International Journal of Technology and Applied Science (IJTAS)

E-ISSN: 2230-9004 ● Website: www.ijtas.com ● Email: editor@ijtas.com

Laborguard Blockchain-Enabled Agricultural Labor Verification and Anti-Human-Trafficking Compliance Device

Oluwaseun Ola[1], Amina Catherine Peter-Anyebe[2], Dr. Bhavesh Chakurbhai Kataria[3]

[1]Researcher, School of Agricultural Sciences, Southern Illinois University, Carbondale, Illinois
[2]Department of Research and Strategic Development, Akondu Integrated Solutions and Consult Ltd, Abuja, Nigeria.
[3]Researcher, Department of Pathology, School of Medicine, Emory University, Atlanta, Georgia, United States of America

Abstract:
The LaborGuard Blockchain-Enabled Agricultural Labor Verification and Anti-Human-Trafficking Compliance Device is a proposed portable, ruggedized data-processing platform intended to strengthen agricultural workforce accountability, crop-production documentation, regulatory compliance and ethical supply-chain transparency. The underlying external design is registered with the United Kingdom Intellectual Property Office under Design No. 6548985, with a registration date of 25 August 2026 and a grant date of 8 September 2026. Classified under International Design Classification 14-02, the registered subject matter is the visible configuration of data-processing equipment. LaborGuard extends this hardware concept into a proposed integrated operational platform for agricultural enterprises, cooperatives, extension services, certification bodies, labor inspectors and other authorized stakeholders. The technical concept links authenticated workforce participation with agronomic operations across economically important crops such as soybean, corn, wheat, rice, cotton, sugarcane, potatoes, tomatoes, lettuce, strawberries, grapes, apples, citrus, almonds and cassava. In the intended implementation, the device records worker identities and employment agreements alongside field assignments, planting, fertilizer management, irrigation, pesticide applications, weed and disease control, harvesting, storage, transportation and post-harvest handling. Each validated operation would be assigned appropriate crop, plot, operator, time and authorization metadata, generating a connected evidence trail for labor oversight and crop-production traceability. The proposed hardware embodiment incorporates a protective angular enclosure, a raised carrying handle, a display, an identification module, sensor connections, grouped control keys, a grille, status indicators and recessed side openings. Electronic subsystems would include secure processing, encrypted local record storage, geographic positioning, communications hardware and, where lawfully justified, biometric-assisted worker authentication. A permissioned blockchain would hold transaction commitments and verifiable audit metadata while sensitive personal records remain under controlled off-chain storage. Offline data capture and subsequent synchronization would support farm operations in locations with intermittent connectivity. LaborGuard also envisages a combined rule-based and analytical compliance layer. Employment-record comparisons and calibrated anomaly-detection models could highlight unexplained wage deductions, mismatches between identities and assignments, excessive recorded working hours, recruitment-fee discrepancies and other indicators associated with labor exploitation. These findings would support structured review and timely referral; they would not independently establish trafficking, child labor or coercion. A worker- centered governance model, human

review, grievance channels, consent or another lawful basis for data processing and protection against retaliation remain necessary. The intended contribution is the coordinated documentation of who performed an authorized agricultural activity, where and when the activity was undertaken, how its production parameters were recorded, and which compliance checks were performed. This structure could support farm certification, responsible sourcing, sustainability reporting, food-safety documentation and transparent production management. The UK design certificate establishes the appearance shown in its registered illustrations; the proposed ruggedized configuration and functional system described in this report require detailed engineering, experimental testing and any appropriate additional intellectual property filings.

Keywords: Laborguard, Blockchain, Agricultural, Labor, Verification, Anti-Human, Trafficking, Compliance, Device.

2. INTRODUCTION

Agricultural production increasingly depends on coordinated seasonal workforces, complex recruitment relationships, digital field records and reliable evidence of responsible sourcing. Conventional labor management and crop documentation are frequently separated into paper attendance books, payroll databases, pesticide registers, agronomic worksheets and independent certification repositories. Such fragmentation weakens the ability of farm operators or inspectors to reconcile employment records with particular farming activities, identify inconsistencies promptly or demonstrate the provenance of work performed throughout a production season. These limitations are especially relevant to high-value crops and export-oriented agricultural supply chains subject to multiple quality, labor, food-safety and sustainability requirements.

The LaborGuard Blockchain-Enabled Agricultural Labor Verification and Anti-Human-Trafficking Compliance Device proposes a unified field-facing architecture for coordinating workforce verification and crop-production traceability. Its intended data inputs include worker credentials, contracts, wage records, field boundaries, crop identifiers, activity schedules, operator authorizations, environmental measurements and agricultural transaction records. A normalization and validation layer would prepare these records for secure storage, cryptographic authentication and rules-based examination. The intended result is an auditable relationship between individual verified activities and the corresponding production lots, plots or supply-chain events, rather than isolated digital entries with uncertain provenance.

The official registration illustrates an electronic device with a predominantly rectangular housing, prominent display, grouped rectangular and circular controls, a circular rear feature and a vertically projecting cylindrical attachment. The broader LaborGuard specification additionally contemplates an angular ruggedized enclosure, raised carrying handle, sensor cluster, identification module, grille, indicators and recessed access openings. These additional hardware features are design objectives rather than features presumed to appear in the existing registered views. Figure 1 reproduces official registration plates as evidence of the recorded appearance; the subsequent architectural figures describe proposed engineering implementation.

Within this intended operational framework, the device would support workforce registration, authenticated field assignments, traceable fertilizer and crop-protection applications, irrigation documentation, harvest crew records and post-harvest logistics. Recording worker identity alongside an operation should be subject to access controls and data minimization, since permanent immutable storage of sensitive personal data would create disproportionate privacy and correction risks. Accordingly, sensitive details should be held off-chain with limited-access encrypted storage, while the blockchain maintains appropriately designed tamper-evident commitments.

LaborGuard's compliance component would compare recorded labor conditions with legal, contractual and ethical sourcing obligations. Discrepancies might identify records requiring further investigation, but neither blockchain verification nor artificial intelligence can prove that a worker is free from intimidation, debt bondage or restricted mobility. The device is therefore conceived as an evidence-management and decision-support system requiring independent worker engagement and competent human investigation. Its long-term usefulness would depend on interoperability, credible field validation, safeguards for migrant and seasonal workers, and measurable performance under practical farm conditions.



Figure 1. Official registered appearance of UK Design No. 6548985 (registration plates reproduced in Appendix A).

3. FIELD OF THE DESIGN

The present registered design pertains to electronic data-processing apparatus within International Design Classification Class 14, Subclass 02, as recorded on the UK registration certificate. The proposed LaborGuard application falls within the associated technological fields of digital agricultural management, labor identity verification, electronic compliance monitoring, blockchain-based record integrity, secure field data acquisition and agricultural supply-chain traceability. It addresses a specialized operational setting in which production information and employment records must be associated across multiple employers, fields, crop types and stages of agricultural handling.

More particularly, the proposed system combines authentication of workforce assignments with geospatially located records of field operations and documented crop-management interventions. The agronomic information domain includes planting schedules, soil fertility management, pesticide and weed-control operations, irrigation activities, disease management, harvest logistics and traceability through transport or storage. Different crop- production environments require different record fields: cereal and oilseed systems emphasize plot-scale machinery and input applications; fruit and vegetable systems may demand intensive seasonal worker administration, harvest lot segregation and post-harvest handling records.

The design concept further intersects with regulatory technology and human-rights due diligence. Employment agreements, attendance, payroll, recruitment records and authorized tasks may be reconciled with applicable legal or contractual requirements. Potential inconsistencies are captured in a structured review system, allowing auditors to examine the underlying evidence and document corrective action. Such tools may make labor information more accessible but are not substitutes for worker interviews, grievance arrangements, inspections, protection procedures or legally competent determinations of trafficking or forced labor.

From a hardware perspective, the registered appearance comprises a visually recognizable electronic housing, display, grouped controls and projecting exterior components. The intended portable engineering embodiment adapts these concepts to farm mobility by considering a carrying structure, sealed connector regions, secure identification peripherals and sensor interfaces. Its industrial-design aspects are distinct from any new technical processes, circuits, software or cryptographic methods. Device appearance and functional patentability must be considered through separate legal and technical analyses.

Accordingly, the field of the proposed LaborGuard system encompasses agricultural workforce assurance, precision-agriculture record management, supply-chain provenance and ethically governed digital compliance. Its prospective advantages would arise from integrated processing and accountable information exchange, subject to successful implementation and validation rather than being established by the UK design registration alone.

4. BACKGROUND OF THE DESIGN

Farm workforce administration has historically relied on independently managed worker registers, time sheets, wage statements, recruitment files and periodic inspection reports. Crop-production records are often collected separately through farm diaries, spray logs, fertilizer records and harvesting documentation. When these systems cannot exchange information, an agricultural enterprise may struggle to demonstrate the relationship between employment agreements, who performed a particular field task and the recorded production conditions. Reconciliation is especially difficult for seasonal labor, outsourced recruiting, multiple farm locations and rapidly changing harvest teams.

Employment oversight faces additional challenges where recruitment intermediaries, temporary housing, pay arrangements and labor movement cross organizational boundaries. Documentary inconsistencies can obscure wage deductions, unauthorized recruitment charges, duplicate worker identities, unrecorded working hours or mismatches between registered workers and individuals present in the field. These irregularities are meaningful screening signals but do not automatically establish exploitation or human trafficking. Reliable response requires confidential channels for workers, evidence preservation, independent assessment and arrangements that protect affected individuals from retaliation.

Agronomic recordkeeping has similarly become more demanding. Traceability and compliance obligations may require crop and field identification, product-use documentation, irrigation and nutrient management records, harvest-lot attribution, storage conditions and movement histories. For high-value export horticulture, incomplete or inconsistent records can hinder certification and product accountability. A technology capable of associating verified operations with a plot and responsible operator can improve record structure, but environmental or production performance gains cannot be assumed without field evidence.

Distributed-ledger technology offers a mechanism for verifying whether recorded transactions have been altered after submission and for coordinating authorized parties without relying solely on one organization's unilateral audit trail. Nevertheless, a blockchain does not establish that a source statement was truthful; it can permanently preserve inaccurate information just as effectively as correct information. Secure system design therefore requires source authentication, dispute resolution, error-correction workflows, carefully chosen on-chain metadata and access-controlled off-chain records. Biometric identification similarly introduces legal, technical and ethical constraints, particularly concerning worker consent, false matches and the practical availability of non-biometric alternatives.

The registered hardware design provides a recognizable physical platform for the proposed integration of worker authentication, agricultural sensing and compliance visualization. Its intended development involves a rugged field-portable device with a display, controls, protected input regions and embedded electronics. The added carrying handle, sensing hardware and visual indicators described in the supplied technical concept may differ materially from the registered visual representations; they should be engineered and documented as an additional embodiment rather than assumed to fall automatically within the existing protection.

Against this background, LaborGuard is presented as an integrated design proposal intended to reduce fragmentation between agricultural labor documentation and crop-production traceability. The system would unify employment verification, field mapping, controlled agricultural data input, encrypted records, blockchain anchoring and structured compliance review. Its proposed value lies in auditable evidence and timely human decision support, with performance, usability, technical novelty and deployment benefits remaining subjects for future validation.

5. DESCRIPTION OF PRIOR ART

The following fifteen published patent records provide representative technological comparisons involving blockchain employment verification, worker records, recruitment authentication, wage handling, supply-chain provenance and agricultural traceability. Publication references correspond to the supplied prior-art comparison. They are technical contextual references, not a formal determination of legally qualifying prior art for the registered UK appearance. The comparison distinguishes methods and systems from the external appearance protected by a registered design.

5.1. US20230028681A1 – System and Method for Blockchain-Based Employment Verification

The published invention concerns distributed-ledger verification of employment credentials and signed authentication transactions. It is relevant because reliable workforce documentation, verifiable transactions or traceable production information constitutes part of the broader technological context in which the proposed LaborGuard system would operate. Its disclosed emphasis lies in its stated method or computing platform rather than the particular visual appearance registered for the LaborGuard source device.

In comparison, LaborGuard adds proposed agricultural field assignments, agronomic activity documentation and exploitation-risk screening to a dedicated electronic device; verification methods themselves remain existing technology. The UK certificate protects the visual design as represented, not an exclusive right over underlying blockchain or employment-verification techniques (Flynn & Lam, 2023).

5.2. US11157876B1 – Intelligent Employment-Based Blockchain

The published invention concerns blockchain-supported employment histories and reliable background information exchange. It is relevant because reliable workforce documentation, verifiable transactions or traceable production information constitutes part of the broader technological context in which the proposed LaborGuard system would operate. Its disclosed emphasis lies in its stated method or computing platform rather than the particular visual appearance registered for the LaborGuard source device.

In comparison, LaborGuard emphasizes ongoing agricultural employment conditions, recorded labor practices and linkage between workers and crop operations, not only historical employment verification. The UK certificate protects the visual design as represented, not an exclusive right over underlying blockchain or employment-verification techniques (Knas et al., 2021).

5.3. US20180293547A1 – Methods and Systems for Employment and Education Verification Using Blockchain

The published invention concerns distributed credential records for prior employment and education. It is relevant because reliable workforce documentation, verifiable transactions or traceable production information constitutes part of the broader technological context in which the proposed LaborGuard system would operate. Its disclosed emphasis lies in its stated method or computing platform rather than the particular visual appearance registered for the LaborGuard source device.

In comparison, LaborGuard contemplates continual farm-operation records and corresponding labor compliance checks rather than primarily educational or career credential validation. The UK certificate protects the visual design as represented, not an exclusive right over underlying blockchain or employment-verification techniques (Randhawa, 2018).

5.4. CN110188109B – Blockchain-Based Information Management Methods, Devices and Equipment

The published invention concerns smart-contract and blockchain validation of individual and enterprise employment records. It is relevant because reliable workforce documentation, verifiable transactions or traceable production information constitutes part of the broader technological context in which the proposed LaborGuard system would operate. Its disclosed emphasis lies in its stated method or computing platform rather than the particular visual appearance registered for the LaborGuard source device.

In comparison, LaborGuard would use authenticated records as inputs to farm-specific workforce and compliance review; this does not render generic blockchain personnel verification novel. The UK certificate protects the visual design as represented, not an exclusive right over underlying blockchain or employment- verification techniques (Zou, 2023).

5.5. CN113128962A – Recruitment Information Authentication Management Based on Blockchain

The published invention concerns candidate credential checks, recruitment review and digitally recorded employment agreements. It is relevant because reliable workforce documentation, verifiable transactions or traceable production information constitutes part of the broader technological context in which the proposed LaborGuard system would operate. Its disclosed emphasis lies in its stated method or computing platform rather than the particular visual appearance registered for the LaborGuard source device.

In comparison, LaborGuard would extend the data scope to worker attendance, field operations, pay inconsistencies and post-recruitment agricultural oversight. The UK certificate protects the visual design as represented, not an exclusive right over underlying blockchain or employment-verification techniques (Yu, 2021).

5.6. CN117149769A – Blockchain-Based Construction Worker Professional File Management

The published invention concerns construction worker identity, qualifications, contracts, attendance and salary records. It is relevant because reliable workforce documentation, verifiable transactions or traceable production information constitutes part of the broader technological context in which the proposed LaborGuard system would operate. Its disclosed emphasis lies in its stated method or computing platform rather than the particular visual appearance registered for the LaborGuard source device.

In comparison, This is a strong functional overlap for workforce administration; the proposed agricultural context and documented UK device appearance are the principal distinctions. The UK certificate protects the visual design as represented, not an exclusive right over underlying blockchain or employment-verification techniques (Zhong et al., 2023).

5.7. CN111988307B – Construction Engineering Work Information Sharing Platform Based on Blockchain

The published invention concerns distributed sharing of construction labor, employment and performance information. It is relevant because reliable workforce documentation, verifiable transactions or traceable production information constitutes part of the broader technological context in which the proposed LaborGuard system would operate. Its disclosed emphasis lies in its stated method or computing platform rather than the particular visual appearance registered for the LaborGuard source device.

In comparison, LaborGuard proposes agricultural plot, crop, field-treatment and harvest attribution as additional record dimensions and a dedicated field device. The UK certificate protects the visual design as represented, not an exclusive right over underlying blockchain or employment-verification techniques (Cen et al., 2023).

5.8. WO2024071864A1 – Electronic Payment of Gig Worker Wages and Sensitive Information Management

The published invention concerns digital-wallet wage transactions, electronic identity and employment documentation. It is relevant because reliable workforce documentation, verifiable transactions or traceable production information constitutes part of the broader technological context in which the proposed LaborGuard system would operate. Its disclosed emphasis lies in its stated method or computing platform rather than the particular visual appearance registered for the LaborGuard source device.

In comparison, LaborGuard incorporates proposed farm compliance and crop-operation traceability; wage authentication and secure identity handling already occur in the cited technology. The UK certificate protects the visual design as represented, not an exclusive right over underlying blockchain or employment-verification techniques (Park, 2024).

5.9. CN111985905B – Blockchain-Based Social Human Resource Management System and Method

The published invention concerns verification and sharing of labor relationships and personnel contracts. It is relevant because reliable workforce documentation, verifiable transactions or traceable production information constitutes part of the broader technological context in which the proposed LaborGuard system would operate. Its disclosed emphasis lies in its stated method or computing platform rather than the particular visual appearance registered for the LaborGuard source device.

In comparison, The proposed LaborGuard embodiment is oriented to agricultural inspection, workforce activities and crop-linked traceability rather than general human resource exchange. The UK certificate protects the visual design as represented, not an exclusive right over underlying blockchain or employment-verification techniques (Zhu et al., 2024).

5.10. US20210004739A1 – Blockchain Based Supply Chain Network Systems

The published invention concerns blockchain-enabled sourcing, traceability and social labor-performance information. It is relevant because reliable workforce documentation, verifiable transactions or traceable production information constitutes part of the broader technological context in which the proposed LaborGuard system would operate. Its disclosed emphasis lies in its stated method or computing platform rather than the particular visual appearance registered for the LaborGuard source device.

In comparison, This is a close reference for labor-related supply-chain transparency; LaborGuard places worker records and agronomic production events in a specific field-facing workflow. The UK certificate protects the visual design as represented, not an exclusive right over underlying blockchain or employment-verification techniques (Gill & Nicol, 2021).

5.11. US20220374823A1 – Tracking Qualitative Parameters Using a Blockchain Provenance System

The published invention concerns provenance records that may include wage, human-rights and trafficking- related characteristics. It is relevant because reliable workforce documentation, verifiable transactions or traceable production information constitutes part of the broader technological context in which the proposed LaborGuard system would operate. Its disclosed emphasis lies in its stated method or computing platform rather than the particular visual appearance registered for the LaborGuard source device.

In comparison, The proposal shifts attention toward individual worker documentation and verifiable farm tasks; blockchain-based social provenance is not inherently new. The UK certificate protects the visual design as represented, not an exclusive right over underlying blockchain or employment-verification techniques (Moss et al., 2022).

5.12. US20200053952A1 – Tracking and Tracing Performance of Agricultural Tasks

The published invention concerns agricultural task records, compliance and field-operation traceability. It is relevant because reliable workforce documentation, verifiable transactions or traceable production information constitutes part of the broader technological context in which the proposed LaborGuard system would operate. Its disclosed emphasis lies in its stated method or computing platform rather than the particular visual appearance registered for the LaborGuard source device.

In comparison, LaborGuard combines similar farm record needs with worker identity and employment-related verification rather than agricultural task tracking alone. The UK certificate protects the visual design as represented, not an exclusive right over underlying blockchain or employment-verification techniques (Rabby & Gerrard, 2020).

5.13. CN115879961A – Blockchain-Based Agricultural Production Information Tracing

The published invention concerns product and production-chain information validation and traceability. It is relevant because reliable workforce documentation, verifiable transactions or traceable production information constitutes part of the broader technological context in which the proposed LaborGuard system would operate. Its disclosed emphasis lies in its stated method or computing platform rather than the particular visual appearance registered for the LaborGuard source device.

In comparison, LaborGuard emphasizes linking authenticated workers with crop production and ethical labor accountability, while product-level blockchain traceability is established prior technology. The UK certificate protects the visual design as represented, not an exclusive right over underlying blockchain or employment- verification techniques (Bai et al., 2023).

5.14. US20230084892A1 – Generating Verifiable Agricultural Data

The published invention concerns cryptographic validation, agricultural imagery and stewardship information. It is relevant because reliable workforce documentation, verifiable transactions or traceable production information constitutes part of the broader technological context in which the proposed LaborGuard system would operate. Its disclosed emphasis lies in its stated method or computing platform rather than the particular visual appearance registered for the LaborGuard source device.

In comparison, LaborGuard targets worker-linked agronomic records and workforce compliance rather than primarily imagery-validated agricultural observations. The UK certificate protects the visual design as represented, not an exclusive right over underlying blockchain or employment-verification techniques (Bliss, 2023).

5.15. CN118172029B – Blockchain-Based Work Information Sharing Platform

The published invention concerns digitally managed work information and electronic labor-service agreements. It is relevant because reliable workforce documentation, verifiable transactions or traceable production information constitutes part of the broader technological context in which the proposed LaborGuard system would operate. Its disclosed emphasis lies in its stated method or computing platform rather than the particular visual appearance registered for the LaborGuard source device.

In comparison, LaborGuard would associate protected labor-contract records with specific georeferenced crop activities and a field-facing device; general agreement storage is established art. The UK certificate protects the visual design as represented, not an exclusive right over underlying blockchain or employment-verification techniques (Duan et al., 2024).

5.16. Comparative Review and Distinguishing Considerations

The reviewed patents collectively establish that employment credential verification, digitally recorded contracts, payroll authentication, workforce information sharing, agricultural record traceability and blockchain-supported labor information are prior technical concepts. Construction-sector workforce systems overlap strongly with the intended identity, attendance, contract and payment records. Supply-chain provenance patents also contemplate labor and human-rights characteristics, demonstrating that such functionality cannot be described as categorically unprecedented.

The proposed LaborGuard system differs chiefly in its intended operational consolidation of worker authentication, field-assignment recording, agronomic activity documentation and agricultural compliance review within a dedicated field-portable electronic interface. A separate technical patent application would need to identify and claim a specific, enabled technical improvement beyond the generic combination of known features. The registered design must be assessed through its overall visual impression against earlier appearances, which is a distinct legal inquiry from the novelty of algorithms or data-processing methods.

6. STATEMENT OF THE REGISTERED DESIGN

The registered design concerns the ornamental and visible external configuration of an electronic apparatus registered as Blockchain-Enabled Agricultural Labor Verification and Anti-Human-Trafficking Compliance Computer under UK Design No. 6548985. The appearance is documented by the official multi-view representations, including its generally rectangular housing, prominent display area, grouped front controls, circular external components and vertically projecting cylindrical attachment. The device is classified as data- processing equipment under Class 14, Subclass 02.

The front elevation establishes the relationship between the dark display region, rectangular buttons and circular controls. Isometric and lateral views describe housing thickness, projection, component alignment and three- dimensional surface transitions. The rear perspective identifies a circular external feature within the housing. Together these representations establish the appearance to be considered when assessing the registered design, independently of any intended electronic function.

The proposed LaborGuard engineering configuration also describes an angular ruggedized enclosure, carrying handle, biometric identification module, agricultural sensor cluster, protective grille, indicators and recessed side openings. These additional features are not automatically included in the original registration merely because they appear in a later functional specification. Their inclusion in a final product may change the overall impression and would warrant comparison with the registered drawings and consideration of a separate filing if appropriate.

The design certificate does not itself establish blockchain transactions, real-time compliance analytics, geospatial mapping, biometric processing or agricultural sensor functionality. Such capabilities require technical specification, software implementation, hardware validation and potentially separate intellectual property protection. Nor does the certificate prove any performance advantage or the ability to detect trafficking.

Accordingly, the statement of registered design is limited to the external appearance and spatial arrangement shown in the official UK representations, while the intended agricultural workforce and crop-production functions explain the industrial context for its proposed use. The legal scope should be interpreted from the filed views and applicable registered-design law rather than extended categorically to every variation in color, material, structure or internal computation.

7. TECHNICAL DESCRIPTION OF THE DESIGN

7.1. Overall System Architecture and Design Configuration

The preferred proposed LaborGuard architecture combines a portable physical interface, data-acquisition subsystem, embedded computing platform, secure transaction services and integration interfaces. The intended

ruggedized device places a display and grouped controls at the operator-facing surface, with identification hardware, peripheral sensor connections and status indicators accessible during field visits. The proposed raised handle and angular protective enclosure support mobility between field plots, packing locations and inspection stations, subject to ergonomic and mechanical testing. The official registered appearance should remain separately identifiable from these proposed additions.

Functional processing is organized into interaction, acquisition, embedded validation, blockchain and compliance, and connectivity layers. Agricultural records are first captured from authorized worker credentials, farm management platforms, field forms, positioning instruments or sensors. Source identities and timestamps are checked, records are normalized and authenticated, and permitted cryptographic commitments are submitted to a permissioned ledger. Compliance rules and analytical models operate on appropriately authorized datasets, after which the device presents traceability status and review alerts. Secure local queuing preserves information if connectivity is unavailable.

$$L = \{L_{I,} L_{D,} L_{P,} L_{B,} L_C\} \quad (1)$$

$$D_{out} = f_C(f_B(f_P(f_D(D_{raw})))) \quad (2)$$

Here L_I denotes interaction, L_D acquisition, L_P embedded processing, L_B blockchain and compliance services, and L_C connectivity; f denotes the corresponding processing transformations. The equations specify the architecture concept and do not report measured throughput or accuracy.

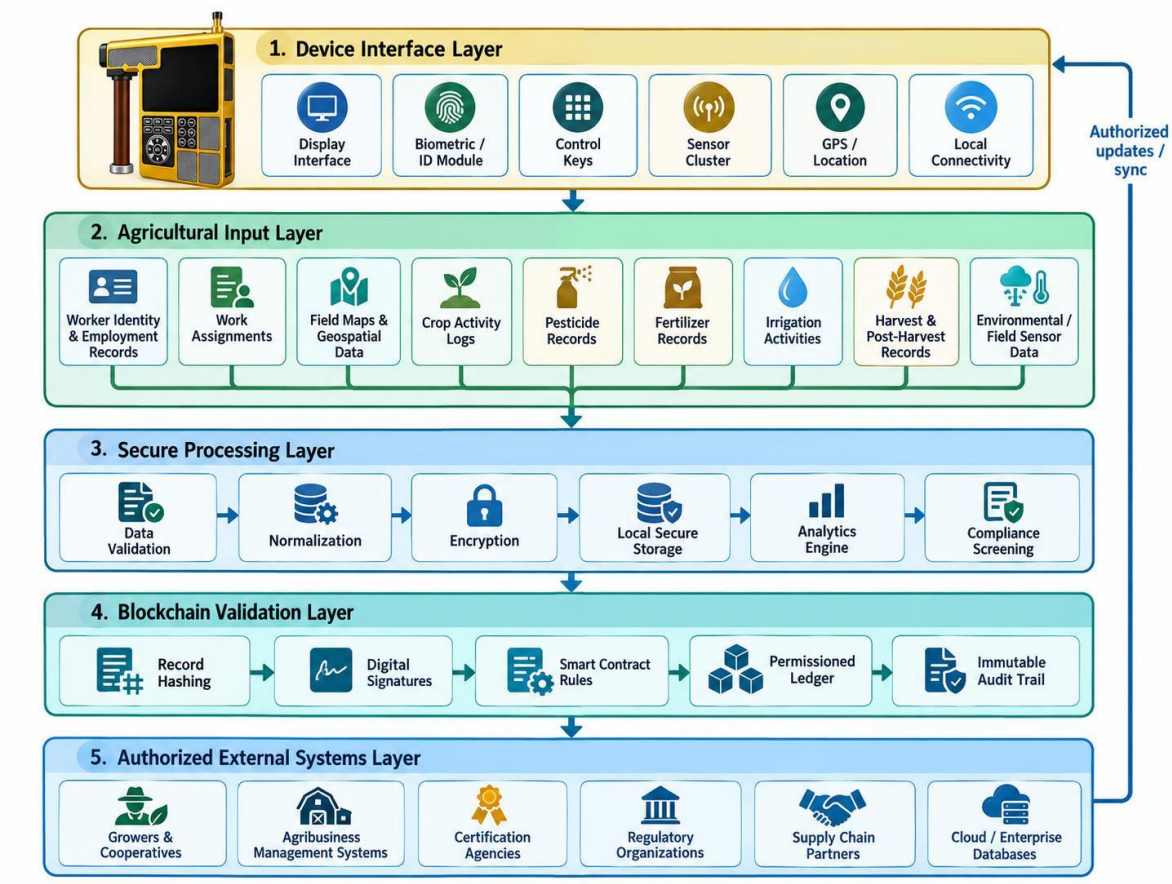


Figure 2. Proposed layered architecture linking device interfaces, agricultural inputs, secure processing, blockchain validation and authorized external systems.

7.2. Hardware Components and Physical Structure

The proposed device integrates a rigid main enclosure, display, identification component, protected sensor and communication connectors, control keys, indicator elements, rechargeable battery and processor with protected cryptographic keys. A raised handle may provide a consistent grasping location. The housing should protect against foreseeable farm dust, moisture, minor impacts and repeated handling, but no ingress-protection or drop- resistance rating is claimed absent testing. Recessed side connections are proposed to reduce direct connector exposure and support detachable peripherals.

The display establishes the primary visual region for worker verification, plot identifiers, work assignments, pesticide-use records, irrigation histories and labor-risk alerts. A proposed biometric interface could support fingerprint or facial recognition where legally justified, with alternative credentials for workers who cannot use biometric processing. Raw biometric images and confidential employment information should not be stored on a public blockchain. The power subsystem should be sized for expected authentication frequency, sensor use, screen-on time, connectivity and offline storage requirements.

$$A_d = W_d \times H_d \tag{3}$$

$$R_d = \frac{W_d}{H_d} \tag{4}$$

$$V_e \approx L_e \times W_e \times H_e \tag{5}$$

$$t_e \geq t_{required} \tag{6}$$

$$M_{total} = M_{enclosure} + M_{processor} + M_{battery} + M_{interfaces} \tag{7}$$

$$T_{operation} \approx \frac{\eta_b E_b}{P_{average}} \tag{8}$$

The displayed expressions define usable display area, aspect ratio, enclosure bounding volume, minimum mechanical thickness, component mass and indicative battery endurance. All physical dimensions and performance limits remain to be established through detailed engineering and validation.



Figure 3. Proposed exploded hardware configuration showing enclosure, display, identification hardware, sensor interfaces, processor, battery and protective components.

7.3. Data Acquisition and Input Interfaces

The data acquisition layer accepts worker credentials, employment agreements, assignment records, wages and recorded hours together with plot boundaries, crop identifiers, planting information, nutrient applications, irrigation, weed and disease treatment, harvest details, transport and storage events. Crop-specific data schemas are necessary: cereal production may emphasize machinery passes and input rates, while fruit and vegetable operations may require harvest crew attribution, food-safety intervals and lot-specific handling documentation. External sources should be interfaced through permissioned APIs, secure wireless services, instrument uploads or controlled operator entry.

Each event should retain an event identifier, origin identifier, authenticated or pseudonymous operator reference, field and crop references, observed timestamp and record provenance. Input checks should distinguish missing data, invalid formats, unauthorized submissions and conflicting information. Accuracy, authorization and authenticity are separate properties; completeness alone does not establish any of them. A normalization stage aligns units, timestamps, crop coding and geographic identifiers before analysis. When network access is absent, encrypted pending records should be queued locally without falsely labeling them blockchain-confirmed.

$$D_{in}(t) = \{D_{worker}(t), D_{employment}(t), D_{geospatial}(t), D_{agronomy}(t), D_{sensor}(t)\} \quad (9)$$

$$R_j = \{ID_j, W_j, F_j, C_j, O_j, T_j, L_j, A_j\} \quad (10)$$

$Qj = Nvalid,required$

$$Q_j = \frac{N_{valid,required}}{N_{total,required}} \quad (11)$$

$Ntotal,required$

$$D_{normalized} = f_{normalize}(D_{in}) \quad (12)$$

$Racq = Naccepted$

$$R_{acq} = \frac{N_{accepted}}{N_{attempted}} \quad (13)$$

$Nattempted$

$$L_{acq} = t_{available} - t_{event} \quad (14)$$

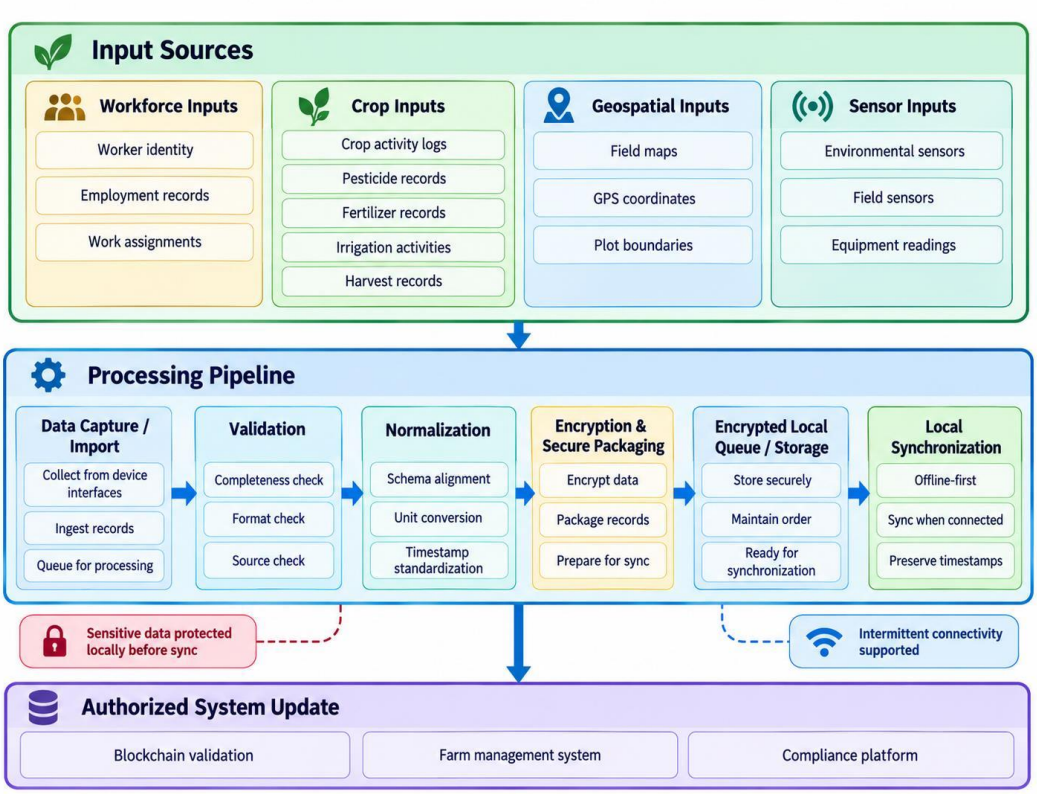


Figure 4. Proposed data ingestion sequence with workforce, crop, geospatial and sensor inputs, validation, normalization and encrypted local synchronization.

7.4. Blockchain, Smart Contracts and Intelligent Processing

A permissioned ledger is proposed for authorized parties rather than unrestricted publication of worker details. Transactions may contain cryptographic commitments to records, digital signatures, event times, permissions and verification status. Employment files, biometrics, confidential allegations and highly identifying geolocation histories should remain in controlled off-chain storage. Appropriate keyed or salted commitments reduce the danger of guessing sensitive information from predictable hashes. Governance arrangements must establish who may validate, correct, revoke or view records and how disputed source information is addressed.

The compliance engine combines deterministic rules and optional anomaly models. Rules evaluate whether a record meets documented authorization, employment or agronomic requirements. Analytical signals may flag unusually long recorded work periods, mismatches between staffing and payroll, unauthorized substitutions or unexpected field-task patterns. Model thresholds require independent calibration on representative data, and outputs remain reasons for review rather than declarations of wrongdoing. Positive worker protections, confidential reporting and human oversight are indispensable.

$$T_j = \{H(R_j), ID_j, t_j, S_j, V_j\} \quad (15)$$

$$I_j = \begin{cases} 1, & H(R_j) = h*_j \\ 0, & H(R_j) \neq h*_j \end{cases} \quad (16)$$

$$V(T_j) = \prod_{k=1}^{m} v_k(T_j) \quad (17)$$

$$D_{anomaly}(X) = \sqrt{(X - \mu)\hat{}T\,(\Sigma + \varepsilon I)^{-1}\,(X - \mu)} \quad (18)$$

$$S_{risk} = \alpha R_{rules} + \beta A_{anomaly} + \gamma E_{discrepancy} \quad (19)$$

$$\alpha + \beta + \gamma = 1 \quad (20)$$

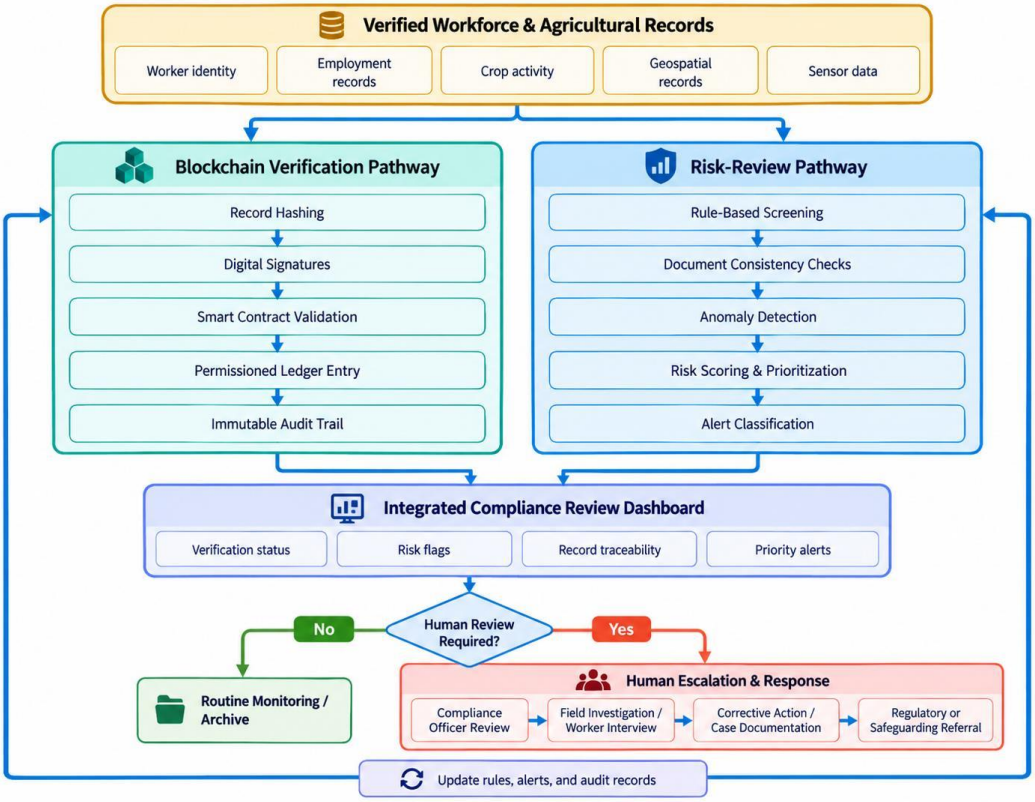


Figure 5. Proposed parallel blockchain verification and rule-based/analytical risk-review framework with human escalation.

7.5. Agricultural Production and Labor Compliance Monitoring

The monitoring layer links the authorized actor, agricultural activity, plot, crop or production lot and associated records. It can compare actual recorded fertilizer and pesticide application parameters against approved farm plans and the applicable product label, and it may reconcile irrigation or harvest operations with task schedules. This is a documentation and decision-support function: real agronomic suitability requires professional agronomic judgment, calibrated measurements, applicable legal rules and verified field conditions. Integrated crop records should facilitate audit retrieval without implying that every logged action was correctly performed.

Worker-related screening would examine documented contract discrepancies, inconsistent identities, wage- record anomalies, excessive hours and suspicious recruitment entries. Indicators may reflect incomplete data or legitimate seasonal variation. They require contextual interpretation and should never be used to label a worker as a trafficking victim or an employer as an offender automatically. A record of alert reasons, reviewer actions, escalation time and corrective outcomes should be preserved, with access minimization and clear retention controls. Serious matters require independent safeguarding and referral pathways.

$$D_j = \sum_{i=1}^{p} w_i \left| x_{ij} - x_{i,reference} \right| \quad (21)$$

$$V_j = \sum_{k=1}^{m} (1 - r_k(R_j)) \quad (22)$$

$$S_{monitor,j} = \alpha D_{normalized,j} + \beta V_{normalized,j} + \gamma A_{normalized,j} \quad (23)$$

$$Status_j = \begin{cases} Normal, & S \le \eta_1 \\ Review, & \eta_1 < S \le \eta_2 \\ Critical\ review, & S > \eta_2 \end{cases} \quad (24)$$

$$L_{processing} = t_{decision} - t_{available} \quad (25)$$

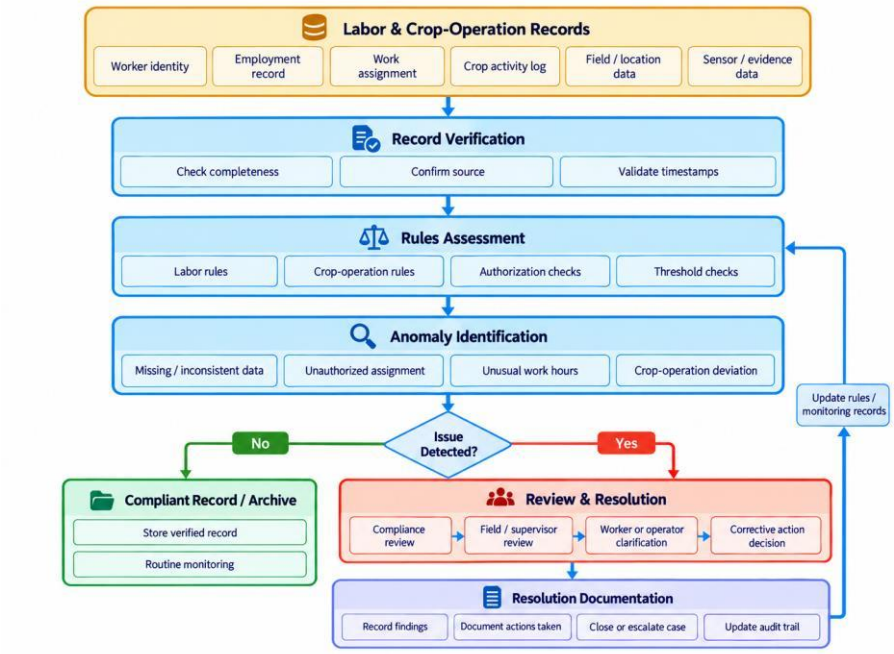


Figure 6. Proposed labor and crop-operation compliance workflow: verify record, assess rules, identify anomalies, review and document resolution.

7.6. User Interface and Visualization System

The front-facing display is intended to present farm selection, crop and plot identifiers, worker-verification status, pending synchronization, upcoming operations, application records, traceability summaries and compliance-review alerts. Critical data should remain distinguishable from ordinary production notifications. The interface must identify the source and age of each record, separate unverified local captures from confirmed ledger entries, and offer a clear path to documented corrections. Physical keys may support operation with gloves or in conditions in which touch interfaces are less reliable, subject to ergonomic testing.

Dashboard panels should be role-specific. Farm managers may review staffing and input applications; inspectors may inspect evidence and unresolved discrepancies; agronomists may focus on crop operations; certification personnel may receive a carefully limited traceability record. Worker personal information must not become widely visible merely because the same device supports agricultural operations. Status indicators should combine text and icons with color so that important alerts remain accessible to color-vision-impaired users.

$$A_{display} = A_{field} + A_{worker} + A_{alert} + A_{log} \tag{26}$$

$$V_i = \frac{A_i}{A_{display}} \tag{27}$$

$$P_i = w_{severity} S_i + w_{time} T_i + w_{recurrence} F_i \tag{28}$$

$$L_{UI} = t_{response} - t_{input} \tag{29}$$

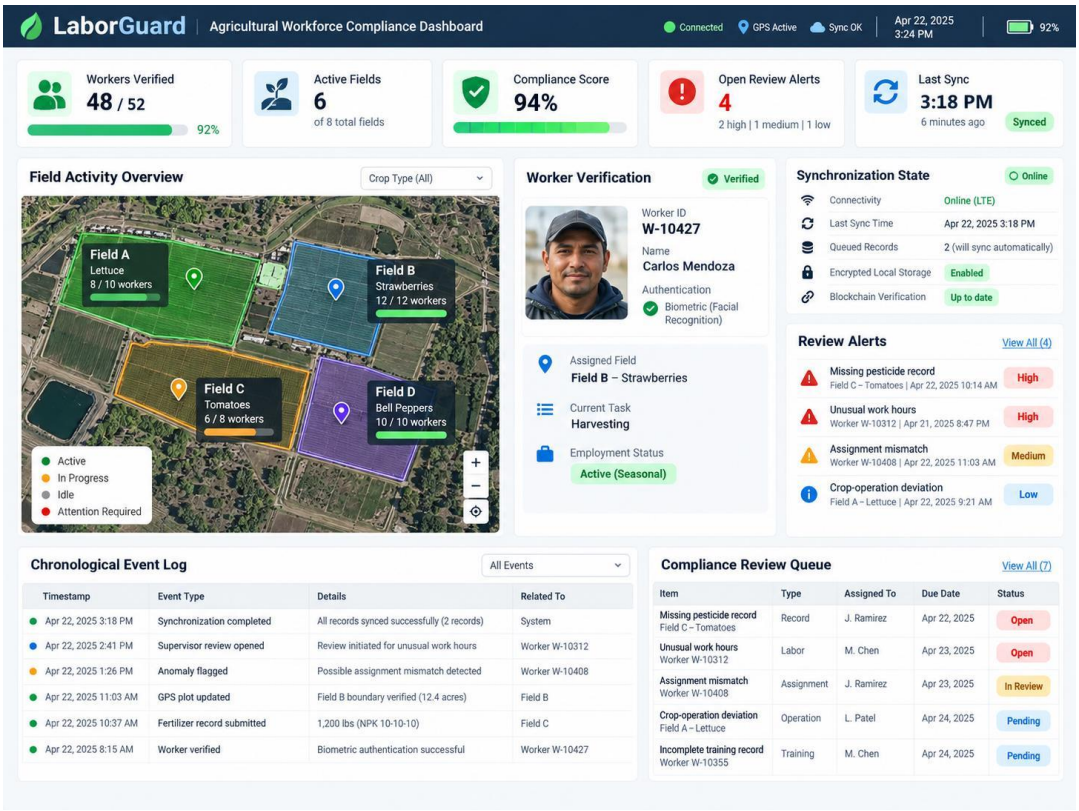


Figure 7. Proposed LaborGuard dashboard with field activity, worker verification, synchronisation state, review alerts and chronological event logs.

7.7. Alert Generation and Decision Support Framework

The alert layer translates detected record inconsistencies into reviewable work items. Events may involve missing labor authorizations, unexplained wage discrepancies, repeated excess-hours records, identity mismatch alerts, unauthorized agrochemical operation entries or incomplete farm certification documentation. A risk indication should carry an explanation, source links, confidence or uncertainty information and instructions for safe human review. Affected workers should have accessible correction and grievance routes independent of their employer wherever practicable.

Alerts may be assigned informational, review-required and urgent-safeguarding categories, but severity labels must not purport to determine criminal conduct. High-risk human-rights indicators should trigger established safeguarding procedures rather than automated punitive action. Alerts can be delivered to authenticated operators through the device or secure connected systems, with acknowledgment, investigator assignment and resolution documentation. Metrics for effectiveness should include sensitivity, specificity, false-alarm rates, time to review and demonstrable protective outcomes under independent evaluation.

$$Trigger_j = \begin{cases} 1, & S_{risk,j} > \tau_{alert} \\ 0, & otherwise \end{cases} \quad (30)$$

$$P_{alert} = w_s\, Severity + w_t\, TimeCriticality + w_r\, Recurrence \quad (31)$$

$$P_{delivery} = 1 - \prod_{i=1}^{n} (1 - p_i) \quad (32)$$

i=1

$$T_{resolution} = t_{closed} - t_{alert} \quad (33)$$

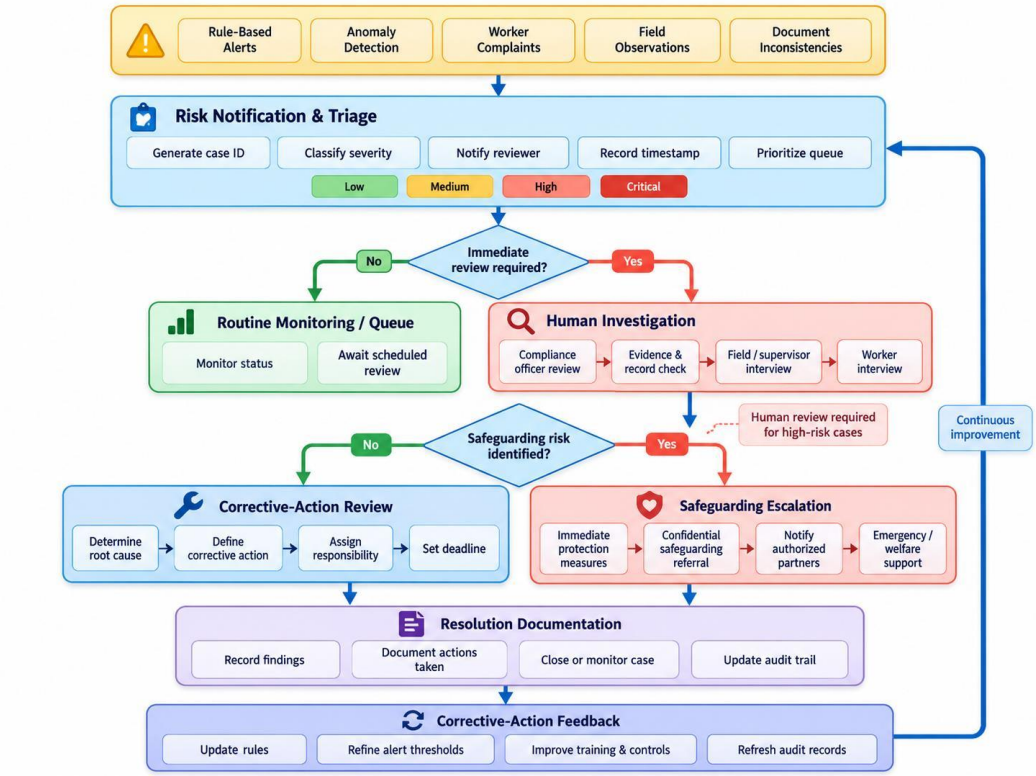


Figure 8. Proposed risk-based notification, human investigation, safeguarding escalation and corrective-action feedback framework.

7.8. System Integration, Scalability and Operational Environment

LaborGuard is conceived as an interoperable node connected to farm management information systems, agricultural cooperative databases, workforce administration systems, approved identity services, certification registers and supply-chain traceability tools. Interfaces would use documented schemas, secure APIs and access- controlled synchronization. A modular data model permits new crops, production practices, regulatory rules and farm organizations to be added without assuming that all farms or jurisdictions use identical definitions. Local- first record capture is important in remote agricultural environments where continuous broadband service cannot be assumed.

Scalability would be addressed through distributed backend services, queued ingestion, permissioned ledger node governance and selective sharing of verifiable records. Its effectiveness requires explicit capacity targets for active users, concurrent events, ledger confirmation delay, offline storage, battery endurance and sensor compatibility. The equipment should undergo mechanical, electrical, cybersecurity, usability, biometric fairness, data-protection and field workflow testing before deployment. Governance must define permission boundaries among employers, workers, inspectors, agronomists, auditors and certification agencies.

$$I_{map} : E_i \rightarrow M_j \tag{34}$$

$$T_{total} = \sum_{i=1}^{n} r_i \tag{35}$$

$$A_{system} = \frac{T_{operational}}{T_{scheduled}} \tag{36}$$

$$L_{factor} = \frac{P_{actual}}{C_{validated}} \tag{37}$$

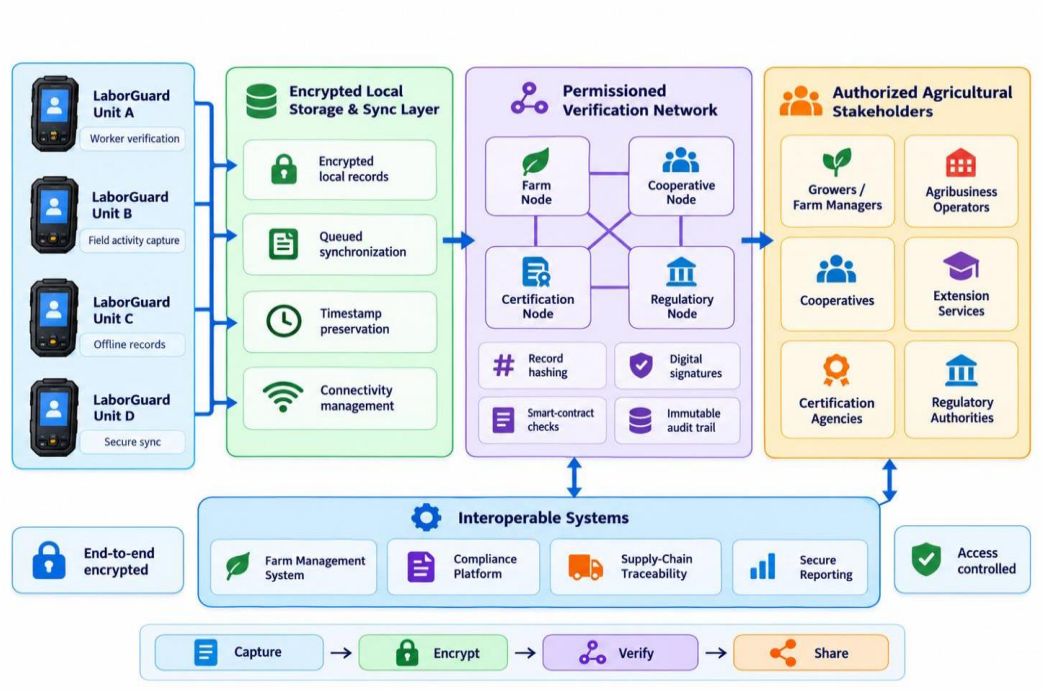


Figure 9. Proposed interoperable deployment linking LaborGuard units, encrypted storage, permissioned verification nodes and authorized agricultural stakeholders.

8. REPRESENTATION OF THE DESIGN

The official UK registration contains multi-view illustrations defining the visible appearance of the electronic device. These illustrate a predominantly rectangular electronic housing, dark front display, rectangular and circular control elements, circular rear feature and projecting cylindrical attachment. The appearance is distinct from the full set of proposed ruggedized features identified in the new LaborGuard abstract. The registration establishes what was filed, while an angular enclosure, raised carrying handle, additional identification module, sensor cluster, grille, indicators and recessed side openings are engineering proposals that may need additional representation and design protection.

The intended agricultural deployment provides context for the proposed equipment: worker registration and verification, crop input records, field location display, production lot attribution, compliance status and traceability from planting through distribution. The illustrations do not independently demonstrate such electronic operations. Captions below distinguish registered views from intended additions and maintain the requested figure sequence. Official multi-view registration plates are reproduced in Appendix A to allow the reader to inspect the actual filed appearance.

Figure 10: Isometric View

The angled three-dimensional representation reveals the spatial relationship among the main rectangular body, display, controls, circular surfaces and projecting attachment. It provides the best overall indication of registered shape. The proposed carrying handle and enhanced angular enclosure should be depicted separately where materially different.



Figure 10. Isometric View of the LaborGuard device (registered appearance where shown; additional field-device features are proposed).

Figure 11: Front View

The front representation emphasizes the dark display and grouped control elements. In the intended LaborGuard application this region would show worker verification, crop field references, production logs and alerts, but those information functions are not inferred from the design image.



Figure 11. Front View of the LaborGuard device (registered appearance where shown; additional field-device features are proposed).

Figure 12: Right Side View

This elevation establishes housing depth, side geometry and alignment of projecting features. Recessed port openings, connector seals and protective equipment described for the rugged engineering version remain proposed details unless clearly shown in the official view.



Figure 12. Right Side View of the LaborGuard device (registered appearance where shown; additional field-device features are proposed).

Figure 13: Left Side View

The opposite lateral perspective clarifies the enclosure outline and cylindrical attachment relative to the main housing. Future integration of sensing or identification peripherals would require actual mechanical drawings showing their precise surfaces and dimensions.



Figure 13. Left Side View of the LaborGuard device (registered appearance where shown; additional field-device features are proposed).

Figure 14: Rear View

The registered rear shows a circular feature and surrounding housing surfaces. Battery access, data connectors, thermal management, supports and cryptographic hardware are intended engineering provisions rather than functions documented by this visual record.



Figure 14. Rear View of the LaborGuard device (registered appearance where shown; additional field-device features are proposed).

Figure 15: Top View

The upper representation provides the registered device outline and position of top projections. The raised carrying handle called for in the proposed LaborGuard abstract is an additional design element, and its effect on the overall appearance should be considered before filing updated drawings.



Figure 15. Top View of the LaborGuard device (registered appearance where shown; additional field-device features are proposed).

Figure 16: Bottom View

The underside view completes the external representation of the original device. Proposed foot pads, seals, charging contacts or maintenance panels should not be treated as registered components unless depicted and must be specified through future engineering documentation.



Figure 16. Bottom View of the LaborGuard device (registered appearance where shown; additional field-device features are proposed).

Collectively, these registered and proposed representations clarify the distinction between the ornamental appearance protected by UK Design No. 6548985 and the proposed apparatus for authenticated agricultural labor documentation and crop-production traceability. The official design views, not new verbal descriptions, determine the scope of the existing registered design.

9. DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The preferred proposed embodiment is a rugged field-portable computing instrument combining workforce identity verification, authorized crop activity registration, secure record processing and compliance decision support. As conceptualized in Figure 10, a protective angular enclosure accommodates the front display and controls while a raised carrying handle supports movement between field plots, farm offices and inspection locations. The engineering description expands upon, but must remain legally distinguished from, the compact device appearance shown in the official UK registration. The preferred embodiment is intended for varied production systems including soybean, maize/corn, wheat, rice, cotton, sugarcane, potatoes, tomatoes, lettuce, strawberries, grapes, apples, citrus, almonds and cassava.

The front interface (Figure 11) provides access to worker registration, workforce assignment, crop field selection, application history, traceability status and audit alerts. The proposed identification module may verify credentials or support approved biometric authentication with appropriate alternatives. The operator selects the agricultural enterprise, crop plot, activity and authorized worker, then reviews the displayed evidence or selects a capture action. The interface should disclose whether a record is verified, locally pending synchronization, rejected for incomplete fields or subject to compliance review. Clearly separated access privileges protect confidential worker information from ordinary farm users.

The right-side proposed enclosure (Figure 12) provides protected access to communication and peripheral connectors. These may permit secure links to field positioning instruments, environmental sensors, external identification devices or farm computers. When the network is unavailable, signed records are placed in encrypted local storage with event timestamps and provenance indicators. On reconnection, the device verifies credentials, uploads permissible records and obtains proof of successful acknowledgment or ledger anchoring. Offline entries cannot be described as immutable blockchain records before their successful authenticated commitment.

The left-side region (Figure 13) accommodates the projecting component visible in the registration and, in a future engineered embodiment, may support additional protected sensing or communication assemblies. Records for fertilizer applications may include plot, crop, material name, input amount, application method, date and authorized operator. Weed- and pest-management records may include treatment target, product used, conditions, applied rate and any relevant regulatory instructions. Such information supports documentation only if captured and independently checked accurately; the device must not substitute for professional pest- management assessment or application safety procedures.

The rear surface (Figure 14) may accommodate an engineered battery cover or protected service zone in a future implementation, while retaining the registered rear appearance where feasible. Internally, a trusted processing component would manage signing keys, access permissions and encrypted storage. A permissioned ledger would preserve commitments and validation metadata. Worker photographs, biometric templates, employment documents, personal addresses or confidential grievances would remain in restricted off-chain repositories, with retention and correction controls established under the applicable legal framework. Keys should be managed so that theft or loss of a device cannot automatically expose sensitive farm or labor data.

The upper surface and proposed carrying structure (Figure 15) are intended for routine transport between plots, storage areas and workforce assembly points. The handle should be structurally tested for repeated lifting, and the enclosure should be evaluated for impact, moisture, dust, solar exposure and usability during seasonal farm operations. A portable device should be engineered for gloved hands, screen legibility under outdoor illumination and suitable navigation during field inspections. The lower surface (Figure 16) may incorporate anti-slip supports and protected fastening points to permit temporary placement on stable inspection surfaces without exposing connectors.

In a representative workforce procedure, an authorized field supervisor selects the agricultural enterprise and plot, confirms the relevant worker credential and associates the worker with a documented task and permitted working interval. The device records the task identifier, crop and plot reference, verification result, event time and responsible supervisor. The underlying employment terms and sensitive worker identity attributes remain available only to authorized reviewers. Work events may be signed and committed through the proposed blockchain infrastructure, permitting later reconciliation between assignments, attendance and payment records. Independent evidence remains necessary where records conflict or where coercion is suspected.

In a representative crop operation, a trained farm operator records an irrigation activity, fertilizer treatment, pest- management activity or harvest event, with crop, location, task, input quantity or production lot as applicable. The event is validated against required fields and operator authorization, then linked to prior authorized farm records. A certification auditor can examine a chain of authenticated production events, subject to permissions and documentary corroboration. A traceability chain does not automatically prove crop quality, sustainable production outcomes or compliance with every relevant agricultural standard.

The proposed analytical subsystem compares recorded working hours, wage entries, authorized worker identities and recruitment records against defined rules and calibrated contextual indicators. It may flag unexplained discrepancies and route them into a safeguarded investigation workflow. Alerts should be visible to qualified compliance personnel with appropriate confidentiality safeguards. The system should never automatically terminate employment, block payment, report a person as a trafficking victim or publish allegations based exclusively on algorithmic output. Resolution outcomes, corrections and review actions should themselves be auditable without permanently exposing confidential worker testimony.

Taken together, Figures 10–16 and the proposed operational procedures describe a unified equipment concept joining farm record acquisition, employment verification, cryptographic integrity and risk-informed regulatory review. The anticipated uses extend from planting through harvesting and post-harvest distribution for crops requiring detailed labor and agronomic documentation. Implementation will require industrial design reconciliation, functional prototyping, laboratory and field verification, data-governance agreements and compliance with relevant labor, privacy and agricultural requirements. The existing UK certificate remains evidence of the registered external appearance only.

10. RESULTS AND DISCUSSION

The following findings arise from the design documentation, specified numerical scenarios and canonical mathematical models; none represents an independently measured LaborGuard field trial. The evidence is reported in four distinct categories: stipulated transaction-capacity behaviour, hypothetical authentication and synchronization counts, a synthetic screening confusion matrix, and analytically defined nonlinear response models. Distinguishing these sources is essential: numerical reproducibility under an assumption

is not evidence that the proposed device meets the same specification in operation (Androulaki et al., 2018; Casino et al., 2019; Uzoma et al., 2024).

10.1. Transaction Processing, Queue Stability, and Latency

Table 1 isolates the internally specified transaction-load scenario from external benchmark quotations. For arrival rates λ of 10–150 transactions per second (TPS), the assumed service capacity μ = 150 TPS is sufficient to complete every transaction within the one-hour accounting window. Reported latency increases from 0.181 s at 10 TPS to 0.390 s at 150 TPS, an absolute change of 0.209 s or 115.5%. The observed shape in these scenario entries is consistent with increasingly severe contention near a capacity limit, although no queue discipline, consensus configuration, variance, or replicate observations accompany the data. The apparent 150-TPS ceiling is an input assumption, not a measured LaborGuard benchmark (Androulaki et al., 2018; Uzoma et al., 2024).

Overload changes the interpretation of latency. At 175, 200 and 250 TPS, the stipulated server continues to complete 150 TPS while incoming work exceeds the service rate by 25, 50 and 100 TPS, respectively. Thus $B(3{,}600\ s) = \max(0, \lambda - \mu) \times 3{,}600$, giving end-hour backlogs of 90,000, 180,000 and 360,000 transactions. The corresponding completed records remain 540,000 per hour. Because the queue is increasing, a stationary mean commitment latency is undefined; reporting the 0.390-s capacity-edge latency as if it also applied under overload would be incorrect. For agricultural use, batch harvesting and delayed field uploads may create bursty arrivals; testing should examine 95th/99th percentile latency, durable queue length, retry idempotence and time to drain after the burst (Saberi et al., 2019; Queiroz & Wamba, 2019).

Table 2 separately records five contextual blockchain benchmark statements appearing in the source table. They involve different performance quantities (write latency, read throughput, tamper-warning accuracy and inclusion delay) with no traceable source methodology, hardware settings or transaction definitions. They are retained as unverified contextual values and excluded from direct performance comparisons. A fair benchmark must specify validator topology, block interval, signing overhead, payload size, endorsement policy and network impairments; neither a higher headline TPS nor a lower isolated delay establishes practical deployment superiority (Casino et al., 2019; Androulaki et al., 2018).

Table 1. Stipulated transaction-capacity scenario; 1-hour observation window (not field observations).

Offered TPS	Completed TPS	End-hour backlog	Mean commit latency (s)
10	10	0	.181
25	25	0	.183
50	50	0	.186
75	75	0	.192
100	100	0	.203
125	125	0	.230
140	140	0	.278
150	150	0	.390
175	150	90,000	unstable
200	150	180,000	unstable

250	150	360,000	unstable

Table 2. Previously reported contextual values without an identifiable controlled benchmark.

Contextual metric	Source-table value	Comparison limitation
Write latency at 50 TPS	0.22–0.24 s	Platform and protocol unstated
Read/write throughput	227 / 121 TPS	Read and write not directly comparable
Throughput / node latency	207.4 ± 10.2 TPS / 259.3–278.7 ms	Unknown test environment
Tamper-warning scenario	390 TPS / 98.2% at 3% tampering	Unknown labels and method
Ethereum inclusion	12.91–35.76 s	Public-chain context differs

10.2. Credential Verification, Offline Synchronization, and Data Integrity

Table 3 separates credential outcomes from event-synchronization outcomes to prevent denominator confusion. In a hypothetical cohort of 20,000 legitimate credential attempts, 19,700 pass an initial check (98.50%) and 300 require assistance or an alternate credential (1.50%). This is a first-pass completion fraction, not a biometric sensitivity, false-acceptance rate or demographic-fairness estimate. A valid evaluation requires independent identity ground truth and separate tests for unauthorized attempts, adversarial presentation, subgroup differences and non-biometric fallbacks. The practical priority is that a verification exception must not prevent a worker from accessing wages, grievance mechanisms or lawful duties (Raji et al., 2020; Ayoola et al., 2024).

The offline record scenario assumes 12,000 captured events, of which 1,800 (15.0%) originate without connectivity. Of the offline subset, 1,782 subsequently synchronize (99.0%) while 18 (1.0%) require reconciliation. Treating 1,782/12,000 as the synchronization success rate would misuse the denominator. The unresolved records may reflect conflicting timestamps, duplicate event IDs, key expiry or interruption, but their causes are not reported. Ledger anchoring verifies later record consistency, not whether an employee actually performed a task or whether a supervisor recorded accurate wages. Accordingly, local entries must be clearly marked pending, and corrections must preserve append-only audit history without publishing confidential worker data (Saberi et al., 2019; Ijiga et al., 2024; Uzoma et al., 2024).

Table 3a. Hypothetical credential-verification counts.

Credential verification scenario	Numerator	Denominator	Fraction
First-pass valid credentials	19700	20000	98.50%
Alternative/manual handling	300	20000	1.50%

Table 3b. Hypothetical offline acquisition and recovery counts.

Offline sync scenario	Numerator	Denominator	Fraction

Captured while offline	1800	12000	15.00%
Synchronized after reconnection	1782	1800	99.00%
Requires reconciliation	18	1800	1.00%

10.3. Documentary-Discrepancy Screening and Classification Trade-offs

The supplied synthetic evaluation contains 10,000 labelled records, including 600 discrepancies and 9,400 non-discrepancies (6.0% prevalence). Table 4 displays the original four confusion-matrix cells; Table 5 derives the performance metrics directly from those cells. There are 480 true alerts and 120 missed discrepancies, resulting in 80.00% sensitivity. Of 9,400 nominally normal records, 9,024 are correctly rejected and 376 incorrectly flagged, giving 96.00% specificity and a 4.00% false-positive rate. Positive predictive value is 480/(480+376) = 56.07%, F1 = 2×480/(2×480+376+120) = 0.6593, and overall accuracy is (480+9,024)/10,000 = 95.04% (Raji et al., 2020; Ijiga et al., 2024).

The operational burden is material: 856 reviews would be opened, of which 376 (43.93%) are false alerts relative to the synthetic labels, while one in five labelled discrepancies is not flagged. At a lower real-world discrepancy prevalence, precision could deteriorate further even if sensitivity and specificity remained constant; for example, at hypothetical 1% prevalence, the same 80% sensitivity and 96% specificity imply precision of about 16.8%. This is a mathematical sensitivity example, not an observed deployment outcome. Moreover, the synthetic class represents recorded documentary discrepancies rather than legally determined trafficking. Human-rights responses require corroborating worker testimony, contextual inquiry, confidentiality, non-retaliation, and accountable escalation, not automated employer sanctions (Ijiga et al., 2024; Ayoola et al., 2024; Raji et al., 2020).

Table 4. Synthetic documentary-discrepancy screening confusion matrix.

Actual label	Flagged	Not flagged	Total
Discrepancy	480	120	600
No discrepancy	376	9024	9400
Total	856	9144	10000

Table 5. Derived synthetic classifier metrics; not trafficking-detection validation.

Measure	Calculation	Value
Sensitivity	480 / 600	80.00%
Specificity	9024 / 9400	96.00%
Precision	480 / 856	56.07%
False-alert share	376 / 856	43.93%
F1 score	960 / 1456	0.6593
Accuracy	9504 / 10000	95.04%

10.4. Nonlinear Stability and Bifurcation Scenario Interpretation

The six conceptual figures illustrate generic nonlinear thresholds rather than fitted models of the device. The saddle-node normal form $dx/dt = r - x^2$ has two equilibria $\pm\sqrt{r}$ for $r > 0$, which merge at $r = 0$; the upper branch is stable. The transcritical normal form $dx/dt = rx - x^2$ exchanges branch stability at $r = 0$,

while the supercritical pitchfork $dx/dt = rx - x^3$ produces two stable nonzero states for $r > 0$. Table 6 extracts the supplied parameter cases independently from the throughput figures. Such illustrations motivate testing for operational regime changes, but their variables have no identified calibration against worker identity, queue growth or detector behaviour. Therefore they cannot be interpreted as demonstrated failures or instabilities of LaborGuard (Strogatz, 2015; Kuznetsov, 2004).

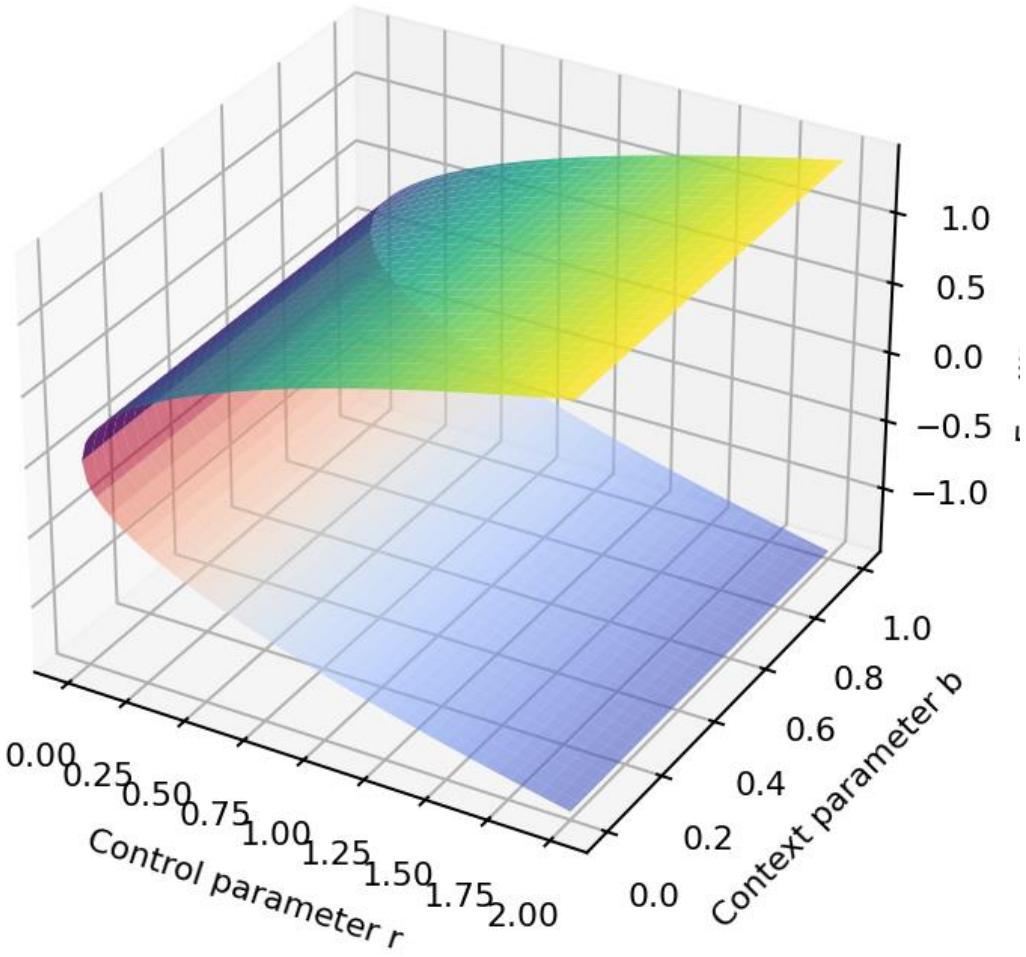


Figure 17. Saddle-node canonical equilibrium sheets: $dx/dt = r - x^2$; upper branch stable and lower branch unstable for $r > 0$. b is a display dimension.

Figure 17 illustrates the saddle-node threshold at $r = 0$. Two steady states exist for $r > 0$, but no real equilibrium exists for $r < 0$. For LaborGuard, this is a conceptual analogy for loss of an operating state under an adverse load or control parameter; the curve is not a fitted queue-performance model and supplies no measured transaction threshold.

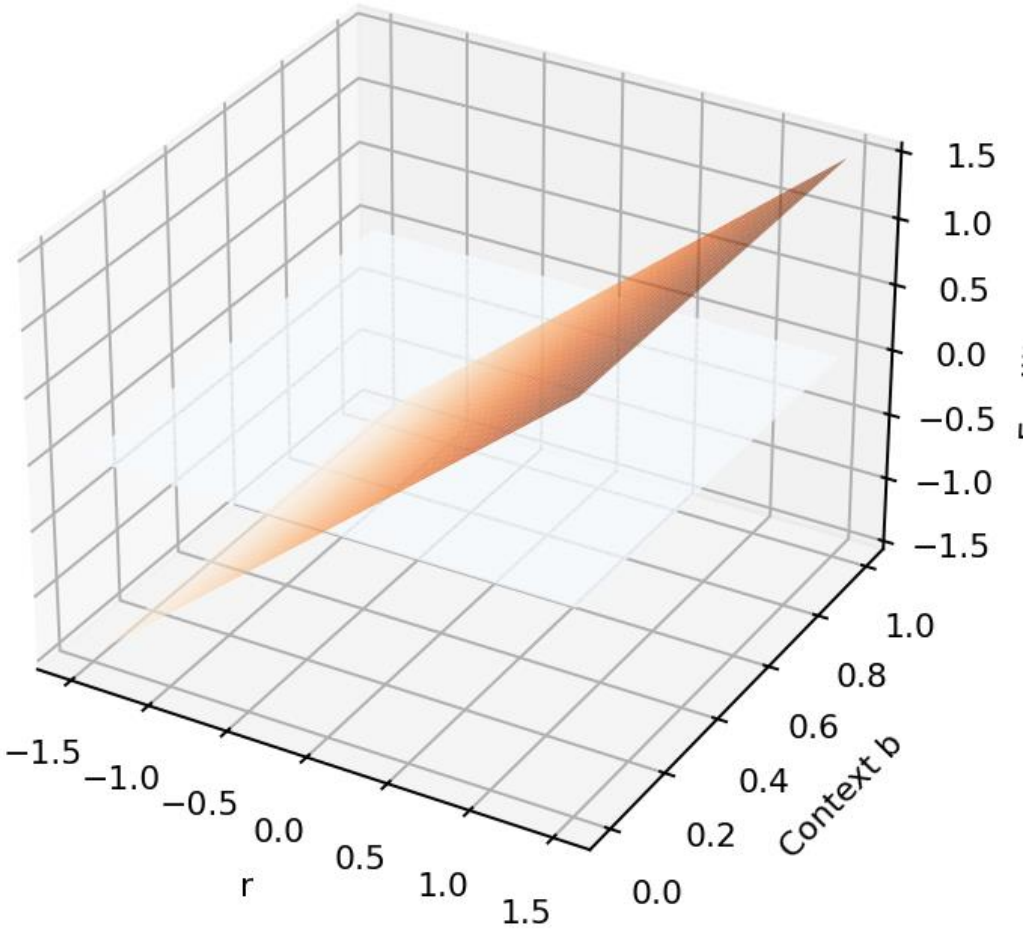


Figure 18. Transcritical canonical equilibria: dx/dt = r x − x², x* = 0

Figure 18 shows a transcritical exchange of equilibrium stability at r = 0. Its relevance is to alternative operating regimes that exchange stability when a control condition changes, such as a hypothetical synchronization-state transition. No LaborGuard-specific stability coefficient has yet been estimated, so this graph remains a mathematical example rather than validation of device behaviour.

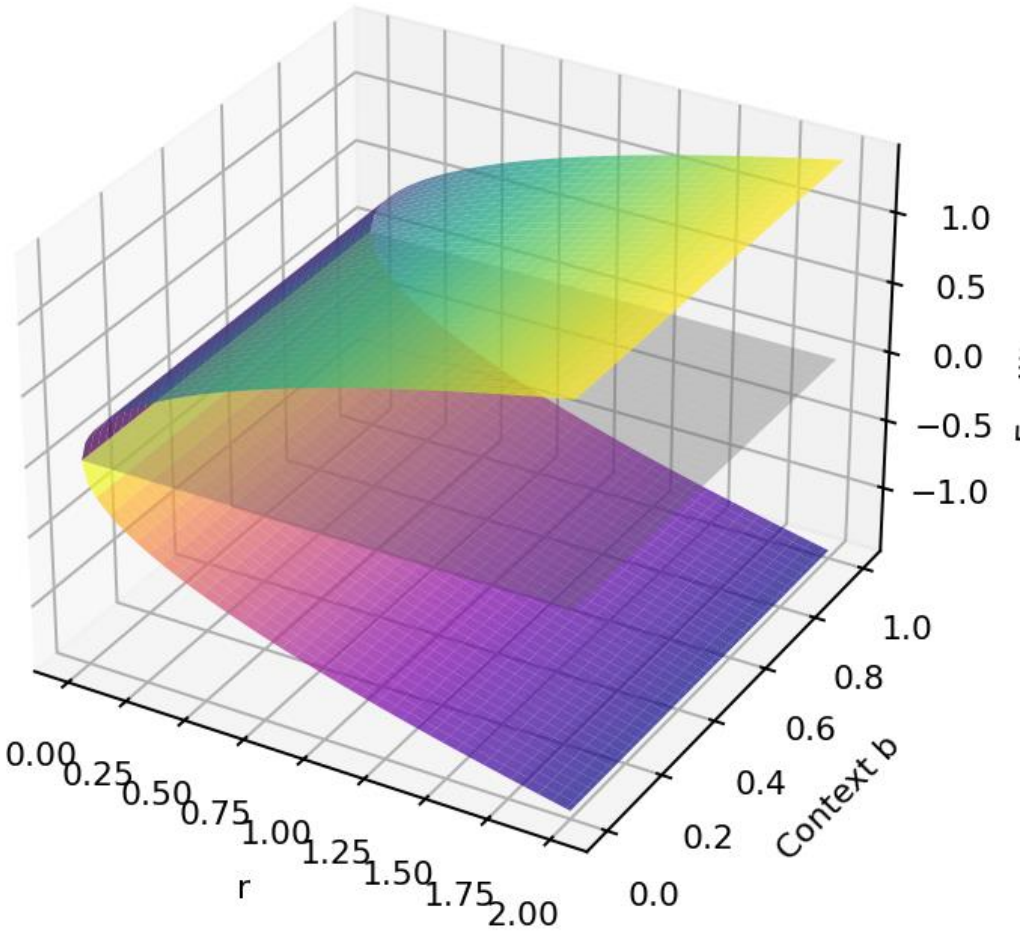


Figure 19. Supercritical pitchfork equilibria $dx/dt = r\,x - x^3$; nonzero branches $\pm\sqrt{r}$ stable for $r > 0$, while $x = 0$ becomes unstable.

Figure 19 depicts the pitchfork model: the zero equilibrium is stable for $r < 0$, while two non-zero stable equilibria appear for $r > 0$. This demonstrates how a simplified nonlinear control model can admit more than one steady response. In the LaborGuard setting, it motivates testing whether retry, backlog, or feedback policies can produce divergent operational states; it does not establish that actual device trajectories bifurcate.

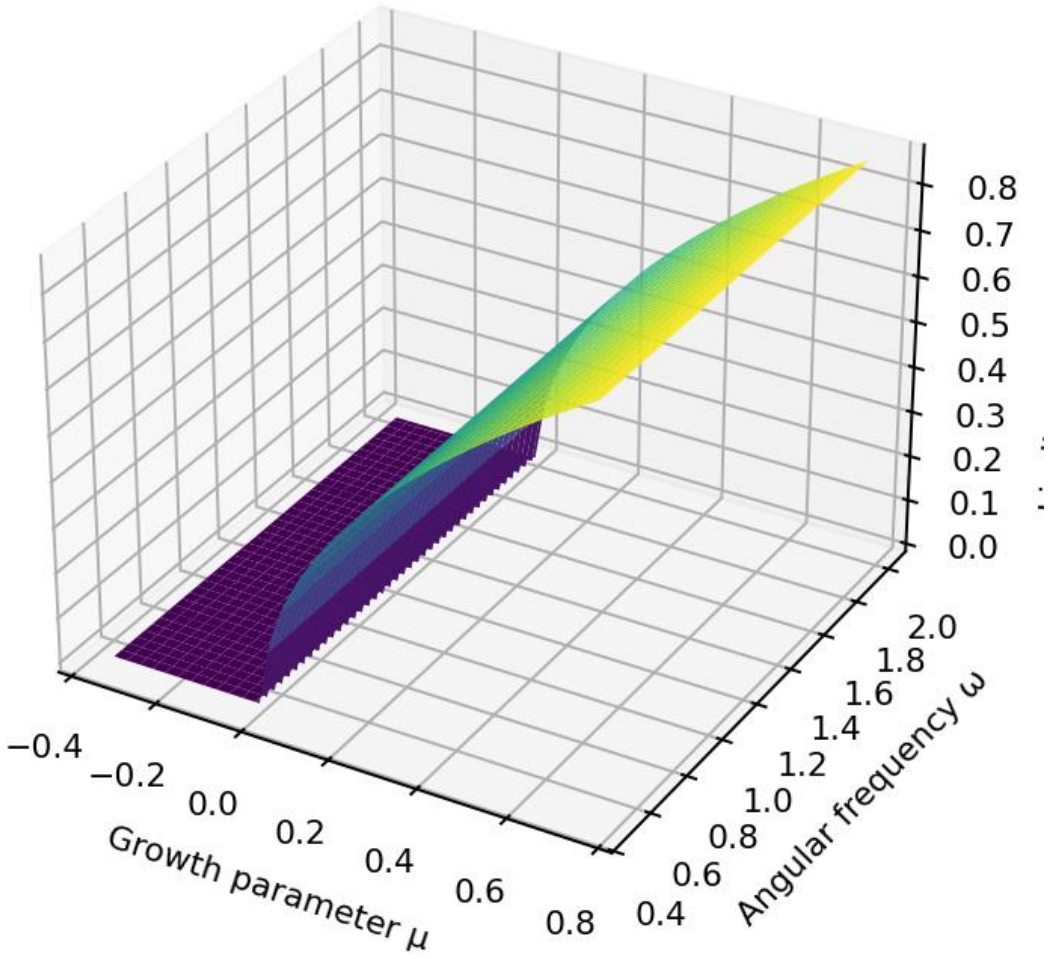


Figure 20. Supercritical Hopf amplitude surface for $dz/dt = (\mu + i\omega)z - |z|^2 z$. Radius $\sqrt{\mu}$ appears for $\mu > 0$. ω changes frequency.

Figure 20 displays the Hopf normal-form limit-cycle amplitude $\sqrt{\mu}$ for $\mu > 0$. As a numerical illustration, $\mu = 0.25$ gives amplitude 0.50. Oscillatory behaviour could matter for batched blockchain submission, network retries, or recurring queue bursts. However, the amplitude is dimensionless and cannot be interpreted as measured latency, alert frequency, or device availability without parameter identification.

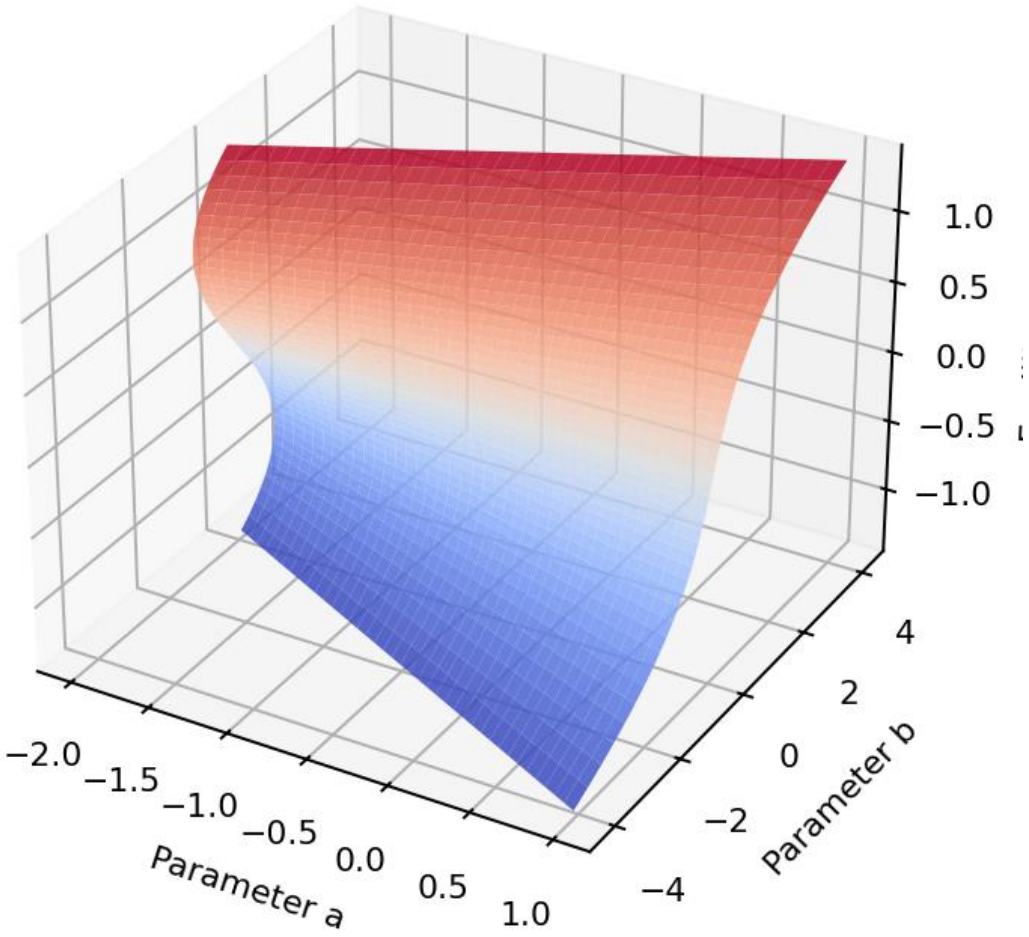


Figure 21. Cusp equilibrium surface for $dx/dt = b - a\,x - x^3$, with equilibrium $b = a\,x + x^3$. Multistability is possible for $a < 0$, bounded by $4a^3 + 27b^2 = 0$.

Figure 21 plots the cusp equilibrium surface $b = ax + x^3$, where the fold boundary $4a^3 + 27b^2 = 0$ separates one-equilibrium and three-equilibrium regions. It illustrates the possibility of abrupt and history-dependent state changes under two interacting controls. For LaborGuard, such behavior is a hypothesis to test under combined input-load and retry-policy variation, not an observed finding.

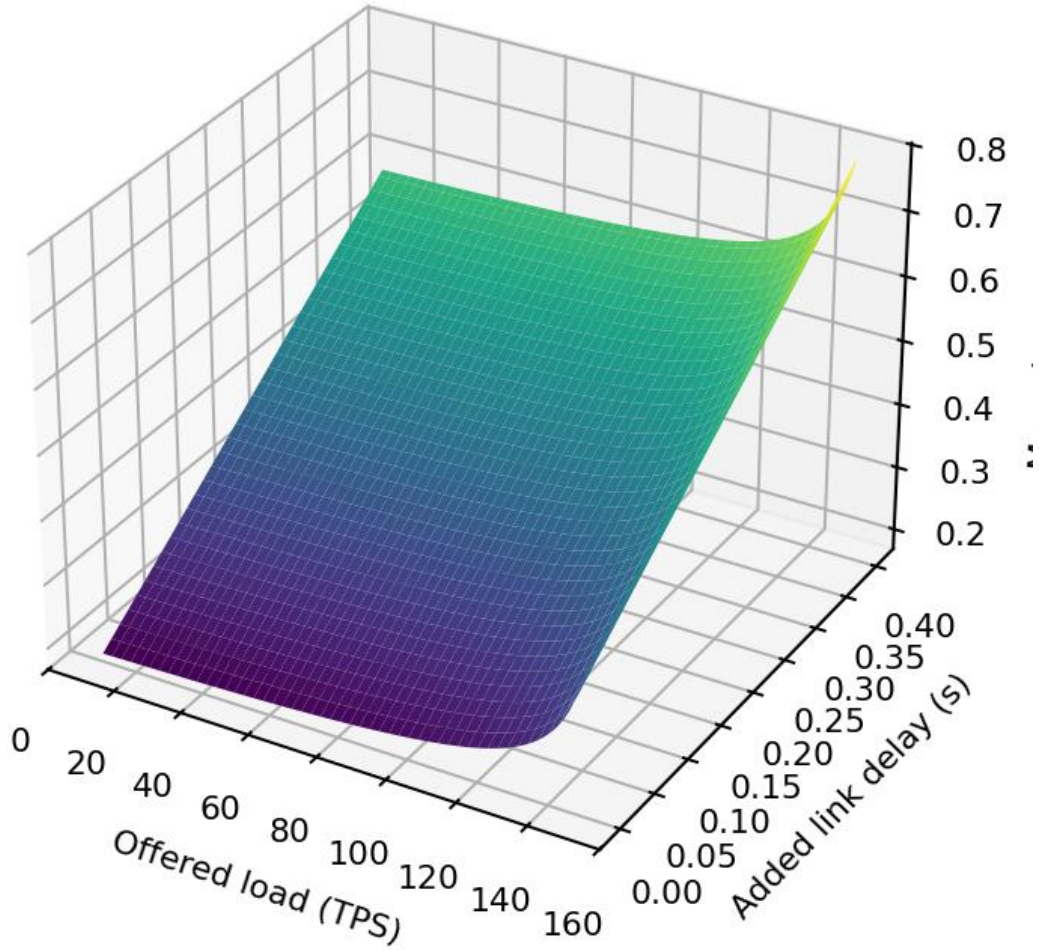


Figure 22. Scenario latency response surface, including an additive 0–400 ms network delay.

Figure 22 examines the stipulated network-delay sensitivity surface. Increasing the added delay from 0 to 400 ms shifts the overall latency upward under the scenario assumptions; the effect is additive rather than a demonstrated instability. Practical evaluation should measure latency percentiles, confirmation time, offline queue depth, and recovery time on a physical prototype under controlled connectivity disruptions.

Table 6. Canonical-model outcomes inferred from specified equations, not device measurements.

Canonical model	Parameter case	Equilibrium or amplitude	Analytical stability
Fold	r=0.25	x=±0.500	+ stable; − unstable
Transcritical	r=−0.50	x=0, −0.50	0 stable
Transcritical	r=+0.50	x=0, +0.50	+0.50 stable
Pitchfork	r=+0.36	x=0, ±0.600	±0.600 stable
Hopf	μ=+0.25	amplitude 0.500	stable cycle
Cusp	a=−1; b=0	x=−1,0,+1	±1 stable

10.5. Hopf, Cusp, and Network-Delay Scenario Interpretation

The Hopf normal form $dz/dt = (\mu+i\omega)z - |z|^2z$ produces a stable periodic solution of amplitude $\sqrt{\mu}$ when $\mu > 0$; at $\mu = 0.25$ the illustrative radius is 0.50. The cusp equation $b = ax + x^3$ has three equilibria at $a = -1$, $b = 0$ $(-1, 0, +1)$; the outer branches are stable for the associated dynamics $dx/dt = b - ax - x^3$. Inside the cusp, $4a^3 + 27b^2 < 0$ implies three real roots. The sixth plot introduces network delay up to 400 ms, but does not supply traces or a fully identifiable empirical response relation. These phenomena are analytically coherent examples, not evidence of Hopf oscillations, hysteresis or measured network jitter in a deployed system (Strogatz, 2015; Kuznetsov, 2004).

The relevant engineering translation is a falsifiable test plan rather than a direct transfer of a canonical diagram. Queue saturation can be explored through controlled arrival bursts and measured backlog; synchronization stability through connectivity loss, retry storms and conflict injection; and reviewer workload through time-stamped alert queues and blinded adjudication. Delay should be decomposed into capture, local validation, transmission, endorsement, ledger confirmation and dashboard acknowledgement. Comparing the distributions under normal and impaired links would establish whether nonlinear behaviour appears and which physical mechanisms produce it (Androulaki et al., 2018; Uzoma et al., 2024).

10.6. Integrated Discussion and Research Contribution

Taken together, the scenario data expose three interacting bottlenecks rather than proving three achievements. At the stipulated processing ceiling, backlog growth can overwhelm periodic synchronization; 1% unresolved offline records can frustrate farm-to-lot reconciliation; and a 43.93% false-alert share can generate costly and potentially harmful investigations. These concerns are coupled: poor record provenance can inflate anomaly scores, while an overloaded ledger can delay evidence availability. The proposed architectural contribution is the linked workflow between task authorization, worker credential, plot or lot metadata, off-chain sensitive records, ledger commitments and human-reviewed compliance decisions. Prior work on blockchain interoperability and cyber-risk screening supports considering these as distinct validation layers (Uzoma et al., 2024; Ijiga et al., 2024; Ayoola et al., 2024; Saberi et al., 2019).

Limitations remain decisive. The manuscript contains no prototype measurement series, field recruitment sample, annotated worker outcomes, inter-rater reliability assessment, ledger testbed configuration or comparison against existing farm software. Neither the UK industrial-design registration nor these synthetic scenarios substantiates a reduction in trafficking, improvement in yields, or enhanced legal compliance. A research-paper claim should therefore be limited to architectural synthesis and scenario-based performance analysis until repeatable bench tests and independent farm pilots provide verifiable outcomes. This evidence distinction also limits comparisons with published blockchain systems and machine-learning audits (Casino et al., 2019; Raji et al., 2020). Existing international guidance provides additional criteria for responsible deployment, including forced-labor risk identification, human-rights due diligence, confidentiality and governance (International Labour Organization, 2014; International Labour Organization et al., 2022; United Nations Office on Drugs and Crime, 2022; United Nations, 2011; Organisation for Economic Co-operation and Development, 2018).

11. RECOMMENDATIONS

11.1. Prototype characterization. Fabricate a documented engineering prototype, retain the registered industrial-design views as a separate legal record, and measure enclosure ingress resistance, handling, battery endurance, screen visibility, power draw, processing capacity, protected-key storage and fault recovery. Define acceptance thresholds before testing rather than retrofitting them to achieved outcomes (Somuah et al., 2024; Idoko et al., 2024). Related engineering examples in power electronics and condition monitoring support hardware assurance planning, without constituting evidence of this prototype's fitness (Idoko et al., 2024; Somuah et al., 2024).

11.2. Reproducible load and synchronization evaluation. Execute repeated tests from 10 to 250 TPS with fixed payloads and validator configurations, reporting median, p95 and p99 confirmation delay, completed TPS, message loss, queue growth, drained-backlog time and confidence intervals. Test airplane-mode periods, intermittent links, duplicate submissions and signing-key revocation to verify idempotent recovery (Androulaki et al., 2018; Uzoma et al., 2024). Scalable information-system and IoT deployment principles should guide architecture design (Idoko et al., 2024; Uzoma et al., 2024; World Economic Forum, 2019).

11.3. Worker-centred safeguards. Store biometric templates, wage records and allegations in access-controlled off-chain repositories; provide non-biometric alternatives, individual correction channels and independent grievance pathways; log reasons for every risk alert and prevent automatic adverse action. Review privacy law, labor protections, referral arrangements and the effects of surveillance on migrant and seasonal workers (Raji et al., 2020; Ijiga et al., 2024). Apply documented information-security controls, identity management and privacy-law assessments (International Organization for Standardization, 2022; European Parliament and Council of the European Union, 2016; National Institute of Standards and Technology, 2017).

11.4. Independent screening validation. Assemble a consent-governed, legally reviewed dataset with blinded expert labels; measure sensitivity, specificity, precision, confidence intervals, calibration, precision–recall curves and subgroup harms at realistic prevalences. Compare rule-based, hybrid and no-algorithm baselines, including the reviewer time and consequences of false alerts (Ijiga et al., 2024; Michael et al., 2024; Ayoola et al., 2024). Threat-detection, fraud-analytics, reinforcement-learning and AI-audit research may guide the evaluation methodology, but their non-agricultural outcomes must not be transferred as measured LaborGuard performance (Idoko et al., 2024; Michael et al., 2024; Ijiga et al., 2024; National Institute of Standards and Technology, 2023; International Organization for Standardization, 2023).

11.5. Cross-site agricultural pilots. Evaluate crop-specific schemas across at least two materially different farming systems and compare the prototype with existing paper and digital records for completeness, traceability lookup time, event correction, worker-reported trust and audit reproducibility. Register study protocols and report failures as well as improvements (Saberi et al., 2019; Idoko et al., 2024). Agricultural automation and environmental data practices offer relevant implementation context (Food and Agriculture Organization of the United Nations, 2022; Ayoola et al., 2024).

11.6. Interoperability and lifecycle governance. Establish schema versioning, role-limited API scopes, ledger governance, key rotation, audit retention limits, correction procedures and offboarding policies. Adoption should depend on demonstrated proportionality, independent oversight and measurable benefit, rather than the use of blockchain as an end in itself (Queiroz & Wamba, 2019; Uzoma et al., 2024).

Independent security governance should also follow recognized risk-management practices (National Institute of Standards and Technology, 2024; International Organization for Standardization, 2022).

12. CONCLUSION

LaborGuard offers a proposed integration of agricultural workforce authentication, georeferenced activity capture, protected off-chain records, permissioned-ledger commitments and human-centred compliance screening. The documented scenario analysis highlights a nominal 150-TPS transaction-capacity boundary, a hypothetical 99% synchronization rate for offline records and an illustrative discrepancy classifier with 80.00% sensitivity but only 56.07% precision. Those quantities arise from specified or synthetic inputs; they are not measurements of the finished device. Their principal value is to identify where engineering tests and safeguarding controls are needed (Androulaki et al., 2018; Uzoma et al., 2024; Raji et al., 2020).

The research contribution at this stage is an integrated and testable design rationale, not proof of trafficking detection or production improvement. A defensible progression to an experimental research article requires reproducible hardware benchmarks, transparent model validation, measured farm workflow outcomes and independent worker-protection review. Cryptographic auditability can support accountability only when source quality, rights protection and human investigation remain integral to the system (Saberi et al., 2019; Ijiga et al., 2024). The integration of ethical supply-chain considerations with AI-enabled anti-trafficking strategies also requires empirical safeguarding evidence (Ijiga et al., 2024; Ijiga et al., 2024).

REFERENCES:

1. Flynn, K., & Lam, P. (2023). System and method for blockchain-based employment verification (U.S. Patent Application Publication No. US20230028681A1). United States Patent and Trademark Office. https://patents.google.com/patent/US20230028681A1/en
2. Knas, M., John, J., Gibadlo, K., & Ferry, R. (2021). Intelligent employment-based blockchain (U.S. Patent No. US11157876B1). United States Patent and Trademark Office. https://patents.google.com/patent/US11157876B1/en
3. Randhawa, J. (2018). Methods and systems for employment and education verification using blockchain (U.S. Patent Application Publication No. US20180293547A1). United States Patent and Trademark Office. https://patents.google.com/patent/US20180293547A1/en
4. Zou, X. (2023). Information management methods, devices and equipment and storage media based on blockchain (Chinese Patent No. CN110188109B). China National Intellectual Property Administration. https://patents.google.com/patent/CN110188109B/en
5. Recruitment information authentication management method and system based on block chain. (2021). Chinese Patent Application Publication No. CN113128962A. China National Intellectual Property Administration. https://patents.google.com/patent/CN113128962A/en
6. A blockchain-based construction worker professional file management method and system. (2023). Chinese Patent Application Publication No. CN117149769A. China National Intellectual Property Administration. https://patents.google.com/patent/CN117149769A/en
7. Construction engineering work information sharing platform based on block chain technology and operation method. (2023). Chinese Patent No. CN111988307B. China National Intellectual Property Administration. https://patents.google.com/patent/CN111988307B/en

8. Methods for providing simple electronic payment of gig worker wages and personal sensitive information management, on basis of electronic wallet. (2024). International Patent Application Publication No. WO2024071864A1. World Intellectual Property Organization. https://patents.google.com/patent/WO2024071864A1/en
9. Socialization manpower resource management system and method based on blockchain technology. (2024). Chinese Patent No. CN111985905B. China National Intellectual Property Administration. https://patents.google.com/patent/CN111985905B/en
10. Gill, J., & Nicol, G. (2021). Blockchain based supply chain network systems (U.S. Patent Application Publication No. US20210004739A1). United States Patent and Trademark Office. https://patents.google.com/patent/US20210004739A1/en
11. Moss, E. E., Likins, G. N., & Simon, A. (2022). Tracking qualitative parameters using a blockchain provenance system (U.S. Patent Application Publication No. US20220374823A1). United States Patent and Trademark Office. https://patents.google.com/patent/US20220374823A1/en
12. Rabby, J. C., & Gerrard, D. L. (2020). Systems and methods for tracking and tracing performance of agricultural tasks (U.S. Patent Application Publication No. US20200053952A1). United States Patent and Trademark Office. https://patents.google.com/patent/US20200053952A1/en
13. Block chain-based agricultural production information tracing method. (2023). Chinese Patent Application Publication No. CN115879961A. China National Intellectual Property Administration. https://patents.google.com/patent/CN115879961A/en
14. Bliss, E. (2023). Generating verifiable agricultural data (U.S. Patent Application Publication No. US20230084892A1). United States Patent and Trademark Office. https://patents.google.com/patent/US20230084892A1/en
15. Work information sharing platform based on block chain. (2024). Chinese Patent No. CN118172029B. China National Intellectual Property Administration. https://patents.google.com/patent/CN118172029B/en
16. Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. World Journal of Advanced Engineering Technology and Sciences. https://www.rankless.org/authors/idoko-peter-idoko
17. Ijiga, A. C., Abutu, E. P., Idoko, I. P., Agbo, D. O., Harry, K. D., Ezebuka, C. I., & Umama, E. E. (2024). Ethical considerations in implementing generative AI for healthcare supply chain optimization: A cross-country analysis across India, the United Kingdom, and the United States of America. https://www.rankless.org/authors/idoko-peter-idoko
18. Ijiga, A. C., Aboi, E. J., Idoko, I. P., Enyejo, L. A., & Odeyemi, M. O. (2024). Collaborative innovations in artificial intelligence (AI): Partnering with leading U.S. tech firms to combat human trafficking. Global Journal of Engineering and Technology Advances. https://www.rankless.org/authors/idoko-peter-idoko
19. Idoko, I. P., Ijiga, O. M., Agbo, D. O., Abutu, E. P., Ezebuka, C. I., & Umama, E. E. (2024). Comparative analysis of Internet of Things (IoT) implementation: A case study of Ghana and the USA. World Journal of Advanced Engineering Technology and Sciences. https://www.rankless.org/authors/idoko-peter-idoko

20. Ayoola, V. B., James, U. U., Idoko, I. P., Ijiga, O. M., & Olola, T. M. (2024). Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. Global Journal of Engineering and Technology Advances, 20(3), 94–117. https://doi.org/10.30574/gjeta.2024.20.3.0164
21. Uzoma, E., Idoko, I. P., & Enyejo, L. A. (2024). Evaluating serverless computing and microservices impact on scalable cloud-native applications and blockchain interoperability frameworks. International Journal of Scientific Research and Modern Technology, 3(4), 14–17. https://doi.org/10.38124/ijsrmt.v3i4.407
22. Idoko, I. P., Tiamiyu, D., Ugochukwu, U. N., & During, A. D. (2024). Advanced data analytics and machine learning driven fraud detection and data loss prevention for automated incident response in the US healthcare corporations. International Journal of Scientific Research and Modern Technology, 3(11). https://doi.org/10.38124/ijsrmt.v3i11.111
23. Michael, C. I., Campbell, T.-A., Idoko, I. P., Bemologi, O. U., Peter-Anyebe, A., & Odeh, I. I. (2024). Enhancing cybersecurity protocols in financial networks through reinforcement learning. International Journal of Scientific Research and Modern Technology, 3(9). https://doi.org/10.38124/ijsrmt.v3i9.58
24. Somuah, J., Idoko, I. P., & Ayoola, V. B. (2024). Condition assessment of civil/structural assets in gas stations: Integrating non-destructive testing with code-conformance audits. International Journal of Scientific Research and Modern Technology, 3(3). https://doi.org/10.38124/ijsrmt.v3i3.922
25. Ayoola, V. B., Idoko, I. P., Eromonsei, S. O., Afolabi, O. T., Apampa, A. R., & Oyebanji, O. S. (2024). The role of big data and AI in enhancing biodiversity conservation and resource management in the USA. World Journal of Advanced Research and Reviews. https://www.rankless.org/authors/idoko-peter-idoko
26. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of EuroSys. https://doi.org/10.1145/3190508.3190538
27. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55–81. https://doi.org/10.1016/j.tele.2018.11.006
28. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261
29. Queiroz, M. M., & Wamba, S. F. (2019). Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. International Journal of Information Management, 46, 70–82. https://doi.org/10.1016/j.ijinfomgt.2018.11.021
30. Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. Proceedings of the Conference on Fairness, Accountability, and Transparency, 33–44. https://doi.org/10.1145/3351095.3372873
31. Strogatz, S. H. (2015). Nonlinear dynamics and chaos: With applications to physics, biology, chemistry, and engineering (2nd ed.). Westview Press.
32. Kuznetsov, Y. A. (2004). Elements of applied bifurcation theory (3rd ed.). Springer.

33. International Labour Organization. (2014). Profits and poverty: The economics of forced labour. International Labour Office. https://www.ilo.org/
34. International Labour Organization, Walk Free, & International Organization for Migration. (2022). Global estimates of modern slavery: Forced labour and forced marriage. International Labour Organization. https://www.ilo.org/
35. United Nations Office on Drugs and Crime. (2022). Global report on trafficking in persons 2022. United Nations. https://www.unodc.org/
36. Organisation for Economic Co-operation and Development. (2018). OECD due diligence guidance for responsible business conduct. OECD Publishing. https://doi.org/10.1787/15f5f4b3-en
37. National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). https://doi.org/10.6028/NIST.AI.100-1
38. National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
39. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements. ISO. https://www.iso.org/standard/27001
40. International Organization for Standardization. (2023). ISO/IEC 42001:2023 Information technology—Artificial intelligence—Management system. ISO. https://www.iso.org/standard/81230.html
41. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj
42. Food and Agriculture Organization of the United Nations. (2022). The state of food and agriculture 2022: Leveraging automation in agriculture for transforming agrifood systems. FAO. https://doi.org/10.4060/cb9479en
43. World Economic Forum. (2019). Inclusive deployment of blockchain for supply chains: Part 1—Introduction. World Economic Forum. https://www.weforum.org/
44. United Nations. (2011). Guiding principles on business and human rights: Implementing the United Nations “Protect, Respect and Remedy” framework. United Nations Human Rights Office. https://www.ohchr.org/
45. National Institute of Standards and Technology. (2017). Digital identity guidelines: Authentication and lifecycle management (NIST SP 800-63B). https://doi.org/10.6028/NIST.SP.800-63b