Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Sustainable Agricultural Asset Compliance via Passive NFC and Selective Blockchain Anchoring.

Design, Implementation, and Validation of the AgriLink Framework

Rossana Caputo
Mediterranean Institute of Innovation, Communication and Technology (MIICT)
Malta

Bernard Mallia
Mediterranean Institute of Innovation, Communication and Technology (MIICT), Institute for the Research and Improvement of Social Sciences (IRISS), Equinox Group
Malta

Keerthi Kumar Masanasetty, Prasad M
Dept. of Electronics and Communication Engineering
NITTE MEENAKSHI Institute of Technology (NMIT), NMIT University
Bengaluru, India

Abstract – Agricultural equipment traceability is a growing requirement in regulated supply chains, and yet existing digital solutions rely on energy-intensive, battery-powered Internet of Things (IoT) infrastructures that are ill-suited to rural environments. This paper presents AgriLink, an energy-efficient, privacy-preserving Distributed Ledger Technology (DLT) framework. This project has received funding from the European Union's Horizon 2020 research and innovation programme through the NGI TRUSTCHAIN programme under cascade funding agreement No. 101093274. AgriLink employs passive, tamper-proof Near Field Communication (NFC) tags combined with selective blockchain anchoring to record only compliance-critical state transitions, eliminating continuous telemetry entirely. A four-layer architecture integrating zero-trust security and privacy-by-design principles enforces General Data Protection Regulation (GDPR) compliance throughout. Experimental validation demonstrates up to 94% reduction in sensing-layer energy consumption versus Bluetooth Low Energy (BLE), ZigBee, and LoRaWAN baselines, as well as resistance to all simulated cloning and replay attacks, and stable performance under peak simulated workloads. AgriLink provides a replicable, cost-effective blueprint for sustainable DLT adoption in rural, asset-intensive agricultural sectors.

Keywords – Distributed Ledger Technology; Passive NFC; Agricultural Traceability; Zero-Trust Architecture; Selective Blockchain Anchoring; GDPR; Green IoT

I. INTRODUCTION

Modern agriculture depends on mechanised equipment whose certification, maintenance, and operator authorisation records must satisfy regulatory, insurance, and cooperative requirements [1]. Despite this need, traceability practices remain fragmented, with small and medium-sized farms relying on paper records, while larger organisations deploy proprietary, non-interoperable platforms creating vendor lock-in and centralised trust dependencies [2].

Distributed Ledger Technology (DLT) offers immutable, multi-stakeholder compliance records. However, dominant approaches couple blockchain storage with continuous IoT telemetry from battery-powered sensors, producing excessive energy consumption, electronic waste, and maintenance overhead [3]. Regulatory frameworks typically require only discrete state-change evidence, such as daily equipment check-out or periodic maintenance records, making high-frequency continuous monitoring economically and environmentally unjustifiable [1].

IoT deployments based on BLE, LoRaWAN, and ZigBee incur substantial recurring costs from battery replacement, gateway infrastructure, and cloud storage [3]. Prior blockchain solutions for agriculture compound these issues by anchoring high-frequency data on-chain, creating scalability bottlenecks and blockchain transaction cost escalation [4]. A clear gap exists wherein solutions either prioritise data granularity at the expense of sustainability, or emphasise immutability without adequate privacy controls.

AgriLink addresses this gap through an event-driven traceability paradigm replacing continuous telemetry with passive NFC-mediated human interactions. By anchoring only compliance-critical state transitions to the DLT and enforcing zero-trust security and privacy-by-design principles aligned with GDPR, AgriLink constitutes a deployable, sustainable, cost-efficient and economically sound solution for rural equipment traceability.

II. RELATED WORK

Early digital traceability relied on centralised databases managed by government agencies or private vendors, which simplified reporting, but introduced non-trivial single points of failure, required unconditional trust in platform operators, and failed to interoperate across organisational boundaries [2].

The adoption of IoT technologies marked a significant evolution. BLE tags, LoRaWAN sensors, and cellular devices have been widely deployed to continuously monitor equipment usage. Despite providing granular telemetry, they incur substantial lifecycle costs, with studies confirming that large proportions of continuously-collected data contribute negligible compliance value (if any at all) while significantly increasing cost and electronic waste [3].

Blockchain frameworks have been proposed to enhance transparency and immutability [4]–[7]. However, tightly coupling high-frequency IoT data streams with blockchain storage leads to severe scalability bottlenecks [4], with

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

recent literature emphasising selective anchoring and off-chain storage to mitigate blockchain bloat [5], notwithstanding which their application in agricultural traceability remains limited, particularly regarding deployability in rural environments.

III. SYSTEM DESIGN

A. Requirements and Design Objectives

The AgriLink framework was derived from requirements analysis under the TrustChain OC5 initiative, incorporating stakeholder interviews and regulatory guidelines, and with core functional requirements including: unique tamper-resistant equipment identification; operator authorisation enforcement; and time-stamped, verifiable logging of all asset state transitions. Non-functional requirements mandate energy minimisation through avoidance of battery-reliant sensing, GDPR compliance through aggressive data minimisation without compromising on functionality aspects, scalability to thousands of assets, and fault tolerance under intermittent rural connectivity.

B. Four-Layer Architecture

AgriLink is structured across four interdependent layers, illustrated in Fig. 1.

Client Layer: A cross-platform mobile application supporting offline-first operation and NFC-based equipment verification, alongside a web administrative console for stakeholder management.

Service Layer: Containerised microservices exposing RESTful endpoints governed by an OpenAPI specification. Key components include the NFC Verification Service implementing cryptographic tag validation, and the User and Machinery Services managing digital twin lifecycles.

Data Layer: A NoSQL document database for digital twins, audit logs, and encrypted user profiles. Document storage is restricted to European-jurisdiction cloud buckets to maintain data sovereignty.

Blockchain Layer: An enterprise-grade DLT node hosting smart contracts managing equipment non-fungible tokens (NFTs), credential verification events, and usage settlements.

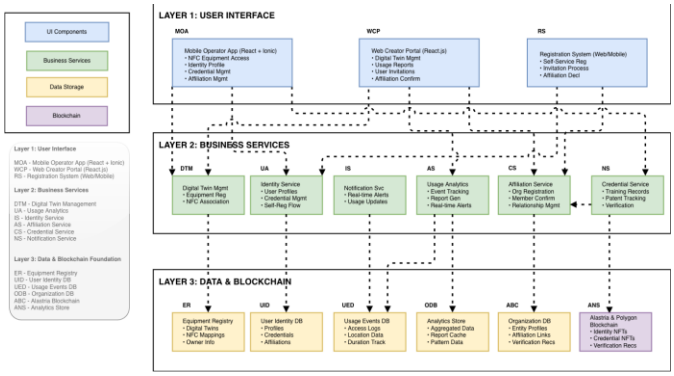

Fig. 1. AgriLink four-layer system architecture.

C. Zero-Trust Security and Oracle Problem Mitigation

AgriLink adopts a zero-trust security model wherein no user, device, or service is implicitly trusted, where access is governed by continuous attribute-based and role-based access control, and where inter-service communications are secured via mutual Transport Layer Security (mTLS).

The Oracle Problem, whereby an adversary detaches an NFC tag from a non-compliant asset and affixes it to a certified one, is mitigated through advanced cryptographic NFC tags (e.g., NTAG 424 DNA) configured as tamper-evident, which therefore permanently alter or destroy their cryptographic payload upon physical removal. Dynamic challenge-response protocols, session identifiers, and strict time-window validations enforced at the backend defend against replay and cloning attacks.

D. Privacy-by-Design and GDPR Compliance

In accordance with GDPR Article 5, data minimisation ensures only event-relevant metadata is captured, and that accordingly all Personally Identifiable Information (PII) is stored exclusively off-chain within encrypted, access-controlled databases. On-chain records contain only pseudonymous identifiers and cryptographic hashes that cannot be reverse-engineered without authorised off-chain context, and consent mechanisms integrated into the onboarding workflow enable operators to exercise rights to access, rectification, and erasure.

E. Event-Driven Methodology and Selective Anchoring

The framework captures only discrete, compliance-relevant events. When an authenticated operator taps a tamper-evident NFC tag, the mobile client generates a cryptographically-signed payload validated against backend policy rules. Routine operational events are retained off-chain but cryptographically linked to anchored milestones through hash chaining. Only events with long-term compliance relevance, like ownership transfers, certification issuances, and major maintenance records, are permanently anchored to the DLT. This selective anchoring strategy [5] prevents blockchain bloat and the associated costs while maintaining tamper-resistant audit trails.

IV. VALIDATION METHODOLOGY

Validation adopted a mixed strategy combining functional testing, scalability simulation, comparative energy modelling, and security evaluation. Functional tests verified end-to-end workflows against TrustChain OC5 regulatory use cases. Scalability was assessed through synthetic workloads simulating regional-scale deployments, measuring API throughput, transaction latency, and smart contract execution times on an enterprise DLT testnet.

Energy consumption was modelled comparatively against published baseline metrics for BLE, ZigBee, and LoRaWAN systems [3], isolating the sensing and radio transmission layers. Security validation encompassed penetration testing, simulated replay and cloning attack scenarios, and GDPR data-flow audits conducted against the deployed architecture.

V. RESULTS AND DISCUSSION

A. Scalability and Performance

Scalability evaluation demonstrated near-linear performance relative to the number of managed assets. API response times and DLT anchoring latencies remained within operational bounds under simulated peak workloads representing thousands of concurrent event submissions, confirming viability for regional-scale deployment.

B. Energy Efficiency

Energy modelling demonstrated up to 94% reduction in sensing-layer energy consumption relative to active BLE-based IoT solutions, with comparable reductions against

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

ZigBee and LoRaWAN baselines. Table I presents the comparative profile. This reduction results directly from eliminating continuous radio telemetry and battery-powered microcontrollers. The passive NFC tag draws zero standby power, harvesting radio frequency energy entirely from the reader device during interaction.

TABLE I. COMPARATIVE ENERGY AND OPERATIONAL PROFILE

Technology	Power Mode	Active Power*	Battery Req.	Energy Saving
BLE	Active push	~15 mW	Yes	Baseline
ZigBee	Active push	~30 mW	Yes	Baseline
LoRaWAN	Active push	~70 mW	Yes	Baseline
AgriLink (NFC)	Passive pull	~0 mW	No	**Up to 94%**

** Representative values from literature [3]. Passive NFC draws zero standby power.*

C. Security Validation

Dynamic cryptographic challenge-response generation in the selected NFC tags successfully resisted all simulated cloning and replay attack scenarios, while the tamper-evident physical mechanism ensured that attempted tag removal was immediately detectable through cryptographic payload invalidation.

D. GDPR Compliance

Audit simulation confirmed that regulatory bodies could cryptographically authenticate compliance records using on-chain hashes without accessing underlying PII, validating the efficacy of the pseudonymisation strategy, and all TrustChain OC5 regulatory workflow scenarios were completed successfully.

E. Comparative and Socio-Economic Impact

AgriLink eliminates per-asset battery replacement cycles, gateway infrastructure, and recurring network subscription fees, significantly reducing the total cost of ownership, thereby cutting down on an important financial barrier to entry that directly impacts the socio-economic reality of small and medium-sized farms, thereby democratising access to regulated supply chains [1]. Table II summarises all validation outcomes.

TABLE II. VALIDATION OUTCOME SUMMARY

Dimension	Method	Outcome
Scalability	Synthetic workload simulation	Near-linear; within operational bounds
Energy	Comparative modelling vs. baselines	Up to 94% reduction at sensing layer
Security	Penetration testing; replay simulation	All attack scenarios resisted
GDPR	Data-flow audit	Zero PII exposed; pseudonymisation verified
Functional	End-to-end workflow testing	All OC5 regulatory scenarios passed

VI. LIMITATIONS AND FUTURE WORK

The pull mechanism requires strict workforce compliance, given that a failure to tap the NFC tag means the event is not recorded, making the framework unsuitable for autonomous theft prevention or real-time location tracking. The architecture presupposes operator access to NFC-enabled mobile devices and intermittent network connectivity for payload synchronisation.

Current validation was conducted in controlled and simulated environments. Future research will focus on large-scale longitudinal field pilots in operational agricultural settings to assess hardware durability and real-world operator compliance rates. Additional directions include integration with European and Indian Decentralised Identity ecosystems, cross-chain interoperability for multinational supply chains, and lifecycle sustainability assessments of the NFC hardware components. The project source code is publicly available at https://github.com/NGI-TRUSTCHAIN/Agri-Link under the Apache License 2.0.

VII. CONCLUSION

AgriLink demonstrates that passive NFC combined with selective blockchain anchoring constitutes a viable, energy-efficient alternative to continuous IoT telemetry for agricultural equipment traceability. The framework achieves up to 94% sensing-layer energy savings, GDPR-compliant pseudonymisation, and tamper-resistant auditability, while eliminating battery-powered sensor infrastructure. By mitigating the Oracle Problem through cryptographic tamper-evident tags and enforcing a zero-trust security model, AgriLink establishes cryptographic trust without reliance on centralised control. The findings provide a replicable blueprint for sustainable DLT adoption in rural, asset-intensive industries where operational cost constraints and environmental objectives must be simultaneously satisfied.

ACKNOWLEDGMENT

This research was conducted under the TrustChain OC5 initiative, funded by the European Union under Grant Agreement Number 101093274. The views expressed are those of the authors and do not necessarily reflect those of the European Union or the granting authority. The authors acknowledge TrustChain consortium partners and pilot stakeholders for their contributions to requirements analysis.

REFERENCES

[1] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldú, "The rise of blockchain technology in agriculture and food supply chains," Trends Food Sci. Technol., vol. 91, pp. 640–652, 2019.

[2] A. Adewusi, "Blockchain technology in agriculture: Enhancing supply chain transparency and traceability," Finance Account. Res. J., vol. 5, no. 12, pp. 1–15, 2023.

[3] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "AgriBlockIoT: A secure traceability system for agri-food supply chain management," in Proc. 3rd Int. Conf. Smart Sustainable Technol. (SpliTech), IEEE, 2018.

[4] A. Reyna, C. Martín, J. Chen, E. Kamiya, and A. Cano, "On blockchain and its integration with IoT: Challenges and opportunities," Future Gener. Comput. Syst., vol. 88, pp. 173–190, 2018.

[5] Y. Teng, J. Lv, Z. Wang, Y. Gao, and W. Dong, "TimeChain: A secure and decentralized off-chain storage system for IoT time series data," in Proc. ACM Web Conf. 2025, ACM, 2025.

[6] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," Comput. Commun., vol. 54, pp. 1–31, 2014.

[7] G. M. Cappelletti, R. Caputo, M. Cariglia, L. Grilli, C. Russo, D. Santoro, et al., "Harnessing the power of blockchain in the agri-food sector: a meta-analysis of current research and best practices," Appl. Math. Sci., vol. 17, no. 10, pp. 477–501, 2023.