International Journal of Innovative Research & Growth
E-ISSN: 2455-1848
homepage: http://www.ijirg.com/ijirg/
Volume: 15 Issue: 2, April 2026

Design of a Blockchain-Enabled Framework for Digital Pension Certificate Scheme

Dhramandra Sharma[1*], Monika Saxena[2]
[1,2]Department of Computer Science, Banasthali Vidyapith, Jaipur-302001, Rajasthan, India

CORRESPONDING AUTHOR

Dhramandra Sharma
e-mail: dhramandra.sharma@gmail.com

KEYWORDS

Blockchain, Digital Pension Certificate, Smart Contracts, Biometric Authentication, Decentralized Framework, Identity Verification

ARTICLE DETAILS

Received 03 January 2026; revised 03 March 2026; accepted 20 March 2026

DOI: 10.26671/IJIRG.2026.2.15.102

CITATION
Sharma, D., Saxena, M. (2026). Design of a Blockchain-Enabled Framework for Digital Pension Certificate Scheme. *Int J Innovat Res Growth*, 15(2), 152001-152009. DOI

Abstract

This research proposes a Blockchain-enabled framework for a Digital Pension Certificate Scheme (DPCA) designed to create a secure, transparent, and tamper-proof system for managing pension certificates. Traditional pension management systems face challenges including fraud, data tampering, and unauthorized access, which compromise user trust and operational efficiency. The DPCA framework integrates key components such as user registration with biometric authentication, smart contract deployment for automated certificate issuance and verification, cryptographically secured block creation, and multi-factor user verification to enhance security and reliability. By leveraging blockchain's decentralized ledger technology, the framework ensures data immutability, traceability, and consensus among stakeholders, including government authorities and pension administrators. The implementation incorporates robust cryptographic algorithms to protect sensitive user information and prevent identity fraud. Experimental insights drawn from related blockchain applications demonstrate the framework's capability to maintain fault tolerance, improve transparency, preserve privacy, and automate authentication processes across diverse use cases. This study validates the scalability and robustness of the proposed DPCA system in addressing critical security vulnerabilities while streamlining pension certificate management. The research also highlights how integrating biometric data with blockchain enhances identity verification and reduces risks of impersonation. Future work will explore interoperability with other government services, optimize consensus mechanisms for computational efficiency, and incorporate advanced privacy-preserving techniques such as zero-knowledge proofs. Overall, this study advances digital identity management in public service delivery, offering a scalable and resilient solution that fosters trust and efficiency in pension administration, aligned with the evolving digital governance landscape.

1. Introduction

The conversation highlights how far we've come in solving long-standing problems in secure and distributed computing systems in a number of fields. The framework's ability to stay fault-tolerant with little delay shows that it is strong and works well for real-time IoT applications, where resilience is very important. Better end-to-end traceability in supply chains makes things more open and helps businesses follow the rules, which is important in emergencies and for keeping items real. Combining federated learning with blockchain technology successfully addresses privacy issues and lessens algorithmic bias, leading to more accurate and fair predictive models. This progress is especially crucial for programs that deal with private information and include a wide range of stakeholders. Also, network frameworks that use blockchain technology make security better by using automatic authentication processes and making things more open, which stops unwanted access and possible assaults. These changes show how blockchain technology and advanced computer architectures may work together to make things safer, fairer, and more efficient. This integration helps build strong and reliable digital infrastructures that can handle complicated, spread-out data environments. Such progress is necessary to build trust in digital systems and make it possible to create scalable, safe, and clear solutions for a wide range of uses in today's linked world of technology(Issa et al., 2025; Shah & Raj, 2025). Digitizing pension certificates not only makes things easier, but it also gives us a chance to deal with important problems including document forgeries, inconsistent record keeping, and the lack of real-time verification. Moving to entirely digital pension systems brings up critical issues of data integrity, privacy, and reliability, especially when there are many parties involved, such as the government, banks, and pensioners. Blockchain technology has become a game-changing way to handle and verify digital certificates. Blockchain is a distributed and decentralized ledger system that keeps track of transactions in a safe, unchangeable, and open way. With this technology, everyone can work together to keep the data accurate and up to date, so there is no need for a trusted central authority(Ahmed et al., 2025; Al-Kfairy et al., 2025). Blockchain's built-in features, such being tamper-proof, being able to be traced, and being validated by consensus, make it a great framework for building secure digital pension certificate systems. A blockchain-enabled architecture for digital pension certificates must include a system that records pension entitlements on a blockchain network. This way, once a certificate is given, it cannot be changed or faked without being found out. Pensioners can now safely access their digital certificates and send verification of their pension status to the right organizations. This not only speeds up the process of checking claims, but it also lowers the chance of identity theft and false claims by a lot. Smart contracts are programmable, self-executing algorithms that may be added to the blockchain. They can automate important pension-related tasks including checking eligibility, issuing certificates, and validating claims. These smart contracts work according to rules that have already been set, which cuts down on the need for human involvement and lowers administrative costs while improving accuracy and efficiency. Also, permissioned blockchain networks and cryptography methods help protect people's privacy by making sure that only authorized people may see sensitive pension data.

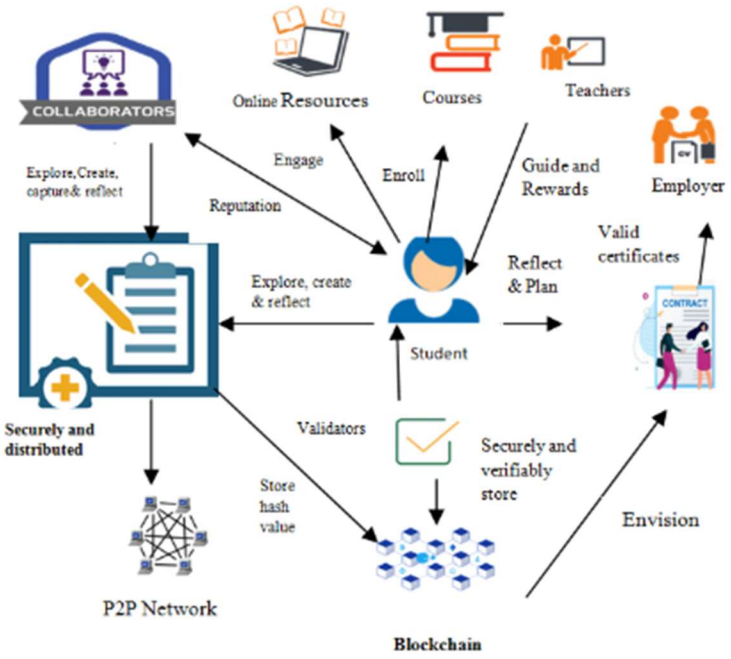

Fig.1 Blockchain-Enabled Framework for Digital Pension.

This framework also stresses compatibility with current pension management systems, which means that it may be adopted slowly and integrated smoothly without affecting present operations. The technology promotes trust, collaboration, and openness throughout the whole pension ecosystem by letting many pension providers and regulatory authorities use the same blockchain network.

This research aims to provide a blockchain-based system for managing digital pension certificates that is safe, open, and works well. The proposed approach seeks to bolster confidence, thwart fraud, and elevate the overall experience for both pensioners and institutions by tackling the principal issues of conventional pension systems and utilizing the distinctive benefits of blockchain technology. The next parts will go into more detail on the technological design, how to put it into action, and how to test how well the proposed framework works.

2. Literature Review

technology will bring transparency and traceability to the industry, which will enable the pensioners to have easy access to their pension records, which will create confidence in the system and hugely mitigate the incidents of disagreement in case of a pension claim (Junaid et al., 2024; Mohammed et al., 2025). The framework is scalable and interoperable with the already existing government IT infrastructures, meaning that it will integrate and employ it without causing disruption to the existing workflow. In a larger sense, this blockchain-enabled pension certificate program is in line with the international trend of digital governance and e-governance programs, which represent the paradigm shift in terms of social security benefits administration in the digital era. It is also financially inclusive because it allows digitally marginalized pensioners to store and retrieve their pension certificates in secure locations and on user-friendly interfaces, which may be interconnectable with mobile platforms (Karakus, 2024; Sarfaraz et al., 2023). The unalterable quality of blockchain data sets aids in countering the threats of forging documents, identity theft, and other unauthorized alterations, enhancing the security status of the entire pension administration. The paper explores some of the design choices that would be appropriate when used in government-supported applications, privacy-enhancing strategies that would be used to safeguard the sensitive pensioner data, and compliance with legal regulations to meet the data protection regulations. Through these aspects, the framework can not only promote technical development but also promote ethical and legal aspects that are imperative in using blockchain successfully in the public welfare programs. Besides theoretical construction, the study involves practical value by developing prototypes and simulating to confirm the aspects of validity of feasibility, performance and security of the designed system. Performance factors, including the transaction throughput, latency and scalability at various loads are measured to make sure that the solution satisfies the requirements of the large-scale pension schemes (Kai et al., 2023; Zhan et al., 2023). Security analysis is concerned with resilience against cyber-attacks, data breaches, and insider threats and it is important to note that blockchain has the potential to provide a strong defense mechanism. In addition, the stakeholder analysis helps to show the interaction of different actors such as pensioners, administrators and financial auditors within the ecosystem where they can enjoy the advantages of increased trust and simplified operations. The innovative power of such blockchain-based framework is not confined to the pension certificates, and the possibilities of its further application in managing digital identity, social security, and government-approved certifications are open (Biswas et al., 2023). As a model of a successful application to the pension segment, this study will add significant values to the digitization of services provided to the population on the basis of blockchain technology, and policymakers and technologists should adopt decentralized technologies to address complicated administrative issues. Finally, the architecture of a blockchain-based system of issuing digital pension certificates is another great leap towards the modernization of the social welfare system and allowing people to obtain their due and receive their benefits in a way that is safe and efficient as well as create a culture of transparency and responsibility in the government (Lee et al., 2022; Rustiana et al., 2022). This introduction provides the background to a critical discussion of the technical architecture, implementation plans, and potential effects on society of the proposed framework that can be used as a reference in the future research and practical implementations in various governmental settings across the globe (Bellagarda & Abu-Mahfouz, 2022; Gurzhii et al., 2022).

Kerrison 2023 et al. Shares the problem of working with blockchain-powered IoT healthcare systems in rural settings with low bandwidth. In a proposed Hybrid Channel Healthcare Chain (HC) communication, two channels of communication are used, including short-range communication channel that allows the device to be authorized and transfer bulk data and long-range radio communication channel, which allows the transfer of lightweight monitoring and event alerts. IoT devices can sign transactions securely without having keys with the help of cryptographic identities and a cloud-based digital twin. The data of the patients is encrypted end-to-end, and the blockchain provides a secure data lifecycle book. The system saves up to 87 times on radio packets over long distances, which is effective and enhances confidence in monitoring in rural healthcare (Kerrison et al., 2023).

Mohammed 2023 et al. An analysis of the adoption of central bank digital currencies (CBDCs) in 67 countries is performed based on structural equation modeling to study the technological, environmental, legal, and economic variables. The results indicate that the greater the degree of democracy and confidence of people in the governance, the better the CBDC use, whereas negative outcomes are caused by the quality of regulation and income inequality. Surprisingly, there was no significant impact of such factors as network readiness, foreign

exchange reserves, and sustainable development goals. The study indicates that democratic governance is an important factor in the acceptance of CBDC and proposal of policy recommendations and directions in future research to help to increase the adoption of CBDC in the global arena (Mohammed et al., 2023).

Radeva 2022 et al. Suggests a blockchain-implemented supply-chain system of a smart crop production system. It examines the blockchain ecosystem as a system of stakeholders and technical components, characterizes a supply-chain model and develops a blockchain reference infrastructure. The model facilitates the certification of the seed, grain tracking, provenance, and optional relations with regulators, logistics, and financial services. It presents a three-tier blockchain architecture, which facilitates five channels of information with nine participants and smart contracts. The paper also includes a user account management tool, describes fundamental smart contract capabilities and sample smart contract code to demonstrate what the system is capable of doing (Radeva & Popchev, 2022).

Almaiah 2022 et al. Handles security issues in the Internet of Things (IoT), specifically the Internet of Medical Things (IoMT) and securing patient health records (PHR). To increase the intrusion detection, it proposes a new algorithm Group Theory-based Binary Spring Search (GT-BSS) algorithm together with a hybrid deep neural network. The solution combines homomorphic encryption and blockchain as a distributed database to allow healthcare information to be searched and accessed by keys in a secure and safe way, which defeats the weaknesses of current systems. It also comprises a secure key revocation scheme and dynamic update of policies. Hyperledger Fabric and Origion Lab simulations show that the systems are more secure, efficient, and transparent and cost-effective than benchmark models (Ali et al., 2022).

Avrilionis 2021 et al. Opposes the existing blockchain-centric paradigm that dominates digital asset and cryptocurrency projects by positing an asset-centric view about the management of the whole lifecycle of real-world assets and their digital counterparts. With the notion of a digital twin, it points out the role of the digital twins as containers that provide off-chain state

persistence and on-chain state traceability. Such containers have the ability to support both blockchain and traditional server environments, and they serve as a transition to the new blockchain environments, which are replacing legacy systems. The asset-centric model is introduced as a superior direction of evolutionary changes in blockchain and decentralized ledger technologies that foster interoperability and uniform management of assets (Avrilionis & Hardjono, 2021).

Table 1: Literature Summary.

Authors/Year	Methodology	Research gap	Findings
Yadav/2021(Yadav et al., 2021)	Ostrom's action arena analyzes stakeholder exchanges in blockchain tourism.	Lack of clarity on stakeholder roles and data trust challenges.	Blockchain adds complexity but offers balanced benefits for stakeholders.
Abougalala/2020(Abougalala et al., 2020)	Conceptual framework and case studies analyze blockchain use in smart universities.	Limited exploration of blockchain's role in student engagement and assessment.	Blockchain enhances education quality via formative assessment and supervision.
Malomo/2020(Malomo et al., 2020)	Designed a blockchain-enabled federated cloud framework for secure storage.	Existing offsite data recovery lacks strong access control and breach detection.	Framework improves efficiency, privacy, scalability, and early breach detection.
Islam/2019(Islam & Shin, 2019)	Blockchain-enabled UAV swarm collects, validates, and encrypts IoT data securely.	Limited secure data acquisition frameworks combining UAVs, IoT, blockchain.	UAV-assisted blockchain improves security, connectivity, and energy efficiency.
Keivanpour/2019(Keivanpour et al., 2019)	Conceptual analysis of blockchain applications across offshore wind supply chains.	Limited studies on blockchain-enabled traceability in offshore wind energy.	Blockchain improves supply-chain efficiency, transparency, collaboration, and adaptability.

3. Method

This study concentrates on the design and implementation of a Blockchain-enabled framework for a Digital Pension Certificate Scheme (DPCA) intended to establish a safe, dependable, and tamper-resistant system for the management of pension certificates. The technique includes important parts including user registration,

biometric authentication, smart contract deployment, block construction, data verification, information broadcasting, and multi-factor user verification to make sure that data is safe, clear, and works well.

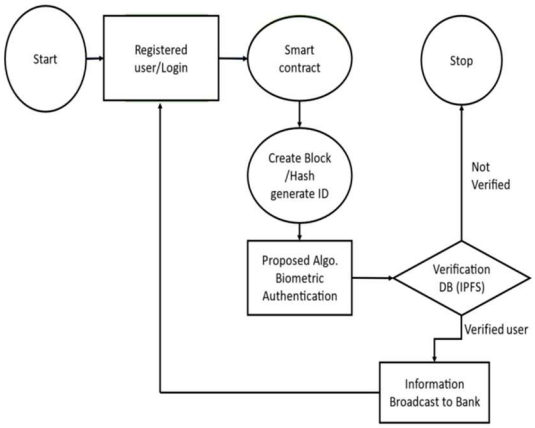

Fig.2 Proposed Flow Chart.

3.1 Research Objectives

The primary goal of this study is to develop an automated Digital Pension Certificate application mechanism powered by Blockchain technology to address existing security vulnerabilities. The specific objectives include:

a) To collect data sets of users from official government. website of Digital pension certificate.
b) To design a Blockchain Enabled Framework for Digital pension certificate.
c) To implement & test proposed framework in different security parameters like computational complexity, confidentiality, integrity, etc.

3.2 User Registration

User registration is the first stage in the DPCA system for safely managing identities. It means getting personal information like your full name, date of birth, address, government-issued ID numbers, and phone number. Biometric data like fingerprints, facial recognition, or iris scans are also collected to make it easier to verify someone's identification and cut down on fraud. All the information that is collected is encrypted using strong cryptographic techniques and validated against official government databases to make sure there are no duplicates or mistakes. This phase makes sure that only real users with validated identities may access the system, which is a safe way to start Blockchain operations.

3.3 Smart Contract Deployment

Smart contracts handle the creation, verification, and updating of pension certificates on the Blockchain network. These programs that run on their own incorporate rules for who can use them, how to verify their identity, and how to get approval. Smart contracts take care of issuing certificates without any human input once user data has been verified. This cuts down on mistakes and makes things clearer. These contracts are put into action on platforms like Ethereum or Hyperledger using programming languages like Solidity. Code audits and formal testing make sure that there are no security holes. Smart contracts are decentralized, which builds confidence and reliability inside the DPCA framework.

3.4 Block Creation

New blocks containing validated user data from registration are cryptographically linked to the Blockchain ledger. Every block has a unique hash, timestamp, block ID, and a link to the block before it. This makes sure that the blocks can't be changed and are in the right order. Consensus algorithms like Proof of Work (PoW) or Proof of Stake (PoS) check and add blocks to the chain, making sure that no one may change them without permission. Digital signatures are used to verify the source of data and make it possible to track it. This stops identity theft and the issuance of fake certificates. This method makes sure that only authorized people, such government officials and pension administrators, can see and use the ledger.

3.5 Biometric Authentication

Biometric authentication makes the system further safer by checking users' unique physical attributes. Biometric data is saved safely and encrypted, so it is never shown in plain form. When users log in or update their certificates, their biometric data is compared to encrypted templates that are saved. This strategy lowers the possibility of impersonation and unwanted access, making it easier to follow privacy laws. Biometric

verification, when used with smart contracts, makes it possible to issue certificates automatically and safely, which increases trust among all parties.

3.6 Data Verification in Database

By checking user information against official government records, you can be sure that the data is correct and consistent. Digital signatures and cryptographic hash functions make sure that stored data hasn't changed. This automated verification method stops fake registrations and makes sure that each digital pension certificate belongs to a real, confirmed subscriber. The system makes sure that information can be traced and audited, and only people who are allowed to see it can do so. This builds confidence among stakeholders.

3.7 Information Broadcast

After checking and creating a block, the validated data is sent to all network nodes, such as banks, pension authorities, and regulators, to make sure that everyone has the same information. This decentralized sharing makes sure that everyone can see the data, stops others from changing it, and allows for real-time updates. Secure communication protocols only let authorized nodes see sensitive data. This makes it easier to reach consensus and keeps the ledger accurate.

3.8 User Verification

User authentication employs multi-factor verification combining biometric data and personal credentials to prevent unauthorized access. Smart contracts enforce rules on certificate issuance and access permissions, automatically restricting anomalies. Verified transactions are permanently stored, providing a tamper-proof audit trail. Continuous user verification maintains data integrity and system trustworthiness among stakeholders, ensuring secure, transparent, and reliable pension certificate management.

4. Results

The study presents key findings demonstrating significant improvements in distributed computing systems through blockchain integration. Trust Mesh achieved fault detection latency under 150 milliseconds while maintaining Byzantine fault tolerance, proving effective for real-time IoT applications. Pharmaceutical supply chains showed enhanced end-to-end traceability and regulatory compliance, crucial during emergencies. Federated learning models improved prediction accuracy and fairness by reducing bias through privacy-preserving collaborative training. Blockchain-enabled SDN frameworks automated controller authentication, boosting network security and transparency. These results collectively highlight advances in security, scalability, and fairness, showcasing blockchain's potential to enhance complex, trustless environments across diverse sectors.

Table 2: Summary of Key Performance Metrics and Findings.

Study / Module	Metric	Performance Value	Findings and Outcomes
Trust Mesh (Rangwala & Buyya, 2025)	Fault Detection Latency	< 150 milliseconds	The framework maintained Byzantine fault tolerance with very low fault detection latency and stable system overhead, proving effective for real-time IoT applications.
Pharma Supply Chain (Amin et al., 2025)	Traceability Coverage	End-to-end (manufacturing to point-of-care)	Provided full traceability across the pharmaceutical supply chain, enhancing transparency, authenticity, and regulatory compliance—critical during pandemic emergencies.
Federated Learning (Liang et al., 2023)	Training Iterations	20,000 local, 1,000 federated	Enabled privacy-preserving collaborative model training across multiple institutions, reducing bias and improving accuracy, resulting in enhanced fairness.
SDN Framework (Das et al., 2023)	Controller Authentication	Automated via smart contracts	Automated SDN controller authentication, improving network security and transparency while preventing man-in-the-middle attacks.

5. Discussion

The discussion underscores significant progress in addressing persistent challenges in distributed and secure computing systems across various domains. The demonstrated capability to maintain fault tolerance with minimal latency confirms the framework's robustness and suitability for real-time IoT applications, where resilience is critical. Enhanced end-to-end traceability in supply chains ensures greater transparency and regulatory compliance, which is vital during emergencies and for maintaining the authenticity of products. The integration of federated learning with blockchain technology effectively mitigates privacy concerns and reduces

algorithmic bias, resulting in more accurate and fair predictive models. This advancement is particularly important for applications involving sensitive data and diverse stakeholder participation. Moreover, blockchain-enabled network frameworks improve security through automated authentication processes and increased transparency, protecting against unauthorized access and potential attacks. Collectively, these developments illustrate the powerful synergy between blockchain technologies and advanced computing architectures in enhancing security, fairness, and operational efficiency. This integration supports the creation of resilient and trustworthy digital infrastructures capable of managing complex, distributed data environments. Such progress is essential for fostering confidence in digital systems and enabling scalable, secure, and transparent solutions across a broad spectrum of applications in today's interconnected technological landscape.

6. Conclusion

In conclusion, this research successfully developed a Blockchain-enabled framework for the Digital Pension Certificate Scheme (DPCA) that significantly enhances the security, transparency, and reliability of pension certificate management. By leveraging biometric authentication, smart contracts, cryptographically secured block creation, and multi-factor user verification, the framework effectively addresses traditional vulnerabilities such as fraud, data tampering, and unauthorized access. The automated processes embedded within the system reduce human error and improve operational efficiency while ensuring strict adherence to regulatory standards. Drawing on insights from related blockchain applications such as TrustMesh's fault-tolerant IoT framework, pharmaceutical supply chain traceability, privacy-preserving federated learning, and blockchain-based SDN security this study validates the framework's robustness, scalability, and real-world applicability. The decentralized nature of data broadcasting fosters consensus and trust among diverse stakeholders, including government authorities, pension administrators, and users. Moreover, the integration of advanced cryptographic methods ensures data immutability and auditability, reinforcing confidence in the digital pension ecosystem. This work represents a meaningful advancement in digital identity management and public service modernization. Future research will focus on expanding interoperability with other government platforms, optimizing consensus algorithms to enhance computational efficiency, and exploring privacy-enhancing technologies like zero-knowledge proofs to further balance transparency with confidentiality. Collectively, these efforts will help realize a resilient, user-centric, and scalable digital pension infrastructure, contributing to improved public trust and streamlined government service delivery in an increasingly digital era.

Acknowledgment

The authors sincerely acknowledge the continuous guidance, valuable suggestions, and constant encouragement received from Prof. Dr. Monika Saxena, Department of Computer Science, Banasthali Vidyapith. Her insightful feedback and academic support greatly contributed to the successful completion of this research work. The authors also express their gratitude to all those who directly or indirectly supported and motivated them throughout the study.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this research work. There are no known financial or non-financial relationships, affiliations, or interests that could have inappropriately influenced the research, analysis, or conclusions presented in this manuscript.

Source of Findings

This research received no specific funding from any public, commercial, or not-for-profit funding agency. The study was conducted as part of academic research activities supported by institutional infrastructure and resources. The authors independently designed, implemented, and evaluated the proposed blockchain-enabled framework without external financial assistance or sponsorship.

Author Contributions

Dhramandra Sharma conceptualized the study, designed the blockchain-enabled framework, implemented the system architecture, conducted experiments, and prepared the initial manuscript draft. Monika Saxena supervised the research work, provided methodological guidance, validated the experimental results, contributed to manuscript review and editing, and offered critical revisions for improving the technical and academic quality of the paper.

References

[1] Abougalala, R. A., Amasha, M. A., Areed, M. F., Khairy, D. (2020). *Blockchain-Enabled Smart University, A*. *98*(17).

[2] Ahmed, I., Toyoda, K., Nakano, T., Kasahara, S., Goyal, S. R., Tran, T. H. (2025). A Systematic Review on Blockchain-Enabled eKYC: Leveraging SSI and DID for Secure and Efficient

Identity Verification. *IEEE Internet of Things Journal,* 12(21), 44381–44401. https://doi.org/10.1109/JIOT.2025.3597356

[3] Al-Kfairy, M., Alfandi, O., Sharma, R. S., Alrabaee, S. (2025). Digital Transformation of Education: An Integrated Framework for Metaverse, Blockchain, and AI-Driven Learning. *International Conference on Computer Supported Education, CSEDU - Proceedings*, *1*(Csedu), 865–873. https://doi.org/10.5220/0013499400003932

[4] Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., Teo, J., Zakarya, M. (2022). An Industrial IoT-Based Blockchain-Enabled Secure Searchable Neural Network. *Sensors*, *22*(2).

[5] Amin, M. R., Akhtar, N., Hoque, M. E., Nabil, A. R., Hossain, K. M. S. (2025). Blockchain-Enabled Traceability in Pharmaceutical Supply Chains: An Integrated Engineering and It Management Framework for Regulatory Compliance and Pandemic Resilience. *Journal of Computer Science and Technology Studies*, 7(10), 343–356. https://doi.org/10.32996/jcsts

[6] Avrilionis, D., Hardjono, T. (2021). *Towards Blockchain-enabled Open Architectures for Scalable Digital Asset Platforms*. http://arxiv.org/abs/2110.12553

[7] Bellagarda, J., Abu-Mahfouz, A. M. (2022). Connect2NFT: A Web-Based, Blockchain Enabled NFT Application with the Aim of Reducing Fraud and Ensuring Authenticated Social, Non-Human Verified Digital Identity. *Mathematics*, 10(21). https://doi.org/10.3390/math10213934

[8] Biswas, M., Das, D., Banerjee, S., Mukherjee, A., AL-Numay, W., Biswas, U., Zhang, Y. (2023). Blockchain-Enabled Communication Framework for Secure and Trustworthy Internet of Vehicles. *Sustainability (Switzerland)*, 15(12). https://doi.org/10.3390/su15129399

[9] Blockchain-Enabled Framework For Digital Pension. Retrieved December 18, 2025, from https://www.researchgate.net/figure/Model-of-Blockchain-Based-Certificate-Verification-System_fig3_352441968

[10] Das, D., Banerjee, S., Dasgupta, K., Chatterjee, P., Ghosh, U., Biswas, U. (2023). Blockchain Enabled SDN Framework for Security Management in 5G Applications. *ACM International Conference Proceeding Series*, 414–419. https://doi.org/10.1145/3571306.3571445

[11] Gurzhii, A., Islam, A. K. M. N., Haque, A. K. M. B., Marella, V. (2022). Blockchain Enabled Digital Transformation: A Systematic Literature Review. *IEEE Access*, 10(July), 79584–79605. https://doi.org/10.1109/ACCESS.2022.3194004

[12] Islam, A., Shin, S. Y. (2019). BUS: A Blockchain-Enabled Data Acquisition Scheme with the Assistance of UAV Swarm in Internet of Things. *IEEE Access*, 7, 103231–103249. https://doi.org/10.1109/ACCESS.2019.2930774

[13] Issa, W., Moustafa, N., Turnbull, B., Choo, K. K. R. (2025). DT-BFL: Digital Twins for Blockchain-enabled Federated Learning in Internet of Things networks. *Ad Hoc Networks*, 178(April), 103934. https://doi.org/10.1016/j.adhoc.2025.103934

[14] Junaid, L., Bilal, K., Shuja, J., Balogun, A. O., Rodrigues, J. J. P. C. (2024). Blockchain-Enabled Framework for Transparent Land Lease and Mortgage Management. *IEEE Access*, 12(March), 54005–54018. https://doi.org/10.1109/ACCESS.2024.3388248

[15] Kai, H., Guo, M., Zeng, F., Chen, Y., Xiao, T., Griffin, J. (2023). Blockchain-enabled authentication platform for the protection of 3D printing intellectual property: a conceptual framework study. *Enterprise Information Systems*, 17(11). https://doi.org/10.1080/17517575.2023.2180776

[16] Karakus, M. (2024). GATE-BC: Genetic Algorithm-Powered QoS-Aware Cross-Network Traffic Engineering in Blockchain- Enabled SDN. *IEEE Access*, 12(March), 36523–36545. https://doi.org/10.1109/ACCESS.2024.3374213

[17] Keivanpour, S., Ramudhin, A., Ait Kadi, D. (2019). Towards the blockchain-enabled offshore wind energy supply chain. *Advances in Intelligent Systems and Computing*, 880, 904–913. https://doi.org/10.1007/978-3-030-02686-8_67

[18] Kerrison, S., Jusak, J., Huang, T. (2023). Blockchain-Enabled IoT for Rural Healthcare: Hybrid-Channel Communication with Digital Twinning. *Electronics (Switzerland)*, 12(9), 1–24. https://doi.org/10.3390/electronics12092128

[19] Lee, W. S., John, A., Hsu, H. C., Hsiung, P. A. (2022). A Smart and Private Blockchain-enabled Framework for Digital Assets. *ACM International Conference Proceeding Series*, December 2022, 34–39. https://doi.org/10.1145/3581971.3581976

[20] Liang, X., Zhao, J., Chen, Y., Bandara, E., Shetty, S. (2023). Architectural Design of a Blockchain-Enabled, Federated Learning Platform for Algorithmic Fairness in Predictive Health Care: Design Science Study. *Journal of Medical Internet Research*, *25*. https://doi.org/10.2196/46547

[21] Malomo, O., Rawat, D., Garuba, M. (2020). Security through block vault in a blockchain enabled federated cloud framework. *Applied Network Science*, *5*(1). https://doi.org/10.1007/s41109-020-00256-4

[22] Mohammed, M. A., De-Pablos-Heredero, C., Botella, J. L. M. (2025). Mapping the transformative realm of blockchain-enabled central bank digital currencies: a bibliometric analysis. *Eurasian Economic Review*, 15(1). https://doi.org/10.1007/s40822-024-00307-6

[23] Mohammed, M. A., De-Pablos-Heredero, C., Montes Botella, J. L. (2023). Exploring the Factors Affecting Countries' Adoption of Blockchain-Enabled Central Bank Digital Currencies. *Future Internet*, 15(10), 1–14. https://doi.org/10.3390/fi15100321

[24] Radeva, I., Popchev, I. (2022). Blockchain-Enabled Supply-Chain in Crop Production Framework. *Cybernetics and Information Technologies*, 22(1), 151–170. https://doi.org/10.2478/cait-2022-0010

[25] Rangwala, M., Buyya, R. (2025). TrustMesh: A Blockchain-Enabled Trusted Distributed Computing Framework for Open Heterogeneous IoT Environments. *Proceedings - 2025 IEEE 22nd International Conference on Software Architecture,* ICSA 2025, 131–141. https://doi.org/10.1109/ICSA65012.2025.00022

[26] Rustiana, D., Ramadhan, D., Wibowo, L., Nugroho, A. W. (2022). State of the Art Blockchain Enabled Smart Contract Applications in the University. *Blockchain Frontier Technology*, 2(2), 70–80. https://doi.org/10.34306/bfront.v2i2.229

[27] Sarfaraz, A., Chakrabortty, R. K., Essam, D. L. (2023). AccessChain: An access control framework to protect data access in blockchain enabled supply chain. *Future Generation Computer Systems*, *148*, 380–394. https://doi.org/10.1016/j.future.2023.06.009

[28] Shah, M. A., Raj, N. (2025). Examining the role of blockchain and public-private partnerships in design and deployment of blockchain-enabled CBDC. *Digital Business*, 5(1), 100111. https://doi.org/10.1016/j.digbus.2025.100111

[29] Yadav, J. K., Verma, D. C., Jangirala, S., Srivastava, S. K. (2021). An IAD type framework for Blockchain enabled smart tourism ecosystem. *Journal of High Technology Management Research*, 32(1), 100404. https://doi.org/10.1016/j.hitech.2021.100404

[30] Zhan, Y., Xiong, Y., Xing, X. (2023). A conceptual model and case study of blockchain-enabled social media platform. *Technovation*, 119, 102610. https://doi.org/10.1016/j.technovation.2022.102610