International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 17 • Issue 2 pp. 142-154 March 2026-Sept 2026 www.csjournals.com

Blockchain for Student Credential Verifier: Blockchain diplomas for tamper-proof verification

Amarjeet Singh[1], Dr. Sneha[2], Dr. Anupam Bhatia[3]
[1]MCA Student, [2]Asst. Prof., [3]Associate Professor
Deptt. of Comp. Sc. and Application, Chaudhary Ranbir Singh University, Jind, Haryana, India

Abstract: Certificates of college and university graduations comprise the most crucial credentials to the graduates since they are a manner of certifying their qualifications and serve in applications for jobs or other connected pursuits. In spite of the developments in technology and availability of quality office supplies making it easy to fake identification cards, passports, and certificates, the old techniques of certifying credentials continue to be expensive and arduous. The objective of this study is to construct a theory that gives a practical manner of academic credentialing and certification through the usage of block chain technology. Cryptography is made up of digital digital networks, digital networks. These components are used in this theoretical model to create two basic processes: the digitally signed certificate issuance process and the academic certificate validation process. This idea highlights how blockchain technology can be used to authenticate academic credentials and meet all the requirements of verification process innovation.

Index Terms: Education, Blockchain Technology, Graduation Certificate Authentication, Verification, Forgery truly.

1.Introduction

Those students who satisfy the requirements for graduation get graduation certificates issued by their educational institutions. Due to the fact that electronic documents do not completely replace physical certificates, the latter are usually issued on paper. But thanks to the widespread availability of inexpensive yet sophisticated scanning and printing technologies, certificate fraud has become more common nowadays, posing a threat to the credibility of both the graduate and the university itself. Thus, it has become necessary to check and verify documents. It is crucial to check whether the person is a legal owner of the certificate, and whether the document is genuine. Moreover, the document should be validated to check its content and prove its trustworthy source.To prevent fraud and forgery, different approaches have been applied at educational institutions; however, all of them have a manual character and take too much time. The verification of certificates requires communication with institutions and takes time, which means high cost of this process, especially in case of checking of numerous candidates. Therefore, the current research aims at creating theoretical model for blockchain academic degree verification.

As a result of online education, technology accessibility, and technology dependency, it is important to develop resource management systems and reduce cases of abuse and mismanagement. New technologies and changes in the mode of studying have put pressure on teachers and students. Technologies like blockchain technology, augmented and virtual reality, online learning, artificial intelligence, and instructional robotics are being used to enhance teaching and learning processes.The main features of blockchain technology are transparency of transaction, secure transaction, distributed ledger, using blocks and chain, encryption, and decentralized system,

whereby multiple nodes verify transactions. This has revolutionized the way security and trust were viewed in online transactions.The application of blockchain technology extends beyond the use of cryptocurrencies, and it is now being used in such diverse areas as supply chains, digital assets management, digital identification, smart contracts, electronic voting, and property registration. Due to this wide range of applications, blockchain is considered to be an emerging technology with shifting boundaries. The coronavirus pandemic has greatly affected education, and the blockchain technology has great promise in revolutionizing several human activities including education.

1.1Falsecertificates-A problem

The importance of academic certifications cannot be underestimated, as they represent the human capital possessed by people skills, knowledge, competences, and abilities acquired through studying. Academic certifications play an important role in the hiring process because they are able to represent skills, reliability, devotion, and knowledge rather than experience of candidates. Grolleau [9] states that 300 unaccredited institutions exist in the United States, and there are around 2 million counterfeit degrees. There are more fraudulent institutions in the United States than in any other country, and in the United Kingdom there are approximately 270 institutions [10]. It has been proved by the research carried out by Helay [11] that 35% of applicants in Australia lie about their academic records. According to the Association of Certified Fraud Examiners, 41% of applicants forge certificates each year. The Wall Street Journal claims that 34% of applicants provide inaccurate data about their certificates and education [12]. Surveys prove that almost all applicants tend to lie about some aspect of skills or education. Certificate frauds cause employers to lose $600 billion per year [13].

There are five major sources of academic certificates fakes:

- Degree Mills – entities which manufacture counterfeit credentials.
- Fabricated Documents - fake documents which pretend to be issued based on a fake degree or educational institution.
- Modified Documents - counterfeit documents based on original one; modifications may include changes in personal data such as student's name, date of birth, speciality, courses taken, grades, attendance and graduation dates.
- In-House Produced fakes - printed on original paper with official seals and signatures by employees of corresponding educational institutions.

Incorrectly translated documents in order to comply with the requirements of receiving country.
Without having a degree, obtaining a white collar job would be problematic. In case of application for any kind of job position, employer expects candidates to prove their academic credentials. The candidate is required to wait for his/her degree to be confirmed by the issuing educational institution. This process may take several days or even several weeks. Employers need to spend their precious time on document verification to make sure the right candidates would be hired. Although it takes some time, verification of documents is essential stage in checking the genuineness of the applicants for jobs, education or visas.

1.2 Limitations of traditional verification system

This part identifies the disadvantages of the current verification process. The process does not ensure tampering, authentication, sealing, and securing of the records. As per the authors [2], there are five major disadvantages of verification, namely ownership, availability, third-party involvement, time-consuming process, and cost. The description of each disadvantage is provided below:

Ownership: Although the certificates are issued to an individual and belong to him/her, the agency which issues these certificates still requires certification or issuance of new certificates. The certificate owners do not necessarily hold all the rights to ownership automatically.

• Availability: Individuals may not be able to obtain paper-based certificates due to their vulnerability to losses and damages. Additionally, in case, unbusiness, records, business, body, records, body, going out of business, going out of business.

• Third-party involvement: Several organizations rely upon third-party verification agencies which contact issuing entities and check the papers.

Time depends on the time as the time consuming authorities's efficiency.

• Cost: Verification and notarization are expensive, and each confirmed document has a cost associated with it.

2.Need of Blockchain

The blockchain technology offers a fast way of transferring data. Since data has been entered into the blockchain, it cannot be modified by any user. The process is faster than conventional banking since there is no need for a third party. Issues affecting the process can be easily traced to their roots for investigation purposes. There are smart contracts within the blockchain that increase consumer confidence. The use of cryptocurrencies in the blockchain reduces costs, increases speed, and enhances security [14]. Apart from enhancing the security of the information, the blockchain can notify the user if his or her information has been changed. Every transaction in the blockchain is always signed digitally and timestamped for non-repudiation purposes.

2.1 Blockchain's relevance to education

The education and health care industries run the highest risks of data breach as they store a vast volume of confidential information that can be exploited by hackers. Given that there are always new types of attacks created every day, it is very important to stay up-to-date in terms of security. Much of the data in the education industry including diplomas and students' records is saved either in the cloud or locally on hard drives. The former is costly and the latter is vulnerable to destruction. Hackers have no problem forging the data, selling it on the dark web and using it for identity theft. Blockchain provides better security as it has features like decentralization, immutability, anonymity, redundancy and faster transaction settlement [8].Blockchain allows performing a direct verification of certificates, bypassing the intermediary. While this procedure is viewed as rather complicated in most countries, blockchain allows validating the accreditation of educational establishments. According to the research conducted by Ghazali and Saleh, there is a Graduation Certificate Verification model based on digital signature that enables verifying certificates without the involvement of universities physically. However, this model does not use smart contract which would make things easier. It is likely that the cryptocurrencies can be used to pay for education expenses which include salaries, scholarships, and tuition fees and are processed via blockchain-based smart contracts. King’s College from New York became the first institution of education to use payments in Bitcoin. The University of the University of the University of the University of the University of MIT. Even if there have been a number of obstacles, there have been a number of obstacles16]. Although there have been many advancements in blockchain usage in education field, there are several obstacles.

2.2 The principal technologies of a blockchain

Blockchain technology is a combination of various features, such as digital signatures, hashing technique, peer-to-peer network, public and private key cryptography, and proof-of-work protocol. The

International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 17 • Issue 2 pp. 142-154 March 2026-Sept 2026 www.csjournals.com

following are the explanations of these technologies one by one

Hash: Hash is defined as a short code that is produced after the input data from a particular document is passed through a hash function. Hashing will yield a unique code, which is of a certain length. Whenever the same input data is fed into the hashing machine, it will always produce the same output. It is, however, worth noting that any variation in the input data, even if just one letter, will produce an entirely different hash.

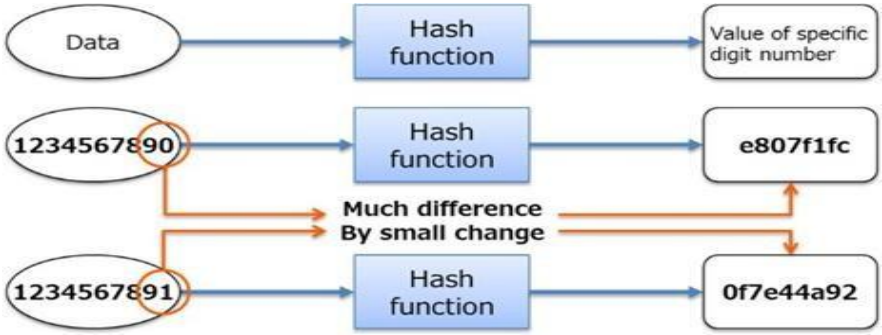

FIGURE1: The hash generator

In Figure1 illustrate show even a slight alteration to the data input can yield are mark ably distinct hash. This feature of a hash can be used to identify any data falsification and is employed as an authentication technique in blockchain systems.

Public and Private Keys: The block is the logic foundation of this particular property of the logic underpinning of this particular property of this particular property. Figure 2 is a public block This is a public key that is used by the public key that can be used by the public key that can be used by the public key that can be used by the owner of the public key. In contrast to symmetric key cryptography which utilizes one and the same key for encryption and decryption, this approach presupposes security of the channel of communication of the message to its destination. Security of file transfer using public-key cryptography becomes achievable only if the entity responsible for certification produces two keys, public and private and gives out the public one to the sender in advance [17].

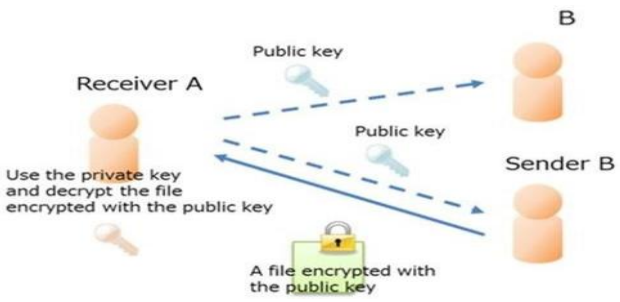

FIGURE2: The public key encryption

Digital Signatures : The digital signatures mechanism, which allows one to verify the accuracy of the given data, is developed using both hashing and public key cryptography techniques. A digital signature is created through encryption of the hash function of the file using the private key of the sender and the

transmission of both of them to the recipient. The calculated by received by the received by the received by the received by the recipient. Then, at the level of verification, the public key of the sender is used to decrypt the digital signature and extract the hash function of the sender. If these hash functions match, then the digital signature turns out to be genuine.

.

Peer-to-peer (P2P) networks: Peer-to-peer (P2P) networks are computer or network architectures that enable peers to share workloads, files, or tasks. This network contains all nodes that form the network, and nodes can be regarded as peers that have the same rights and abilities within the network [18].

2.3 Potential of blockchain technology

The blockchain technology is capable of doing away with the use of traditional paper-based certificate issuing. The ease of forgery in issuing digital certificates has prevented their wider usage in the past. Nevertheless, digital certificates issued using the blockchain technology are irreversible and always valid since the authenticity of the certificates can be validated using the blockchain. These benefits make digital certificates more preferable than the traditional process. Blockchain makes it unnecessary for educational institutions to validate documents manually; thus, they benefit from saving time. Blockchain is the contemporary method used in exchanging, certifying, and protecting academic achievements. PKI enables a decentralized system to replace centralized authority, making the network more resilient since the signatures will be stored on several copies of the blockchain [8]. Due to the decentralized nature of blockchain, external forces cannot tamper with the transactions stored in the blocks since they would also have to undo the proof of work made earlier in the validation process. An accurate timestamp is necessary to control the validity period of credentials. For securing the system from possible key compromise, issuers need to periodically renew their keys. Timestamps generated independently allow confirming whether the particular authority issued a record within the validity period of the key. The blockchain signature process does not depend on the type of the file, thus the same application can sign any document irrespective of its format [16].

3. Related Work

In the era of digitization, there are many challenges faced by the education sector, one of which is forgery of the certificate by the user itself. There is also the challenge of counterfeit certificates available online. The researchers, Park et al., [8], did an extensive analysis on this matter and showed that online certificates are printed or computerized in such a way that data can be accessed and changed when it is being printed. The techniques for creating counterfeit certificates include memory hacking, API hooking, and ActiveX hooking, all researched by Park et al. [8]. Digital certificates are also subject to forgery. Verification and validation of digital certificates using blockchain technology is suggested to overcome this challenge. Similarly, limitations of verification processes like problems regarding certificate ownership, availability, costly verification process, and time-consuming verification process have been discussed by Nargis, Tanzila, et al. [20]. Technological advancement has provided an easy method of making and sharing digital copies of educational material without permission from its owner. Though the use of the content is allowed under the law, educational organizations are using more digital content created by the owner of those rights.

TABLE 1. A Thorough Analysis Of Previous Studies Based On A Blockchain Technology Parameter {R1: Smart ContractsR2: Digital Currency/Ethereum R3:SafetyR4: Danger,SHA-256IsR5. R6:ApplicationsR7: Restrictions R8: Verification And Management Of IdentityR9: Consensus, Denotes Null Conversations.

Authors	Key contribution	R1	R2	R3	R4	R5	R6	R7	R8	R9
Gururaj, H.L.et al[7]	Blockchain: A New Era of Technology	----	----	R3	R4	----	-----	---	R8	R9
Steiu , Mar a-Florina[6]	Blockchain in education: Opportunities, applications, and challenges	R1	R2	R3	-----	R5	R6	---	----	----
Ali, Sura Moham m - ed et al[4]	A blockchain-based models for student information systems	R1	----	----	R4	R5	-----	---	R8	----
Kutt y, Rida Javed[19]	Secure Blockchain for Admission Processing in Educational Institution	----	----	-----	-----	R5	-----	---	R8	----
Gaikwad, Hrithik et al[16]	A Blockchain-Based Verification System for Academic Certificates	R1	----	R3	------	----	R6	---	R8	----
Park,Jae et al[8]	Promises and challenges of Blockchain in Education	----	----	R3	------		R6	---	----	----
Zheng, Zibin[15]	An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends	----	----	R3	R4	---	R6	R7	----	----
Chen, Guang et al[15]	Exploring blockchain technology and its potential applications for education	----	----	R3	------	----	R6	---	----	----
Bhashk er et al[17]	Blockchain in education management: present and future applications	----	R2	R3	R4	----	-----	---	----	----
Nargis, Tanzila et al[20]	Secure Platform for Storing, Generating and Verifying Degree Certificates using Blockchain	R1	R2	-----	------	R5	-----	---	R8	R9

International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 17 • Issue 2 pp. 142-154 March 2026-Sept 2026 www.csjournals.com

Some of the attributes of blockchain technology include privacy, integrity, auditability, public verifiability, persistence, anonymity, and trust anchoring. Some of the problems associated with blockchain technology include high cost of setting up, huge energy requirements to solve puzzle, need for validation and verification, complexity, privacy issues, lack of scalability, and human errors. Ishaani Priyadarshini explains how blockchain technology can be used in big data analytics, banking, and many other applications, as well as fight against crime. According to the comparative analysis of blockchain and conventional databases carried out by Bhashker et al., [17], the former is more advantageous if trust, robustness, and data provenance are very important factors. Personal and confidential information becomes vulnerable to exploitation when it is with unauthorized persons. Blockchain technology's decentralized system, immutability, and encryption & hashing makes it secure. Furthermore, blockchain-based smart contracts aid in building trust among the parties. Park et al. [8] have studied the application of blockchain and smart contracts in different industries like healthcare, supply chain, automotive, and business. Even though blockchain technology is more secure than the conventional systems, Kutty and Rida Javed [19] recognize that there are various security issues with it.Table 1 presents a detailed comparison of previous studies based on metrics related to blockchain technology.

4. Proposed Model For Graduation Certificate Verification

There have been many expansions within the universities over time due to the increased number of faculties, students, and associated institutions. The management of the large number of students and graduates has increasingly become difficult, leading to problems within the running of the university. It has progressively led to reduced levels of service offered to the students and the graduates. Some of the reasons why there have been challenges in terms of operational efficiency include the verification of academic documents. The approach that will be taken in this case, which is depicted in Figure 3, entails using blockchain technology to verify graduation certificates.

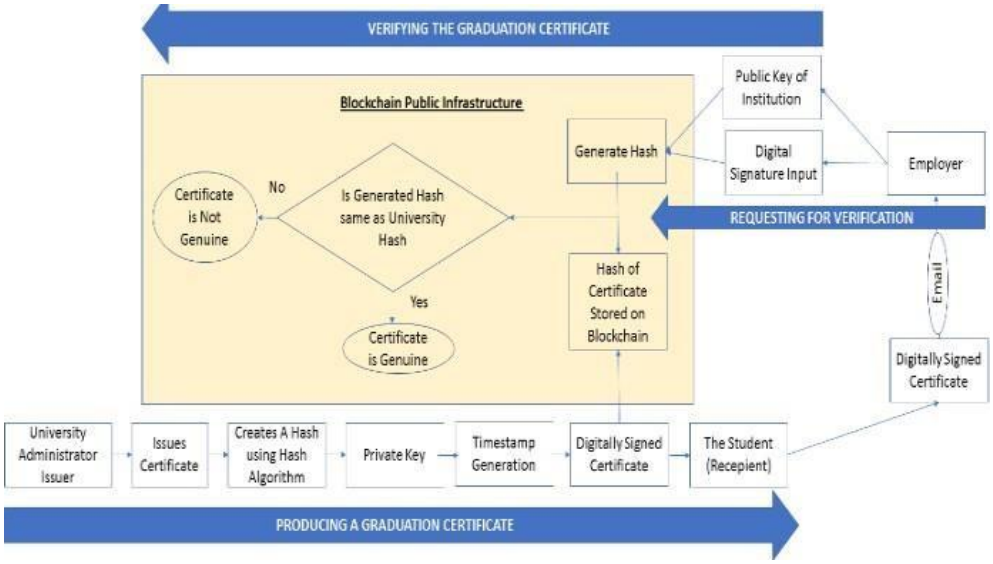

FIGURE3: Blockchain-basedmodelforgraduationcertificateverification

4.1 Discussion

Academic credentials are required by firms for offering white-collar jobs because they have to be shown to prove qualifications for recent graduates. The colleges validate the qualifications of students before they receive their certificates; however, the process takes days or even weeks. The companies spend considerable time cooperating with colleges to verify credentials in order to recruit the most qualified employee. Document verification is indeed a troublesome procedure; however, it is an important procedure that ensures that the candidate is legitimate for employment, education, or obtaining a visa. Blockchain is a new approach that allows simplifying the process of academic credential validation both for employers and applicants. Using the technology, people are able to share cryptographically signed documents, including academic degrees, thus facilitating the work of hiring or admission processes. For this purpose, it is necessary for the relevant authorities who issue the digital credentials to connect them to the blockchain system and save using one-way hash coding [19].The employer can get access to academic credentials and documents provided by educational institutions through the blockchain system when the candidate gives them the permission. This way, the institution where the graduate studied should get its public key from the person.

4.2 Analysis Of The Proposed Solution

The blockchain is an integration of a number of concepts already mentioned above including hashing, digital signatures, peer-to-peer networking, cryptography based on public and private keys, and proof of work. In this research, these elements are classified into two categories which involve issuance of a digitally signed academic certificate and its authentication. A conceptual diagram is presented in Figure 3.

- *Producing the Academic Certificate with Digital Signature:* According to research findings, the task of digitally signing academic credentials belongs mainly to the educational institution. This is demonstrated in Figure 3 through the use of the following blockchain technologies.
- *Hashing:* According to this study, you can generate the SHA-256 hash of any string of data using an open-source web application called the SHA-256 hash generator. It also produces hashes with consistency.
- *Public and Private Keys:* Both public and private keys are used in the model this study proposes. The university receives the public key. After that, the student receives a private key from the institution that needs to be kept a secret.
- *Digital signatures:* A digital signature scheme has been designed by applying the concepts of hashing and public key encryption to ensure the legitimacy of transmitted data on the Internet. From the study results, the procedure entails encrypting the hash value of the file using the sender's private key before the transmission to the receiver [7]. The file itself is also transmitted to the receiver via the Internet. The receiver creates the hash value from the received file contents. This enables the receiver to retrieve the original hash value through decryption of the digital signature using the sender's public key.
- *Timestamping:* Thus, digital academic certificates become safer. In this technology, digital timestamping technology is applied for the creation of the document, where the exact date, month, and year of issuance are recorded using peer-to-peer network technology. The process of creating the digital timestamp and digital certificate becomes encrypted in blocks and turns into the unique code denoting the date of document issuance.

- *Signing The Document Digitally:* The digital signature created by the model consists of four important parts: the time stamp, which gives the exact time when the certificate was created, the public key, the private key, and the hash value generated by hashing process. All these elements make up a special digital signature that is used to sign the document. The use of the timestamp, keys and hash function makes the process of signing the document safe and authentic. As the consequence, every digital signature is uniquely connected to its own document and it can be opened by the student's private key only. It is impossible to reverse engineer the digital signature and receive the private key from it. Moreover, any change in the document's content will lead to the generation of another hash value.

- *Issuing and Hosting the Certificate:* The educational institution ensures that each student receives not only the physical copy of their academic certificate but also a digitally signed one. This digital certificate then undergoes a process of hash generation, which results in an unique alphanumeric hash code[23]. The reason for doing so is that the information included in the certificate cannot be changed and remains secure. Next, a transaction entry is made with the use of the private key of the university and the generated hash, which is placed in the blockchain.
- *Confirming the Academic Credential:* Once a student (second party) makes an application for job, the third party, i.e., the employer verifies the validity of the educational qualification provided by the university (first party). The steps involved in this process are illustrated in Table 2 below for verification and validation of the digital signature of the certificate.

TABLE2: Issuingadigitallysigneddocument

Step no	Particulars
1.	Public keys of educational institutes are widely available on the internet or in public directories. Additionally, the graduates may give them to the employer.
2.	Toscanandenterthedigitallysigneddocumentandpublickey,theemployeremploys Verification software.
3.	Thepublickeyandthedigitallysigneddocumentarescannedandenteredbytheemplo yer Using verification software.
4.	Thedigitalsignatureandthepublickeyareusedbytheverificationsoftwaretocreateah ash
5.	Theoriginalcertifiedcopy'shashandthehashproducedbytheverificationsoftwarear e compared. Additionally, the verification software looks for a connection between the digital signature and the school's public key.
6.	Studentsareabletocompletebothphaseswithouthavingtorevealtheirprivatekeys.
7.	Theresultproducedbytheverificationsoftwarenotifiesthepotentialemployerthatth e Certificate is legitimate if both conditions are met.
8.	Shouldoneorbothoftheconditionsbeuntrue,theverificationsoftwaregeneratesano utput Alerting the potential employer to the phony nature of the certificate

Blockchain technology can further enhance the existing digital certification framework by

facilitating certificate issue and validation without any intermediaries. Using blockchain notarization, privately issued student certificates will be immutable and verifiable. Such certificates will be available for validation by authorized third parties via a public blockchain whereas certification metadata will be confidential for public validation [1].Students will be able to keep private details private while giving their credentials to employers and schools. The third parties will have access to only such data as they share during the process of validation. Blockchain certification will combine the efforts of the academic community and real-world implementation of the idea. One of the problems faced by university admission offices include fake payments and altered student records of foreign applicants[22]. Sometimes centralized authorities are used as a part of a solution to add credibility to credentials. However, for a certificate to be credible, it should be accepted by an independent verifier[21].Two criteria should be met in order to validate a certificate – these are authenticity and integrity [3]. Authenticity is proof of the fact that the certificate is issued by the legitimate entity whereas integrity is unaltered nature of the content, identity, etc. It also demands that the person who issued the certificate be the issuer.

4.3 Benefit of proposed model

This section will address the advantages of using the suggested model for issuing parties, beneficiaries, and customers. The advantages of using the suggested model are listed below for each of the mentioned parties.

Granting Benefits to Authorities

- Information that is cryptographically secure and immutable is only revealed.
- Every document can be stored safely and accessed promptly.
- No extra time is needed to deliver official documents to certain people.
- The records can be verified right away without relying on the authority that issued them.
- Official documents can be owned, managed, and delivered easily.
- As every transaction is registered on the blockchain, the records stay saved and cannot be lost.
- Other parties can access and verify the records anytime they want.
- No need for separate requests to get rid of the old or wrong certificates.

Advantages for Recipients and Customers

- *Encryption makes it possible to exchange and own information safely.*
- *All the documentation is stored in one electronic wallet.*
- *Verified information can be accessed quickly without any delays.*

- *Information can be instantly validated without any need to depend on the source of issuance.*
- *Verification systems will be accessible by employers and verification companies when necessary.*
- *Blockchain technology guarantees that the information is safe and nothing can be lost.*
- *Certificates are always available, and records can be updated or verified anytime.*
- *The integrated system allows verification of records based on the latest version of information.*

5. Implication of the Findings

The following table outlines the impacts that are expected from the use of this blockchain-based verification system for graduation certificates, taking into account the provided document and its context.

TABLE3: Implications of findings in blockchain technology for document verification in education sector

Implications	**Explanation**
Security	Academic certifications can be securely stored and verified on blockchain, lowering the possibility of fraud and unauthorized changes.
Efficiency	The use of blockchain technology stream lines the verification process, making it faster and less labor-intensive compared to traditional methods.
Decentralization	The decentralized storage of certificates reduces dependency on a central authority and boosts stakeholder trust.
Transparency	The transparent nature of blockchain ensures that all transactions and changes are visible and traceable, enhancing accountability.
Verification	Blockchain-based certificates can be easily verified world wide, facilitating international mobility and recognition of academic credentials.
Global Recognition	Blockchain-based certificates can be easily verified world wide, facilitating international mobility and recognition of academic credentials.

6. Conclusion and Future Work

In this research work, the blockchain based model was introduced to verify the academic certificate. The proposed approach was designed in such a way to minimize the possibility of forgery as well as improve the security, validity and privacy of academic credentials. The proposed framework possesses a number of advantages for issuing authority, the owner and final consumer of the certificate. First, all required information about certificate authentication and verification is recorded on the blockchain network. Therefore, verification is done independently without communication with the issuing authority. It is achieved due to comparison of digital signature hash with the university verification key. The certificate is considered valid when both the keys match. With respect to further development, the proposed framework should be implemented in selected educational organizations followed by its extension using smart contracts.

References

1. R. D. SanjekarandB. M. Patil,“ Securing EducationalDocument Using Blockchain & IPFS, ”vol. 20,no. 9, pp. 3246–3251, 2020.
2. D.Serranito,A.Vasconcelos,S.Guerreiro,andM.Correia,“BlockchainEcosystemforVerifiableQualifications,”*20202ndConf.BlockchainRes.Appl.Innov. NetworksServ.BRAINS2020*, pp.192-199, 2020.
3. H. Li andD. Han,“EduRSS: A Blockchain-Based Educational RecordsSecure StorageandSharing Scheme,” *IEEE Access*, vol. 7, pp. 179273–179289, 2019.
4. S.I.M.Ali,H.Farouk,andH.Sharaf,“A blockchain-based models for student information systems,” *Egypt. Informatics J.*, vol. 23, no. 2, pp. 187–196, 2022.
5. E.KARATAŞ,“DevelopingEthereumBlockchain-BasedDocumentVerificationSmartContractfor Moodle Learning Management System,” *Bilişim Teknol. Derg.*, vol. 11, no. 4, pp. 399–406, 2018.
6. M.-F.Steiu,“Blockchainineducation:Opportunities,applications,andchallenges,” *First Monday* ,no. July, 2020.
7. H. L. Gururaj, A. Manoj Athreya, A. A. Kumar, A. M. Holla, S. M. Nagarajath, and V. Ravi Kumar, “Blockchain: A New Era of Technology,” *Crypto currencies Blockchain Technol.Appl.*,no.May2020,pp. 3–24, 2020.
8. J.Park,“PromisesandchallengesofBlockchainineducation,”*SmartLearn.Environ.*,vol.8,no.1,2021.
9. G. Grolleau,T. Lakhal,andN. Mzoughi,“ An introduction to the economics of fake degrees,” *J.Econ.Issues*, vol. 42, no. 3, pp. 673–694, 2008.
10. E.C.GARWE,“Qualification,AwardandRecognitionFraudinHigherEducationinZimbabwe,” *J.Stud.Educ.*, vol. 5, no. 2, p. 119, 2015.
11. P. Rani, R.K. Sachan, and S. Kukreja, *A systematic study on blockchain technology in education: initiatives, products, applications, benefits, challenges and research direction*, vol. 106, no. 2. Springer Vienna, 2024.
12. J. Rajendra,S.Kartiki,G.Vishal,andS.SKhatal,“Smart Contract for Educational Digital Certificate using Blockchain,” *Int. Res. J. Eng. Technol.*, no. May, pp. 795–800, 2020, [Online]. Available: www.irjet.net
13. W.Xie,“AnalysisoftheSituationofBlockchainCreditInvestigationanditsDevelopment,”vol.2,no.11, pp.37–39, 2022.
14. C.Reis-Marques,R.Figueiredo,andM.deC.Neto,“Applicationsofblockchaintechnologytohighereducationarena: A biblio metric analysis,” *Eur.J.Investig.Heal. Psychol.Educ.*,vol. 11,no.4,pp.1406–1421, 2021.
15. Z.Zheng,S.Xie,H.Dai,X.Chen,andH.Wang,“An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *Proc. - 2017 IEEE 6th Int. Congr. Big Data, Big Data Congr. 2017*, no. June, pp. 557–564, 2017.
16. H. Gaikwad, N. D’Souza, R. Gupta, and A. K. Tripathy, “A Blockchain-Based Verification System for AcademicCertificates,”*2021Int.Conf.Syst.Comput.Autom. Networking,ICSCAN2021*,pp.1–6,2021.
17. P.Bhaskar,C.K.Tiwari,andA.Joshi,“Blockchainineducationmanagement:presentandfutureapplications,”*Interact.Technol.SmartEduc.*,vol.18,no.1,pp.1–17,2020.
18. X.Chen, “Blockchain challenges and opportunities: a survey Zibin Zheng and Shao an XieHong-NingDai Huaimin Wang,” vol. 14, no. 4, pp. 352–375, 2018.
19. R.J.Kutty,“Secure Blockchain for Admission ProcessinginEducationalInstitutions,”pp.2021–2024, 2021.
20. T.Nargis,K.Preethi Salian,Prathyakshini,J.Vanajakshi, G.R. Manasa,andS.Salian,“A Secure

Platform for Storing, Generating and Verifying Degree Certificates using Blockchain," *7th Int. Conf. TrendsElectron. Informatics, ICOEI 2023 - Proc.*, no. Icoei, pp. 532–536, 2023.

21. Suman and A. Bhatia, "Unleashing the Potential: A Bibliometric Analysis of Blockchain Applications in Education (2016-2024)," *2024 4th Int. Conf. Adv. Electron. Commun. Eng. AECE 2024*, no. November 2024, pp. 887–892, 2024, doi: 10.1109/AECE62803.2024.10911681.
22. Suman and A. Bhatia, "Blockchain based graduation certificate verification framework: Ensuring security and authenticity in educational documents," *AIP Conf. Proc.*, vol. 3325, no. 1, 2025, doi: 10.1063/5.0291763.
23. S. Malik and A. Bhatia, "Blockchain technology for document verification in education : a bibliometric analysis and future research directions," 2025, doi: 10.1108/JM2-09-2025-0478.

International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 17 • Issue 2 pp. 142-154 March 2026-Sept 2026 www.csjournals.com