www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 14 Issue 06 June 2025, Page No. 27369-27375
ISSN: 2319-7242 DOI: 10.18535/ijecs/v14i06.5164

Blockchain Solutions for the Verification of Manufacturing Data in Supply Chains

Vladyslav Vodopianov

Senior Software Engineer at Wirex
Kyiv, Ukraine

Abstract
The article investigates the problem of ensuring the veracity and traceability of production data in digital factories, where EU regulatory requirements and a high level of counterfeiting create a critical deficit of trust in source information. The objective of this study is to analyze the architectures of blockchain solutions for data verification in supply chains and to develop a phased implementation plan that considers regulatory obligations and the protection of trade secrets. The novelty lies in a combined approach: classification of DLT networks according to scalability, cost, and privacy criteria; use of Merkle trees and zero-knowledge proofs to preserve confidential data while proving authenticity; and justification of architecture choice through practical case studies (IBM Food Trust, VeChain, Airbus/Circularise, SAP). The study demonstrates that blockchain enables a reduction in batch traceability time from days to seconds, a reduction in manual operations to 67%, and an increase in data matching accuracy to 92%. However, the immutability of the ledger does not eliminate the immutable garbage problem: the veracity of records depends on sensor calibration and procedural control, which requires preliminary semantic normalization and master data management. A phased implementation enables the minimization of risks and the assessment of economic impacts. To comply with DPP, it is recommended to introduce decentralized identifiers (DID) and Verifiable Credentials, as well as the integration of zero-knowledge proofs. Thus, blockchain transitions from a trial technology to a necessary component of the practical infrastructure for sustainable production chains. This article will help managers and experts in digitalization and supply chain management.

Keywords: Blockchain, Data Verification, Supply Chains, Digital Manufacturing, Digital Product Passport, Smart Contracts, Merkle Trees, Zero-Knowledge Proofs, Permissioned Networks, Verifiable Credentials.

Introduction

Digital factories generate terabytes of data daily from sensors, MES systems, and ERP modules; this information feeds AI models, enables rapid line reconfiguration, and meets growing regulatory requirements. In a 2025 survey [1], 92% of executives identified smart manufacturing as the primary factor of competitiveness for the next three years, and 78% already allocate more than one-fifth of their improvement budgets to such initiatives. However, the information flow is only as valuable as the trust that supply chain participants place in it. Nearly 70% of manufacturing companies acknowledge that the most serious obstacle to scaling AI remains issues of quality, contextualization, and validation of source data [2]. It was no surprise that, in August 2024, 61% of the surveyed logistics top managers stated that trust is extremely important, and only 11% of them expressed a high level of confidence in technology providers. As a result, the risks—regulatory and commercial related to counterfeits, errors in certification, and untimely product recalls are increasing [3].

It is against this background that blockchain is considered a technological response, as it constructs an immutable, distributed trust layer on top of existing IT systems. Every transaction—from test results of a

batch to heat treatment parameters—is recorded cryptographically, and retroactive alteration becomes virtually impossible.

Thus, on the one hand, the industry is ripe for systematic data management, and on the other hand, it experiences a critical deficit of trust in the data itself. Blockchain, which ensures the provable provenance and integrity of records, forms the necessary foundation. In subsequent sections, we will examine the DLT architectures manufacturers apply and how this is already changing practice in the verification of materials, operations, and the sustainability of supplies.

Materials and Methodology

The study is based on an analysis of industry reports and practical case studies described by Deloitte [1, 2] and Talking Logistics [3, 5]. The market dynamics of blockchain are illustrated by the report of The Business Research Company [4]. EU regulatory requirements (CSRD and DPP) establish the obligation to have a verifiable digital product passport by 2027–2030 [6, 11], while U.S. FAA data show that up to 2% of aviation components annually turn out to be counterfeit [7].

The methodology includes four stages: (1) collection and content analysis of data from Deloitte, Talking Logistics, and EU directives [1–6] to identify key trust issues and regulatory requirements; (2) classification of blockchain architectures considering scalability, privacy, and transaction cost issues [4]; (3) qualitative analysis of practical cases [8–10]; (4) collection of quantitative metrics (reduction of traceability time, share of manual operations, nonconformance coefficient, percentage of automated audits—as exemplified by the SAP solution [12]) and assessment of hidden costs. Based on this, a phased implementation plan was developed, which included mapping the product lifecycle, semantic normalization of data, selection of network architecture, piloting on a limited SKU group with the recording of baseline metrics, and subsequent scaling. This plan took into account regulatory requirements and zero-knowledge proof mechanisms to protect trade secrets.

Results and Discussion

Most manufacturers still manage data in isolated ERP, MES, and PLM systems, and information exchange between supply chain participants occurs via spreadsheets and email. As a result, visibility breaks down already at the Tier-2 level: according to a survey [5], only 6% of companies reported having an end-to-end view of all material and operational flows, whereas the remainder must reconcile data manually, losing time and creating room for errors.

At the same time, the regulatory burden is tightening. Since 2024, the first enterprises have come under the CSRD directive, which requires the inclusion of verifiable sustainability and traceability indicators in annual reports. With the same horizon, the EU has launched the Digital Product Passport program, demanding that almost every good have a digital passport with a verifiable provenance history and carbon footprint. Inability to rapidly collect confirmed data threatens fines and loss of access to the European market [6]. The stages of development are shown in Fig. 1.

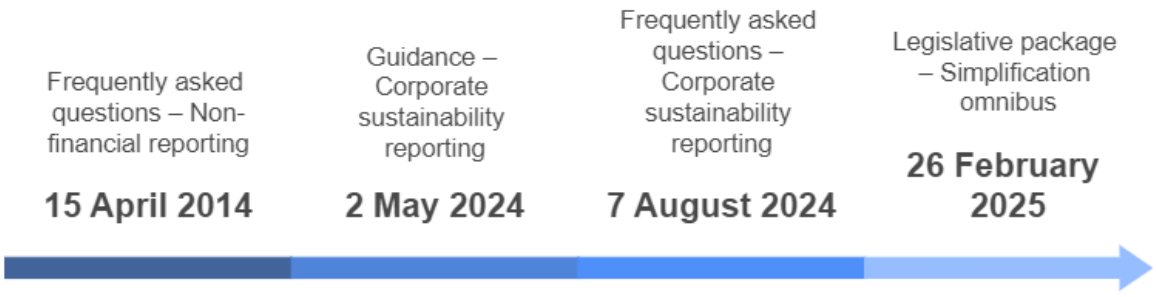

Fig. 1. Timeline of Development of CSRD [6]

To the transparency deficit is added the factor of counterfeiting: the U.S. Federal Aviation Administration estimates that up to 520,000 uncertified or counterfeit parts enter airplanes annually, comprising approximately 2% of the turnover of aviation components and directly affecting passenger safety [7].

Blockchain eliminates these systemic vulnerabilities by creating an immutable ledger that all participants in the supply chain have equal access to. In this model, information on a batch, heat treatment

settings, or test results is noted by a hash reference; backward changes to the record can't happen without the approval of most nodes, which turns trust into a checkable mathematical promise.

Along with basic immutability, it shifts quality control and standard compliance from manual to automated transfer. The code that is deployed on the network verifies, for instance, that all protocols for sterilization and the serial numbers of sensors for a medical device are correctly loaded. If at least one parameter is missing or falls outside the MDR tolerance, the batch is blocked before shipping.

Cryptographic mechanisms underlying the ledger enhance transparency without disclosing trade secrets. The Merkle-tree root hash enables verification that a specific report is included in a block without revealing other records, and zero-knowledge proofs allow for proving compliance with a formulation or emission norm without disclosing the formula itself. Finally, the linkage of blockchain with physical sensors and digital twins closes the last gap between the real object and the digital record. Thus, the distributed ledger unifies the fragmented IT landscape, responds to regulators' challenges, and sharply reduces counterfeiting risks, moving the discussion of trust from agreements to the realm of algorithmic guarantees.

Deployment models of blockchain for production data verification can be categorized into three types: consortium permissioned networks, open L1/L2 platforms with native tokens, and hybrid schemes where private ledgers are periodically anchored on the public layer. Choice of architecture has a direct economic dimension: analysts [4] estimate that by 2025 the global blockchain market for supply chains will amount to USD 3.27 billion with a forecasted CAGR of 59.8% until 2034; therefore, the ability of the network to scale without explosive cost growth becomes critical, as shown in Fig. 2.

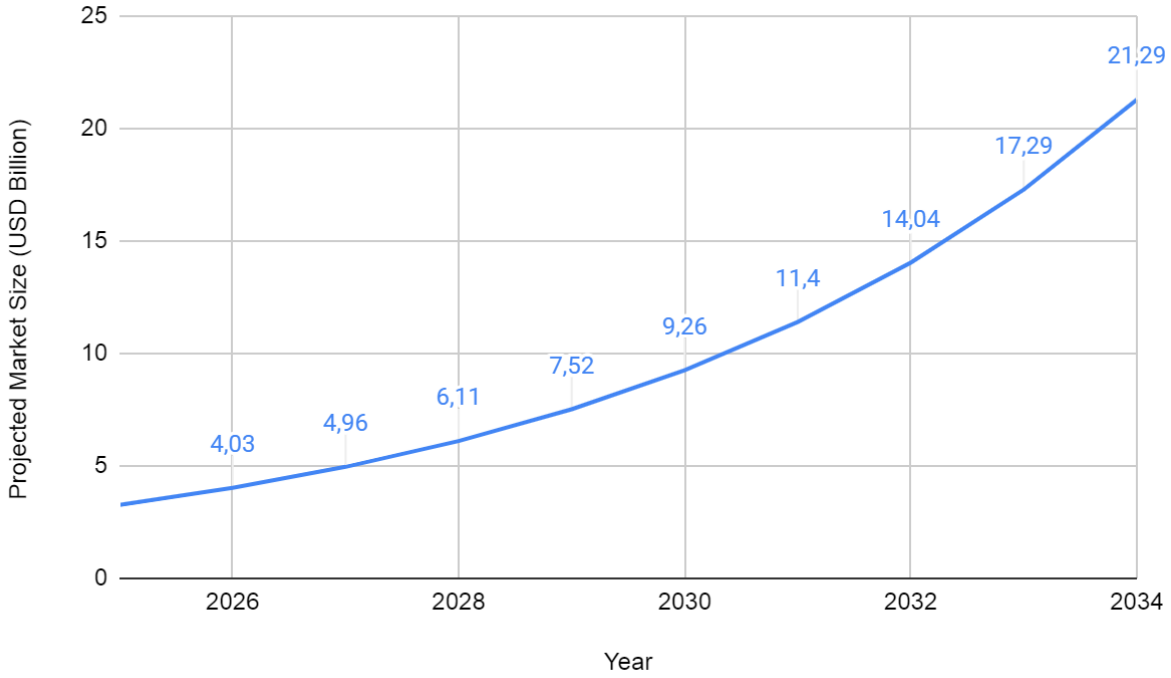

Fig. 2. Projected Global Blockchain Market Size for Supply Chains [4]

Consortium networks are built around a limited circle of validators and a built-in service for participant identity management. Hyperledger Fabric, the underlying technology of IBM Food Trust, is illustrative: a transaction is admitted into the ledger only after verification of X.509 certificates and signatures from multiple organizations, which eliminates the need for a centralized intermediary and reduces the risk of unilateral history alteration. Walmart's practice has proven the effectiveness of the approach: mango traceability time from store shelf to farm was reduced from seven days to 2.2 seconds, with more than twenty products and five major suppliers already participating in the network [8].

Public L1/L2 platforms rely on open consensus and economic incentives, which are facilitated by a native token. This design simplifies the onboarding of new enterprises, which only need to generate a smart contract and pay gas to anchor data; the absence of a closed list of nodes increases credibility in the eyes of regulators. The hybrid variant combines the privacy of the first and the openness of the second: the complete set of technological parameters is stored in the enterprise's private database. At the same time, only a hash fingerprint of the data block is committed to the public chain.

These architectural principles are already reflected in active projects. In the food industry, IBM Food Trust demonstrates that a permissioned network can reduce outbreak investigation time from weeks to seconds, thereby diminishing the scope of preventive product recalls [8].

In pharmaceuticals, VeChain put together blockchain with the cool chain of vaccine keeping: every temperature shift is noted by a sensor, signed, and shared in the open system, which lets authorities and hospitals check batch truthfulness right away, thus dealing with the main reason of more than 100 000 yearly deaths from fake medicines [9].

At the aviation cluster, Airbus finished a Proof of Concept with Circularise. It means digitizing passports for aircraft cabin materials. This digital passport compiles data from suppliers, MRO centers, and recyclers. The record is public, but the specifications are stored by participants themselves, which makes later recycling easier and increases trust in secondary components [10].

The run of the regulatory vector is set not by the market but by Brussels. In spring 2024, the Regulation on Ecodesign of Sustainable Products (ESPR) adopted the Digital Product Passport (DPP) as the mandatory mechanism for verifying product provenance and environmental characteristics. The document defines a unified machine-readable data format to be retained for at least ten years. It prescribes that by 2027, batteries, electronics, and textiles must have a passport, and by 2030, almost all goods entering the EU market must be likewise [11]. The legislative development grid is presented in Fig. 3.

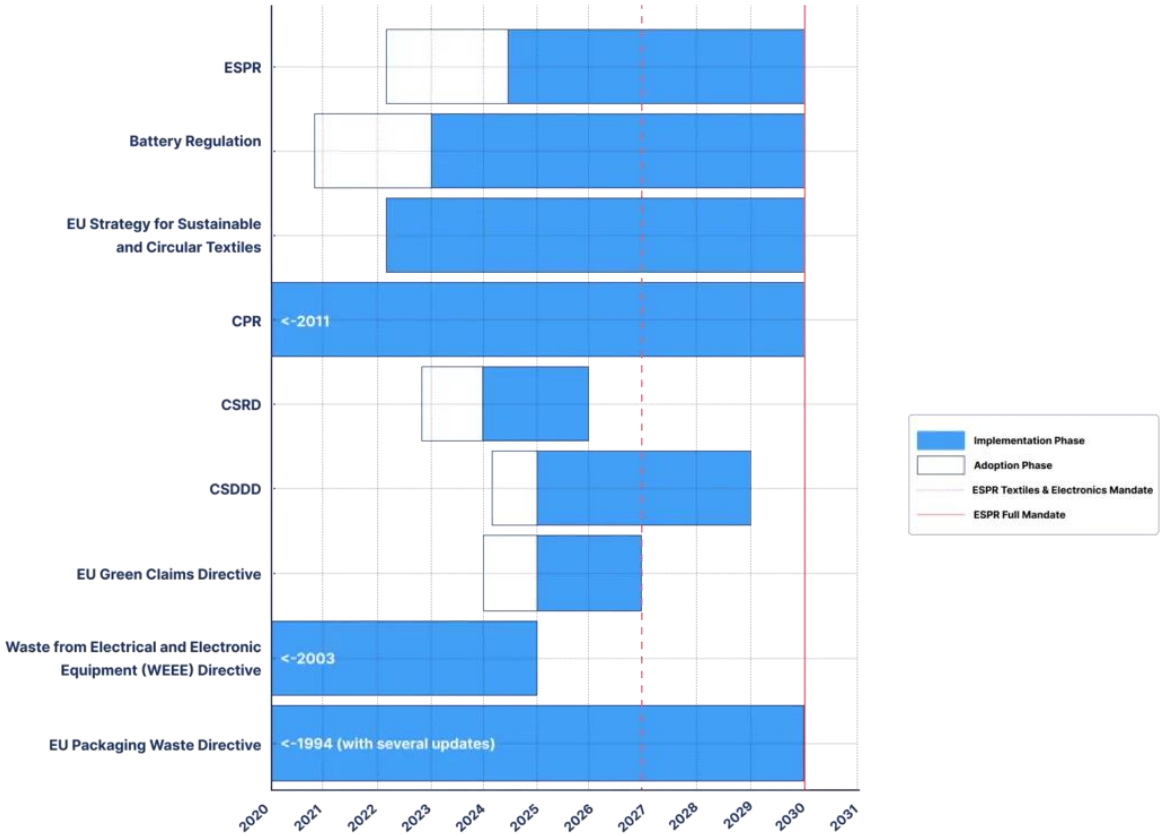

Fig. 3. EU Regulatory Implementation Timeline for Sustainability and Circular Economy Directives [11]

To ensure that DPP remains open while protecting trade secrets, the European blockchain service infrastructure, EBSI, has implemented a model using decentralized identifiers (DIDs) and Verifiable Credentials. Each participant—from fiber manufacturer to service center—issues a credential signature, and the consumer or inspector verifies the trust chain without resorting to a central registrar.

The technological landscape is rapidly adapting to new requirements. First, manufacturers increasingly use zero-knowledge proofs to confirm that a formulation or heat-treatment regime has been followed without disclosing the process formula itself. Second, the demand for scalability has compelled enterprises to transition from private networks to modular L2 solutions with a separate data availability layer. Third, immutable logs create new grounds for analytics. Finally, sustainability is becoming a digital

asset: tokenized carbon-neutrality certificates enable automatic emission verification, making the circulation of carbon units as transparent as the movement of parts along the production line.

Thus, the regulatory pressure codified in DPP has accelerated the technological shift: blockchain is gradually becoming not an auxiliary technology but a mandatory infrastructure layer on which both the legal and economic models of the future supply chain are built.

Experience in deploying distributed ledgers in manufacturing shows that the primary operational advantage is a dramatic reduction in traceability cycle time. Such a short response time is critical, even in hard industries. Aircraft manufacturers integrating blockchain into load-testing logs report a decrease in delays due to manual checks, as every change in a part's parameters is recorded and validated before the item leaves the shop floor, rather than at the end of the production cycle.

This is where the monetary effect gets manifested in audits and reports. In another study on an SAP-centric reconciliation framework, smart contracts increased invoice-matching correctness to 92%, reduced the time for each reconciliation by 41%, and eliminated 67% of manual operations — thus transforming three-way matching into a constant background process [12]. Still, cryptographic immutability does nothing to fix the so-called oracle issue: if either a device or a human supplies incorrect information, then that immutable garbage will be retained by the blockchain forever. Therefore, trust in the records still depends on sensor calibration, procedural discipline, and multi-level selective audit schemes. Another barrier is the cost of integration and standardization. Capex is exacerbated by multi-stage harmonization of formats. Consequently, companies evaluating the efficacy of blockchain must account not only for the direct benefits of rapid traceability and automated auditing but also for the hidden costs of ensuring the veracity of source data and bringing systems to common standards.

Deploying blockchain technologies in manufacturing supply chains should begin with a formalized mapping of data flows. It is necessary to identify product lifecycle events that lead to non-conformity with quality or regulatory requirements and to record them in a system of key performance indicators in a quantitative manner. Such preliminary taxonomy ensures verifiable implementation effects and eliminates the risk of transferring redundant or irrelevant information into the immutable ledger, which in turn reduces storage and processing infrastructure load.

After clarifying the data composition, semantic normalization and master data management procedures must be implemented. Eliminating duplicate entries, unifying measurement units, and introducing unified identifiers for counterparties and materials ensure unambiguous matching of records in the distributed ledger. Blockchain immutability will thereby preserve whatever initial sampling errors it has picked up and hence maintain or increase the probability of false triggers in automated control mechanisms.

The degree of trust between the parties, the throughput desired, and the sensitivity of the data being transmitted should dictate the choice of network architecture. Under a consortium permissioned network, rules are established regarding who can enter and what transactions are permitted; however, this limits the system's growth potential if there are many external helpers. Open L1/L2 platforms make starting easy and cheap, but we want a tighter secret-keeping rule. A mix model is a bet: all the making data remains nearby, and only code-like marks are shared with the public layer, preserving unchangeable proof without disclosing business secrets.

Implementation is advisable in a phased approach: first, a pilot project is conducted on a limited section of the production line or within one SKU group. Then, based on the experimental evaluation results, scaling is implemented to adjacent sections, tier-2 suppliers, and logistics nodes. During the pilot, it is critical to record baseline metrics, such as average batch traceability time, the number of manual operations, and the non-conformance coefficient. Further expansion should be accompanied by reviewing the role and permission matrix and adapting smart contracts for the extended set of scenarios.

The final element of the strategy is proactive alignment with the upcoming regulatory context. Considering the mandatory digital product passport in the EU, the architecture must support decentralized identifiers and Verifiable Credentials, ensuring verifiable provenance without requiring queries to closed ERP systems. To protect intellectual property, the integration of zero-knowledge proofs is recommended, allowing for the validation of process compliance or carbon limits without revealing commercial information.

Conclusion

With the rapid increase in data volumes in digital factories and the tightening of rules, old ways of sharing information, which often rely on spreadsheets through ERP and MES systems, no longer provide the necessary clarity and trustworthiness. This leads to dangers in developing AI solutions and also in fulfilling EU rules for a Digital Product Passport, which requires verifiable histories of where items have been and environmental labels for goods.

Blockchain provides a solution by forming an immutable and distributed ledger, wherein all transactions relating to both heat-treatment parameters and test results are recorded cryptographically. Smart contracts automatically execute quality checks and regulatory compliance. Merkle trees and zero-knowledge proofs maintain business secrets in the presence of data authenticity. Integration with physical sensors and digital twins reduces the 'bucket-of-garbage' immaturity risk. Still, blockchain immutability itself does not resolve the veracity of source data: record reliability depends on sensor calibration and procedural control.

The architecture choice (permissioned consortium, open L1/L2 platforms, or hybrid schemes) must consider the level of trust among participants, the required throughput, and data confidentiality. Phased implementation—starting with a pilot project and recording key traceability metrics, the number of manual operations, and non-conformances—allows for the assessment of effects and the adaptation of smart contracts and permission matrices before scaling. Semantic normalization and master data management eliminate duplication and increase verification accuracy.

Given the mandatory Digital Product Passport and evolving European legislation, the architecture must support decentralized identifiers (DID) and Verifiable Credentials. The integration of zero-knowledge proofs will enable the verification of technological processes and carbon footprint without disclosing confidential information. Thus, blockchain gradually transitions from an experimental technology into a critical element of operational infrastructure capable of providing a mathematically guaranteed level of trust in production data.

References

1. T. Gaus, “2025 Smart Manufacturing and Operations Survey: Navigating challenges to implementation,” Deloitte, May 01, 2025. https://www2.deloitte.com/us/en/insights/industry/manufacturing/2025-smart-manufacturing-survey.html (accessed May 05, 2025).
2. J. Coykendall, K. Hardin, and J. Morehouse, “2025 Manufacturing Industry Outlook,” Deloitte, Nov. 20, 2024. https://www2.deloitte.com/us/en/insights/industry/manufacturing/manufacturing-industry-outlook.html (accessed May 06, 2025).
3. A. Gonzalez, “Trust More: A New Year’s Resolution for Supply Chain Executives,” Talking Logistics, Jan. 08, 2025. https://talkinglogistics.com/2025/01/08/trust-more-a-new-years-resolution-for-supply-chain-executives/ (accessed May 08, 2025).
4. “Blockchain Supply Chain Global Market Report 2025,” The Business Research Company, 2025. https://www.thebusinessresearchcompany.com/report/blockchain-supply-chain-global-market-report (accessed May 08, 2025).
5. “Supply Chain Statistics,” Procurement Tactics, Apr. 23, 2025. https://procurementtactics.com/supply-chain-statistics/ (accessed May 09, 2025).
6. “Corporate Sustainability Reporting,” European Commission. https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en (accessed May 10, 2025).
7. D. Shaff, “Counterfeit Components Ground Airlines,” Connector Supplier, Dec. 12, 2023. https://connectorsupplier.com/counterfeit-components-ground-airlines/ (accessed May 10, 2025).
8. “How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric,” The Linux Foundation. https://www.lfdecentralizedtrust.org/case-studies/walmart-case-study (accessed May 12, 2025).
9. A. Makena, “VeChain’s Blockchain Gives WHO a New Weapon Against Counterfeit Drugs - Crypto News Flash,” Crypto News Flash, May 28, 2025. https://www.crypto-news-flash.com/vechain-gives-who-a-new-weapon/ (accessed Jun. 04, 2025).
10. “Circularise, Airbus complete blockchain traceability PoC for recycling aircraft cabins,” Ledger Insights, May 30, 2024. https://www.ledgerinsights.com/circularise-airbus-complete-blockchain-traceability-poc-for-recycling-aircraft-cabins/ (accessed May 15, 2025).

11. “Digital Product Passport: The Complete Guide,” Protokol, Oct. 21, 2022. https://www.protokol.com/insights/digital-product-passport-complete-guide/ (accessed May 16, 2025).
12. N. H. Jamithireddy, “Blockchain-Based Supply Chain and Finance Reconciliation Frameworks in SAP Environments,” Research Briefs on Information and Communication Technology Evolution, vol. 10, pp. 190–210, Dec. 2024, doi: https://doi.org/10.69978/rebicte.v10i.206.