Title

# DESIGN AND IMPLEMENTATION OF MALA-LINK: A CITIZEN-CENTRED INTER-AGENCY SERVICE PLATFORM FOR MALAWI

Author

**LEE RODRICK CHIZINGA**

Co-Author

**MISS FANNY CHATOLA**

Issued October 2026 Certificate

AR2026SDTJBK

## ABSTRACT

Financial fraud, fragmented record keeping, weak supply chain visibility and counterfeit goods continue to reduce accountability in many Malawian organisations. Government institutions, non-governmental organisations (NGOs), small and medium-sized enterprises (SMEs) and agricultural cooperatives often manage accounting, procurement, inventory and logistics through separate tools, spreadsheets or paper records. Commercial enterprise resource planning (ERP) systems that could unify these functions are frequently too costly and complex for resource-constrained settings. This paper presents the Artificial Intelligence Secure Financial Supply Chain System (AI-SFSS), a web-based platform that consolidates financial management and supply chain operations in a single browser-accessible environment. The frontend is implemented with React 19, TypeScript and TanStack Router. The backend uses Supabase, which supplies a PostgreSQL database, authentication, file storage, Row-Level Security (RLS) and real-time subscriptions. Serverless Supabase Edge Functions running on Deno perform fraud scoring, receipt extraction, forecasting and hash generation, and the application is deployed on Cloudflare Workers. The system supports six user roles and covers transaction and budget management, AI-assisted fraud risk scoring, OCR-based invoice and receipt processing, inventory, supplier and purchase order management, shipment tracking on an interactive map, QR-based product verification, predictive analytics, notifications, integrations, settings and reporting. A lightweight blockchain-style ledger records SHA-256 hashes of financial and supply chain records, linked to the previous record, so that inconsistent changes to stored records are detectable through a Verify Record function. It is a hash-chained ledger within the application's own database, not a decentralised blockchain network. The project report documents 24 functional test cases, all recorded as passing, together with qualitative feedback from a selected group of potential users. No formal survey instrument, participant count or performance measurement is available, and the platform has not been connected to live bank, government or logistics systems. The work therefore demonstrates an implemented application prototype and the technical feasibility of combining these capabilities on low-cost cloud infrastructure, rather than a field-validated reduction in fraud or operating cost. The paper describes the system design, the integrity-ledger mechanism, the preliminary functional evidence, and the limitations that must be addressed before operational deployment.


**KEYWORDS:** Artificial intelligence, fraud detection, supply chain management, blockchain, SHA-256, optical character recognition, predictive analytics, role-based access control, Supabase, Malawi

## INTRODUCTION

Information and communication technologies have changed how organisations manage money, goods and records. Artificial intelligence (AI), machine learning (ML), cloud computing, blockchain-style record keeping and optical character recognition (OCR) allow routine tasks to be automated, anomalies to be flagged earlier, and decisions to be supported by data rather than assumption. In Malawi and many other developing economies, however, these benefits are unevenly realised. Public institutions, NGOs, SMEs and agricultural organisations frequently run finance, procurement, inventory and logistics as disconnected activities, supported by spreadsheets, paper files and separate applications. The effects are familiar to practitioners: duplicated data, inconsistent reports, delayed reconciliation, limited visibility of goods in transit, and few automated safeguards against irregular payments.

Traditional accounting and procurement software tends to record transactions after they have happened. Fraud is then discovered through periodic audits or rule checks, by which time the money may already be lost. Documents such as invoices and receipts are typed in by hand, which introduces errors and delays. Stock levels, purchase orders and shipments are tracked in different places, so a manager cannot easily see whether goods ordered have been received, where a consignment is, or whether a product is genuine. Conventional databases also offer little help when an auditor wants evidence that a record has not been altered since it was created.

This paper describes the design and implementation of the Artificial Intelligence Secure Financial Supply Chain System (AI-SFSS), a cloud-based platform intended to address these problems within one environment. AI-SFSS combines financial management, supply chain management, AI-assisted fraud risk scoring, OCR-based document processing, QR-based product verification, shipment tracking, predictive analytics and a hash-chained integrity ledger. It is built on commodity, pay-as-you-use cloud services so that the cost of adoption stays within reach of organisations that cannot afford a conventional ERP system.

## BACKGROUND OF THE STUDY

Sub-Saharan African organisations operate under constraints that shape how enterprise software must be designed. Connectivity can be unreliable, technical staff are scarce, budgets are limited, and many users have little formal training in information systems. At the same time, the sectors that matter most to national development, including public administration, health supply, agriculture and humanitarian relief, depend on accurate financial control and dependable logistics. Weak financial governance in these sectors has direct consequences: money intended for services is lost to duplicate payments, inflated invoices or fictitious suppliers, and goods intended for beneficiaries are delayed, diverted or replaced by substandard or counterfeit products.

Four related problems motivate this study.

- **Fragmentation.** Accounting, procurement, inventory, shipment tracking and reporting are commonly handled in separate tools or on paper. Data must be re-entered between them, and no single view of an organisation's financial and physical position exists.
- **Late detection of fraud.** Duplicate payments, invoice manipulation, unusual vendors and unauthorised expenditure are typically found during periodic audits rather than at the time of the transaction.
- **Limited traceability and counterfeit risk.** Without product-level identification and shipment histories, it is hard to confirm that goods are genuine or to reconstruct where they have been. In agriculture and healthcare, counterfeit inputs and medicines threaten both livelihoods and safety.
- **Weak assurance of record integrity.** Ordinary database records can be edited without leaving a visible trace unless extensive audit logging is in place, which reduces confidence during audits.

Commercial ERP suites can integrate finance and supply chain functions, but licensing, infrastructure and specialist support requirements place them out of reach for many Malawian organisations. Modern serverless platforms change this calculation. A backend-as-a-service layer provides database, authentication and real-time messaging without dedicated servers, edge hosting provides global delivery at low cost, and open-source front-end frameworks remove licence fees. AI-SFSS was developed to test whether these building blocks can deliver an integrated, intelligent and secure platform suitable for the Malawian context.

The contribution of the paper is practical rather than theoretical. It documents how financial control, supply chain visibility, document automation and tamper-evident record keeping were combined in one working prototype, how the components were designed and tested, and what the available evidence does and does not show.

## RESEARCH OBJECTIVES

### General Objective

- To design, develop and implement an Artificial Intelligence Secure Financial Supply Chain System (AI-SFSS) that improves financial management and supply chain operations through the integration of artificial intelligence, hash-based record verification, optical character recognition, predictive analytics and cloud computing.

**Specific Objectives**

- To design and develop a secure web-based platform that integrates financial management and supply chain management in a unified cloud environment.
- To implement AI-based analysis of financial transactions that assigns fraud risk scores, classifies risk levels and generates alerts for review.
- To integrate OCR so that vendor, date, currency, amount and line-item information is extracted automatically from invoices and receipts.
- To implement hash-based verification that supports the integrity, traceability and auditability of financial and supply chain records.
- To develop integrated modules for suppliers, inventory, purchase orders, shipment tracking and QR-based product verification.
- To implement predictive analytics for expenditure, procurement and inventory demand.
- To implement secure authentication and role-based access control (RBAC) so that users reach only the resources their roles permit.
- To generate financial, procurement, inventory, fraud and management reports that support auditing and decision-making.

## LITERATURE REVIEW

The literature relevant to AI-SFSS spans software engineering practice, information security, blockchain in supply chains, machine learning for fraud detection, document automation and cloud-native platforms. Each strand informed part of the design. Each also leaves a gap that the integrated system attempts to address.

### Software Engineering and Security Foundations

*Pressman and Maxim (2020)* explain that agile software development improves quality by promoting iterative delivery, continuous testing and regular user feedback. Agile methods let teams respond to changing requirements while still producing maintainable software. Their treatment is deliberately general, however, and does not address intelligent financial and supply chain systems. These principles nevertheless guided the sprint-based development of AI-SFSS, where requirements such as inventory management, shipment mapping and record verification were added during later stages.

*Sommerville (2020)* emphasises that modern enterprise software should be scalable, maintainable, secure, reliable and flexible so that it can support long-term organisational growth. The argument is persuasive, but the book gives limited attention to applications that combine AI, blockchain-style verification and predictive analytics. The modular, layered design of AI-SFSS follows these quality attributes.

*The National Institute of Standards and Technology (2020),* in its security and privacy control catalogue, stresses confidentiality, integrity and availability, and recommends authentication, access control, encryption and audit logging to protect organisational information systems. The guidance does not consider AI or blockchain as components of financial and supply chain security. It nevertheless shaped the role-based access control, Row-Level Security policies and activity logging implemented in AI-SFSS.

### Blockchain in Supply Chains

*Kshetri (2021)* reviews how blockchain can increase supply chain transparency by providing secure, tamper-resistant records for procurement, logistics and inventory. The study provides limited discussion of combining blockchain with AI for fraud detection and predictive decision-making. Caldarelli, Zardini and Rossignoli (2021) report that blockchain strengthens trust, data integrity and transparency among business partners and so contributes to supply chain sustainability. Their work does not consider OCR or predictive analytics for intelligent enterprise operations.

*Tsolakis et al. (2022)* show that combining AI with blockchain improves supply chain performance through better decisions, sustainability and efficiency. They report limited practical implementation inside integrated financial management systems. *Charles, Emrouznejad and Gherman (2023)* offer a critical analysis of blockchain and AI integration for supply chains, and *Hossain et al. (2025)* examine blockchain-AI approaches to fraud detection and transparency across multi-tier global supply chains. Both emphasise the potential of the combination while noting that practical implementations remain uneven.

*Baayeh et al. (2025),* in a systematic review of blockchain-based transparency in global supply chains, report that blockchain improves traceability and organisational trust but continues to face scalability and interoperability challenges, with little integration with OCR or predictive analytics. These findings are relevant to the design choice made here. Full distributed ledgers bring operational complexity and cost, so AI-SFSS adopts a lighter hash-chaining approach and identifies a permissioned ledger as future work.

*Anjum and Dutta (2022)* investigate blockchain and QR code technology for product authentication and show that QR codes linked to blockchain records help reduce counterfeit products entering supply chains. Their study concentrates on counterfeit detection and does not address wider enterprise functions such as financial management, procurement, inventory control or predictive analytics. *Yadav, Singh and Gupta (2024)* similarly examine QR-based authentication systems for counterfeit detection, which supports the use of QR codes as a low-cost verification channel in field settings.

**Artificial Intelligence and Fraud Detection**

*IBM (2024)* describes the growing role of AI in enterprise information systems, including intelligent automation, anomaly detection, predictive analytics and data-driven decision-making. The publication is a broad overview and does not discuss implementation within integrated financial and supply chain systems. *Lokanan and Maddhesia (2025)* demonstrate that machine learning improves the accuracy of supply chain fraud prediction by identifying hidden transaction patterns and abnormal financial behaviour. They also stress that human oversight remains necessary to interpret high-risk transactions and validate AI-generated decisions. This point directly influenced the review workflow in AI-SFSS, in which flagged transactions are queued for authorised users rather than blocked automatically.

*Farrukh et al. (2025)* demonstrate that combining blockchain with machine learning and federated learning can improve fraud detection while preserving organisational privacy. They recommend further research on adaptive AI models and cross-industry validation. *Allaparthi (2024)* discusses the use of AI in supply chains for fraud detection and authenticity verification, and *Alevizos (2025)* explores AI, blockchain and smart contracts for automated cybersecurity compliance. Together these studies indicate that the individual techniques are mature enough to be combined, but they do not describe a deployable, affordable platform for low-resource organisations.

**Document Automation and Cloud-Native Platforms**

*Google Cloud (2025)* explains that OCR automates document processing by extracting structured information from invoices, receipts and scanned documents, reducing manual entry while improving accuracy. The material does not integrate OCR with AI-based fraud detection or a wider financial management system. In AI-SFSS the output of OCR is linked to transaction records, which are in turn passed to the fraud scoring service.

*Supabase (2025)* describes cloud-native backend platforms as providing scalable databases, secure authentication, storage and real-time synchronisation. The discussion is focused on infrastructure rather than on intelligent business processes. The PostgreSQL Global Development Group (2025) documents PostgreSQL as a secure, reliable and scalable relational database with strong transactional consistency, and notes its row-level security facilities. It does not address AI or predictive analytics inside enterprise databases. These two sources underpin the technology choices of AI-SFSS, particularly

the enforcement of access rules at the database level.

Studies of digital transformation in developing economies and of governance in African organisations *(Alzoubi, Ahmed and Alshurideh, 2023; Osei and Asante, 2024)* point to the value of integrated systems for accountability but also to resource and skills constraints. These constraints reinforce the case for low-cost, simple-to-use platforms.

## SUMMARY REVIEW AND RESEARCH GAP

The literature shows considerable progress in each of the technologies considered. Software engineering and security guidance *(Pressman and Maxim, 2020; Sommerville, 2020; NIST, 2020)* establishes the importance of iterative development, scalability and strong access control. Blockchain studies *(Kshetri, 2021; Caldarelli et al., 2021; Tsolakis et al., 2022; Baayeh et al., 2025; Farrukh et al., 2025)* demonstrate benefits for transparency, traceability and fraud prevention. AI and machine learning studies *(IBM, 2024; Lokanan and Maddhesia, 2025)* show gains in anomaly detection and forecasting, and OCR material *(Google Cloud, 2025)* shows the effect of document automation on accuracy and efficiency.

The same literature identifies consistent limitations.

- Most studies concentrate on one technology or one organisational function, such as fraud detection, blockchain, counterfeit control or cloud infrastructure.
- Few describe an integrated platform that joins financial management, procurement, inventory, shipment tracking, counterfeit detection, record verification and forecasting.
- Little attention is given to affordability and operational simplicity for organisations in low-resource settings.
- Studies that combine blockchain and AI typically report limited practical implementation within financial management systems.

The research gap is therefore the absence of an integrated, intelligent, secure and affordable cloud-based system that combines AI, OCR, hash-based record verification, predictive analytics, and financial and supply chain management on one web platform. AI-SFSS is proposed as an implemented prototype that addresses this gap, while recognising that its evidence base is currently limited to functional testing and formative user feedback.

## METHODOLOGY

AI-SFSS was developed using the Agile Software Development methodology. Agile was chosen because the system integrates several technologies (AI, OCR, hash-based verification, cloud computing and real-time synchronisation) whose interaction could not be fully specified in advance. An iterative approach allowed each component to be built, tested and integrated incrementally, and allowed new requirements to be accommodated without disturbing completed modules. Inventory Management, Invoices and Receipts, Verify Record, Shipment Mapping, Integrations and Settings were all introduced or expanded during later sprints for this reason.

### Research and Development Approach

The study followed a software design and implementation approach. Needs identified through the problem analysis and literature review were translated into functional and non-functional requirements, then into a system design, an implementation and a set of functional checks. The development process comprised requirements identification, system analysis, system design, implementation of the principal modules, integration, testing and user feedback. The objective was to demonstrate the technical feasibility of combining financial management, supply chain management, AI-assisted analysis and record verification in one platform, and to examine whether selected

features operated as intended in the implemented environment.

The study did not involve deployment as a live system inside a partner organisation, connection to production banking or logistics services, or a controlled measurement of fraud losses, processing times or operating costs. These outcomes would require a separate study with a defined measurement protocol, baseline data and organisational participation.

### Requirements Analysis

Requirements were derived from the problem analysis and from the typical responsibilities of the organisational roles the system is intended to serve. They were recorded as 28 functional requirements (FR01 to FR28) and 12 non-functional requirements (NFR01 to NFR12). Functional requirements cover authentication and password recovery, six user roles, role-specific dashboards, transaction and budget management, fraud scoring and alerts, receipt upload and OCR, inventory, suppliers, purchase orders, shipments and shipment events, QR scanning, counterfeit incident recording, SHA-256 hashing and verification, predictive analytics, notifications, reports, integrations, settings and audit logging. Non-functional requirements address performance, security, reliability, availability, scalability, maintainability, usability, compatibility, portability, data integrity, backup and recovery, and auditability.

The platform is intended to run in a standard web browser (Google Chrome, Mozilla Firefox, Microsoft Edge or Safari) on a computer with at least an Intel Core i3 (8th generation) or AMD Ryzen 3 processor, 8 GB of memory, a 256 GB solid-state drive and a stable broadband connection. A smartphone running Android 10 or iOS 14 or later is recommended for QR scanning in the field. No client-side installation is required.

### Technologies Used

- **Front-End Framework and Language:** React 19 with TypeScript
- **Client-Side Routing:** TanStack Router
- **Backend platform:** Supabase backend as a service
- **Database:** PostgreSQL with Row-Level Security
- **Authentication:** Supabase Authentication (JWT-based)
- **Real-time updatets:** Supabase Realtime subscriptions
- **AI and ML processing:** Supabase Edge Functions (Deni and TypeScript) calling AI gateway

### Feasibility Considerations

Technical feasibility rested on the use of mature, well-documented technologies. Economic feasibility relied on free-tier and pay-as-you-use services, open-source libraries and the absence of dedicated server infrastructure, which together make the cost of building and running the platform low relative to a conventional ERP deployment. Operational feasibility considered whether users with varied technical expertise could use the system. A simplified interface, role-based dashboards and browser-only access were chosen for this reason, and QR scanning lets field agents verify products and shipments without full system access. These were design judgements recorded during analysis. No formal cost model or return-on-investment calculation was prepared.

## SYSTEM DESIGN AND DEVELOPMENT

### System Architecture and Technologies

AI-SFSS uses a multi-tier cloud architecture that separates presentation, application, AI, integrity, data and external integration concerns. Separation keeps each layer independently replaceable and supports the scalability and maintainability requirements.

- **Presentation layer.** A responsive React 19 and TypeScript single-page application, with client-side navigation managed by TanStack Router. It runs in desktop and mobile browsers and renders role-specific navigation and dashboards.

- **Application layer:** Business logic for transactions, budgets, procurement, inventory, shipments, reporting, authentication and notifications. Most of this logic runs in the client against the Supabase data API, with privileged operations placed in Edge Functions.
- **AI layer:** Supabase Edge Functions written in TypeScript and executed in the Deno runtime. They perform fraud scoring, receipt extraction, forecasting and hash generation. Calls to external AI models go through a configurable AI gateway whose address and key are held as environment secrets rather than in client code.
- **Integrity layer:** SHA-256 hashing of financial transactions, shipment events, purchase orders and inventory records, with stored hashes used by the Verify Record function.
- **Data layer:** PostgreSQL hosted on Supabase, with authentication, object storage for receipt files, Row-Level Security policies and Realtime subscriptions.
- **Integration layer:** Configuration for external banking, logistics, payment and ERP interfaces through secure APIs. This layer stores connection details and status. Live connections to production external systems were not established in this project.

### Algorithm Specification

The specified algorithm compares each new transaction with the submitting user's history and combines three indicators.

- Retrieve the user's previous transactions and compute their mean and standard deviation.
- Compute the z-score of the new amount: how many standard deviations it lies from the user's mean.
- Assign a vendor score of 0.8 if the vendor has not appeared in the user's history and 0.1 otherwise.
- Assign a duplicate score of 0.7 if a matching transaction occurred within the previous ten minutes, and 0 otherwise.
- Combine the indicators as a weighted sum.

The score is mapped to a risk level: 0.80 or higher is Critical, 0.60 to below 0.80 is High, 0.40 to below 0.60 is Medium, and below 0.40 is Low. High and Critical results trigger alerts. The method is transparent, and an auditor can see exactly why a transaction was flagged: an unusual amount, an unfamiliar vendor, a possible duplicate, or a combination. It also has limits that should be recognised. The z-score is undefined for users with fewer than two previous transactions or with zero variance, so a policy for new users is needed. The weights and thresholds are design parameters that were set by judgement, and they have not been tuned or validated against labelled fraud data.

## RESULTS AND EVALUATION

### Evaluation Procedure

The evaluation evidence consists of functional test cases recorded in the project report and qualitative feedback gathered from a selected group of potential users after the system was completed. Testing was carried out in the implemented environment after the modules had been integrated. Each test case was run with predefined input data, and the observed behaviour was compared with the expected result. Defects found were corrected before the final round. Four kinds of testing were applied during the sprints: functional testing of individual modules, integration testing of connected modules, system testing of the whole application, and user acceptance testing.

The evaluation is limited to the functionality exercised in this environment. It does not establish reductions in fraud losses, invoice processing time, stock-outs or audit effort. Such outcomes would need a separate study with baseline measurements and the participation of an operating organisation.

## DISCUSSION

AI-SFSS brings financial management, procurement, inventory, shipment tracking, product verification, forecasting and record verification into one web platform. The 24 recorded functional test cases provide preliminary evidence that the main workflows operate as intended. The feedback from potential users suggests that the integrated approach, role-based views and document automation are well received, though that feedback is informal.

The design responds to the gap identified in the literature. Individual studies show the value of AI-based fraud detection, blockchain traceability, QR authentication and OCR, but they rarely describe a single deployable system in which these functions share data. In AI-SFSS the link between functions is the main benefit. An OCR-extracted receipt becomes a transaction, the transaction receives a fraud score and a hash, a high score creates an alert and a notification, and an auditor can later verify the record. Likewise a purchase order leads to a shipment, each shipment event is hashed, and a field agent can scan the product QR code to see its history. Fragmented tools cannot provide this connected chain without manual re-entry.

Three design decisions deserve comment. First, fraud results are advisory: flagged transactions go to a human reviewer, which suits the current maturity of the scoring models and the consequences of wrongly blocking a payment. Second, the integrity ledger deliberately uses a lightweight hash chain instead of a distributed blockchain. This keeps cost and complexity low, and it gives auditors a practical tamper-evidence check, but it does not provide decentralised trust. Third, the architecture depends on managed cloud services. This lowers the barrier to adoption and removes the need for server administration, but it creates reliance on connectivity and on external providers, which matters in settings with unreliable internet access. The offline synchronisation requested by users is therefore an important next step.

Technical implementation alone does not prove better organisational outcomes. The absence of live integration and of measured results means that AI-SFSS should not be presented as a replacement for an organisation's accounting or audit controls. Its present value is as a demonstrated architecture and working prototype from which a pilot can be planned.

## CONCLUSION

This paper presented the design and implementation of the Artificial Intelligence Secure Financial Supply Chain System (AI-SFSS), a web-based platform that consolidates financial management and supply chain operations for organisations in Malawi and similar settings. The implemented functions include role-based authentication, transaction and budget management, AI-assisted fraud risk scoring and alerting, OCR-based invoice and receipt processing, inventory, supplier and purchase order management, shipment tracking on an interactive map, QR-based product verification, predictive analytics, notifications, integrations, settings and reporting. The system runs on React 19, TypeScript, Supabase, PostgreSQL, Edge Functions and Cloudflare Workers, which keeps infrastructure costs low.

A distinctive element is the blockchain-style integrity ledger. It records SHA-256 hashes of protected records linked to the previous entry and provides a verification function so that inconsistent changes can be detected. The ledger is a hash chain within a single database. It is tamper-evident against ordinary edits but is not decentralised, not externally anchored and not tamper-proof against an actor who can rewrite the database and recompute the hashes.

The project report documents 24 functional test cases that passed, together with favourable qualitative feedback. This is limited evidence that the selected workflows operate. It does not establish detection accuracy, OCR accuracy, forecast accuracy, performance, scalability, security assurance or readiness for national deployment. AI-SFSS has also not been connected to live banking, logistics or government systems, so operational interoperability has not been demonstrated. Within these boundaries, the work shows that an integrated, AI-assisted and verifiable financial supply chain platform can be built on affordable cloud services, and it provides a practical basis for pilot studies in Malawian organisations.

**REFERENCES**


1. Agarwal, R., Prasad, A., & Sharma, P. (2024). Artificial Intelligence-based financial fraud detection using machine learning techniques. Expert Systems with Applications, 237, 121457.
2. AI and Financial Fraud Prevention: Mapping the trends and challenges through a bibliometric lens. (2025). Journal of Risk and Financial Management, 18(6), 323.
3. Alevizos, L. (2025). Automated cybersecurity compliance and threat response using AI, blockchain and smart contracts. International Journal of Information Technology, 17, 767–781. https://doi.org/10.1007/s41870-024-02324-9
4. Allaparthi, S. (2024). AI in supply chains: Transforming fraud detection and authenticity verification. International Journal of Supply Chain Management, 9(6), 1–7. https://doi.org/10.47604/ijscm.3131
5. Alzoubi, H., Ahmed, G., & Alshurideh, M. (2023). Digital transformation and enterprise system integration in developing economies. Sustainability, 15(7), 5892.
6. Anjum, N., & Dutta, P. (2022). Identifying counterfeit products using blockchain technology in supply chain systems. arXiv. https://arxiv.org/abs/2206.08565
7. Baayeh, K., Beleya, P., Airawaty, D., & Salehi, S. (2025). Blockchain-based transparency in global supply chains: A systematic literature review. Journal of Networking and Network Systems.
8. Baryannis, G., Dani, S., & Antoniou, G. (2021). Predictive analytics and Artificial Intelligence in supply chain management. Computers & Industrial Engineering, 157, 107293.
9. Beck, K., et al. (2021). Manifesto for Agile Software Development. https://agilemanifesto.org
10. Caldarelli, G., Zardini, A., & Rossignoli, C. (2021). [Title, journal, volume and pages to be completed. Cited in the text but absent from the project report's reference list.]
11. Charles, V., Emrouznejad, A., & Gherman, T. (2023). A critical analysis of the integration of blockchain and artificial intelligence for supply chain. Annals of Operations Research. https://doi.org/10.1007/s10479-023-05169-w
12. Chen, Y., Wang, X., & Zhao, L. (2024). Blockchain-enabled financial transparency and auditability in enterprise systems. Information Systems Frontiers, 26(2), 541–557.