IJSRA

International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Research Article)

Check for updates

Innovative blockchain solutions for enhanced security and verifiability of academic credentials

Suhag Pandya *

Independent Researcher.

International Journal of Science and Research Archive, 2022, 06(01), 347-357

Publication history: Received on 26 May 2022; revised on 24 June 2022; accepted on 27 June 2022

Article DOI: https://doi.org/10.30574/ijsra.2022.6.1.0225

Abstract

The growing demand for secure and tamper-proof academic credential management has exposed the limitations of traditional systems, including susceptibility to fraud, inefficiency, and dependency on centralised authorities. Blockchain technology, with its decentralisation, immutability, and cryptographic security, offers a transformative approach to issuing, storing, and verifying academic credentials. This paper explores blockchain architectures—public, private, and consortium—and their application in academic systems. Applying smart contracts and decentralised architectures, blockchain improves trust and transparency and optimises credential checking. OpenCerts and eScroll are presented, referring to existing implementations, to demonstrate possibility and impact on the real world. The study outlines issues such as scale, privacy and interoperability Lastly, the study outlines directions for future research for enhanced blockchain use in managing academic credentials globally.

Keywords: Blockchain technology; Academic credentials; Credential management; Security and privacy; Credential Authentication

1. Introduction

The data in blockchain is located in a consensual and unalterable register, so blockchain can be helpful for safely processing academic records. Blockchain network enables credential owners to issue, read, verify and resume the credential stored on the distributed ledger and ensures that the data is accurate and immutable. The use of block technology ensures that once credentials recorded cannot be erased or altered, eliminating issues to do with manipulation and fabrication of documents. Blockchain technology is a system that provides the confirmation and safeguard of the records and enables the use of cryptographic techniques such as a digital signature and hash to enhance the validity of owners records.

Blockchain technology structures data into a linked chain of blocks[1]. Every block consists of a header (management information) and a body (transaction details), where academic credentials can be stored as verified records. A decentralised peer-to-peer network has nodes that approve transactions through digital signatures eliminating the need for an authority structure [2]. To maintain synchronization and integrity across a network, consensus protocols like PoW and PoS are employed.

The fundamental characteristics of blockchain technology, like immutability, transparency, decentralisation, and auditability, have attracted a lot of interest from academic systems. It enables institutions to securely award academic credentials while providing institutions, employers, and students easy means of verifying these credentials [3]. Further, blockchain eliminates cases of fake documents, builds confidence, and accelerates the confirmation of various certifications. Still, problems such as scalability, privacy, and integration must be solved in order to make such technologies accessible to anyone [4].

[*] Corresponding author: Suhag Pandya

In the context of academic credential management, blockchain is a transparent, immutable and decentralised database where educational providers can issue and verify unalterable certificates across their recipients without centralised bureaucratic entities [5]. All form of academic assets which are physical (e.g., diplomas, certificates) and non-physical (e.g., digital badges, micro-credentials) can be captured, monitored, and validated on the blockchain network. Lessening of expenditures and risks to all the stakeholders involved is coupled with the enhancement of academic record credibility, transparency and alterability [6].

1.1. Motivation of the study

The new cases of spitting on academic credentials and failures in formal methods of verification have imposed the need for a secure and efficient solution. Previous methods are easy to forge, lose or delay which causes mistrust among the educational institutions, employers and the students. The decentralised, immutable and transparent blockchain solution gives a chance to solve these challenges by storing and verifying the credentials on the blocks. The need to create novel blockchain solutions that improve the reliability and efficiency of the system by increasing the safety, authenticity, and auditability of academic credentials motivates this research.

1.2. Structure of the paper

The paper is structured as follows: Section II explains blockchain technology and its features. Section III discusses its applications and challenges in academic credential management. A survey of relevant research is presented in Section IV. Section V wraps up with important results and suggestions for further study.

2. Understanding blockchain technology

A number of loosely connected nodes could log transactions in the form of a decentralised, secure, and immutable ledger called a blockchain. They safeguard the identity and purity of the information; remove the middleman using crypto-technical procedures; and utilise consensus-basing techniques. Blockchain is a record of operations that can't be changed and can only be added to over time [7]. The chain grows in a safe way as more transactions are added, and the blocks within the chain are protected by cryptographic algorithms that make sure the details of the transactions are kept safe. Immutable records are the building blocks of the blockchain [8]. This verifies the accuracy of the data. The data on the blockchain is carried by several nodes in the network. Figure 1 illustrates the blockchain technology described below:

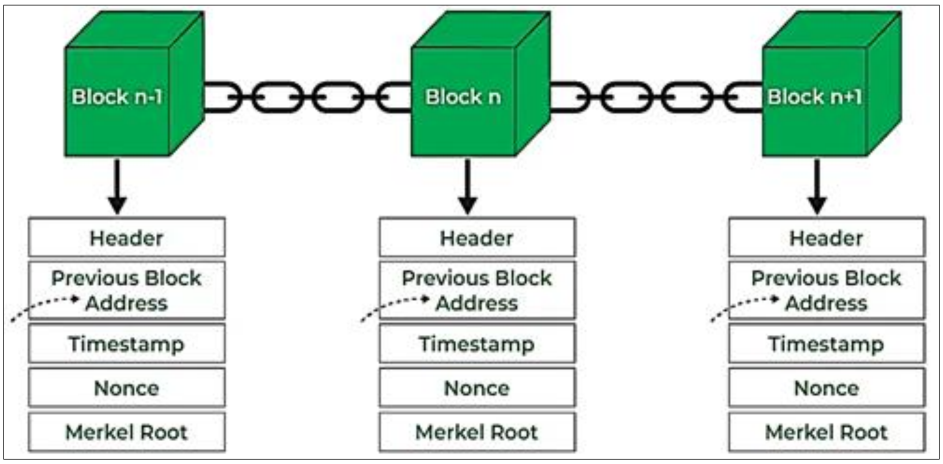

Figure 1 Blockchain Technology

Blockchain technology illustrates a blockchain structure in Figure 1, where blocks (Block n-1, Block n, Block n+1) are linked sequentially to form a chain. Every block contains a header that includes a previous block address (ensuring immutability), a timestamp (to record creation time), a nonce (used in mining for proof of work), and a Merkel Root (summarising all transactions in the block). The chaining mechanism ensures data integrity, as modifying one block would require altering all subsequent blocks, making blockchain tamper-resistant.

The blockchain is different from other technologies because it dates and timestamps the data records, which gives a full list of the blocks and their order. In addition to the hash value of the previous block's contents, each block also stores its own hash value [9]. This helps link the blocks in a chain. The addition of a new block to the blockchain is contingent upon the completion of a consensus procedure [10]. This consensus process has to decide who can join the chain and follow the rules for safely checking the blocks and making sure that the records are the same at all nodes in the network. Finally, the blockchain may be described as a distributed ledger that securely and verifiably records all financial transactions throughout a network [11]. A blockchain-based framework can handle security problems like people getting into data or transactions without permission, relying on a third party or central authority, and other participants not being trustworthy [12].

2.1. Key Features of Blockchain

Blockchain will provide a secure and reliable platform for the administration of academic records to some of the problems among them being fraud, inefficiency, and integrity of records. The following key features of blockchain make it particularly suitable for improving a security and verifiability of academic records:

- **Decentralization:** A blockchain transaction between any two entities or individuals is possible since no central authority is required for authentication [13]. As a result, blockchain technology has the potential to greatly cut server costs while also soothing central server performance concerns.
- **Persistency:** The system is almost impossible to manipulate since all transactions are recorded and confirmed in blocks distributed across the network [14].
- **Anonymity:** The blockchain network allows users to connect with one another using addresses. In addition, a person might create a flood of addresses to conceal their true identity [9]. It should be noted that only a small fraction of blockchain implementations provide anonymity. Their majority are pseudonymous.
- **Auditability:** Through the use of a timestamp and confirmation of each transaction, users are able to readily reach any node in the dispersed network to see and track previous records.

2.2. Blockchain architectures

Blockchain architecture is classified into three main categories: public, private, and consortium blockchains.

2.2.1. Public Blockchain

Public blockchains are open to everyone, allowing any participant to access, validate, and add data to the network. These blockchains are fully decentralised and do not require permissions (e.g., Bitcoin, Ethereum, and Litecoin).

2.2.2. Private Blockchain

Private blockchains are controlled by a single organisation and accessible only to authorised participants with an invitation. The organisation has full control over the network, including data validation and participation (e.g., Corda, Hyperledger, and Quorum).

2.2.3. Consortium Blockchain

Consortium blockchains are partially private and governed by multiple organisations rather than a single entity. In this setup, participating organisations collaborate on consensus and decision-making processes. Unlike private blockchains, where one organisation monopolises control, consortium blockchains share authority equally among participants while maintaining privacy features.

Each type serves specific use cases, with public blockchains prioritising decentralisation, private blockchains focusing on control, and consortium blockchains enabling collaborative governance. Table 1 compares the three blockchain systems with respect to their most distinguishing features [15].

Table 1 Comparison of Blockchain Architectures

Property	**Public**	**Private**	**Consortium**
Centralisation	No	Yes	Partial
Read Permission	Public	Public or restricted	Public or restricted
Peer Participation	All miners	Within an organization	Selected set of nodes
Consensus Process	Permission less	Needs permission	Needs Permission

2.3. Smart Contracts in Blockchain

Blockchain-based smart contracts and decentralised apps can boost trust in computer-connected cities by using machine learning, data visualisation tools, and spatial data mining. Blockchain technology can play a big role in building smart cities by automating business transactions and lowering running costs in digital transactions [16]. Data-driven cities try to define smart government in a way that makes transactions and public services more open and trustworthy. This makes it easier for people to be involved in making decisions [17].

3. Blockchain applications and challenges in academic credential management

Traditional systems for managing academic credentials face challenges like fraud, inefficiency, and reliance on centralised authorities. By providing a decentralised, secure, and tamper-proof system, blockchain technology allows for the transparent, real-time authentication of credentials. By leveraging cryptographic security and smart contracts, blockchain ensures the integrity, authenticity, and accessibility of academic records, empowering learners and enhancing trust between institutions and employers.

3.1. Blockchain in education

According to Tapscott and Kaplan, blockchain technology has the potential to enhance learning and teaching in many important ways.

3.1.1. Empowerment for learners (self-sovereignty)

Blockchain technology can improve academic credential management by improving security, transparency, and verifiability. Decentralised and irreversible, it secures credential issuance and verification without third parties, eliminating fraud and inefficiencies [18]. Scalability, privacy, and system integration must be solved for wider usage.

3.1.2. Security and efficiency enhancement for educational institutions, businesses, and learners:

Blockchain can protect student data's identity, privacy, and security. Since its hash chain is immutable, blockchain provides security and validity, as proven earlier in this article. Students cannot change blockchain-stored educational credentials, but they may with traditional records [19]. Instead, than keeping data, blockchain hashes it, ensuring privacy. Data can be encrypted before being stored on the blockchain [20].

3.1.3. Trust and transparency integration

Companies can trust that job applicants have the skills they need since blockchain makes it impossible for students to alter their grades, degrees, or certifications [21][22]. The transformation of blockchain into a "trust anchor of one truth for credentials"[23]. Connections between employers and job-seekers are also enhanced by this anchor. Through the integration of trust and transparency into skills transactions and sharing, distributed ledger technologies enhance "colleges, universities, employers, and their relationships to society" by securing academic records and supporting learning [24][25].

3.2. Challenges of Blockchain in Education

The Technology, Organization, and Environment (TOE) model is used to categorise factors affecting blockchain adoption in education.

- TOE has been widely used to study information technology adoption.
- The model considers three factors: technological, organisational, and environmental [26].
- Technological factors affecting blockchain usage include security, privacy, scalability, immutability, and low cost.
- Organizational factors include the organisation’s strengths, weaknesses, and readiness to accept new technology.
- Environmental factors include legal and regulatory protection [27].
- Problems with data accessibility, immutability, security, privacy, restricted interoperability and standardisation (the blockchain's immaturity), and poor usability are all examples of technological hurdles [28].
- Organizational challenges include lack of skills, insufficient funds, and lack of management support.
- Environmental challenges include legal issues, regulatory compliance, concerns about ecosystem and market readiness, and long-term viability.

3.3. Blockchain Technology for Academic Credentials Authentication

The use of blockchain technology for academic credential authentication has gained significant attention in recent years, with successful implementations in countries like Malta, Estonia, and Singapore [29]. These regions have demonstrated how blockchain can verify academic credentials and secure digital certificates, addressing issues like fraud and inefficiency.

In 2019, GovTech Singapore introduced OpenCerts, an open-source blockchain-based schema that uses cryptographic techniques to encrypt and secure academic credentials. The platform allows educational institutions to issue digital certificates and provides a public website for verification and authentication [30]. The authors noted that the use of Ethereum blockchain technology significantly reduces barriers to publishing cryptographically protected credentials [31].

Similarly, in 2018, the Malaysian Ministry of Education launched the eScroll system, developed through a collaboration with Dagang NeX change Berhad (DNeX) and LuxTag. The eScroll system leverages blockchain technology to verify academic credentials and eliminate counterfeiting. Each certificate includes a QR code for enhanced security, immutability, and verification [32]. This system has proven to be fast, efficient, and highly secure, saving time and resources by reducing reliance on manual verification methods such as phone calls and emails [33].

The report highlights that the black-market sale of fake credentials has posed significant risks, particularly in sectors like healthcare, where valid medical certifications are critical. Blockchain's decentralised and tamper-proof nature ensures that academic records remain immutable and transparent, solving these issues [34].

Additionally, blockchain enables self-sovereignty for students and workers, allowing them to have maximum ownership and mobility of their academic qualifications. Countries like Brunei Darussalam are also exploring blockchain’s potential to confirm academic credentials for students, institutions, employers, and scholarship units using advanced cryptographic methods [35].

By eliminating intermediaries and ensuring the authenticity of academic records, blockchain technology establishes a secure, efficient, and trustworthy system for academic credential management [36].

4. Academic Credential Management

Graduations, certifications, placement certificates, academic transcripts, and other forms of proof of a student's learning accomplishments are all examples of academic credentials. A credential's worth is directly proportional to its admission criteria and graduation threshold. As an example to help understand the complicated terrain, the current education credentialing processes may be reduced to four stages:

- **Credentialing programs:** applicants submit their applications, either in person or online, to an accredited education provider, such as HEI or a Registered Training Organisation (RTO), for a credential-targeted program of study. The education provider will ask for proof of the student's prior coursework and relevant job experience as part of their admissions requirements [37]. It is possible for the student to acquire an enrolment offer and begin the program after passing the admission exam.
- **Learning credits or micro-credentials:** Education providers provide students digital micro-credentials or conventional learning credits based on their performance in learning activities and assessments [38]. A relatively new concept, "micro-credentials" function in a manner similar to learning credits, which stand in for discrete units of education and may be used to obtain a more substantial credential (such as a degree) over time. A micro-credential may also be known as a "nano-degree," "learning badges," or "endorsements."[39].
- **Education Credentials:** Education providers will issue transcripts, completion certificates, and qualifications to students after they have earned a sufficient number of learning credits or micro-credentials in all required subjects and have met graduation requirements [27][40].
- **Verifiable Credentials:** Recruiters, such as companies, may request official education credentials from students when they apply for jobs or further degrees after graduation [41]. Graduates of most Australian institutions are strongly encouraged to utilise the My Equals portal to acquire a cryptographically signed PDF or secure link that verifies their credentials.

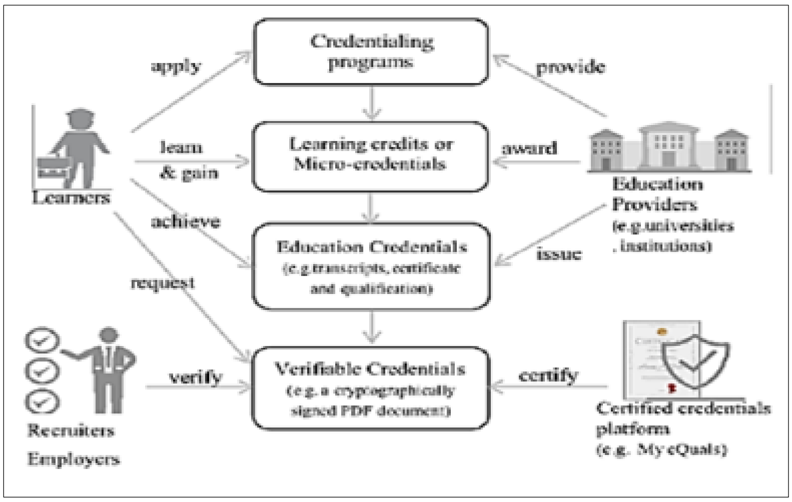
Credentialing programs
apply
provide
Learning credits or Micro-credentials
learn & gain
award
Learners
Education Providers (e.g.universities , institutions)
achieve
Education Credentials (e.g.transcripts, certificate and qualification)
issue
request
Verifiable Credentials (e.g. a cryptographically signed PDF document)
verify
certify
Recruiters
Employers
Certified credentials platform (e.g. My eQuals)

Figure 2 Credentialing workflow and involved stakeholder

4.1. Blockchain Solutions for Enhanced Security and Verifiability of Academic Credentials:

- Enhances academic credential administration and verification security, transparency, and efficiency.
- Decentralized ledger ensures unalterable credentials without third-party verification [42].
- Employers and institutions can quickly verify records stored on the blockchain by authorised parties.
- Features selective sharing for enhanced security of credentials.
- Efficient record issuance and verification through smart contracts.
- Enables worldwide document sharing while ensuring confidentiality.

4.2. Blockchain-based Framework for Digital Credential in Academic Education:

Digital badges and certificates are two forms of online credentialing. Substitute digital credentials, awards, and recognition for their paper-based counterparts. Digital credentials are simple to issue, manage, and verify. Some of the most common examples are degrees from colleges and universities, certificates for successfully completing a certain course, and acknowledgement for developing a certain skill set.

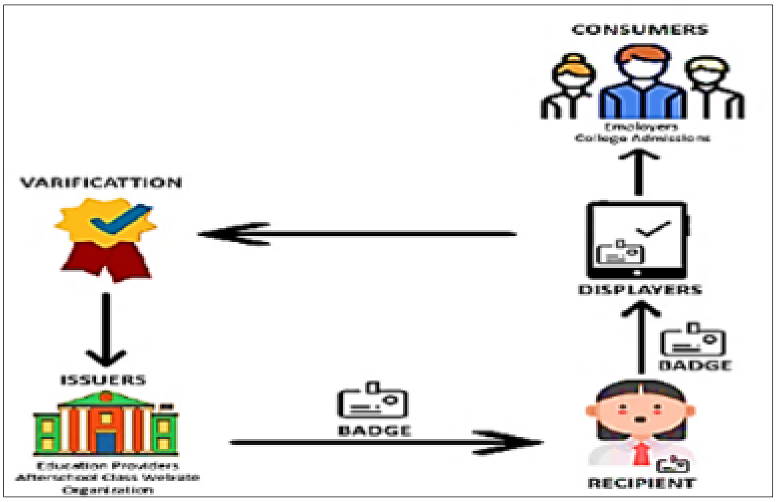

Figure 3 Digital verification of academic records

A digital certificate is a useful credential since it shows both the holder's competence and the organisation or department that checked their credentials [43]. A high-level framework for electronic academic record verification is shown in Figure 3. Like this Colorado Community College System Faculty Development badge of Course and Curriculum Mastery, most credentials contain a symbol that distinguishes the competence and the giving institution. Due to the rise of digital certificates, transcripts from universities will become more and more irrelevant and obsolete. The completion of a degree will still be valued by companies, although course marks on transcripts are not taken into account when applying for jobs. The ability to measure and share thorough learning achievements is one advantage of digital certification [44].

5. Literature review

Table 2 summarises the previous study on blockchain solutions for academic credential security and verifiability, as discussed below:

In, Reza et al. (2021) suggests the Academic Credentials Chain (ACC), a blockchain-based system for worldwide authentication and distribution of credentials. The suggested system can tell who is certifying whom based on their credentials. Users may securely save their credentials data in a decentralised application inside the planned Blockchain network. The results of the assessment demonstrate the degree of performance, as well as the practicality and security of the project [45].

Table 2 Summary of innovative blockchain solutions for academic credential security and verifiability study

Reference	Objectives	Key Findings	Challenges	Future Work
[45]	Develop ACC, a blockchain-based Academic credential chain for global verification and sharing.	Identifies who certifies whom; enables private credential data storage. Demonstrates feasibility and security.	Limited scalability and privacy concerns in global credential management.	Explore wider adoption and integration with existing verification systems.
[46]	Develop a blockchain framework for academic certification and higher education applications.	Validated architecture for decentralised apps (Dapps); highlights benefits, risks, and standards.	Understanding risks and limitations in decentralised frameworks.	Create standards for decentralised app (Dapp) deployment in higher education.
[47]	Propose a decentralised, tamper-proof certificate verification system using blockchain.	Enhances security, avoids single points of failure, automates reliable and cost-effective verification.	Addressing transparency while maintaining confidentiality.	Optimise system for broader adoption and scalability.
[48]	To establish a permissioned blockchain-based academic certificate verification system (HLFeCERT) using the SHA256 hash algorithm and digital watermarking to prevent tampering.	HLFeCERT ensures reliable encryption and decryption of certificates, enabling students to share selected certificates securely. Utilises private blockchain for enhanced privacy and selective sharing.	Integration of digital watermarking technology with blockchain may introduce computational overhead. Managing the scalability and storage requirements of a private blockchain system.	Explore methods to optimise the computational efficiency of the watermarking process. Investigate further integration with global academic systems and interoperability.
[49]	To enhance the degree issuance workflow by supporting both physical and digital documents using OCR.	Seamless integration with existing workflows supports OCR for semantics understanding and allows bulk submission.	Ensuring accuracy of OCR, managing large-scale integration, and handling variations in document templates.	Refining OCR capabilities, scalability for large datasets, and broader adoption across educational institutions.

In, Jaramillo and Piedra (2020) establishes and implements a strategy for using BC technology in the academic sector. Multiple decentralised applications (Dapps) may make advantage of the frame's sturdy construction. Academic certification provides validation of the framework, which encompasses beneficiaries, benefits of technology, dangers, and downsides. The framework offers helpful assistance in quickly and logically comprehending how BC technology operates and how it contributes to higher education. It also helps to establish a standard for Dapps' operations in this field [46].

In, Bahrami, Movahedian and Deldari (2020) a technique for verifying certificates that is both dependable and impenetrable is suggested. The suggested solution uses blockchain technology and is decentralised by design, in contrast to conventional verification techniques. By eliminating single points of failure and the need to rely on any one entity, decentralisation improves the system's security and resilience. A rapid, reliable, and cost-effective verification system may be built with the help of the suggested design, which uses cryptographically secured smart contracts that are based on the blockchain to automate the verification process [47].

In, Kumutha and Jayalakshmi (2021) The goal is to examine blockchain technology and create the HLFeCERT permissioned blockchain-based academic certificate verification system, which uses the SHA256 hash algorithm and digital watermarking technology to encrypt and decrypt academic certificates as well as prevent tampering. This implies that students are free to choose which of their credentials to make public rather than being required to do so. Private blockchain technology enables this [48].

In, Rasool et al. (2020) established the docschain to address the three issues with the blockcerts that were previously identified. By running its algorithms on paper copies of the degree papers, Docschain simply integrates into the current degree issuing system. OCR is used to do this, and each degree document is recorded together with the specifics of the relevant OCR template. This allows us to interpret the data contained at various portions of the degree document based on its semantics. When compared to blockcerts, docschain allows for the bulk submission of degree data for both current and past students [49].

6. Conclusion and future scope

Blockchain technology has emerged as a transformative solution for managing and verifying academic credentials, addressing the critical challenges of fraud, inefficiency, and reliance on centralised authorities in traditional systems. In conclusion, blockchain-related solutions play not only a role in improving the process of academic credential issuance and verification but also enhance a progressive, global, and interoperable environment, which is necessary in the context of digital demands. Further research in this area should be directed to the improvement of further scalability concerns, privacy, and promotion of blockchain applications in as many educational institutions all around the globe as possible.

For future work, it is important to focus on three main areas: making privacy better using advanced cryptographic techniques like zero-knowledge proofs; making scalability better using more efficient consensus mechanisms; and looking into how blockchain could be used to manage professional certifications and other types of credentials across many industries

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] V. V. Kumar, F. W. Liou, S. N. Balakrishnan, and V. Kumar, “Economical impact of RFID implementation in remanufacturing: a Chaos-based Interactive Artificial Bee Colony approach,” *J. Intell. Manuf.*, vol. 26, no. 4, pp. 815–830, Aug. 2015, doi: 10.1007/s10845-013-0836-9.

[2] V. V. Kumar and F. T. S. Chan, “A superiority search and optimisation algorithm to solve RFID and an environmental factor embedded closed loop logistics model,” *Int. J. Prod. Res.*, 2011, doi: 10.1080/00207543.2010.503201.

[3] V. V. Kumar, M. K. Pandey, M. K. Tiwari, and D. Ben-Arieh, “Simultaneous optimization of parts and operations sequences in SSMS: A chaos embedded Taguchi particle swarm optimization approach,” *J. Intell. Manuf.*, 2010, doi: 10.1007/s10845-008-0175-4.

[4] T. T. Huynh, T. D. Nguyen, and H. Tan, “A Survey on Security and Privacy Issues of Blockchain Technology,” *Proc. 2019 Int. Conf. Syst. Sci. Eng. ICSSE 2019*, pp. 362–367, 2019, doi: 10.1109/ICSSE.2019.8823094.

[5] V. V Kumar, M. Tripathi, M. K. Pandey, and M. K. Tiwari, “Physical programming and conjoint analysis-based redundancy allocation in multistate systems: A Taguchi embedded algorithm selection and control (TAS&amp;C)

approach," *Proc. Inst. Mech. Eng. Part O J. Risk Reliab.*, vol. 223, no. 3, pp. 215–232, Sep. 2009, doi: 10.1243/1748006XJRR210.

[6] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 858–880, 2019, doi: 10.1109/COMST.2018.2863956.

[7] V. V. Kumar, S. R. Yadav, F. W. Liou, and S. N. Balakrishnan, "A Digital Interface for the Part Designers and the Fixture Designers for a Reconfigurable Assembly System," *Math. Probl. Eng.*, vol. 2013, pp. 1–13, 2013, doi: 10.1155/2013/943702.

[8] V. V. Kumar, F. T. S. Chan, N. Mishra, and V. Kumar, "Environmental integrated closed loop logistics model: An artificial bee colony approach," in *SCMIS 2010 - Proceedings of 2010 8th International Conference on Supply Chain Management and Information Systems: Logistics Systems and Engineering*, 2010.

[9] V. V Kumar, "An interactive product development model in remanufacturing environment : a chaos-based artificial bee colony approach," *MASTER Sci. Manuf. Eng.*, 2014.

[10] V. V. Kumar, A. Sahoo, and F. W. Liou, "Cyber-enabled Product Lifecycle Management: A Multi-agent Framework," *Procedia Manuf.*, vol. 39, pp. 123–131, 2019, doi: 10.1016/j.promfg.2020.01.247.

[11] V. V Kumar, M. Tripathi, S. K. Tyagi, S. K. Shukla, and M. K. Tiwari, "An integrated real time optimization approach (IRTO) for physical programming based redundancy allocation problem," *Proc. 3rd Int. Conf. Reliab. Saf. …*, 2007.

[12] S. M. Idrees, M. Nowostawski, R. Jameel, and A. K. Mourya, "Security Aspects of Blockchain Technology Intended for," *Electronics*, vol. 10, no. 951, pp. 2–24, 2021.

[13] S. Pandya, "Predictive Analytics in Smart Grids : Leveraging Machine Learning for Renewable Energy Sources," *Int. J. Curr. Eng. Technol.*, vol. 11, no. 6, pp. 677–683, 2021, doi: https://doi.org/10.14741/ijcet/v.11.6.12.

[14] V. Kumar, V. V. Kumar, N. Mishra, F. T. S. Chan, and B. Gnanasekar, "Warranty failure analysis in service supply Chain a multi-agent framework," in *SCMIS 2010 - Proceedings of 2010 8th International Conference on Supply Chain Management and Information Systems: Logistics Systems and Engineering*, 2010.

[15] K. Bhumichitr and S. Channarukul, "AcaChain: Academic Credential Attestation System using Blockchain," 2020. doi: 10.1145/3406601.3406614.

[16] N. G. Singh, Abhinav Parashar A, "Streamlining Purchase Requisitions and Orders : A Guide to Effective Goods Receipt Management," *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 5, 2021.

[17] S. Bauskar and S. Clarita, "AN ANALYSIS: EARLY DIAGNOSIS AND CLASSIFICATION OF PARKINSON'S DISEASE USING MACHINE LEARNING TECHNIQUES," *Int. J. Comput. Eng. Technol.*, vol. 12, no. 01, pp. 54-66., 2021, doi: 10.5281/zenodo.13836264.

[18] S. G. Jubin Thomas, Kirti Vinod Vedi, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," *Int. J. Res. Anal. Rev*, vol. 8, no. 3, pp. 874–878, 2021.

[19] K. R. V. K. Sunil Kumar Reddy Anumandla, Vamsi Krishna Yarlagadda, Sai Charan Reddy Vennapusa, "Unveiling the Influence of Artificial Intelligence on Resource Management and Sustainable Development: A Comprehensive Investigation," *Technol. Manag. Rev.*, vol. 5, no. 1, pp. 45–65, 2020.

[20] S. G. Thomas Jubin, Kirti Vinod Vedi, "Enhancing Supply Chain Resilience Through Cloud-Based SCM and Advanced Machine Learning: A Case Study of Logistics," *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 9, 2021.

[21] M. R. Kishore Mullangi, Vamsi Krishna Yarlagadda, Niravkumar Dhameliya, "Integrating AI and Reciprocal Symmetry in Financial Management: A Pathway to Enhanced Decision-Making," *Int. J. Reciprocal Symmetry Theor. Phys.*, vol. 5, no. 1, pp. 42–52, 2018.

[22] S. R. Bauskar, "EVALUATION OF DEEP LEARNING FOR THE DIAGNOSIS OF LEUKEMIA BLOOD CANCER," *Int. J. Adv. Res. Eng. Technol.*, vol. 11, no. 3, pp. 661–672, 2020.

[23] S. K. R. A. Sai Charan Reddy Vennapusa, Takudzwa Fadziso, Dipakkumar Kanubhai Sachani, Vamsi Krishna Yarlagadda, "Cryptocurrency-Based Loyalty Programs for Enhanced Customer Engagement," *Technol. Manag. Rev.*, vol. 3, no. 1, pp. 46–62, 2018.

[24] M.-F. Steiu, "Blockchain in education: Opportunities, applications, and challenges," *First Monday*, 2020, doi: 10.5210/fm.v25i9.10654.

[25] M. A. Shajahan, N. Richardson, N. Dhameliya, B. Patel, S. K. R. Anumandla, and V. K. Yarlagadda, "AUTOSAR Classic vs. AUTOSAR Adaptive: A Comparative Analysis in Stack Development," *Eng. Int.*, vol. 7, no. 2, pp. 161–178, Dec. 2019, doi: 10.18034/ei.v7i2.711.

[26] N. Richardson, R. Pydipalli, S. S. Maddula, S. K. R. Anumandla, and V. K. Yarlagadda, "Role-Based Access Control in SAS Programming: Enhancing Security and Authorization," *Int. J. Reciprocal Symmetry Theor. Phys.*, 2019.

[27] M. Gopalsamy, "Artificial Intelligence (AI) Based Internet-ofThings (IoT)-Botnet Attacks Identification Techniques to Enhance Cyber security," *Int. J. Res. Anal. Rev.*, vol. 7, no. 4, pp. 414–420, 2020.

[28] B. P. Vamsi Krishna Yarlagadda, Sai Sirisha Maddula, Dipakkumar Kanubhai Sachani, Kishore Mullangi, Sunil Kumar Reddy Anumandla, "Unlocking Business Insights with XBRL: Leveraging Digital Tools for Financial Transparency and Efficiency," *Asian Account. Audit. Adv.*, vol. 11, no. 1, pp. 101–116, 2020.

[29] R. Arora, "Mitigating Security Risks on Privacy of Sensitive Data used in Cloud-based Mitigating Security Risks on Privacy of Sensitive Data used in Cloud-based ERP Applications," *8th Int. Conf. "Computing Sustain. Glob. Dev.*, no. March, pp. 458–463, 2021.

[30] V. K. Yarlagadda, "Harnessing Biomedical Signals: A Modern Fusion of Hadoop Infrastructure, AI, and Fuzzy Logic in Healthcare," vol. 8, 2021.

[31] V. S. Thokala, "Integrating Machine Learning into Web Applications for Personalized Content Delivery using Python," *Int. J. Curr. Eng. Technol.*, vol. 11, no. 6, pp. 652–660, 2021, doi: https://doi.org/10.14741/ijcet/v.11.6.9.

[32] M. Z. Hasan, R. Fink, M. R. Suyambu, and M. K. Baskaran, "Assessment and improvement of elevator controllers for energy efficiency," in *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, 2012. doi: 10.1109/ISCE.2012.6241747.

[33] V. S. Thokala, "Utilizing Docker Containers for Reproducible Builds and Scalable Web Application Deployments," *Int. J. Curr. Eng. Technol.*, vol. 11, no. 6, pp. 661–668, 2021, doi: https://doi.org/10.14741/ijcet/v.11.6.10.

[34] M. Z. Hasan, R. Fink, M. R. Suyambu, and M. K. Baskaran, "Assessment and improvement of intelligent controllers for elevator energy efficiency," in *IEEE International Conference on Electro Information Technology*, 2012. doi: 10.1109/EIT.2012.6220727.

[35] M. Z. Hasan, R. Fink, M. R. Suyambu, M. K. Baskaran, D. James, and J. Gamboa, "Performance evaluation of energy efficient intelligent elevator controllers," in *IEEE International Conference on Electro Information Technology*, 2015. doi: 10.1109/EIT.2015.7293320.

[36] Z. L. Abdul Hadi and T. W. Au, "Blockchain for the Authentication and Immutability of Academic Credentials Issued in Brunei Darussalam," 2021, pp. 75–84. doi: 10.1007/978-3-030-68133-3_8.

[37] K. Patel, "Quality Assurance In The Age Of Data Analytics: Innovations And Challenges," *Int. J. Creat. Res. Thoughts*, vol. 9, no. 12, pp. f573–f578, 2021.

[38] Rajesh Goyal, "THE ROLE OF BUSINESS ANALYSTS IN INFORMATION MANAGEMENT PROJECTS," *Int. J. Core Eng. Manag.*, vol. 6, no. 9, 2020.

[39] R. Goyal, "THE ROLE OF REQUIREMENT GATHERING IN AGILE SOFTWARE DEVELOPMENT: STRATEGIES FOR SUCCESS AND CHALLENGES," *Int. J. Core Eng. Manag.*, vol. 6, no. 12, pp. 142–152, 2021.

[40] Mani Gopalsamy, "Enhanced Cybersecurity for Network Intrusion Detection System Based Artificial Intelligence (AI) Techniques," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 12, no. 1, pp. 671–681, Dec. 2021, doi: 10.48175/IJARSCT-2269M.

[41] M. Gopalsamy, S. Cyber, and S. Specialist, "Advanced Cybersecurity in Cloud Via Employing AI Techniques for Effective Intrusion Detection," *IJRAR*, vol. 8, no. 1, pp. 187–192, 2021.

[42] R. Bishukarma, "The Role of AI in Automated Testing and Monitoring in SaaS Environments," *Int. J. Res. Anal. Rev.*, vol. 8, no. 2, pp. 846–851, 2021.

[43] V. S. Thokala, "A Comparative Study of Data Integrity and Redundancy in Distributed Databases for Web Applications," *Int. J. Res. Anal. Rev.*, vol. 8, no. 4, pp. 383–389, 2021.

[44] S. Alam, H. Abdullah, R. Abdulhaq, and A. Hayawi, "A Blockchain-based framework for secure Educational Credentials," *Turkish J. Comput. Math. Educ.*, vol. 12, pp. 5157–5167, 2021, doi: 10.17762/turcomat.v12i10.5298.

[45] M. S. Reza, S. Biswas, A. Alghamdi, M. Alrizq, A. K. Bairagi, and M. Masud, “ACC: Blockchain Based Trusted Management of Academic Credentials,” in *Proceedings - 2021 IEEE International Symposium on Smart Electronic Systems, iSES 2021*, 2021. doi: 10.1109/iSES52644.2021.00104.

[46] M. P. Jaramillo and N. Piedra, “A blockchain model proposal for the decentralized management of academic credentials in Ecuadorian universities,” in *Applications in Software Engineering - Proceedings of the 9th International Conference on Software Process Improvement, CIMPS 2020*, 2020. doi: 10.1109/CIMPS52057.2020.9390104.

[47] M. Bahrami, A. Movahedian, and A. Deldari, “A Comprehensive Blockchain-based solution For Academic Certificates Management Using Smart Contracts,” in *2020 10th International Conference on Computer and Knowledge Engineering (ICCKE)*, 2020, pp. 573–578. doi: 10.1109/ICCKE50421.2020.9303656.

[48] K. Kumutha and S. Jayalakshmi, “Hyperledger Fabric Blockchain Framework: Efficient Solution for Academic Certificate Decentralized Repository,” in *Proceedings of the 5th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2021*, 2021. doi: 10.1109/I-SMAC52330.2021.9640785.

[49] S. Rasool, A. Saleem, M. Iqbal, T. Dagiuklas, S. Mumtaz, and Z. U. Qayyum, “Docschain: Blockchain-Based IoT Solution for Verification of Degree Documents,” *IEEE Trans. Comput. Soc. Syst.*, 2020, doi: 10.1109/TCSS.2020.2973710.