applied sciences

MDPI

Article

Educational Blockchain: A Secure Degree Attestation and Verification Traceability Architecture for Higher Education Commission

Abdullah Ayub Khan [1,2,*], Asif Ali Laghari [1,*], Aftab Ahmed Shaikh [1], Sami Bourouis [3], Amir Madany Mamlouk [4] and Hammam Alshazly [5]

1 Department of Computer Science, Sindh Madressatul Islam University, Karachi 74000, Sindh, Pakistan; aftab.shaikh@smiu.edu.pk
2 Research Lab of Artificial Intelligence and Information Security, Faculty of Computing Science and Information Technology, Benazir Bhutto Shaheed University Lyari, Karachi 75660, Sindh, Pakistan
3 Department of Information Technology, Collage of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; s.bourouis@tu.edu.sa
4 Institute for Neuro- and Bioinformatics, University of Lübeck, 23562 Lübeck, Germany; madany@inb.uni-luebeck.de
5 Faculty of Computers and Information, South Valley University, Qena 83523, Egypt; hammam.alshazly@sci.svu.edu.eg
* Correspondence: abdullah.khan00763@gmail.com (A.A.K.); asif.laghari@smiu.edu.pk (A.A.L.)

Abstract: Degree attestation verification and traceability are complex one-to-one processes between the Higher Education Commission (HEC) and universities. The procedure shifted to the digitalized manner, but still, on a certain note, manual authentication is required. In the initial process, the university verified the degree and stamp seal first. Then, a physical channel of degree submission to the receiving ends is activated. After that, the degree is attested while properly examining and analyzing the tamper records related to degree credentials through e-communication with the university for verification and validation. This issue poses a serious challenge to educational information integrity and privacy. Potentially, blockchain technology could become a standardized platform to perform tasks including issuing, verifying, auditing, and tracing immutable records, which would enable the HEC, universities, and Federal Education Ministry (FEM) to quickly and easily get attested and investigate the forge proof versions of certificates. Besides, decentralized distributed data blocks in chronological order provide high security between distributed ledgers, consensus engine, digital signature, smart contracts, permissioned application, and private network node transactions that guarantee degree record validation and traceability. This paper presents an architecture (HEDU-Ledger) and detail design of blockchain-enabled hyperledger fabric applications implementation for degree attestation verification and traceable direct channel design between HEC and universities. The hyperledger fabric endorses attestation records first, and then validates (committer) the degree and maintains the secure chain of tracing between stakeholder peer nodes. Furthermore, this HEDU-Ledger architecture avoids language and administrative barriers. It also provides robustness in terms of security and privacy of records and maintains integrity with secure preservation as compared to that of the other state-of-the-art methods.

Keywords: blockchain; distributed cybersecurity and privacy; hyperledger fabric; higher education commission (HEC); information security; smart contracts

Citation: 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. https://doi.org/10.3390/app112210917

Academic Editor: George Drosatos

Received: 21 October 2021
Accepted: 16 November 2021
Published: 18 November 2021

1. Introduction

Higher educational institutions and universities play a pivotal role in creating an enabling environment and opportunities to uplift social mobility, economic turnaround, and a skilled workforce that promotes and achieves humanity's well-being around the globe [1]. It helps to create innovations in the job market to fulfil local and international

requirements. The certificates and degrees issued by higher educational institutes and universities significantly impact job seekers, primarily students, recruitment agencies, and various job providers, such as universities, multinational companies, government departments, and agencies [2,3].

These academic documents and degrees are undoubtedly official documents for professional credential completion proof of a higher education institution's degree requirements. These educational documents allow job recruitment agencies to decide whether a candidate possesses the desired knowledge and technical skills and satisfies the specific job requirements [4]. Dishonesty, fraud, and bribery are some of the prevailing issues in the education sector causing a wide range of damaging and detrimental effects. Many reports highlighted the essence of forgery and fraud in academic credential verification and attestation processes [5]. Such documented instances are widespread in developing countries like Pakistan, where the existing systems are one of the main contributors towards such frauds and forgeries, which became systemic and pervasive [6]. It leads to the ever-growing problems of credential fraud including issuance and misrepresentation and forgery of academic documents, such as degrees and certificates issued by higher educational universities and institutions, and compromised accreditation services [7].

A lot of fake and forged academic credential cases are being identified and successfully procured and reported [8,9]. According to a report, over one-third of applicants admit that they submitted fake and forged degrees to get better job positions while appearing for a job interview [10,11]. Much existing research shows that there are around 5000 unrecognized universities and institutes functioning worldwide, issuing over 200,000 fake or forged degrees annually, with earnings exceeding $1 billion.

The research proposed in this paper precisely emphasizes the problem of fake academic credentials they are submitted for verification and attestation in HEC in Pakistan. Many applicants misrepresent and forge their academic credentials to outperform their peers in highly competitive job markets. These forged credentials enable applicants to a free ride by using these benefits.

Pakistan HEC is a government body responsible for managing, attesting, and verifying the degrees and certificates issued by higher educational institutions and universities. However, unfortunately, the current legacy credential verification and attestation system in HEC is time-consuming, costly, and bureaucratic, and struggles against certain known credential fraud classes that undermine investment and confidence in higher education systems and bears high economic and social costs. During a recent meeting (2021) in HEC headquarters, one of the top IT experts stated that forgery of academic documents was becoming rampant. On the other hand, holders of genuine educational documents face many problems during the attestation and verification of their academic documents.

Furthermore, the legacy system used by universities and HEC for the issuance, verification, traceability, and provenance of degrees and certificates is semiautomated, slow, costly, time-consuming, complicated, and most importantly not secure; hence, the degree attestation process can easily be forged, and fake degrees can be illegitimately verified through the existing system [4]. During the COVID-19 pandemic, online teaching and learning education was significantly and widely adopted, and it transformed current academic systems including degree verification and attestation systems in Pakistan. Currently in the higher education system in Pakistan, there is no proper mechanism available to securely manage, trace, and provide provenance for the student's entire educational needs and requirements for attaining and verifying their degree certificate. As a result, the development and enactment of a secure, online, fully automated, and decentralized solution for degree verification, attestation, and traceability is essential to provide a transparent and traceable system to various participating stakeholders in the higher education system in Pakistan, as well as for recruitment agencies and job seekers.

The higher education degree attestation and verification process involves several stakeholders. The Ministry of Federal Education is the root node of the stakeholder's hierarchy, in which the higher education commission is distributed in regional-based

departments in different provinces to provide easy and accessible services across different provincial headquarters. The current degree attestation and verification process involves a collaborative mechanism comprising of both online and manual process as shown in Figure 1.

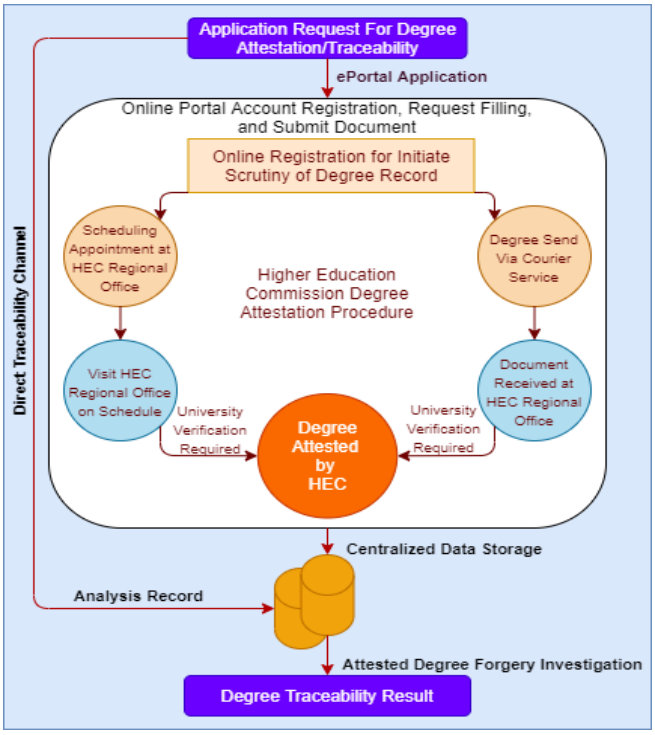

Figure 1. Current semiautomated higher education commission degree attestation and traceability architecture.

During a degree attestation and verification process, if an applicant wants to attest or verify his/her degree, they need to generate an online request through the HEC online portal. Once the request is generated, the applicant gets an appointment to submit the required list of documents online or through a designated courier service. In the next phase, the HEC starts the scrutiny process of degree verification and attestation and forwards the submitted documents to the appropriate degree issuing university or institute to verify the credentials [5,11]. Furthermore, this process also involves various other stakeholders and subordinated HEC regulatory bodies who regulate and verify the degree verification and attestation process between the applicant and HEC and HEC to universities. The current system used by HEC involves the following stakeholders, who are directly or indirectly involved in the degree attestation process.

- Federal Ministry of Education (FME)
- Higher Education Commission (HEC)
- HEC Recognized Universities and Institutes
- Employment Agencies
- Students/Candidates

Blockchain technology serves various potential advantages in pervasive higher education, learning, and development, such as enabling students' certifications to be quickly attested and easily verified in a secure fashion [6,9]. They could also allow to analyze forge proof versions, as well as guarantee the secrecy and integrity of their mark certificates. Moreover, there is no additional cost for permanence, accessibility, or a high level of security pertinent to preserving the data records [7]. For instance, a modular blockchain enterprise architecture of hyperledger fabric acts on a permissioned distributed ledger

technology [8]. At the same time, the HEC technical steering committee handles a diverse set of maintenance protocols and automates a configurable architecture that enables versatility, innovation, and optimization for a vast range of organizational stakeholders. This hash-encrypted distributed ledger architecture can support authored smart contacts in the general-purpose programming language, a private network that is a truly trustworthy and pluggable consensus protocol, with a more effective and customizable crash fault tolerance (CFT) [8,9]. Through the experiment, the encrypted, hash-based transaction nodes decentralized in chronological order can succeed by avoiding administrative barriers and third-party authenticity. The higher educational degree attestation verification design performs better, allowing smooth transaction processing, confirmation latency, and transactional smart contract privacy and confidentiality.

The main motivation behind this research is to address the issues and challenges of degree attestation and verification in Pakistan using blockchain technology. The research proposes a new blockchain-enabled degree attestation and verification system for the Higher Education Commission of Pakistan, a federal government body responsible for attesting and verifying the degrees issued by HEC-recognized universities and institutes. In our proposed solution, we used Hyperledger Fabric technology to create a private permissioned blockchain network. Different stakeholders are identified and added to the private permissioned network to achieve transparency, privacy, and secrecy. The proposed solution provides a robust, decentralized, and distributed hash-enabled chain-like structure called a ledger to store and record various transactions performed on the network. The research achieves the following objectives:

- We studied, examined, and analyzed several online degree credential verification methods, including traditional centralized database storage systems.
- In this paper, we evaluated the data authentication and privacy protection mechanisms used by the HEC to verify and attest to the degrees/certificates.
- A new and novel hyperledger fabric blockchain architecture is proposed for HEC to replace the existing e-portal centralized system that delivers improved performance, transparency, security, and complete provenance to authenticate and verify the originality of academic credentials.
- The transaction activities and operations of events delivery are illustrated using sequence diagrams to show how various steps are executed on the blockchain network while performing a degree verification traceability process.
- Finally, we designed the consensus policy for nodes transactions execution and explained their uses along with some open challenges, and we also discussed implementation-related issues that emerged while simulating this proposed solution in the future by the use of an educational benchmark dataset.

The rest of this paper is organized as follows. The related work section discusses different degree verification and attestation processes and solutions using blockchain technology. Section 3 focuses on blockchain-enabled digital ledger technology and its impact on higher education degree attestation security and privacy process. Section 4 explains the proposed novel architecture using hyperledger fabric technology for degree attestation and verification using the distributed application (DAPP). Section 5 presents the sequence diagrams to show the implementation of the proposed solution. Finally, various implementation challenges are discussed, and conclude this paper in Section 6.

2. Literature Review

Blockchain technology has high scientific and distinct network attention, the positive use of permissioned network architecture, a potentially distributed role in different domains, and operates free from central authorities [10]. Due to the devoted disruptive nature, the adaptation of blockchain technology is highly preferred in every aspect in real-time application with the needs of society. Despite this, most related work was discussed in relation to the limitations it may pose and not the use of blockchain technology in digital education.

The advent of blockchain and its radical impact compared to that of the new technological innovation of the internet proposed by Beck et al. also indicate the potential transformation within distinct business enterprises [11]. However, the concept of digital distributed ledger and manual ledger metamorphosis was proposed by Haber et al. [12]. With this concept, robust timestamping and the creation of intellectual property management established the modern blockchain-enabled distributed ledger innovation. Hyperledger enabled consortium, public, and fully private network is used as one of the strategic pillars in blockchain technology. There are various hyperledgers proposed for distinct purposes, and hyperledger fabric is one of the main research topics, as shown in Table 1.

In fact, the majority of research was conducted on blockchain security, information immutability, decentralized transaction, encrypted node privacy, distributed data preservation and storage, and hyperledger [13]. Based on these highlights, some critical disruptive and traditional centralized technological drawbacks in higher education, pervasive learning, investigating degree tampering and forgery, certificate attestation, traceability, and the importance of hyperledger are as follows:

Table 1. Related literature of blockchain hyperledger enables higher education degree attestation traceability.

Paper Title	Proposed Methodology/ Techniques	Towards a Blockchain	Challenges/Limitations	References
Decentralized Attestation of Conceptual Models Using the Ethereum Blockchain	The paper discussed the existence of cryptographic certificate records that publicly verify immutability and transparency. Implement attestation unique identifier model based on decentralization by using ADOxx metamodel and Ethereum network application.	• Similar security mechanism used • Difference in blockchain network	• Public network • Permissionless • Conceptual modeling • Content-based identification • SHA-256	[14]
AcaChain: Academic Credential Attestation System using Blockchain	This research explores blockchain technology for academic credential attestation in the educational environment. The paper improves the process of higher education credential attestation by reducing the cost, resources, and human involvement.	• Ethereum-based, design-customized public blockchain network	• No hyperledger used for public architecture • Permissionless network • Lack of data collection for preservation • Content-based model	[15]
Towards a Blockchain-based Digital Identity Verification, Record Attestation and Record Sharing System	In this study, authors investigate the traditional accreditation verification system inefficiency and difference in utilization of blockchain technology. Furthermore, this paper proposed blockchain-enabled framework for digital identification, record verification, and attestation.	• There is no hyperledger used • Consortium similarity	• For public credential verification • Self-sovereign identity • Permissionless network architecture	[16]
Exploring the Perceptions of Applying Blockchain Technology in the Higher Education Institutes in the UAE	The proposed blockchain method is applied to students' academic record verification and evaluation of students' study-based life cycle on the campus of higher education commission in UAE.	• Predefined blockchain consensus policy used	• Lack of research implementation • No proper use of blockchain consensus policy and management • Risk and implementation challenges	[17]

Table 1. *Cont.*

Paper Title	Proposed Methodology/ Techniques	Towards a Blockchain	Challenges/Limitations	References
A Preliminary Review of Blockchain-Based Solutions in Higher Education	This study provides a student-centric solution, which also presents some crucial use cases within the educational domain. A preliminary review and study of these cases identified that the student-centric approach is better than the record-keeping procedure.	• Restricted because only permissionless public network structure was designed	• Public-based academic verification architecture • Streamline credential security issues • Implementation challenges in EduCTX project	[18]
Blockchain and Smart Contracts for Higher Education Registry in Brazil	L. M. Palma et al. describe the critical problem related to academic credit and issuance of higher education degrees, for example, noncomputerized or semi computerized systems in Brazil. The proposed blockchain-enabled decentralized model for record-keeping, maintaining transparency, detecting forgery, both distributed and immutable.	• SH-256 re-encryption	• Hash-encryption SH-256 ECDSA signature algorithm • Public architecture • Permissionless • For specific degree category • Public key infrastructure	[19]
Application of Blockchain Technology in Higher Education	This study investigates how blockchain technology's consequences influence the domain of education. Authors also conducted the MIT certification verification and issued a real-time case study.	• There was no hyperledger modular architecture used	• Case study • No private policy defined • MIT verification based on public network architecture • Without hyperledger implementation	[20]
Blockchain-Based Approach to Create a Model of Trust in Open and Ubiquitous Higher Education	D. Lizcano et al. address the trusted ubiquitous learning model, the blockchain distributed ledger system used to manage the education-based content transaction, registration, and validation of the profile of institutional employees and competencies, student consensus, and maintain pervasive learning.	• Conceptual modular architecture	• Ethereum architecture used multichain • Hash encryption SH-256 • Permissionless network • Supervised testing	[21]
Cerberus: A Blockchain-Based Accreditation and Degree Verification System	A. Tariq et al. proposed a comprehensive blockchain-enabled credential verification solution (Cerberus). This study addresses the on-chain digital contract and disallows the student to entail digital identity.	• QR code-based verification	• Conceptual prototype • Mitigating educational fraud specifically • Credential revocation • Security SH256 used	[22]
Blockchain Based Framework for Educational Certificates Verification	O. S. Saleh et al. proposed a blockchain hyperledger fabric framework for degree verification. Furthermore, they identified the blockchain security loopholes in the educational degree verification solution.	• No customized digital contracts policy	• Desktop application • Lack of endorser and ordering management	[23]

Table 1. *Cont.*

Paper Title	Proposed Methodology/ Techniques	Towards a Blockchain	Challenges/Limitations	References
BCEAP-A Blockchain Embedded Academic Paradigm to Augment Legacy Education through Application	A. Ghaffar and M. Hussain proposed a blockchain-based educational record verification and validation system. The stakeholders for verification, such as HEC, PEC, and IBCC, which also allow the student to apply for institute admission and resist tampering or forgery, are more efficient and reliable.	• Ethereum Architecture	• Public network • Permissionless • Conceptual model • No hyperledger used	[24]
Blockchain Ecosystem for Verifiable Qualifications	D. Serrantio et al. address the solution for higher education affiliated institutes to register the degree issuance through blockchain, as well as check the certificate integrity and authenticity.	• Ecosystem but designed for specific domain	• Architecture implementing only • Six components of the blockchain used • The consortium network structure • Ethereum-based network prototype implementation	[25]
Design Framework on Tertiary Education System in Indonesia Using Blockchain Technology	U. Rahardja et al. present the blockchain-based framework with the platform of AI. This proposed system provides a solution for the tertiary education system in Indonesia. The main objective is to provide quality education across the country and resolve the national education implementation challenges.	• Permissionless network • Consortium nature	• Collaborate artificial intelligence platform, • Limited to the specific region • Conceptual model • Disruptive waves of the fourth industrial revolution concept	[26]

3. Blockchain-Based Secure Record Preservation and Security for HEC

The blockchain distributed ledger of digital transactions duplicates maintains across the stakeholders in the network [27]. Every node in the chain contains more than one transaction, and each transaction is recorded and immutable data are added and shared in the network to the entire participant ledger. These ledgers operate as a decentralized database handled by several stakeholders in the chain. However, this technology has a unique block-based hash-encrypted structure in chronological order, and crucial characteristics of the distributed ledger technology are as follows: timestamp, secure, unanimous, anonymous, and programmable smart contract [28]. Moreover, this technology security and data preservation are at the peak. The nodes are connected in sequential form. Each new block is attached at the end of the chain and generates a cipher code to protect data in the block [29]. In this way, blockchain networks are categories depending on the stakeholders' permissioned or permissionless, either public or private architecture. Some security features of this technology for the higher education commission are discussed below [30]:

- Firstly, the connected stakeholders get a complete ledger as long as the federal Ministry of Education is allowing them to participate. These stakeholders access the data records and make any further queries regarding the degree of data modification in the chain via the open interface of SDK/DAPP.
- Secondly, a peer-to-peer network connection is used to communicate individual participants in the decentralized higher education ledger architecture. Each block of stakeholders is treated uniformly. Furthermore, no additional vendor support or connection to third-party platforms are required.

- Most importantly, the individual node has a sort of cipher-encrypted address since the hash was previously stored in each block in the educational chain. For every single data record of a specific node, the transaction updates. After the change, the updated records of the attached nodes in the chain are recalculated. Furthermore, consensus approval is required; most probably degree record modification is impossible because of the digital contract sign between participants to achieve node data. Therefore, the digital ledger architecture stores educational data in the form of a node. Once the records are stored, the verification is also stored on it.

The Role of Hyperledger

Hyperledger focuses on the development suite of a stable blockchain-enabled (such as 'HEDU-Ledger') architecture and records traceability, libraries, and tools [31]. It provides a modular approach for implementing the degree traceability system, including digital ledgers and customized smart contracts. Higher education degree attestation traceability-based blockchain applications rely on the permissioned trust relations, intrinsic stakeholder interest in the defined consensus policy, and not required to run proof-of-work algorithm [32]. In addition, hyperledger promises, educational records, transparency, distributed data transactions, and immutable digital ledgers are spread across the nodes in a private network. If one maintains the duplication of the common system and keeps the data recorded, nothing will be erased or altered. However, the copy of the digital ledger is identical to the other stored ledgers in the peer network. There are distinct hyperledgers available, differentiating the role in a different enterprise environment, and its critical features and importance (shown in Table 2) are described as follows:

Table 2. Role of hyperledger.

Hyperledger	Features Details
Hyperledger Sawtooth [33]	Distributed private network ledger and applications; business rules; smart contract; enterprise enabled and consortium-based policy decision; consortium blockchain; permissioned network; parallel transactional execution; event-based execution; pluggable and customize consensus algorithm
Hyperledger Indy [34]	Interoperable platform; distributed storage; shared components; libraries and client tools facility; decentralized identifier correlation-resistant; permissionless network
Hyperledger Besu [35]	Open-source; allow to develop Ethereum client; enterprise Ethereum alliance; user-facing APIs; IBFT and clique consensus algorithms; consortium blockchain network
Hyperledger Grid [36]	A framework for building supply chain solution (business enterprises); modular components; client interface; domain-specific data model; digital contracts.
Hyperledger Iroha [37]	A role-based access; assets; identity management; general purpose system; permissioned network, easy deployment; command query and separation
Hyperledger Fabric [38,39]	A modular architecture; plug and play services; customized consensus mechanism; scalability; secure data preservation; distributed ledger solution and storage; private network

4. Hyperledger Fabric-Enabled Paperless Education Degree Issuance and Secure Attestation and Verification Platform

Through the proper implementation and sequence-of-working of digital contracts of high education degree issuance, attestation, verification, and traceability using blockchain security technology, the fabric is an extensible blockchain solution that enables developers to maintain a distributed digital ledger [40]. It provides robust security features and credential privacy that allow block data scalability and node transaction flexibility, and no additional cost is required to run the distributed application. The operational advantage is to maintain self-sovereign of the online proof of educational credentials and to preserve the evidence of higher education, academic protection, and digital achievement secrecy. The digital proof can handle timestamping efficiently, integrate existing application requests seamlessly, ensure academic credential protection and high data integrity, and provide a secure pathway and intellectual property rights to the connected stakeholders [41,42]. Here, we discuss some key factors of blockchain hyperledger fabric enabling ubiquitous credential attestation traceability security:

- The higher education degree attestation traceability system requires a private key. The main objective is to sign the university academic credentials and issuance certificate to adding verification signature in every aspect.
- In this regard, a unique hash-encrypted ID generates in every content verification of the education certificate that allows stakeholders to trace records.
- This system also ensures the credential contents, consistency, and degree records.
- At every level, hyperledger fabric smart contract technology manages and executes the digital contract, and a digital multigeniture is used to verify the contents of degree and information authorization.

Figure 2 presents the blockchain distributed ledger architecture that enables hyperledger fabric smart contract technology to execute the smart contract and digital signature for degree attestation traceability. This block-based architecture is categorized into three main phases or levels; the one-to-one communication between the Higher Education commission and universities starts hiring bodies and state government officials to apply for scrutiny. However, the scrutiny process in the blockchain is quite different, as there is a digital verification of candidates' degree credentials and tracing of the signature of the document attestation. Through phase 1, the application layer of blockchain architecture aims to conduct the attestation traceability procedure and provide HEC eportal distributed platform. In this regard, the blockchain-enabled distributed SDK application allows stakeholders to generate a request for degree attestation and traceability. Phase 2 maintains the overall transactions between the smart contracts and architectural validation, handles hash-based encrypted blocks, and keeps ledgers private in the network. Moreover, the transactional layer also manages the digital rewards between consensus and makes distributed copies of the transaction in the private network ledger in the smart contract. In phase 3, there is a digital degree record exchange within the chain because of peer-to-peer network connection, and data are preserved in the decentralized storage.

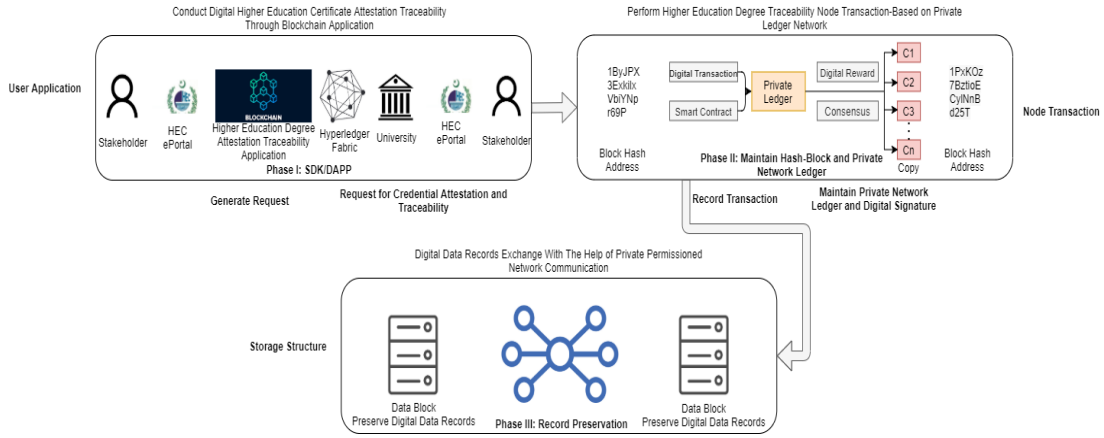

Figure 2. Blockchain hyperledger fabric-enabled distributed phases for higher education commission degree attestation traceability.

4.1. Proposed Degree Attestation Traceability Architecture for Higher Education Commission

The proposed blockchain peer-to-peer network-enabled architecture provides a structural development solution for HEC degree attestation traceability, which is deployed on fabric hyperledger. This solution uses two distinct sorts of traceability for the organization: hiring bodies to the respective university and universities to HEC. Individual universities and record-keeping departments contain a minimum of two peers of hyperledger fabric-based nodes that are used to create the distributed network as shown in Figure 3. In this peer node, a single-order node in the Apache KAFKA ordering service provides the solution in solo mode. This service also handles degree credentials or record data block creation and consensus verification. Moreover, the fabric hyperledger uses the consensus algorithm to manage certificate's identity verification and validation. In addition, it is

deployed in the node and provides membership services to the institutes, state government officials, hiring bodies, and HEC regional sectors.

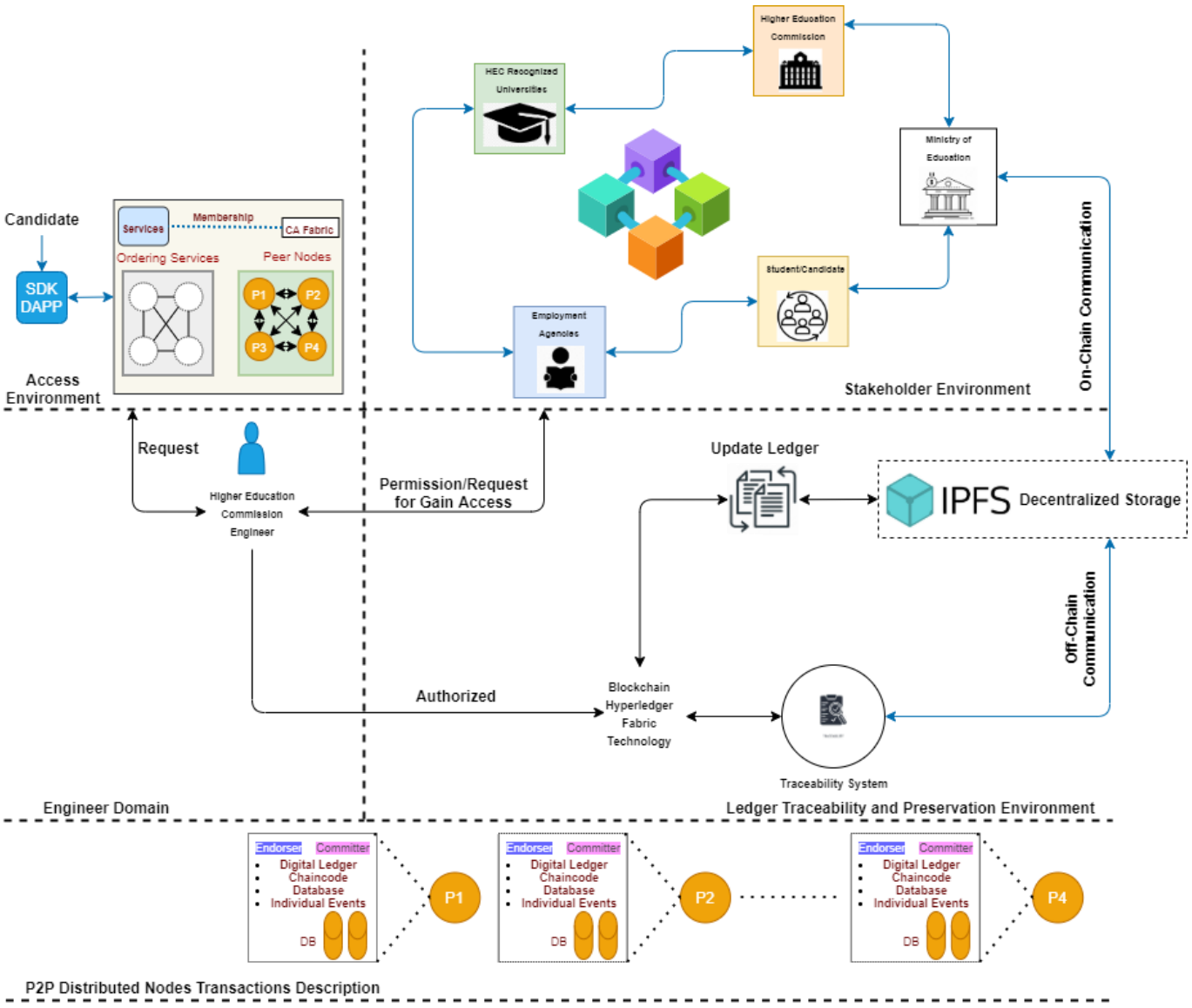

Figure 3. Proposed blockchain hyperledger fabric-enabled degree attestation verification and traceability architecture for HEC.

Although the InterPlanetary File System (IPFS) storage is used as an external storage structure for HEC degree attestation, traceability to preserve candidate degree credentials and personal information are protected and shared only among the stakeholders within the permissioned private chain network architecture. This file-sharing system more efficiently leverages data record preservation. Furthermore, the system allows to transfer, share, track, and store large files along with domain efficiency. The IPFS depends on the cryptographic hash encryption as a direct and robust way to store on the blockchain, as shown in Figure 3. However, the storage does not require or permit users to share any files with the selected stakeholders. The implementation of the node transaction and the process of execution are shown in Figure 4.

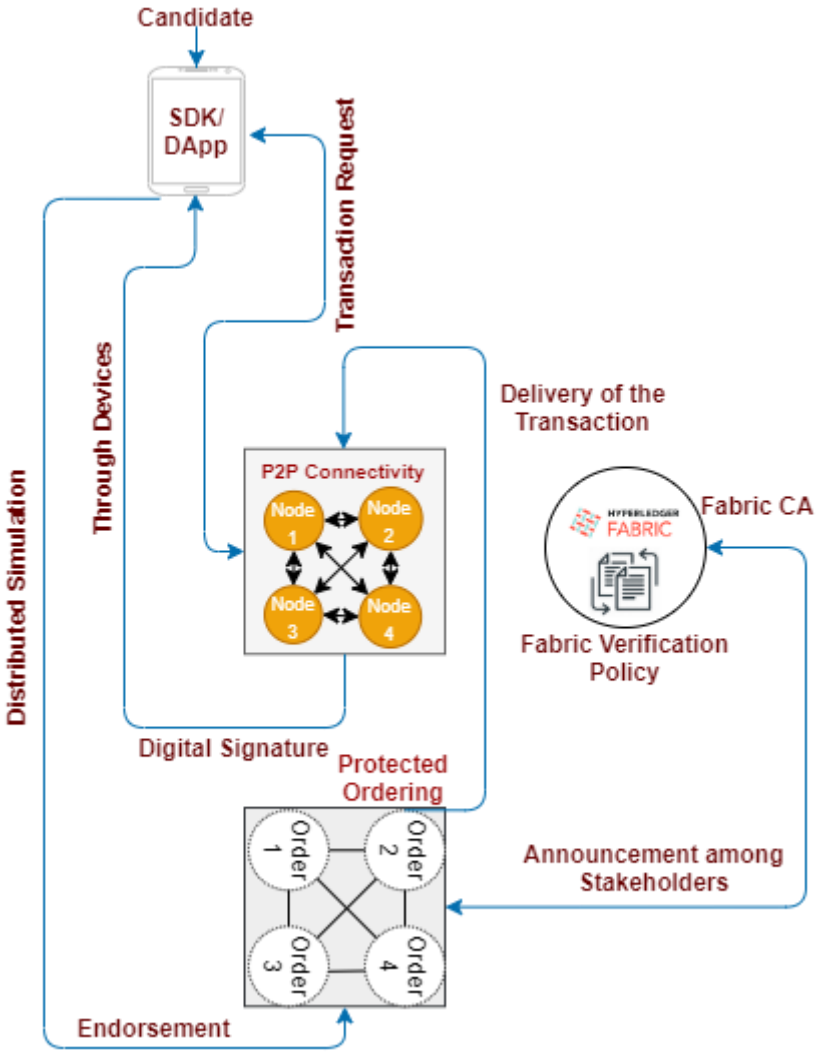

Figure 4. Implementation of block transactions execution process.

The bundle of degree records is used to trigger the hyperledger fabric-enabled smart contract specifically. The transaction proposal is sent to the peer nodes in the chain for endorsement, where smart contract executes the endorsing for the ledger to satisfy the successful transaction shown in Figure 4. After this process, the endorsing peer digitally signs and returns to the committer. The committer in the peer validates the integrity of the transaction and concatenates it to the digital ledger. However, the REST API (used for obtaining HTTP requests to access and use data) runs through the fabric Swagger directly, where the system can GET (current state) and POST (target smart contract) block services in the peer network. Block API retrieves the degree contents or credentials in the various blocks from the blockchain. The programmable ledger of higher education degree attestation is preserved on the blockchain fabric IPFS file storage; moreover, the smart contract is implemented for robust information integrity preservation and secure interaction among stakeholders. These privately permissioned encrypted blockchain ledgers are immutable, as shown in Figure 4, meaning they cannot be manipulated, and thereby enhance the attestation traceability features for the HEC. A hyperledger fabric comprising the three main parts discussed are as follows:

1. The HEC distributed ordering service initiates the proposal of the transaction, with the order being endorsed by the peer nodes on the blockchain fabric network. The degree-related block transaction contains a digital signature and hash encrypted by each peer for endorsement, which is then submitted to the orderer service and

forwarded to the committer with the HEDU digital ledger. After completing this process, the service is broadcast from the orderer to the committer on the blockchain hyperledger fabric for validation (KAFKA) and verified according to the defined consensus policy, as shown in Figures 3 and 4.

- In this proposed educational blockchain-ledger architecture, we built private channels and restrict the direct path of messages delivered and received because of transaction privacy and confidentiality between a subspace of network members. The HEDU-ledger relates information including node transactions, participating stakeholders, communication channels, and channel-related details, which are inaccessible, and there is no visibility of any member on the network, so this channel cannot be operated by a third-party participant.
- The execution of block transactions is completely private and separate from ordering to the committer. It provides an efficient procedure of transaction execution, including maintaining the ledger maintenance, consensus workload, and comparing with that of other state-of-the-art blockchain technologies.
- The smart contract functionality enables transaction encryption and business logic invoked specific kinds of block transaction execution on the private communication channel. Meanwhile, it tackles the entire execution transaction and private channel operations in this blockchain system.

2. In this proposed network, multiple peer channels are used to update and query (log and state) execution on the HEDU-ledger. This system auto-synchronizes and executes two roles mainly, such as endorsing to committing transactions or vice versa. This block-based transaction proposal is submitted according to the policy of endorsement after the procedure of peering; in the private network channel of the blockchain ledger architecture, as shown in Figure 4.
3. For permissioned private blockchain networks, we designed a Certificate Authority (CA) network of distinct untrusted participating stakeholders in the Higher Education Commission. These identified stakeholders are enrolled only if they have a unique root certification. The Certificate Authority provided by the Ministry of Education to HEC (and HEC to universities) that binds specific peers and order. By allocating Certificate Authority to individual stakeholders, the private HEDU-ledger network mimics where the participants (also responsible for transaction renewal and revocation) use their own Certificate Authority. The transaction and private communication ledger are signed by the stakeholder's private key, and for verification, it uses the public key within the fabric hyperledger.

In this proposed HEDU-ledger, a hyperledger fabric enabled architecture is presented for the degree attestation traceability system that connects participating stakeholders from a peer-to-peer (P2P) private permissioned network, as shown in Figure 4.

4.2. Smart Contracts-Based Result and Discussion

4.2.1. Blockchain Enabled Fabric Certificate Authority for Participating Candidate Registration Contract (DARC())

The degree attestation registration contract and design consensus for participating stakeholders are initiated and deployed between universities and HEC to register new enrolments of degree and degree programs along with stakeholder registration. The degree attested register() function is created to add and execute degree-related information used by HEC engineers, which also records stakeholder participation according to the policy of consensus in the DARC(). This contract also records additional data such as degree code, degree title, degree program, candidate details, timestamp, degree counter, and other activation registration steps. Furthermore, the degree attestation and participating stakeholders' registration are recorded on the DARC(). Then, the system initiates another contract named AAC() as mentioned in Appdendix A, deployed between DARC() and universities, and managed by HEC Engineers.

4.2.2. Distributed HEC Accumulator and Accreditation Contract (AAC())

The HEC accumulation and accreditation contract is deployed and automates updates whenever a new event is added to the DARC(). The AAC() contract is preserving the accreditation-related information, even though all distinct types of degree programs registered by HEC and updated in the DARC() contract. The addAccrediation() function is created to add program accreditation and execute update-related information in the AAC() contract. This contract also preserves relevant records such as accreditation ID, accreditation program, current semester enrolment, timestamp, add, TDRUC, HEC accreditation manager for the count. Moreover, the successfully deployed AAC() contract shares its updated addresses of the contract with the connected DARC().

4.2.3. Digital Signature and Permissioned Private Transaction of Degree Record Update Contract (TDRUC())

The HEC transaction of degree record update contract (TDRUC()) is deployed and automates the updates whenever new accreditation-related information is added to the AAC contract. In this contract, the information is shared among the stakeholders according to the Certificate Authority and mentioned policy. This updated information is all about the degree-related transaction added to DARC() and AAC(), respectively. The updatetrans() function is created to add transaction records and execute updates of the transaction history of new degree-related accreditation information in the TDRUC() contract. This contract also preserves related information records such as assignee, present transactions, past transactions, timestamp, and transaction count to added and updated in respective smart contract. Furthermore, the well-deployed TDRUC() contract shares its updated addresses of the contract to the AAC() contract.

4.2.4. HEC Degree Attestation and Credential Verification Transactions Flow

The advantage of employing the proposed hyperledger fabric enabled degree attestation and credential verification traceability solution in the higher education commission ensures the availability of complete and abiding records among the stakeholders without the direct involvement of the federal educational authority. In the processes of degree attestation traceability, the involved stakeholders can investigate the history of attestation, track and trace provenance, source, and degree number along with the program accreditation and enrolment registration through mobile DAPP. The registered stakeholders are authorized to preserve, update, and retrieve degree attestation and verification-related transaction information on the HEDU-ledger. In this proposed architecture, the highlighted and most significant aspect is that the system validates, authenticates, and authorizes, and will only be updated and added to the ledger on the HEDU-ledger transaction based on the Certificate Authority verification. This section discusses the implementation of HEDU-ledger-related events' flow, and the node transactions' execution, verification, and validation procedural steps are explained in Figure 5 (activity diagram) and Table 3 (description).

4.2.5. Fabric with Hash Re-Encryption and Privacy Measurement

In the proposed architecture, the hash protocol used as a proof of stake in the degree attestation traceability allows proxy reEncrption of degree credentials. Moreover, the system builds an encryption infrastructure such as managing secret SSH credentials, X.509 certificate, and signing key generation between DARC(), AAC(), and TDRUC() contracts. HEC engineers utilize hash (reEncrypt()) dynamic control, access, or invoke to access sensitive degree-related information to the stakeholders. This information is encrypted while preserving the records in the IPFS storage. This information is encrypted while preserving the records in the IPFS storage, as shown in Appdendix A.

Table 3. List of events of nodes transactions and execution of proposed HEC degree attestation traceability architecture.

Series of Events	Working Description
1	HEC degree attestation registration (register()) ledger deployed by the Higher Education Commission.
2	The HEC Engineers received a request (applicational request) for degree attestation and verification through the distributed application in the registration contract (register()).
3	A new HEC accumulation and accreditation contract is deployed and created in the image of it.
4	The addresses of HEC accumulation and accreditation manages contract to the HEC Engineer registration contract (register()).
5	Send the registration details to the transactions (addAccrediation()) of degree record and update the contract.
6	Return the addresses of transaction of degree record and update contract to the HEC accreditation and accreditation contract.
7	Similarly, return addresses of the registration contract (register()) to the degree attestation.
8	Once the degree-related information is added to the HEC registration (register()) contract, updated in the respective contract, and attached to the stakeholder participation consensus, this information is passed by the HEC to state regions/regional offices.
9	The new registered candidates' contract will be deployed for degree credentials and verification.
10	HEC registration contract added new degree related information and registration updates to HEC accumulation and accreditation contract (AAC()).
11	Return the addresses.
12	HEC regional office/state office added new university accreditation and board of studies-related transactions in the accumulation contract (AAC()) and deployed.
13	Get acknowledgment back to the HEC accumulation and accreditation contract (addAccrediation()).
14	The new transaction of degree record update contract is deployed (updateTrans()).
15	Addresses of transactions of degree record updates maintain contract to HEC accumulation and accreditation contract.
16	Maintain a new copy of updated HEC accumulation and accreditation contract, and deploy in the image of update contract.
17	Return addresses to the HEC accumulation and accreditation contract, and acknowledge back the addresses.
18	The universities update the information of registered candidates passed from the university to HEC, then HEC/regional office/state office updates and passes on to the transaction of degree record to update the contract.
19	The candidate registration related information is passed on from HEC to universities, then universities pass on to transaction degree record to update contract.
20	The registered degree record (credentials) is passed from university to HEC.
21	The HEC get approval for the educational activities from the federal Education Regulatory Authority.
22	The federal education regulatory authority tracks and trace individual records of the candidate traceability system using the transaction degree record update contract.
23	The registered degree record (credentials) is passed from HEC to government officials/Hiring bodies.
24	The registered degree record (credentials) individuals will be passed between government officials/hiring bodies to candidates.
25	The candidate will trace and track the degree credentials and verify easily from the traceability system using transaction degree record update contract.
26	The federal education regulatory authority will trace and track the degree credentials and verify easily from the traceability system using transaction degree record update contract.
27	Maintain a new copy of updated transaction degree and record update to contract and deploy.
28	Return addresses to the transaction degree record update contract and acknowledge back (addresses).

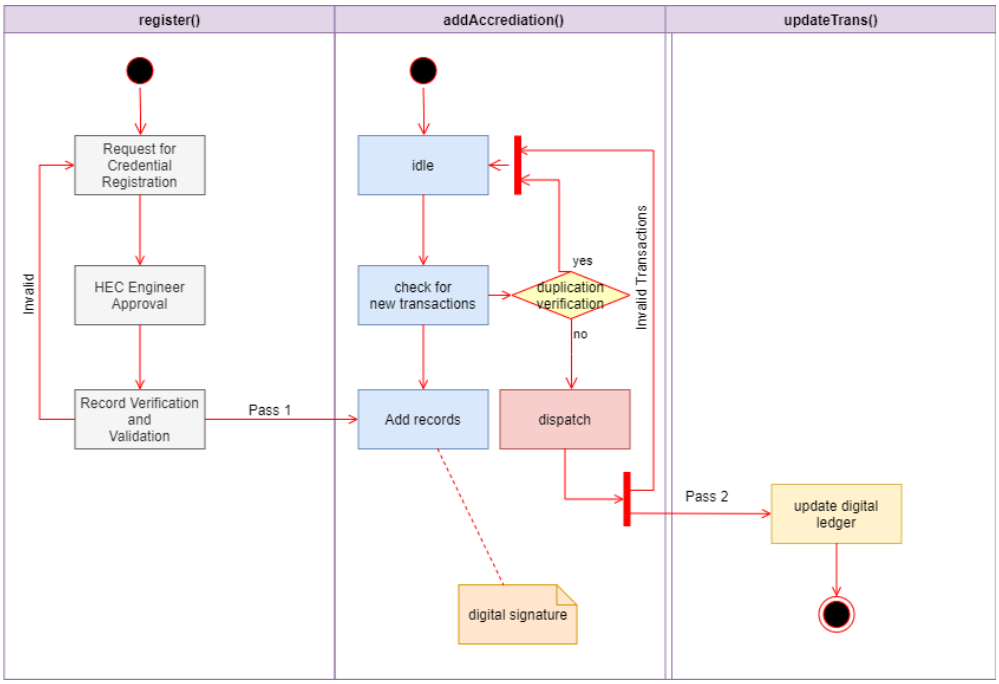

Figure 5. Event of nodes transactions execution through activity diagram.

5. Working Operations of the Proposed Architecture and Discussion

Figure 6 presents the identification and registration of degree attestation traceability sequence process in which HEC engineers maintain the main chain code of the system. The chain code is able to initialize procedures until the completion of transaction. Firstly, the proposal sends to the HEC regulatory authority, responsible for creating, executing, transferring, tracking, verifying, and validating transactions of the submitted proposal among the registered stakeholders. Then smart contract assists in acquainting, preparing, analyzing, uploading, transfer, and sharing degree credential registration details on the HEDU-ledger, as shown in Figure 6.

This contract designed to check the corresponding credentials is already submitted previously or not; if yes, then it reverts. If the system is not registered yet, then the degree attestation and credential verification register() function is added a new records and update ledgers successfully in the smart contract, as defined in Appendix A.

The attestation and credential verification process are executed between the universities and HEC once the consensus reaches the specific point of record submission, in which both stakeholders at the level of interaction sign digital and encrypted. After the universities receive updated record authentication from HEC and smart contracts update information, the (updateTrans()) function is used to preserve according to that shown in Figure 7. The implementation of the degree attestation traceability process executes the updateTrans() functions in which government state officials track and trace individual records before the procedure of hiring bodies and schedule employment interviews. HEC engineers and registration smart contract manager produces proper statistics information on the basis of university program activities and accreditation, board of studies, admission, semester course enrolment related information, year of passing out, degree related credential information including meta-record, record timestamp, and affiliation information.

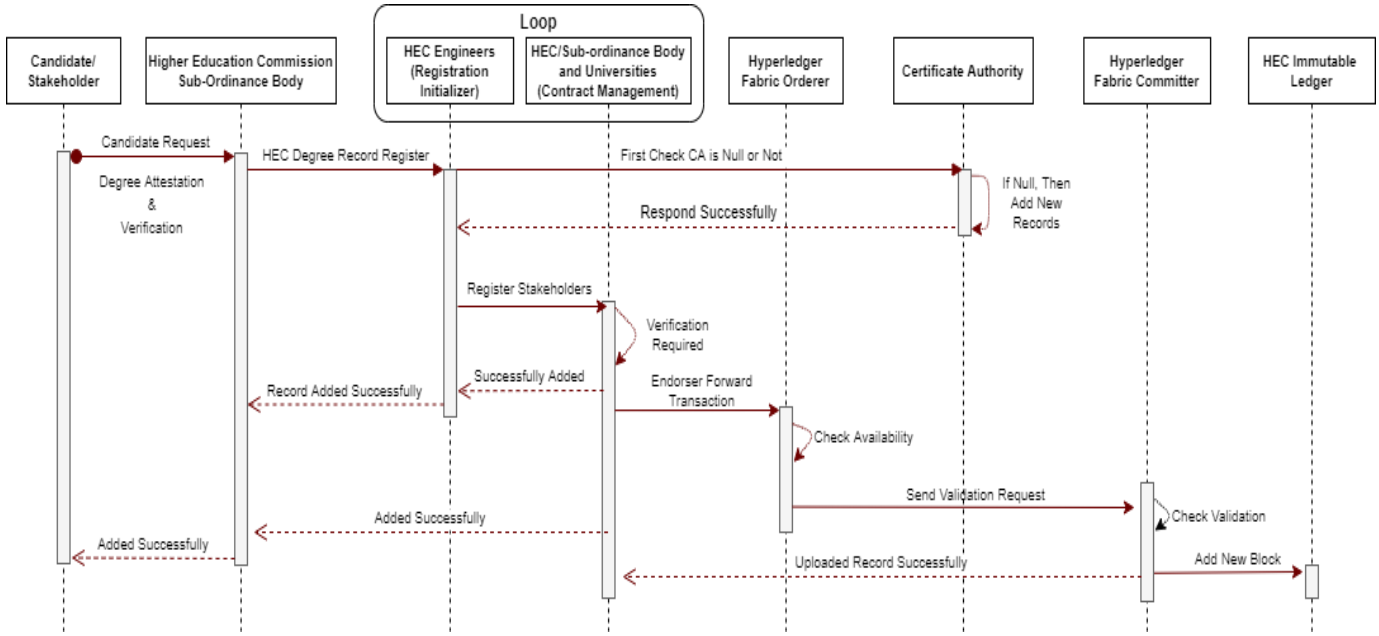

Figure 6. Sequence diagram of degree attestation and credentials verification, and validation of registration of node transaction processes.

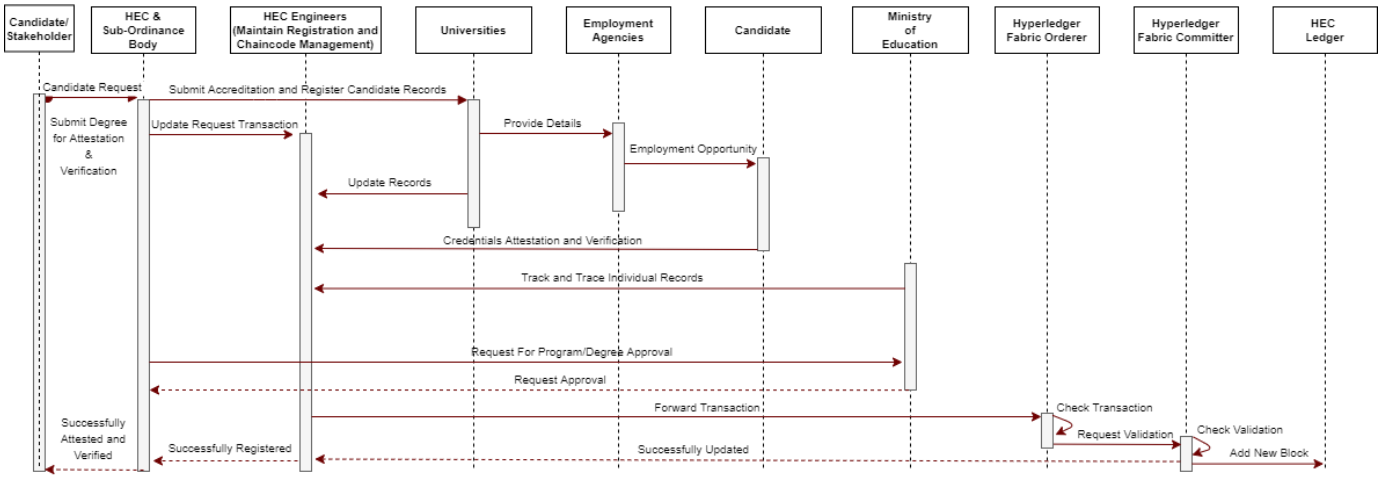

Figure 7. Sequence diagram of degree attestation and credential verification transaction processes.

5.1. Challenge, Limitations, and Issues Emerged in the Current System

5.1.1. Governance and Regulatory Related Challenges

The HEC authority needs to consider, design, and develop distinct educational policies and pathways regarding the blockchain technology-based hyperledger fabric smart contract implications and ascriptions such as digital record, protected maintainability and block stakeholder on the ledger, decentralized storage preservation, and stakeholder changes permission along with the rights of consensus in the private ledger network architecture [27,43]. The HEC needs to collaborate with universities and other state regional sectors and facilitate with manual degree attestation verification, a regulatory architecture for certificate credentials, privacy, and compatibility for the development of the online secure blockchain-enabled system for degree attestation traceability, and also evaluate the HEC environs to calculate the difference and formulate new authoritative policies and objectives.

5.1.2. Cross-Chaining

The primary objective of using blockchain is to protect critical data organizations of data to gratify the particular kind of data that will be preserved on the digital ledger using the blockchain technology along with the process of storage, such as off-chain and on-chain data preservation storage [44]. In the higher education degree attestation, the overall data is more sensitive and confidential; therefore, the data must be preserved and checked against and investigate the hashes of on-chain. The most prominent aspect of structured critical data is the size and storage of data in chunks and data preservation on the distributed ledger. Additional storage of noncrucial data records on the private network ledger creates more cost of the transactional size that will impact the blockchain performance in terms of efficiency and accuracy [27].

The cross-chain platform of HEC allows multiple institutes, federal education officials, and regional offices to use an effective and efficient business service model for degree attestation and traceability. The end-users of the platform and distinct various users of the different domains of blockchain platform can intercommunicate, interact, proper utilization of services, and conduct meaningful education transaction. The existing legacy HEC degree attestation and verification solution, the current blockchain-based platform, has a lack of cross-platform because of disunion and less connection, which make it difficult to adoptability and platform implementation among the users of the system [43].

5.1.3. Streamlined Process Automation of Attestation Traceability with Digital Contracts

A blockchain is a decentralized private digital ledger where universities exchange critical information such as educational credentials, previous candidate information, recent records, and complete certification in a chain of blocks [27,45]. The stakeholders record these core ledgers electronically for further employment or admission to a higher education certificate and trace accordingly. These education-related data records were provided on the blockchain hyperledger fabric enabled platform that allows access to this sensitive private information. The challenging problem is to restrict several repetitive activities that consume high time, increase execution cost, and utilize more computation power. However, manual insertion is tedious, difficult, leads to apathy and is considered a timewasting strategy in the current distributed environment. The tasks are identified in a way that is robust to automate the processes of higher education certificate attestation traceability, which is still a platform implementation challenge with blockchain Hyperledger-enabled technology. The major problem is to design customized digital contracts and certificate authority verification policies between stakeholders and automate (smart contract) them along with the digital signature.

5.1.4. HEC Standardization and Compliances Limitations

The HEC regulatory authority plays an important role to manage the standards of degree attestation and verification including the secrecy of candidate certificate credentials and authenticity, checking system quality and maintainability, safety, data protectability, sensibility, resource effectiveness, transfer and exchange records between the universities and federal education authorities. These regulatory authorities look after the complete mechanism of retrieval, preserve, share, transfer, store, and exchange degree, attestation, and verification related data records, and more crucial to provide transparency, scalability, cross-chaining, and security [43,44]. In this way, the degree traceability limitations and issues can be solved with more efficiency, and they can be reorganized to deliver a better educational solution for HEC. Another challenging aspect is to cope with the manual credential records feeding to the distributed system and the requirement of system and legislation in blockchain networks. Until now, blockchain technology is still not decisive on the laws and rules regarding the predefined system of HEC.

5.1.5. Security & Privacy of Nodes Issues and Domain Efficiency Challenge

In this era, the blockchain services enabled solutions are more demanding as a proficient-based and private platform for different organizations. However, the exist-

ing security technology and its solutions are untrusted and unreliable [27,43]; moreover, it cannot provide large scalability services with a high rate of data dependency. In addition, it restricts the continuous process of node transaction, data records, transparency, domain efficiency, size of inheriting data and latency, and the robust additional cost of security scalability [45]. In this regard, the HEC degree attestation and verification, permissioned-based private blockchain network architecture solution, is considered the most crucial and important compared to the collaboration of the manual and digital procedural mechanism regarding robustness of performance and efficiency of solutions. It also has more powerful computational abilities as well as high processing execution compared to that of the permissionless public and customized blockchain hyperledger technology.

6. Conclusions

This paper discusses the security- and privacy-related issues and procedures in the existing HEC degree attestation and record traceability architecture. Identified the solution of such mentioned issues by using blockchain, especially hyperledger fabric-enabled attested degree verification. For this purpose, we proposed HEDU-ledger (educational blockchain ledger), which is a permissioned private network architecture created between stakeholders for certificate record traceability. In addition, this proposed novel and secure architecture provides robust security and protection in terms of maintaining decentralized candidate degree credentials and data records in a distributed ledger. These ledgers are completely immutable in nature, registration, transfer, and tracking through hash encryption and collaboration between smart contracts, used to protect node transaction and information secrecy, timestamp, anonymous, unanimous, and programmed for permissioned private network interface.

The HEDU-Ledger solution is a complete package that is purely decentralized. The processes such as nonrepudiation with provenance and traceability for agile courage are without a single conflict in the HEC degree attestation. The stakeholders and other connecting parties are initially identified and authenticated by HEC engineers using their digital signature and cryptography encryption. Moreover, we described and presented the whole mechanism of the proposed architecture, including the policy of HEC, attestation and verification criteria, and the other elements involved through the activity diagram. Additionally, the HEDU-Ledger also records more detail regarding the stored ledger in an IPFS data storage structure in the protected and immutable form. This system also provides transparency, security, forgery-proofing, and auto tackling cyberattacks such as distributed denial of service.

Author Contributions: A.A.K. has written the original draft and preparation; A.A.L., A.A.S. and S.B. have reviewed, rewrote, edited, and investigated; A.M.M. and H.A. have designed architecture, tested algorithm, and applied software tools. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to thank Taif University Researchers Supporting Project (TURSP-2020/26), Taif University, Taif, Saudi Arabia. The authors acknowledge the financial support by the Federal Ministry of Education and Research of Germany in the framework of AI-Campus (project number 16DHBQP041).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank Taif University Researchers Supporting Project (TURSP-2020/26), Taif University, Taif, Saudi Arabia. The authors acknowledge the financial support by the Federal Ministry of Education and Research of Germany in the framework of AI-Campus (project number 16DHBQP041).

Conflicts of Interest: The authors did not have any conflict of interest.

Appendix A

Table A1. Implementation of Smart Contracts.

Contract 1: Certificate Authority of the Degree Attestation and Traceability and Stakeholder Registration (register())
Contact Initialization: HEC Engineer Initiates HEDU-Ledger **Data:** HEC Engineer Start System and Manage Addresses int main: x [file], degree number (degreeNumber), degree title; (degreeTitle), degree program; (degreeProgram), candidate name; (candidateName), recent **blockchain** timestamp, [go]; HEC accumulation and accreditation contract address (aacAddress), degree registrar; (degreeReg), degree counter (degreeCoun); HEC Engineer authorized degreeReg individual and set of authorization and Also, responsible to maintain address of degree registrar in the contract; **if** int main.x = true **then** **if** degreeNumber is not in the contract **then** state of the contract changes and add new details record degreeNumber, degreeTitle, degreeProgram, candidateName, **blockchain** timestamp [go], and aacAddress; degreeCoun +1 by a count; **else** State and Rollback, end; **else** State and Rollback, end;
Contract 2: HEC Accumulation and Accreditation Contract (addAccrediation()).
Contact Initialization: HEC Engineer Initiate Transactions **Data:** The Distributed System Addresses Manages by HEC Engineer int main: x [file], Accreditation id (accredID), accreditation program; access (accredProgram), current semester enrolment; **blockchain** timestamp, [go]; transaction of degree record update contract (TDRUC add); Accreditation Manager (AM)/HEC Engineers, HEC AAC count (AACCount); Accreditation Manager is a set of all authorized addresses of the HEC state-based sub-engineers **if** int main.x [file] is Accreditation Manager (true) **then** **if** accumulation and accreditation program has not existed **then;** Accumulator and Accreditation Contract state is distinct or changed allow to add new records: accredID, accredProgram, current semester enrolment, int main.x, Add on TDRUC to the blockchain; AACCount + 1; **else** State and Rollback, end; **else** State and Rollback, end;

Table A1. *Cont.*

Contract 3: Transaction of Degree Record Update Contract (updatetrans())
Contact Initialization: HEC Engineer Initiates Nodes Transactions **Data:** HEC Engineer Maintain System and their Addresses int main: x [file], assignee address (assignee), present; **blockchain** timestamp [go], present transaction (presentTrans); past transaction (pastTrans), HEC Engineers; HECE, transaction calculate (transCalc) HECE is a set of all authorize contract and also, responsible to managed contract transaction; **if** int main.x [file] is = HECE (true), **then** **if** check pastTrans has true in the blockchain, **then;** AAC state is updated to assignee and add new addresses, Also, TDEUC updated new records addresses accordingly: such as, assignee(), presentTrans(), blockchain timestamp[go], pastTrans(), and transCalc() **else** State and Rollback, end; **else** **S**tate and Rollback end;
Contract 4: Hash Re-Encryption and Privacy Measurement (reEncrypt())
Contact Initialization: HEC Engineer Generate Privacy Re-Encryption Mechanism **Data:** HEC Engineer also Initiates System and manages Addresses int main: x [file], HEC uses encryption symmetric to encrypt information gets (encryptedInformation); HEC uses public symmetric for a candidate degree submission to encrypt credentials, gets (encryptedInformationOfCandidate); Stakeholder requests for datafile, IPFS sends encrypted symmetric to HEC; **Then**, stakeholder uses private key for candidate's credentials to decrypt encrypted symmetric of HEC, gets (encryptedSymmetric); **Finally**, stakeholder uses encryptedSymmetric to decrypt candidate's credentials, gets (information).

References

1. Shi, N.; Tan, L.; Li, W.; Qi, X.; Yu, K. A blockchain-empowered AAA scheme in the large-scale HetNet. *Digit. Commun. Netw.* **2020**, *7*, 308–316. [CrossRef]
2. Capece, G.; Levialdi Ghiron, N.; Pasquale, F. Blockchain Technology: Redefining Trust for Digital Certificates. *Sustainability* **2020**, *12*, 8952. [CrossRef]
3. Turkanović, M.; Hölbl, M.; Košič, K.; Heričko, M.; Kamišalić, A. EduCTX: A blockchain-based higher education credit platform. *IEEE Access* **2018**, *6*, 5112–5127. [CrossRef]
4. Feng, W.; Li, Y.; Yang, X.; Yan, Z.; Chen, L. Blockchain-based data transmission control for Tactical Data Link. *Digit. Commun. Netw.* **2020**, *7*, 285–294. [CrossRef]
5. Lutfiani, N.; Aini, Q.; Ali, M.I.; Wijayanti, L.; Nabila, E.A. Transformation of Blockchain and Opportunities for Education 4.0. *Int. J. Educ. Learn.* **2021**, 3.
6. Aamir, M.; Qureshi, R.; Khan, F.A.; Huzaifa, M. Blockchain Based Academic Records Verification in Smart Cities. *Wirel. Pers. Commun.* **2020**, *113*, 1397–1406. [CrossRef]
7. Song, J.; Zhang, P.; Alkubati, M.; Bao, Y.; Yu, G. Research advances on blockchain-as-a-service: Architectures, applications and challenges. *Digit. Commun. Netw.* **2021**. [CrossRef]
8. Graf, M.; Küsters, R.; Rausch, D. Accountability in a Permissioned Blockchain: Formal Analysis of Hyperledger Fabric. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy (EuroS&P), Genoa, Italy, 7–11 September 2020; pp. 236–255.

9. Peng, L.; Feng, W.; Yan, Z.; Li, Y.; Zhou, X.; Shimizu, S. Privacy preservation in permissionless blockchain: A survey. *Digit. Commun. Netw.* **2020**, *7*, 295–307. [CrossRef]
10. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2019**, *100*, 143–174. [CrossRef]
11. Quiniou, M. *Blockchain: The Advent of Disintermediation*; John Wiley & Sons: Hoboken, NJ, USA, 2019.
12. Sunyaev, A. Distributed ledger technology. In *Internet Computing*; Springer: Cham, Switzerland, 2020; pp. 265–299.
13. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R. A systematic literature review of blockchain cyber security. *Digit. Commun. Netw.* **2020**, *6*, 147–156. [CrossRef]
14. Härer, F.; Fill, H.G. Decentralized attestation of conceptual models using the Ethereum blockchain. In Proceedings of the 2019 IEEE 21st Conference on Business Informatics (CBI), Moscow, Russia, 15–17 July 2019; Volume 1, pp. 104–113.
15. Bhumichitr, K.; Channarukul, S. AcaChain: Academic Credential Attestation System using Blockchain. In Proceedings of the 11th International Conference on Advances in Information Technology, Bangkok Thailand, 1–3 July 2020; pp. 1–8.
16. Aydar, M.; Ayvaz, S. Towards a Blockchain based digital identity verification, record attestation and record sharing system. *arXiv* **2019**, arXiv:1906.09791.
17. Nokiti, A.E.; Yusof, S.A.M. Exploring the Perceptions of Applying Blockchain Technology in the Higher Education Institutes in the UAE. *Multidiscip. Digit. Publ. Inst. Proc.* **2019**, *28*, 8. [CrossRef]
18. Kamišalić, A.; Turkanović, M.; Mrdović, S.; Heričko, M.A.; Turkanović, M.; Mrdović, S.; Heričko, M. A preliminary review of blockchain-based solutions in higher education. In *International Workshop on Learning Technology for Education in Cloud*; Springer: Cham, Switzerland, 2019; pp. 114–124.
19. Palma, L.M.; Vigil, M.A.; Pereira, F.L.; Martina, J.E. Blockchain and smart contracts for higher education registry in Brazil. *Int. J. Netw. Manag.* **2019**, *29*, e2061. [CrossRef]
20. Fedorova, E.P.; Skobleva, E.I. Application of Blockchain Technology in Higher Education. *Eur. J. Contemp. Educ.* **2020**, *9*, 552–571.
21. 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]
22. Tariq, A.; Haq, H.B.; Ali, S.T. Cerberus: A blockchain-based accreditation and degree verification system. *arXiv* **2019**, arXiv:1912.06812.
23. Saleh, O.S.; Ghazali, O.; Rana, M.E. Blockchain based framework for educational certificates verification. In *Studies, Planning and Follow-up Directorate*; Ministry of Higher Education and Scientific Research: Baghdad, Iraq; School of Computing, University Utara Malaysia: Kedah, Malaysia, 2020.
24. Ghaffar, A.; Hussain, M. BCEAP-A Blockchain Embedded Academic Paradigm to Augment Legacy Education through Application. In Proceedings of the 3rd International Conference on Future Networks and Distributed Systems, Paris, France, 1–2 July 2019; pp. 1–11.
25. Serranito, D.; Vasconcelos, A.; Guerreiro, S.; Correia, M. Blockchain ecosystem for verifiable qualifications. In Proceedings of the 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 28–30 September 2020; pp. 192–199.
26. Rahardja, U.; Hidayanto, A.N.; Hariguna, T.; Aini, Q. Design Framework on Tertiary Education System in Indonesia Using Blockchain Technology. In Proceedings of the 2019 7th International Conference on Cyber and IT Service Management (CITSM), Jakarta, Indonesia, 6–8 November 2019; Volume 7, pp. 1–4.
27. Uddin, M. Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. *Int. J. Pharm.* **2021**, *597*, 120235. [CrossRef]
28. Xu, X.; Weber, I.; Staples, M. *Architecture for Blockchain Applications*; Springer: Cham, Switzerland, 2019; pp. 1–307.
29. Zhang, R.; Xue, R.; Liu, L. Security and privacy on blockchain. *ACM Comput. Surv.* **2019**, *52*, 1–34. [CrossRef]
30. Mohanta, B.K.; Jena, D.; Panda, S.S.; Sobhanayak, S. Blockchain technology: A survey on applications and security privacy challenges. *Internet Things* **2019**, *8*, 100107. [CrossRef]
31. Dhillon, V.; Metcalf, D.; Hooper, M. The hyperledger project. In *Blockchain Enabled Applications*; Apress: Berkeley, CA, USA, 2017; pp. 139–149.
32. Xu, X.; Sun, G.; Luo, L.; Cao, H.; Yu, H.; Vasilakos, A.V. Latency performance modeling and analysis for hyperledger fabric blockchain network. *Inf. Process. Manag.* **2021**, *58*, 102436. [CrossRef]
33. Ampel, B.; Patton, M.; Chen, H. Performance modeling of hyperledger sawtooth blockchain. In Proceedings of the 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), Shenzhen, China, 1–3 July 2019; pp. 59–61.
34. Bhattacharya, M.P.; Zavarsky, P.; Butakov, S. Enhancing the Security and Privacy of Self-Sovereign Identities on Hyperledger Indy Blockchain. In Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 20–22 October 2020; pp. 1–7.
35. Turkanović, M.; Podgorelec, B. Signing Blockchain Transactions Using Qualified Certificates. *IEEE Internet Comput.* **2020**, *24*, 37–43. [CrossRef]
36. Elrom, E. Hyperledger. In *The Blockchain Developer*; Apress: Berkeley, CA, USA, 2019; pp. 299–348.
37. Vlachou, V.; Kontzinos, C.; Markaki, O.; Kokkinakos, P.; Karakolis, V.; Psarras, J. Leveraging Hyperledger Iroha for the Issuance and Verification of Higher-Education Certificates. *Int. J. Educ. Pedagog. Sci.* **2020**, *14*, 755–763.

38. Gorenflo, C.; Lee, S.; Golab, L.; Keshav, S. Fastfabric: Scaling hyperledger fabric to 20,000 transactions per second. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Atlanta, GA, USA, 14–17 July 2019; pp. 455–463.
39. Andola, N.; Gogoi, M.; Venkatesan, S.; Verma, S. Vulnerabilities on hyperledger fabric. *Pervasive Mob. Comput.* **2019**, *59*, 101050. [CrossRef]
40. Lu, N.; Zhang, Y.; Shi, W.; Kumari, S.; Choo, K.K.R. A secure and scalable data integrity auditing scheme based on hyperledger fabric. *Comput. Secur.* **2020**, *92*, 101741. [CrossRef]
41. Benhamouda, F.; Halevi, S.; Halevi, T. Supporting private data on hyperledger fabric with secure multiparty computation. *IBM J. Res. Dev.* **2019**, *63*, 3:1–3:8. [CrossRef]
42. Chen, W.-K. *Linear Networks and Systems*; Wadsworth: Belmont, CA, USA, 1993; pp. 123–135.
43. Khan, A.A.; Uddin, M.; Shaikh, A.; Laghari, A.A.; Rajput, A. MF-Ledger: Blockchain Hyperledger Sawtooth-enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture. *IEEE Access* **2021**, *9*, 103637–103650. [CrossRef]
44. 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 Process.* **2021**. [CrossRef]
45. Khan, A.A.; Laghari, A.A.; Awan, S.; Jumani, A.K. Fourth Industrial Revolution Application: Network Forensics Cloud Security Issues. In *Security Issues and Privacy Concerns in Industry 4.0 Applications*; Wiley: Hoboken, NJ, USA, 2021; pp. 15–33.