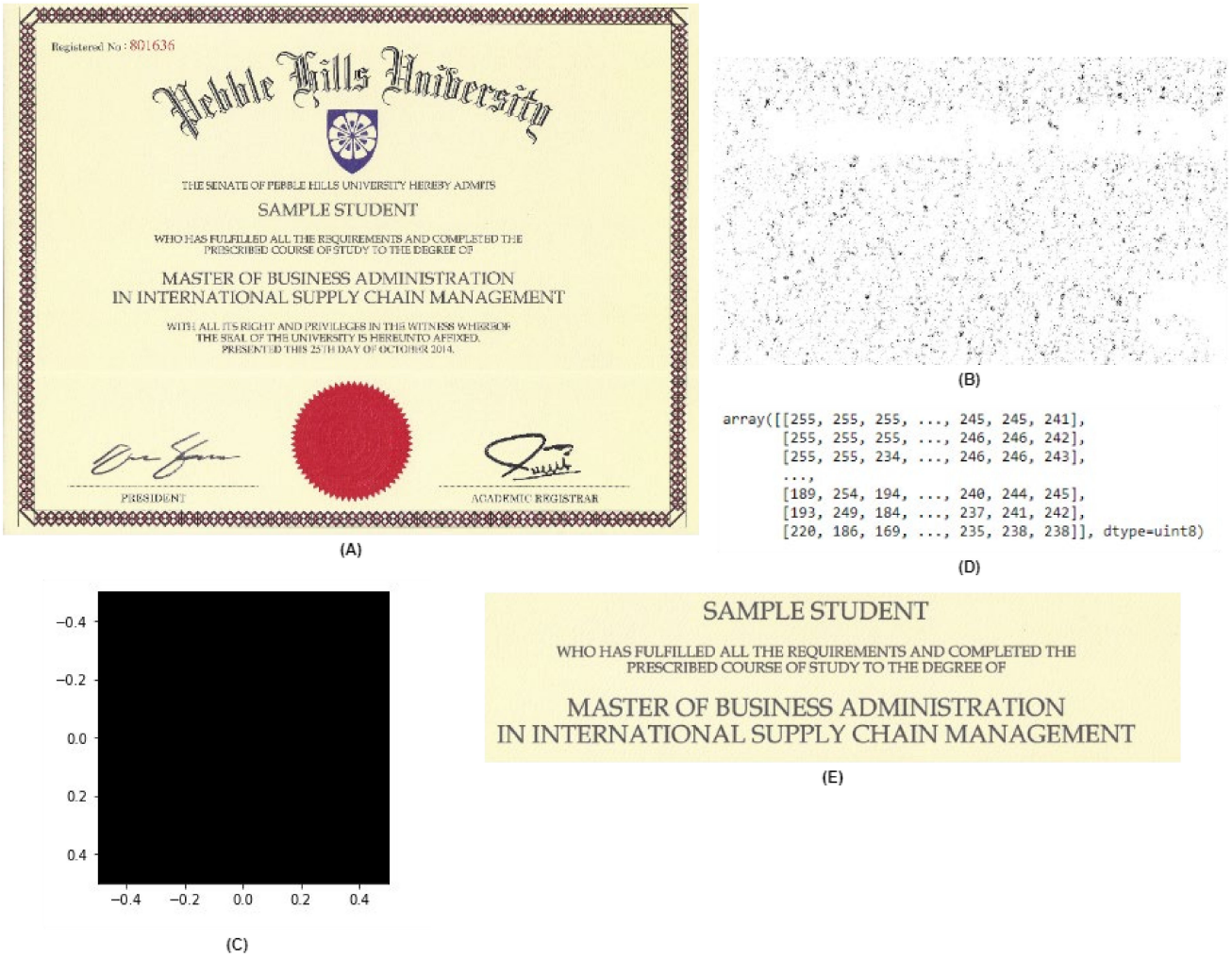

Figure 8. Another simulation result of the proposed accreditation model. (**A**) Input image, (**B**) encode to identify tampering, (**C**) convert into grayscale to fine trace, (**D**) image matrix, and (**E**) output to check individual aspects.

We test our proposed blockchain hyperledger sawtooth-enabled accreditation model with other public network blockchains (Ethereum) and customized blockchain to check the security and privacy of the education ledger, as shown in Table 2. Our proposed model and preservation mechanism provides better results and performs great with an accuracy of 91.7% and is efficient in accordance with the dynamic collection of records (variable nature). The criteria of analysis privacy and protection are as follows: (i) transparency, (ii) integrity, (iii) provenance, (iv) consensus protocols and policies, (v) immutability, (vi) network communication (on-chain and off-chain), (vii) hash-based protection, and (viii) preservation mechanism, as shown in Figure 9.

Table 2. Comparison table.

Research Methods	Research Description	System Matrix	Comparison with Our Proposed Model
Blockchain-based online education content ranking [32]	This paper presented a blockchain-enabled online content ranking system, which is distributed in nature and provides a trustworthy environment to preserve the educational ledger and ensure the integrity of the rating independently.	The proposed system matrix is categorized into distinct aspects as follows: - Hyperledger: No hyperledger used - Network: Public network - Consensus: Pre-defined/proof Sketch - Chain: Simple blockchain chain structure - Protection: Hash-encryption - Accuracy: Not applicable - System Efficiency: Not applicable	On the other side, the proposed model infrastructure is designed and created for secure pre-verification of candidate certificate credentials and to submit the analysis report to the accreditation before actual registration. For this purpose, we have used an artificial neural network for high-dimensional classification that helps in the finding of tamper detection/forged proof. After that, we have collaborated with blockchain hyperledger sawtooth to design secure connectivity and the communication channel between stakeholders and maintain protected distributed immutable ledger storage for further use. - Hyperledger: Hyperledger Sawtooth - Network: Consortium - Consensus: PoET - Chain: Chronological - Protection: SHA-256 - Model Accuracy: 91.7% - System Efficiency: Variable dynamically - Cost of Storage: 13.31% decreases - Transactional Deliverance: 11.84% increases
Use of blockchain technology in implementing information system security on education [33]	This paper presented a blockchain-based framework for information security in the education department. It designs and creates distributed applications that evaluate the educational ledger security and prevent information systems using edge-based fingerprints enabled identity verification for smart credentials registration and privacy.	- Hyperledger: No hyperledger is used - Network: Public - Consensus: SWOT - Chain: Pre-defined blockchain-enabled chain structure - Protection: Cryptographic chain encryption - Accuracy: Not applicable - System Efficiency: Not applicable	
Blockchain technology enhances sustainable higher education [34]	This study enhanced the existing state of educational records preservation, including document analysis, literature review, content analysis, the case study method, and the survey method. For this reason, the authors used blockchain-enabled architecture to secure all the educational transactions in the defined network.	- Hyperledger: No hyperledger used - Network: Private network - Consensus: Blockchain pre-defined consensus - Chain: Simple blockchain connected chain-like structure - Protection: Hash-encryption - Accuracy: Not applicable - System Efficiency: Not applicable	
A blockchain-enabled e-learning platform [35]	The authors of this paper proposed a method of proof-of-concept in the education environment. A blockchain-enabled e-learning platform was designed and implemented to increase transparency in the assessment of student learning.	- Hyperledger: No hyperledger used - Network: Public - Consensus: Pre-defined - Chain: Simple blockchain pre-defined structure - Protection: Hash-encryption - Accuracy: Not applicable - System Efficiency: Not applicable	

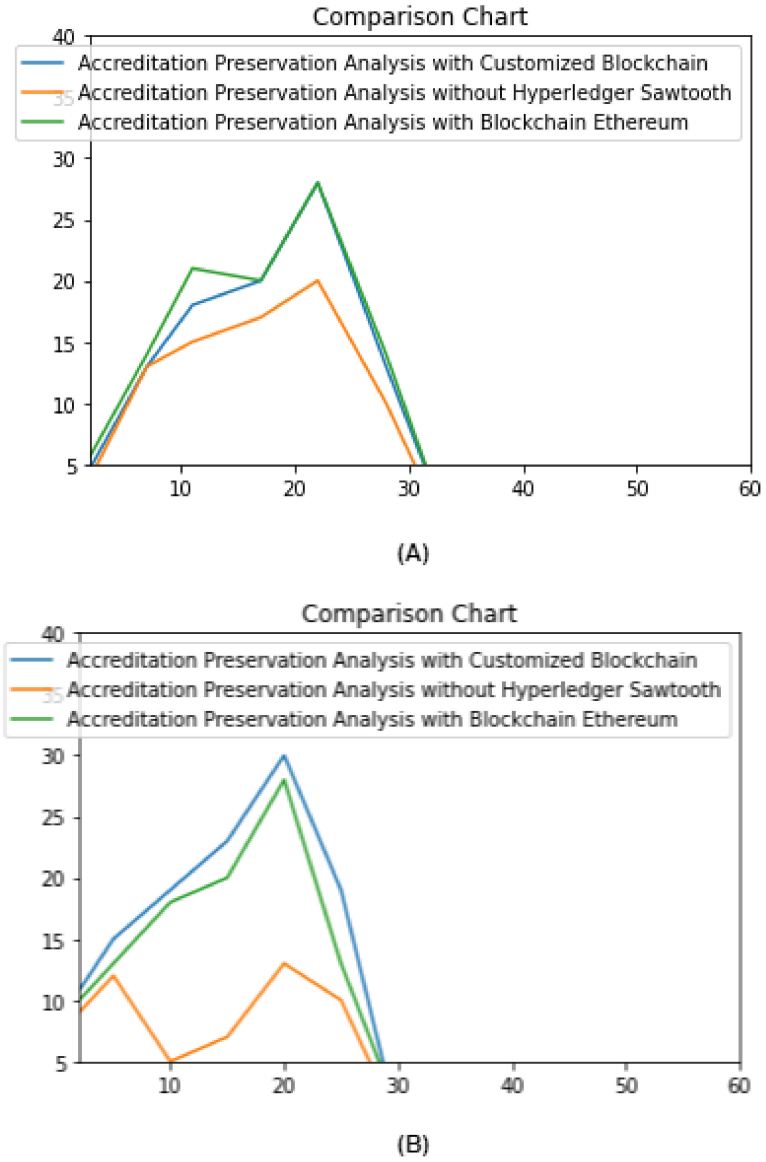

Figure 9. Blockchain comparison chart **(A)** Comparison Between Blockchain Permissioned Architecture with Public Permissionless Structure, **(B)** Analytical Relationship.

4.2. Open Challenges, Limitations, and Issues

In this context, we discuss the proposed blockchain hyperledger sawtooth-enabled accreditation credential evaluation and management with security for HED and its distributed application-related challenges and issues. However, we also highlight and elaborate on a few credibility-related, critical emerging aspects in the higher education environment and the existing technological difference between them as follows:

4.2.1. Blockchain Connectivity and Communication Issues

The HED needs to adopt a blockchain hyperledger-based distributed preservation modular solution for accreditation record management and protection. Because of chain scalability, still, there are no single platforms and no efficient protocols are designed in the centralized system that achieves proper exclusivity. An interoperable solution is surely required at the stage of pervasive education/learning; the efficient distributed blockchain-enabled ecosystems require interconnectivity [36,37]. Integrity is the main concern required in the design, creation, maintenance, and deployment of distributed accreditation analytical systems for credentials of candidate certificates to be secure and safe. However, the

scalability delimitation in the blockchain connectivity and communication protocols and the flexible capacity of the size of nodes make ecosystems more reliable in node-time and transaction storage with increased security. Developing a cross-chain platform improves performance in terms of secrecy and reduces operational costs.

However, the lack of direct cross-chaining ability between nodes of blockchains prevents pervasive learning and academic accreditation transactions using serverless distributed peer-to-peer environments within the proposed model. This interoperable mechanism is used to facilitate blockchain hyperledger sawtooth-enabled P2P network events of node transactions across distinct chains without involving vendor variation. Stateless educational transactions, atomic swaps, relays, consensus, collaborative architecture, and policies for secure and efficient blockchain connectives must be of concern to regional and state education departments, including blockchain connectivity and communication issues as well. The interoperable cross-chain limitation is still an untouched problem in the field of pervasive learning and distributed educational accreditation ledger preservation and management, for example, the safety and nodes of education transaction bottlenecks.

4.2.2. Credential Privacy and Preservation Challenges

Accreditation record management and storage generate logs of duplicates and redundancy [37]. Privacy and preservation are the main agendas that require maintenance and traceability. A distributed storage structure needs to be arranged so that it cannot create additional slots and focuses on the management of meta record storage [38,39]. Thus, maintaining the integrity and confidentiality of records and consistency of distributed educational applications during sharing is a complex task for an immutable storage structure with scalability and availability. The key distribution is another type of challenging aspect in accordance with the random generation in a blockchain hyperledger sawtooth-enabled distributed system.

4.2.3. Governance Body and Compliance Related Limitations

Various educational problems are associated with the current centralized accreditation system, including an analysis system for detecting errors in digital educational transactions, especially keeping secure credential information in central storage and relying on the cloud solution for preservation and security [36,38,40]. In addition, there are inappropriate techniques and inappropriate mechanisms used to register the device, collect universities' records, and accredit it. The connectivity between external edge devices to store sensitive information is also a compromising factor in educational node transactions. Through this process, regulatory compliance such as GDPR, which is going to have implications for the HED, means that the HED needs to examine, analyze, and monitor every aspect while organizing and managing distributed accreditation, classification, and preservation.

4.2.4. Accreditation Transparency for HED

The major challenging aspect of accreditation is to provide candidates' certificate-sensitive credentials transparency in a distributed environment [36,37]. The hyperledger sawtooth enables the provision of pre-defined information integrity and confidentiality policies [38]. In the proposed model, we have designed and created a customized protection mechanism using hash-encryption (SHA-256), which manages overall educational node transaction verification and validation, and implemented a consensus policy (PoET: range of parameter tuned) that allows for efficient performance in terms of security, privacy, and protection. Hyperledger sawtooth also provides a modular infrastructure to preserve records in a secure channel, which is completely transparent, provenanced, and immutable. This complete process can easily track records. No additional cost is required for managing accreditation records and reducing redundancy.

5. Conclusions

This paper discusses certificate credential secrecy and privacy and secure verification-related challenges in the centralized database. The protection of such accredited records of registered certificates and the retention of sensitive credentials from alteration, forgery, and tampering, as well as the maintenance of secure ledger investigation and preservation procedures, pose serious issues in terms of credibility in the central-storage environment. For this reason, we proposed a blockchain hyperledger sawtooth-enabled secure distributed candidate accreditation and certificate credential verification process. This proposed model creates an analytical platform for investigating certificate credentials while processing evaluation (pre-verification) using an artificial neural network for record classification before submitting them to the HED for further attestation. However, the stakeholders participate in the overall process of investigation and get details (read-only) of the complete educational transactions because of the consortium network.

A detailed certificate credential verification and accreditation investigation process by an engineer includes certification collection, examining each credential, forgery analysis, presenting details, storing them in immutable storage, and reporting. This paper presented and deployed smart contracts—one is the candidate registration contact (candidateReg()) for accreditation and records analysis, another is new issuance certificates related-node transactions (CIssuanceTrans()), and the third is an updated ledger after attestation and verification (ULedgerAV()). This whole blockchain-enabled mechanism provides integrity, provenance, transparency, immutability, and availability and performs efficiently the accreditation analysis process of execution and management. A flow control diagram is presented to demonstrate the working operations of educational transactions. Thus, we explain the implementation challenges that emerge while developing and deploying the proposed model with future objectives.

Author Contributions: Z.A.S. and A.A.K. have written the original draft and preparation; A.A.K., L.B., G.Z., N.Y., N.I., A.A.L. and S.E.B. have reviewed, rewrote, performed part of the literature survey, and edited, investigated, designed the architecture, and explored software tools. All authors have read and agreed to the published version of the manuscript.

Funding: The research of SEB is partially funded by the Ministry of Science and Higher Education of the Russian Federation under the strategic academic leadership program 'Priority 2030' (Agreement No. 075-15-2021-1333 dd 30 September 2021).

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

System Initialization: Blockchain Hyperledger Sawtooth Engineer Initiate System
Manage all the Educational Node Transactions
Handle Addresses

Data: Collect Data from Universities
Initially Pre-Verify Ledger before Records
HED Register Records and Details
Exchange Records with Federal Education Ministry

Procedure: int main():
type.text[Z].file:
candidate registration ID
(cID());
candidate national registration
(cNationalReg());
candidate name
(cName());
candidate batch
(cBatch());
candidate result
(cResult());
Blockchain Hyperledger Sawtooth timestamp
[execute];
Blockchain Hyperledger Engineer Associate with HED;

The Engineer handle all the registration and validation process;
Records overall Details with Addresses;
if candidate registration == to (true)
then,
if detail of the candidate != true
then,
Add records through CIssuanceTrans() contract
Add additional records for example, candidate registration ID (cID()), candidate national registration (cNationalReg()), candidate name (cName()), candidate batch (cBatch()), candidate result (cResult()), Blockchain Hyperledger Sawtooth timestamp [execute];
Counter ++;
else change state, analysis error, generate result
rollback
terminate;
else change state, analysis error, generate result
rollback
terminate;
Output: Candidate Registration for Accreditation (**candidateReg()**);

System Initialization: Blockchain Hyperledger Sawtooth Engineer Initiate System
Handle all the Educational Node Transactions
Manage Addresses
Data: Collect Data from Universities
Add New Accreditation
Pre-Verify Ledger before Records
Exchange Records with HED Regarding Credentials and Additional Details
HED Exchange Records with FEM
Procedure: int main():
type.text[Z].file:
candidate issuance certificate detail
(cICDetail());
individual accreditation registration
(iAReg());
number of enrolled candidates
(nECandidates());
number of candidate registered accreditation
(nCRAcc());
number of remaining candidates
(nRCan());
Blockchain Hyperledger Sawtooth timestamp
[execute];
Blockchain Hyperledger Sawtooth Engineer Associated with HED, Accreditation Dept, and FEM,
Engineer manages all the Accreditation Nodes Transactions;
Handle overall addresses and details;
if candidate accreditation registration == to (true)
then,
if number of enrolled accreditation != true
then,
Add records through CIssuanceTrans() and Update Ledger ULedgerAV () contracts
Add additional records such as, candidate issuance certificate detail (cICDetail()), individual accreditation registration (iAReg()), number of enrolled candidates (nECandidates()), number of candidate registered accreditation (nCRAcc()), number of remaining candidates (nRCan()), Blockchain Hyperledger Sawtooth timestamp [execute];
Counter ++;
else change state, analysis error, generate result
rollback
terminate;
else change state, analysis error, generate result
rollback
terminate;
Output: Add Individual Candidate Record and Exchange Information with FEM (**CIssuanceTrans()**);

System Initialization: Blockchain Hyperledger Sawtooth Engineer Initiate System
Manage all the Educational Update Nodes Transactions
Handle Addresses and Records
Data: Collect Added Accreditation Records from HED
Pre-Verify Recorded Ledger
HED Records all the Details with Addresses
Exchange Records with Federal Education Ministry and Universities

Procedure: int main():
type.text[Z].file:
get records
(gRecords());
update ledger
(uLedger());
secure preservation
(sPreserve());
manage chain
(mChain());
Blockchain Hyperledger Sawtooth timestamp
[execute]**;**
Blockchain Hyperledger Sawtooth Engineer Associated with HED, Accreditation Dept, and FEM,
Engineer manages all the Accreditation Nodes Transactions;
Handle overall addresses and details;
if get records == to (true)
then,
if update ledger != true
then,
Add update records through Update Ledger ULedgerAV () contracts
Add additional records such as, get records (gRecords()), update ledger (uLedger()), secure preservation (sPreserve()), manage chain (mChain()), Blockchain Hyperledger Sawtooth timestamp [execute];
Counter ++;
else change state, analysis error, generate result
rollback
terminate;
else change state, analysis error, generate result
rollback
terminate;
Output: Secure Update Ledger of Accreditation and Preservation (**ULedgerAV()**);

References

1. Ayub Khan, A.; Laghari, A.A.; Shaikh, A.A.; Bourouis, S.; Mamlouk, A.M.; Alshazly, H. Educational Blockchain: A Secure Degree Attestation and Verification Traceability Architecture for Higher Education Commission. *Appl. Sci.* **2021**, *11*, 10917. [CrossRef]
2. Lutfiani, N.; Aini, Q.; Rahardja, U.; Wijayanti, L.; Nabila, E.A.; Ali, M.I. Transformation of Blockchain and Opportunities for Education 4.0. *Int. J. Educ. Learn.* **2021**, *3*, 222–231.
3. Bhaskar, P.; Tiwari, C.K.; Joshi, A. Blockchain in education management: Present and future applications. *Interact. Technol. Smart Educ.* **2020**. [CrossRef]
4. Fedorova, E.P.; Skobleva, E.I. Application of Blockchain Technology in Higher Education. *Eur. J. Contemp. Educ.* **2020**, *9*, 552–571.
5. Sunarya, P.A.; Rahardja, U.; Sunarya, L.; Hardini, M. The Role of Blockchain As A Security Support For Student Profiles In Technology Education Systems. *InfoTekJar J. Nas. Inform. Dan Teknol. Jar.* **2020**, *4*, 203–207.
6. Oganda, F.P.; Lutfiani, N.; Aini, Q.; Rahardja, U.; Faturahman, A. Blockchain Education Smart Courses of Massive Online Open Course Using Business Model Canvas. In Proceedings of the 2020 IEEE 2nd International Conference on Cybernetics and Intelligent System (ICORIS), Manado, Indonesia, 27–28 October 2020; pp. 1–6.
7. Alam, T.; Benaida, M. Blockchain and Internet of Things in Higher Education. Tanweer Alam, Mohamed Benaida." Blockchain and Internet of Things in Higher Education. *Univers. J. Educ. Res.* **2020**, *8*, 2164–2174. [CrossRef]
8. Steiu, M.-F. Blockchain in education: Opportunities, applications, and challenges. *First Monday* **2020**. [CrossRef]
9. Lizcano, D.; Lara, J.A.; White, B.; Aljawarneh, S. Blockchain-based approach to create a model of trust in open and ubiquitous higher education. *J. Comput. High. Educ.* **2020**, *32*, 109–134. [CrossRef]
10. Shah, D.; Patel, D.; Adesara, J.; Hingu, P.; Shah, M. Exploiting the Capabilities of Blockchain and Machine Learning in Education. *Augment. Hum. Res.* **2021**, *6*, 1–14. [CrossRef]
11. Khan, A.A.; Shaikh, A.A.; Cheikhrouhou, O.; Laghari, A.A.; Rashid, M.; Shafiq, M.; Hamam, H. IMG-forensics: Multimedia-enabled information hiding investigation using convolutional neural network. *IET Image Processing* **2021**, 1–9. [CrossRef]
12. Ma, Y.; Fang, Y. Current Status, Issues, and Challenges of Blockchain Applications in Education. *Int. J. Emerg. Technol. Learn.* **2020**, *15*, 20–31. [CrossRef]
13. Perera, S.; Nanayakkara, S.; Rodrigo, M.; Senaratne, S.; Weinand, R. Blockchain technology: Is it hype or real in the construction industry? *J. Ind. Inf. Integr.* **2020**, *17*, 100125. [CrossRef]
14. Ghosh, A.; Gupta, S.; Dua, A.; Kumar, N. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. *J. Netw. Comput. Appl.* **2020**, *163*, 102635. [CrossRef]
15. Moriggl, P.; Asprion, P.M.; Schneider, B. Blockchain Technologies Towards Data Privacy—Hyperledger Sawtooth as Unit of Analysis. In *New Trends in Business Information Systems and Technology*; Springer: Cham, Switzerland, 2021; pp. 299–313.
16. Yang, G.R.; Wang, X.-J. Artificial Neural Networks for Neuroscientists: A Primer. *Neuron* **2020**, *107*, 1048–1070. [CrossRef] [PubMed]

17. Ali, O.; Ally, M.; Clutterbuck; Dwivedi, Y. The state of play of blockchain technology in the financial services sector: A systematic literature review. *Int. J. Inf. Manag.* **2020**, *54*, 102199. [CrossRef]
18. Guustaaf, E.; Rahardja, U.; Aini, Q.; Maharani, H.W.; Santoso, N.A. Blockchain-based Education Project. *Aptisi Trans. Manag.* **2021**, *5*, 46–61. [CrossRef]
19. Lee, D.; Park, N. A Blockchain-based Untact Education System for the Post-COVID-19 Era. *Ilkogr. Online* **2021**, *20*, 716–721.
20. Arcinas, M.M. A Blockchain Based Framework for Securing Students' Educational Data. *Linguist. Antverp.* **2021**, *2021*, 4475–4484.
21. Dudhat, A.; Santoso, N.P.L.; Henderi; Santoso, S.; Setiawati, R. Blockchain in Indonesia University: A Design Viewboard of Digital Technology Education. *Aptisi Trans. Technopreneurship* **2021**, *3*, 68–80. [CrossRef]
22. Guo, J.; Li, C.; Zhang, G.; Sun, Y.; Bie, R. Blockchain-enabled digital rights management for multimedia resources of online education. *Multimed. Tools Appl.* **2020**, *79*, 9735–9755. [CrossRef]
23. Khan, A.A.; Ali, S.A. Network forensics investigation: Behaviour analysis of distinct operating systems to detect and identify the host in IPv6 network. *Int. J. Electron. Secur. Digit. Forensics* **2021**, *13*, 600. [CrossRef]
24. Yan, Z.; Peng, L.; Feng, W.; Yang, L.T. Social-chain: Decentralized trust evaluation based on blockchain in pervasive social networking. *ACM Trans. Internet Technol.* **2021**, *21*, 1–28. [CrossRef]
25. Delgado-Von-Eitzen, C.; Anido-Rifón, L.; Fernández-Iglesias, M. Application of Blockchain in Education: GDPR-Compliant and Scalable Certification and Verification of Academic Information. *Appl. Sci.* **2021**, *11*, 4537. [CrossRef]
26. Moschou, K.; Theodouli, A.; Terzi, S.; Votis, K.; Tzovaras, D.; Karamitros, D.; Diamantopoulos, S. Performance Evaluation of different Hyperledger Sawtooth transaction processors for Blockchain log storage with varying workloads. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020; pp. 476–481.
27. Aggarwal, S.; Neeraj, K. Hyperledger. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2021; Volume 121, pp. 323–343.
28. Vignesh, V.; Gopalan, S.H.; Mohan, M.; Ramya, R.S.; Ananthakumar, R. A Quantum-Based Blockchain Approach to Voting Protocol Using Hyperledger Sawtooth. In Proceedings of the 2021 International Conference on Computing, Communication, Electrical and Biomedical Systems (ICCCEBS), Coimbatore, India, 25–26 March 2021; IOP Publishing: Bristol, UK, 2021; Volume 1916, p. 012088.
29. Khan, A.A.; Shaikh, Z.A.; Belinskaja, L.; Baitenova, L.; Vlasova, Y.; Gerzelieva, Z.; Laghari, A.A.; Abro, A.A.; Barykin, S. A Blockchain and Metaheuristic-Enabled Distributed Architecture for Smart Agricultural Analysis and Ledger Preservation Solution: A Collaborative Approach. *Appl. Sci.* **2022**, *12*, 1487. [CrossRef]
30. Li, Y.; Qiao, L.; Lv, Z. An Optimized Byzantine Fault Tolerance Algorithm for Consortium Blockchain. *Peer-Peer Netw. Appl.* **2021**, *14*, 2826–2839. [CrossRef]
31. Yang, J.; Paudel, A.; Gooi, H.B. Compensation for Power Loss by a Proof-of-Stake Consortium Blockchain Microgrid. *IEEE Trans. Ind. Inform.* **2021**, *17*, 3253–3262. [CrossRef]
32. Garg, A.; Kumar, P.; Madhukar, M.; Loyola-González, O.; Kumar, M. Blockchain-based online education content ranking. *Educ. Inf. Technol.* **2021**, 1–23. [CrossRef]
33. Rizky, A.; Kurniawan, S.; Gumelar, R.D.; Andriyan, V.; Prakoso, M.B. Use of Blockchain Technology in Implementing Information System Security On Education. *BEST J.* **2021**, *4*, 62–70.
34. Bucea-Manea-Ţoniş, R.; Martins, O.M.D.; Bucea-Manea-Ţoniş, R.; Gheorghiță, C.; Kuleto, V.; Ilić, M.P.; Simion, V.-E. Blockchain Technology Enhances Sustainable Higher Education. *Sustainability* **2021**, *13*, 12347. [CrossRef]
35. Lam, T.Y.; Dongol, B. A blockchain-enabled e-learning platform. *Interact. Learn. Environ.* **2020**, 1–23. [CrossRef]
36. Khan, A.A.; Shaikh, Z.A.; Baitenova, L.; Mutaliyeva, L.; Moiseev, N.; Mikhaylov, A.; Laghari, A.A.; Idris, S.A.; Alshazly. H. QoS-Ledger: Smart Contracts and Metaheuristic for Secure Quality-of-Service and Cost-Efficient Scheduling of Medical-Data Processing. *Electronics* **2021**, *10*, 3083. [CrossRef]
37. Khan, A.A.; Laghari, A.A.; Liu, D.-S.; Shaikh, A.A.; Ma, D.-D.; Wang, C.-Y.; Wagan, A.A. EPS-Ledger: Blockchain Hyperledger Sawtooth-Enabled Distributed Power Systems Chain of Operation and Control Node Privacy and Security. *Electron* **2021**, *10*, 2395. [CrossRef]
38. Khan, A.A.; Shaikh, Z.A.; Laghari, A.A.; Bourouis, S.; Wagan, A.A.; Ali, G.A.A.A. Blockchain-Aware Distributed Dynamic Monitoring: A Smart Contract for Fog-Based Drone Management in Land Surface Changes. *Atmosphere* **2021**, *12*, 1525. [CrossRef]
39. Halpin, H.; Piekarska, M. Introduction to Security and Privacy on the Blockchain. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, France, 26–28 April 2017; pp. 1–3.
40. Piao, Y.; Ye, K.; Cui, X. A Data Sharing Scheme for GDPR-Compliance Based on Consortium Blockchain. *Future Internet* **2021**, *13*, 217. [CrossRef]