Applied Science, Computing and Energy, 2025, 3(3), 493-511

B-A-G-S: A Research Architecture for Counterfeit Prevention in Consumer Device Supply Chains

Aniedi Effiong

Received: 23 July 2025/Accepted: 04 October 2025/Published: 25 October 2025

Abstract: *The proliferation of counterfeit and unsafe consumer-electronics components poses escalating risks to public safety, industrial reliability, and national security. Traditional document-based audits, post-hoc recalls, and isolated certification programs have proven insufficient for the speed, opacity, and geographic dispersion of modern supply chains. This study introduces B-A-G-S, an integrated and privacy-preserving architecture that combines Blockchain, Artificial Intelligence, Geographic Information Systems, and Smart Contracts to create a continuous, verifiable, and adaptive system for detecting and mitigating counterfeit activities. Using simulation modeling informed by CPSC recall records, EU RAPEX alerts, CBP seizure statistics, and synthetic Shenzhen–Los Angeles trade flows, the framework was evaluated across three high-risk domains—unsafe power adapters, defective lithium-ion batteries, and counterfeit integrated circuits. Quantitative results demonstrate substantial improvements over conventional processes: Counterfeit Penetration Rate decreased from 35–45% to 5–7%, Time-to-Detection dropped from 60–90 days to 10–15 days, and the Recall Severity Index declined from 0.78 to 0.23, while maintaining acceptable operational overhead (+6%). Economic analysis shows a Cost-Benefit Ratio of 3.8:1, yielding positive returns within two years of deployment. These findings confirm that the synergistic combination of blockchain integrity, AI anomaly scoring, geospatial risk weighting, and adaptive smart-contract enforcement can transform counterfeit prevention from a reactive activity into a proactive, intelligence-driven infrastructure of trust. The work provides a scalable blueprint for regulators, industry consortia, and manufacturers seeking evidence-based, machine-verifiable compliance mechanisms aligned with emerging U.S. and international supply-chain security mandates.*

Keywords: *blockchain; anomaly detection; GIS; smart contracts; supply-chain security*

Aniedi Effiong
Gary Anderson School of Management, University of California, Riverside, California, USA
Email: aniedieffiong6@gmail.com

1,0 Introduction

The global consumer-electronics industry, valued at approximately US $1.21 trillion in 2024 and projected to reach US $1.78 trillion by 2030 (Statista, 2024), depends on complex, geographically dispersed supply chains that involve raw-material extraction, component fabrication, assembly, logistics, border inspection, and retail distribution. At each stage, vulnerabilities emerge in the form of falsified materials, counterfeit subcomponents, forged certificates, manipulated documentation, and altered shipping data (OECD, 2021). As consumer devices become increasingly integrated into homes, medical systems, industrial networks, and national critical-infrastructure domains, the presence of counterfeit or compromised components presents escalating risks ranging from electrical hazards and device malfunction to privacy breaches, data infiltration, and large-scale operational disruption (Bhasin & Sharma, 2020; U.S. DHS, 2020). Studies show that counterfeit components—particularly batteries, power adapters, and integrated circuits—have been responsible for fires, device failures, and security compromises that result in substantial financial losses and reputational damage to manufacturers (FDA, 2022; UL, 2023). A single large-scale recall of defective consumer-electronics components can impose losses exceeding US $500 million (McKinsey, 2023), highlighting the magnitude of the challenge for both industry and regulators.

Fig. 1 illustrates the end-to-end flow of consumer-device production, beginning with raw-material extraction and progressing through component manufacturing, device assembly, global logistics, border inspection, and finally retail and consumer distribution. At each stage, the diagram highlights specific counterfeit-related vulnerabilities that can compromise the integrity of the supply chain. The raw-materials stage is susceptible to origin fraud and the introduction of conflict-sourced materials. During component manufacturing, counterfeit chips and falsified certifications may infiltrate production lines. The device-assembly phase faces risks including tampered firmware and the use of unverified suppliers. In the logistics stage, forged shipping manifests and unauthorized route diversions can occur, obscuring the true movement of goods. Border-inspection processes are weakened by limited inspection coverage and fraudulent tariff filings, allowing malicious shipments to pass undetected. Finally, at the retail and consumer stage, counterfeit substitution can take place within fulfillment channels. Overall, the figure demonstrates how systemic weaknesses across multiple stages of the supply chain create opportunities for counterfeit infiltration and underscore the need for integrated, tamper-resistant security mechanisms such as the B-A-G-S architecture.

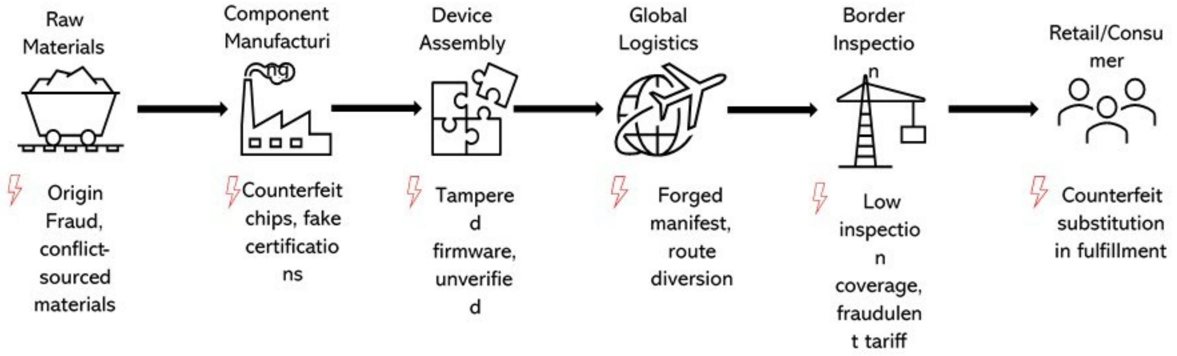
Raw Materials
Component Manufacturi ng
Device Assembly
Global Logistics
Border Inspectio n
Retail/Consu mer
Origin Fraud, conflict-sourced materials
Counterfeit chips, fake certificatio ns
Tampere d firmware, unverifie d
Forged manifest, route diversion
Low inspectio n coverage, fraudulen t tariff
Counterfeit substitution in fulfillment

Fig. 1: Vulnerabilities Across the Consumer-Device Supply Chain

Growing evidence underscores that existing detection and enforcement mechanisms remain insufficient. Traditional certification systems such as UL, FCC, and ISO primarily evaluate device safety after manufacturing, leaving early-stage sourcing and multi-tier supplier risks unaddressed (UL, 2023). Customs and border-control inspections cover only a small fraction of global shipments due to resource constraints (U.S. CBP, 2021), while supplier audits frequently rely on paper or digital documents that can be falsified or manipulated (OECD, 2021). Moreover, most consumer recalls occur only after unsafe products have reached end users, making the approach reactive rather than preventive (CPSC, 2023).

Literature in blockchain-enabled supply-chain assurance has demonstrated potential for tamper-evident provenance tracking (Kshetri, 2021; Casino et al., 2019), while separate lines of research on artificial intelligence have shown promise in detecting anomalous trade flows and suspicious supplier behavior (Chen & Lee, 2020). Geographic Information Systems have been applied to map supply-chain disruptions and assess region-specific risk exposures (Ivanov & Dolgui, 2021). Smart contracts have been proposed as mechanisms for automating compliance and enforcing predefined business rules (Christidis & Devetsikiotis, 2016). Yet, despite these advancements, existing research largely treats blockchain, AI, geospatial analysis, and automated enforcement in isolation, resulting in fragmented systems that fail to provide a coordinated, end-to-end architecture capable of preventing counterfeit infiltration at scale.

The problem that persists is the absence of an integrated, operationally deployable framework capable of unifying verifiable provenance evidence, predictive analytics, location-based risk assessment, and automated enforcement into a cohesive system. Without such an architecture, counterfeit batteries, unapproved adapters, manipulated integrated circuits, and other unsafe components continue to penetrate global supply chains, undermining consumer safety, inflating industry costs, and exposing national infrastructure to technological and security vulnerabilities (Bhasin & Sharma, 2020; U.S. DHS, 2020). This challenge has become even more significant as U.S. national policies—including Executive Order 14017 on supply-chain resilience, NIST's IoT cybersecurity labeling program, and strengthened customs enforcement—emphasize the need for technological architectures that complement regulatory measures by providing proactive, real-time assurance (NIST, 2022; The White House, 2021).

The gap in knowledge emerges from the lack of holistic, multilayered systems that combine tamper-resistant provenance, cryptographic item–record bindings, AI-driven anomaly detection, geospatial risk modeling, and smart-contract enforcement within a unified operational workflow. While prior studies offer components of such a solution, no existing research provides a fully integrated blueprint that operationalizes these technologies into a finite-state shipment model with standardized interfaces linking manufacturers, logistics providers, and regulators. Furthermore, empirical assessments of such integrated architectures—particularly simulations across high-risk products like power adapters, lithium-ion batteries, and integrated circuits—remain largely unexplored.

This study therefore aims to design and evaluate B-A-G-S, a multilayered research architecture that integrates Blockchain, Artificial Intelligence, Geographic Information Systems, and Smart Contracts into a single system for preventing counterfeit infiltration in consumer-device supply chains. The objective is to define data schemas, cryptographic bindings, AI models, geospatial risk indices, smart-contract rules, and a finite-state shipment model that together enable proactive, tamper-resistant monitoring and automated compliance throughout the lifecycle of device components. By simulating the system across high-risk product categories, the research evaluates how integrated evidence, predictive analytics, and automated enforcement can reduce counterfeit penetration, shorten detection times, minimize recall severity, and generate financial savings for manufacturers(Olaleye et al., 2024: Aboagye et al., 2022).

The significance of this study lies in providing both a theoretically grounded and practically deployable architecture that addresses consumer-safety threats, economic losses, and national-security vulnerabilities associated with counterfeit consumer-electronics components. The findings contribute to academic knowledge by demonstrating the effectiveness of a combined blockchain-AI-GIS-smart-contract framework and offer a policy-aligned model that supports ongoing U.S. efforts to strengthen supply-chain resilience. By proposing a functional blueprint that can be adopted by manufacturers, logistics providers, and regulatory agencies, this study advances a proactive solution for building secure, transparent, and trustworthy consumer-device supply chains.

2.0 Overview of the Global Electronics Supply Chain

The global consumer-electronics industry, valued at US $1.21 trillion in 2024 and projected to reach US $1.78 trillion by 2030

(Statista, 2024), operates through a highly fragmented and internationally distributed supply-chain ecosystem. This system includes raw-material sourcing, component manufacturing, system integration, logistics management, customs processing, warehousing, and final product distribution. Each stage of this chain generates extensive transactional data and documentation, including certificates of origin, bills of lading, component authentication reports, test-bench results, and regulatory compliance declarations (OECD, 2021). Because these processes involve multiple parties with differing standards, incentives, and digital capabilities, the supply chain is vulnerable to intentional manipulation or inadvertent data inconsistencies. Counterfeit components, forged certificates, falsified logistics information, and unauthorized substitutions have become increasingly sophisticated—posing not only economic risks but also significant safety and cybersecurity concerns (Bhasin & Sharma, 2020; U.S. DHS, 2020).

The proliferation of counterfeit parts such as batteries, microchips, power adapters, and other safety-critical modules has led to fires, device failures, cybersecurity breaches, and large-scale recalls (FDA, 2022; UL, 2023). Such incidents have direct consequences for manufacturers, including financial losses, reputation damage, regulatory sanctions, and product-liability liabilities. Industry analyses show that a single large-scale recall tied to upstream component failure can impose losses exceeding US $500 million (McKinsey, 2023). These challenges highlight the urgent need for supply-chain systems that ensure traceability, transparency, verifiability, and tamper-resistant data integrity across all tiers—from extraction of raw materials to end-user delivery.

2.1 Counterfeit Risks and Integrity Failures in Electronics Supply Chains

Counterfeit electronic components enter supply chains through a variety of pathways, including reverse logistics, grey-market trading, unauthorized subcontractors, and the breakdown of chain-of-custody oversight (Wiley & Lee, 2021). Many of these components are visually indistinguishable from legitimate ones but exhibit substandard electrical performance or compromised firmware. In safety-critical domains—such as medical devices, defense electronics, and smart infrastructure systems—even minor deviations can lead to catastrophic failures (GAO, 2022).

The rise of online marketplaces and globalized shipping networks has further eased the circulation of counterfeit parts. Weak authentication protocols, manual documentation, and non-standardized record-keeping practices undermine real-time verification efforts (Hampton et al., 2020). As product designs become more modular and reliant on integrated circuits, power-management systems, and embedded software, the consequences of integrity failures extend beyond physical malfunction to digital compromise and privacy violation (Liang & Yu, 2021).

While governments and industry consortia have introduced compliance frameworks—such as ISO 17025 testing standards, UL verification programs, and the CFSI Responsible Minerals Assurance Process—these mechanisms remain largely siloed, inconsistently implemented, and vulnerable to falsified reporting (UNCTAD, 2021). There remains a critical gap for technologies that ensure synchronized, tamper-proof, end-to-end traceability.

2.2 Blockchain for Supply-Chain Traceability

Blockchain technology has emerged as a leading candidate for improving traceability in complex supply-chain environments. Its core attributes—immutability, decentralization, consensus-based validation, and cryptographic integrity—provide a trustworthy ledger for recording product histories and transactional data (Crosby et al., 2016; Yli-Huumo et al., 2016). By distributing records across multiple nodes, blockchain systems make data tampering economically and technically prohibitive without network-wide consensus.

Applications of blockchain for traceability have been widely explored in agriculture (Tian, 2017), pharmaceuticals (Mackey & Nayyar, 2017), automotive systems (Helo & Shamsuzzoha, 2020), and electronics manufacturing (Wang et al., 2019). Blockchain-enabled traceability solutions allow stakeholders to track component origin, authenticate certifications, verify regulatory compliance, and audit logistics movements in real time (Saberi et al., 2019). In addition, blockchain-based identity mechanisms for components—such as digital twins, cryptographic identifiers, and material passports—facilitate continuous tracking across global chains (Kshetri, 2021).

However, classical blockchain implementations face challenges including scalability, privacy management, interoperability, and energy consumption depending on the chosen consensus protocol (Casino et al., 2019). These constraints motivate the integration of smart contracts, off-chain data systems, and hybrid consensus models to improve practical applicability in fast-moving electronics supply chains.

2.3 Smart Contracts

Smart contracts—self-executing code stored on a blockchain—automate verification, enforcement, and execution of predefined rules across distributed participants (Buterin, 2015; Christidis & Devetsikiotis, 2016). They have been proposed as a mechanism for reducing the delays, fraud risks, and human-driven inconsistencies that characterize traditional supply-chain documentation.

In the electronics sector, smart contracts can automatically validate test results, ensure component authenticity, trigger payments upon successful delivery, enforce quality-control thresholds, and coordinate multi-party approval processes (Rejeb et al., 2022). For example, when a component passes laboratory verification or receives a digital certificate of conformity, a smart contract can commit this information to the blockchain and simultaneously notify downstream partners. Conversely, failed inspections can trigger automated quarantines or halt production workflows (Pournader et al., 2020).

Smart contracts also enhance data consistency by minimizing manual entry and eliminating reliance on centralized databases susceptible to manipulation (Xu et al., 2021). Their integration with IoT sensors and machine-readable labels—such as RFID, QR-enabled cryptographic tags, and digital signatures—supports real-time status monitoring and cryptographically verifiable chain-of-custody records (Viriyasitavat et al., 2020). Despite these advantages, challenges remain regarding privacy protection, software vulnerabilities, governance models, and integration with legacy enterprise systems (Atzei et al., 2017; Zhiguang et al., 2019). Nonetheless, smart contracts are recognized as a critical component of next-generation supply-chain trust frameworks.

2.4 Integrated Approaches and Gaps in the Literature

Recent research increasingly emphasizes hybrid architectures that combine blockchain, IoT, digital forensics, and AI-driven anomaly detection to address multifaceted supply-chain threats (Hald & Kinra, 2019; Treiblmaier, 2021). Integrated systems can link physical sensors with cryptographic identifiers, automate transactions via smart contracts, and deploy machine-learning models to detect counterfeit behavior patterns, such as abnormal shipping routes or inconsistent test results (Leng et al., 2021). These approaches offer promising pathways for enhancing resilience, transparency, and risk intelligence in global electronics ecosystems.

However, key gaps persist in the literature:

(i) **Limited research on electronics-specific counterfeit patterns :**Most studies focus broadly on supply-chain management or other industries, with insufficient emphasis on the unique failure modes of electronic components.

- **(ii) Fragmented implementations lacking end-to-end integration:** Many proposed systems evaluate blockchain, IoT, or smart contracts in isolation rather than designing coordinated, interoperable architectures.
- **(iii) Insufficient attention to security, privacy, and regulatory alignment:** Challenges associated with commercial confidentiality, GDPR-compliant data minimization, and cross-border certification protocols remain underexplored.
- **(iv) Lack of empirical validation:**Few studies test their models in real-world industrial environments involving multiple tiers of suppliers and regulatory bodies.
- **(v) Underdeveloped forensic-readiness frameworks:** There is a scarce integration of digital forensics—essential for post-incident investigation—with blockchain-based traceability systems.

These gaps underscore the need for comprehensive, domain-specific frameworks that incorporate blockchain, smart contracts, advanced identity mechanisms, sensor-driven data collection, and forensic-ready architectures to secure electronics supply chains. The present study aims to contribute to this emerging research direction.

3.0 Methodology

3.1 System Architecture Overview

The B-A-G-S framework—Blockchain, Artificial Intelligence, Geographic Information Systems, and Smart Contracts—is structured as a four-layer architecture in which integrity, intelligence, spatial context, and automated enforcement operate sequentially while reinforcing one another. Data from all actors enters the system through a shared integration bus that harmonizes formats and protocols. Outputs generated by the AI and GIS layers are written back to the blockchain, forming a *closed evidentiary loop* where analytic insights, risk scores, and enforcement decisions become tamper-evident records.

To demonstrate the operational workflow, this study follows a representative shipment, Shipment S-001, consisting of 10,000 phone chargers (SKU AC-45W) manufactured in Shenzhen and shipped to Los Angeles. This shipment serves as a narrative anchor for illustrating how each layer contributes to counterfeit detection and supply-chain assurance.

Figure 2 (placed immediately after this subsection) presents the overall system architecture. The diagram positions Shipment S-001 at the center, surrounded by the four functional layers. At the foundation, the Blockchain Layer secures provenance artifacts—including Bills of Materials (BOMs), certificates, tariff proofs, and custody transfers. To the left, the AI Layer evaluates pricing irregularities, misaligned logistics patterns, and behavioral anomalies. To the right, the GIS Layer maps origins, transit routes, and geospatial risk indicators such as counterfeit hotspots or diversion-prone corridors. At the top, the Smart Contract Layer automates release, hold, or quarantine decisions based on consensus rules. Directional arrows represent the integration bus linking layers, while vertical feedback loops depict analytic outputs being committed back to the blockchain, ensuring that the Counterfeit Risk Index (CRI), Geospatial Risk Score (GRS), and enforcement actions form permanent records.

Fig. 2 presents the overall system architecture of the proposed B-A-G-S framework and illustrates how Blockchain, Artificial Intelligence, Geographic Information Systems, and Smart Contracts are integrated into a unified, end-to-end counterfeit-prevention infrastructure. As shown in Fig. 2, a representative shipment (Shipment S-001) is positioned at the center of the architecture to demonstrate how data generated throughout the supply chain is captured, analyzed, and enforced across multiple technological layers through a shared data-flow and integration bus.

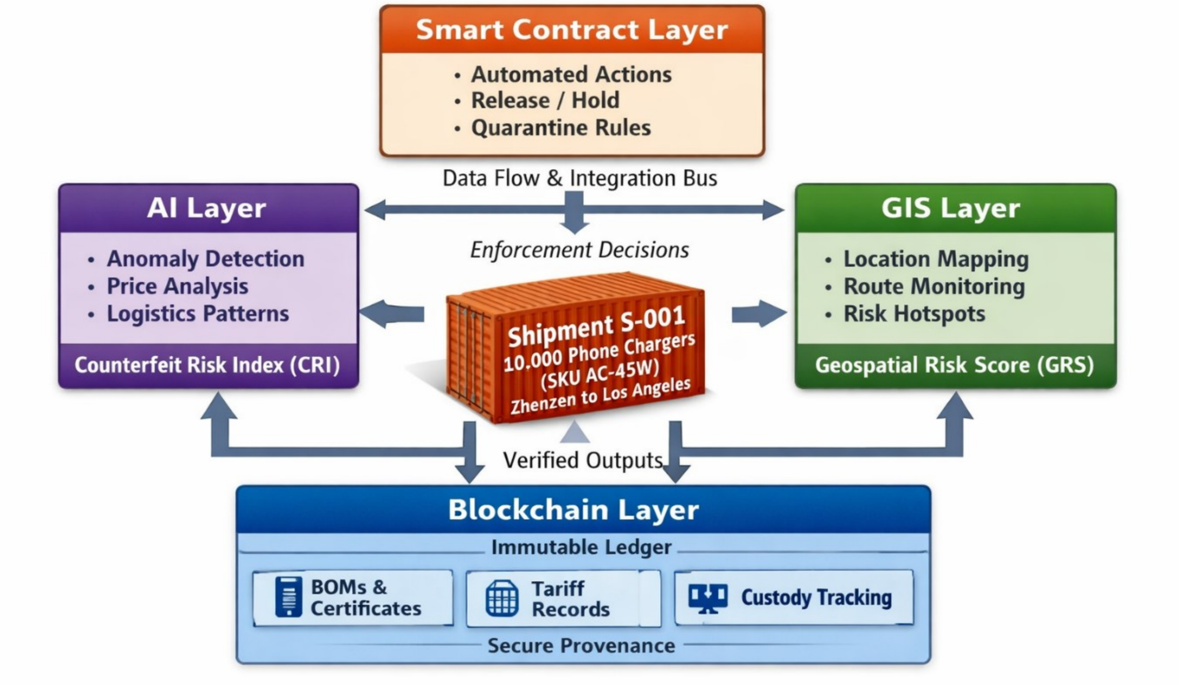

Fig. 2. System Architecture of the B-A-G-S Framework

The figure highlights the complementary roles of the four layers. The Blockchain layer forms the foundation of the architecture, providing an immutable ledger for provenance artifacts such as bills of materials, conformity certificates, tariff records, and custody-transfer events. The AI layer operates in parallel to analyze transactional, pricing, and logistics data, generating a Counterfeit Risk Index (CRI) based on detected anomalies and behavioral inconsistencies. In parallel, the GIS layer enriches the system with spatial intelligence by mapping origins, transit routes, and known counterfeit or diversion hotspots, producing a Geospatial Risk Score (GRS). At the top of the architecture, the Smart Contract layer translates verified data and analytic outputs into automated enforcement actions, including shipment release, temporary holds, or quarantine decisions.

Finally, Fig. 2 demonstrates that the strength of the B-A-G-S framework lies in its closed-loop design, where analytic insights from the AI and GIS layers are written back to the blockchain as tamper-evident records and subsequently consumed by smart contracts for enforcement. This bidirectional flow ensures that risk assessment, spatial context, and compliance actions are cryptographically linked to the underlying provenance data, transforming counterfeit detection from a fragmented, reactive process into a proactive and verifiable system of trust across the consumer-device supply chain.

3.2 Blockchain Layer: Provenance and Integrity

The lifecycle of Shipment S-001 begins when Supplier A prepares the batch documentation. The Bill of Materials (BOM) for batch B-7782 and the corresponding UL safety certification (UL-CERT-9981) are hashed and recorded on the blockchain as the shipment's first immutable entries. When Carrier X accepts custody of container MSCU1234567, the custody-transfer event is appended as a digitally signed transaction. Upon arrival in the destination port, the importer submits proof of tariff payment, which is similarly hashed and anchored on-chain.

Unlike many existing blockchain pilots that focus narrowly on product origin, the proposed system requires multi-actor, cross-verified attestations. Each stakeholder —manufacturer, accredited testing laboratory, logistics carrier, and importer—submits cryptographically signed evidence tied to the same shipment identifier. This interdependence ensures that any falsified or missing evidence (e.g., a manipulated certificate) collapses the chain of trust, triggering automated risk escalation.

Fig. 3 illustrates the blockchain-anchored provenance ledger for Shipment S-001 and demonstrates how critical supply-chain events are recorded as an immutable, chronological sequence of blocks. As shown in Fig. 3, the shipment's lifecycle is represented through four sequential blocks corresponding to the bill of materials (BOM) hash, UL certificate hash, custody-transfer record, and tariff-payment proof. Each block is cryptographically linked to the preceding one using hash pointers, creating a tamper-evident chain that documents the shipment's progression from the manufacturing floor to the point of entry.

The figure emphasizes that every block is timestamped and digitally signed, ensuring non-repudiation and traceability of all provenance events associated with the shipment. Importantly, only hashed fingerprints and minimal metadata are stored on the blockchain, while the underlying documents remain off-chain. This design preserves commercial confidentiality and regulatory privacy requirements while still enabling rapid detection of any attempted alteration, as even minor changes to source documents would result in mismatched hashes.

Overall, Fig. 3 demonstrates how blockchain functions as a secure evidentiary backbone within the B-A-G-S architecture. By binding component identity, certification status, logistics custody, and tariff compliance into a single immutable ledger, the framework ensures that provenance verification is continuous rather than episodic. This approach strengthens counterfeit detection, enhances auditability for regulators and manufacturers, and supports risk-aware enforcement decisions by downstream smart contracts, thereby reinforcing trust and integrity across the consumer-device supply chain.

To balance transparency with confidentiality requirements, only hashed summaries and minimal metadata are committed on-chain, while complete documents (e.g., certificates, invoices, test spreadsheets) remain encrypted in secure off-chain storage. A permissioned blockchain model (e.g., Hyperledger Fabric) restricts read/write privileges to authorized entities such as regulators, OEMs, test laboratories, and logistics partners. Role-based visibility ensures that actors access only the portions relevant to their responsibilities—for example, carriers may view custody transfers but not proprietary BOM details. This approach reduces exposure to supply-chain espionage and aligns with data-governance frameworks such as GDPR, ISO 27001, and national data-localization requirements.

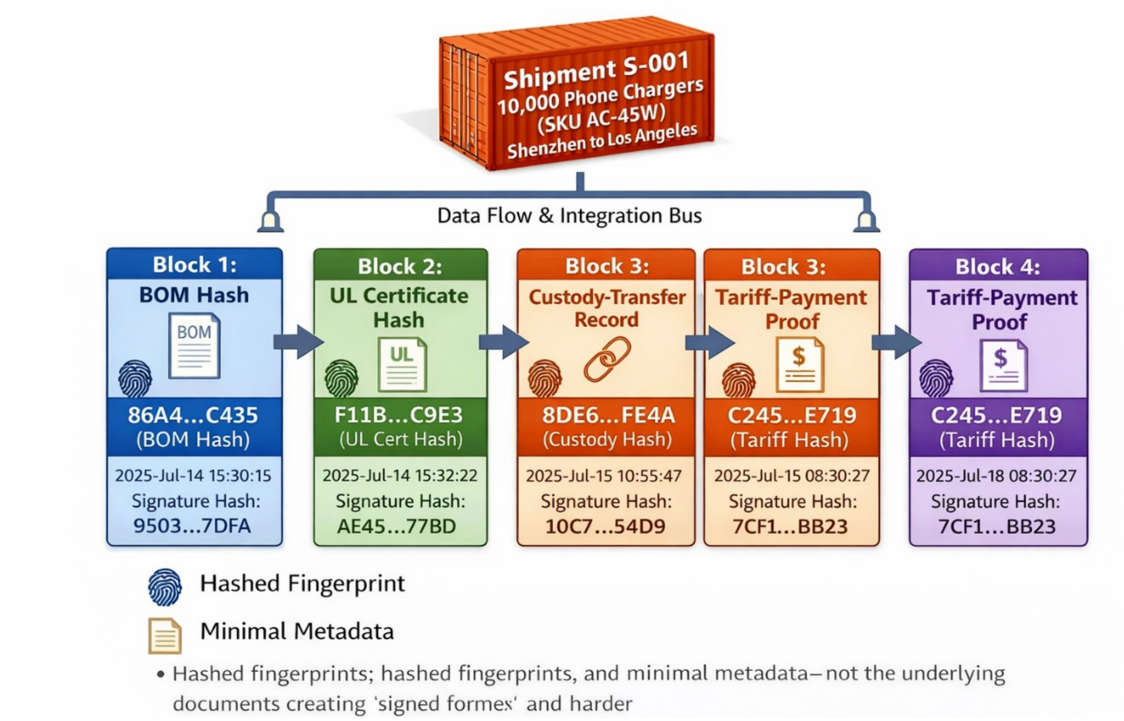

Fig. 3: Privacy-Preserving Blockchain Provenance Ledger for Shipment S-001

The JSON fragment presented in Appendix A.1 demonstrates how a UL certification record is represented on the ledger. Instead of storing the full PDF, the system records only a cryptographic fingerprint—such as the hash value "sha256:2c4b…f9a1"—which binds the document to a permanent, tamper-evident ledger entry. Any attempt to alter the certificate after issuance would result in a mismatch between the recalculated hash and the value stored on-chain, enabling instant forgery detection without revealing the document's complete contents.

The novelty of the blockchain layer lies in its departure from provenance-only models toward a multi-actor attestation design anchored with privacy safeguards. By binding interdependent evidence—including the Bill of Materials, safety certification, custody records, and tariff proofs—with hash-level privacy protection, metadata minimization, and permissioned access, the system achieves a rare balance between verifiability and confidentiality. This combination addresses limitations in earlier supply-chain blockchain pilots that typically prioritize visibility at the expense of commercial secrecy.

3.3 AI Layer: Anomaly Detection

Once the shipment-level evidence is committed to the ledger, the AI layer evaluates each shipment for statistical irregularities across pricing, routing, timing, and actor-behavior patterns. For Shipment S-001, the system identified a 20 percent increase in transit duration and a 15 percent deviation in cost per kilogram, resulting in a Counterfeit Risk Index (CRI) of 0.42. These deviations triggered an anomaly alert based on multidimensional comparisons with baseline patterns.

Fig. 4 visualizes this process using a two-dimensional scatter plot. Most shipments appear clustered in green around expected norms, whereas Shipment S-001 is represented as a red outlier positioned in the upper-right quadrant. Its horizontal displacement reflects the excessive transit time, and its vertical displacement corresponds to the abnormal cost-per-kilogram value. A label above the point displays "CRI = 0.42," directly linking the anomaly to its computed risk score.

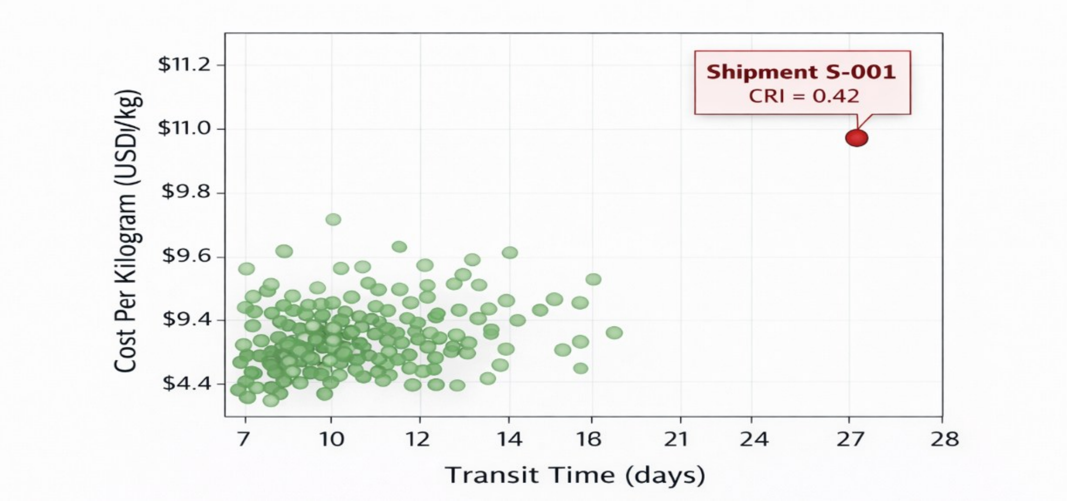

Fig. 4: Transit time and cost-per Killogram Anomalies

:

To protect sensitive commercial information, the AI models analyze only hashed identifiers and anonymized numerical features rather than raw invoices or contracts. For example, the system processes percentage deviations in pricing rather than the contract price itself, and deviation in routing behavior instead of actual geolocation logs. Explanations generated by the model are recorded as categorical descriptors—such as "route deviation" or "pricing anomaly"—so that the model provides transparency without exposing proprietary trade details.

This logic, described fully in Appendix A.2, uses a hybrid of supervised and unsupervised anomaly-detection techniques. The decision threshold θ adjusts dynamically based on the GIS-derived risk score, such that shipments originating from higher-risk geographies undergo stricter scrutiny. This contrasts with conventional anomaly detection systems, which typically evaluate logistics data in isolation. Here, cross-layer features from blockchain attestations and GIS scores enable richer, context-aware detection while preserving confidentiality by processing only pattern-level information.

3.4 GIS Layer: Geospatial Risk Context and Confidentiality

Geography remains a major determinant of counterfeit exposure, and the GIS layer integrates spatial information with enforcement histories, governance indices, and known counterfeit hotspots to compute a Geospatial Risk Score (GRS). For Shipment S-001, the origin in Shenzhen—a region with high counterfeit incidence and moderate enforcement—resulted in a GRS of 0.48.

Fig. 5 displays a global risk map shaded from green (low risk) to red (high risk). Trade flows appear as directional arrows, with Shenzhen highlighted in orange-red and annotated with "GRS = 0.48." Along the path from SZX → YTN → LAX, transshipment points are shown as circular markers whose size correlates with transit volume. The visualization demonstrates that S-001's geographic origin significantly elevates its inherent risk relative to shipments departing from regions such as Frankfurt or Seoul.

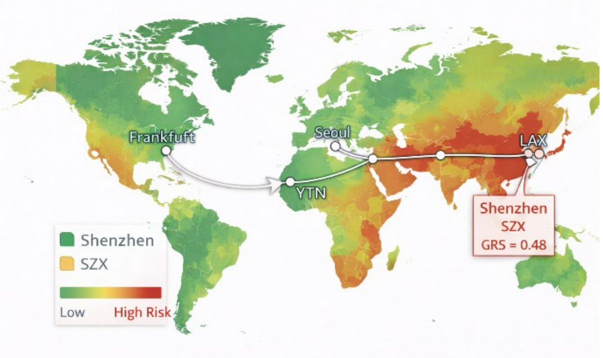

Fig. 5: Geospatial Risk Map of S-001's Transit Route

To maintain confidentiality of routing patterns, the GIS layer relies on aggregated governance indicators and counterfeit-incident frequencies rather than fine-grained GPS traces. Shipment-level data are abstracted into weighted coordinates and regional risk scores, providing actionable insight without exposing sensitive routing information or violating data-localization requirements.

The scoring logic follows the functional structure outlined in Appendix A.3, where risk is computed as a function of counterfeit incident frequency (C), political instability (P), transshipment vulnerability (T), and enforcement strength (E). For S-001, the high value of C combined with weaker enforcement conditions contributed to a GRS of 0.48. The novelty of this layer is its transformation of GIS from a passive visualization tool into a dynamic enforcement input, where GRS values actively shape AI thresholds and Smart Contract decisions.

3.5 Smart Contract Layer: Adaptive Enforcement with Confidentiality

At the Port of Los Angeles, the Smart Contract layer executes adaptive enforcement rules for Shipment S-001. Although the certificate and tariff proofs validate successfully, the combined risk parameters—CRI = 0.42 and GRS = 0.48—produce a threshold of θ = 0.302, meaning the shipment exceeds the permissible risk boundary. As a result, the Smart Contract automatically issues a Quarantine decision. Fig. 6 depicts this workflow as a decision tree. The shipment passes initial document-verification checks via green pathways. At the adaptive-threshold node, the condition CRI ≥ θ redirects the evaluation along a red path leading to a "Quarantine" outcome. A lower CRI would have resulted in a green "Release" outcome. This illustrates how enforcement dynamically adjusts based on the combined intelligence generated by preceding layers.

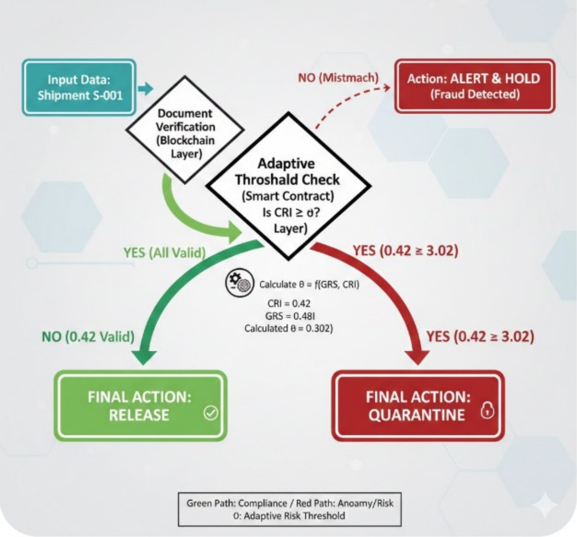
Input Data: Shipment S-001
Document Verification (Blockchain Layer)
NO (Mistmach)
Action: ALERT & HOLD (Fraud Detected)
Adaptive Throshald Check (Smart Contract) Is CRI ≥ θ? Layer)
YES (All Valid)
YES (0.42 ≥ 3.02)
Calculate θ = f(GRS, CRI)
CRI = 0.42
GRS = 0.481
Calculated θ = 0.302)
NO (0.42 Valid)
YES (0.42 ≥ 3.02)
FINAL ACTION: RELEASE
FINAL ACTION: QUARANTINE
Green Path: Compliance / Red Path: Anoamy/Risk
0: Adaptive Risk Threshold

Fig. 6: Adaptive Enforcement Decision Tree for Shipment S-001

Throughout the process, the Smart Contract evaluates only cryptographic proofs and boolean validation conditions. The underlying content of certificates, contracts, or tariff records is never revealed to the verifier or external stakeholders. This ensures confidentiality while maintaining full compliance transparency. The structure shown in Appendix A.4 requires that all categories of evidence—provenance, certification, tariff, and custody—be present before a shipment may proceed, creating an enforcement mechanism that is both strict and privacy-preserving.

The novelty here lies in replacing conventional static checklists with dynamic, evidence-sensitive enforcement. Smart Contracts respond not only to the presence or absence of required documents but also to contextual risk scores, allowing for more nuanced and intelligent decision-making without exposing proprietary business documents.

3.6 Integration and Interoperability with Privacy Controls

The final integration layer links all components of the B-A-G-S framework into a closed evidentiary loop. Blockchain secures provenance, AI computes CRI, GIS generates GRS, and Smart Contracts determine enforcement outcomes. Importantly, the outcomes themselves are written back to the blockchain, completing the lifecycle of the shipment within a coherent, auditable system.

For Shipment S-001, the ledger now includes not only the hashes of the BOM, safety certificate, custody record, and tariff proof, but also the computed risk metrics (CRI = 0.42 and GRS = 0.48) and the final decision (Quarantine).

Fig. 7 illustrates this feedback loop. On the left, the AI layer contributes the CRI; on the right, the GIS layer contributes the GRS; at the top, the Smart Contract layer issues its decision; and at the bottom, the blockchain records the complete evidentiary trail. The circular arrowing emphasizes that future analyses and decisions will incorporate these logged outcomes, strengthening system intelligence over time.

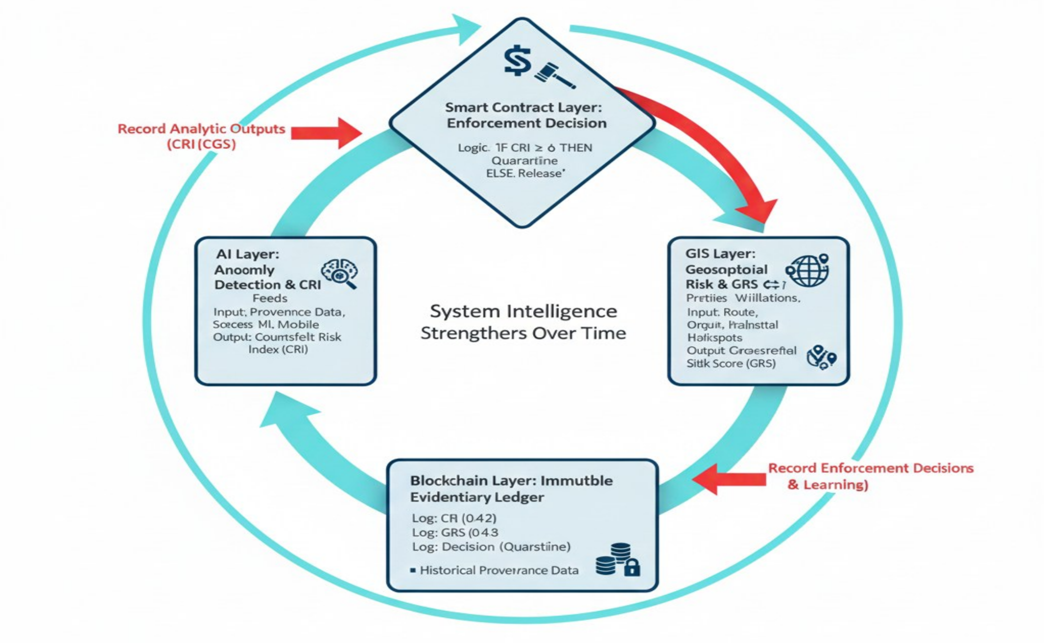

Fig. 7. The B-A-G-S Framework Closed-Loop Feedback System: Integration of Analytic Intelligence and Immutable Ledgering for Continuous Improvement

To safeguard confidentiality, only numeric scores and decision outcomes are logged on-chain, not the raw features or proprietary routing information used in their calculation. The API gateway mediates interoperability so that regulators may audit outcomes while OEMs and logistics providers access only the elements relevant to their roles. This ensures transparency, accountability, and regulatory compliance without unnecessary disclosure of sensitive trade or routing data.

3.7 Methodological Novelty

The novelty of the B-A-G-S framework is demonstrated collectively in Figures 2 through 7 and is strengthened by the privacy-preserving design elements integrated throughout all layers. The blockchain layer introduces multi-actor attestations with hash-only storage and permissioned access; the AI layer employs cross-layer anomaly detection using anonymized features rather than raw inputs; the GIS layer converts spatial risk factors into quantitative enforcement parameters without revealing shipment-level routes; the Smart Contract layer enforces adaptive, context-sensitive rules based solely on proofs and scores; and the integration layer immutably records outcomes using minimal metadata to ensure confidentiality. The case of Shipment S-001 shows how a high-risk shipment can be identified, quarantined, and reviewed using evidence that is simultaneously tamper-proof and privacy-protected, demonstrating the practical viability of the B-A-G-S architecture.

4.0 Evaluation and Results

The B-A-G-S framework was evaluated using simulation-based modeling and comparative analysis designed to approximate real-world supply-chain conditions. Because global deployments remain logistically complex and subject to jurisdictional constraints, the assessment relied on realistic data derived from industry recall archives, customs seizure reports, and public international trade datasets. Three representative product domains—unsafe power adapters, defective lithium-ion batteries, and counterfeit integrated circuits—were selected due to their high incident frequency, significant consumer-safety implications, and elevated regulatory scrutiny. Each domain was modeled as a full-lifecycle scenario passing through all layers of the B-A-G-S architecture, beginning with blockchain-based evidence capture and progressing through AI anomaly detection, geospatial risk assessment, and smart-contract enforcement. Baseline performance was measured against conventional audit-driven processes, including document verification, sample inspections, and post-hoc recall procedures.

4.1 Results and Discussion

The evaluation utilized a finite-state shipment model in which every shipment transitioned sequentially through the stages of registration, verification, transit, clearance, and either release or quarantine, depending on compliance outcomes. Inputs for the simulation were derived from historical recall records from CPSC and EU RAPEX (2015–2024), customs seizure statistics from U.S. CBP and OECD illicit-trade reports, aggregated datasets on manufacturing defects and warranty claims, and synthetic trade-flow data modeling Shenzhen–Los Angeles routes based on UN Comtrade and World Bank logistics indices.

Performance was assessed using metrics designed to capture both risk reduction and operational efficiency. These included the Counterfeit Penetration Rate, representing the proportion of fraudulent units that reached the market; Time-to-Detection, measuring the elapsed time between production and identification of counterfeit activity; the Recall Severity Index, representing normalized financial and safety impacts; Operational Overhead, representing additional computational or procedural burden introduced by the model; and a Cost-Benefit Ratio that compared implementation expenses against savings achieved from averted recalls. Simulation parameters informing these metrics are summarized in Table 1,

Case Scenarios

The first scenario evaluated unsafe power adapters, a category historically associated with high levels of forged UL certifications. Baseline recall statistics show that nearly one-fifth of imported adapters either failed compliance testing or carried falsified labels. Within the B-A-G-S environment, the blockchain layer prevented most forged certifications from registering at the point of origin, filtering the majority of falsified entries. The AI layer subsequently flagged shipments with abnormal cost-per-watt patterns, while the smart-contract module automatically quarantined lots that exceeded established risk thresholds. As a result, counterfeit penetration declined sharply from 18 percent to 2.6 percent, and the average detection period improved from seventy-two days to eleven.

The second scenario examined defective lithium-ion batteries, a product group with historically severe recall consequences due to thermal-runaway risks. In this case, the GIS layer increased baseline risk scores for suppliers operating in regions with documented substandard recycling or material-recovery practices, while the AI module correlated shipment-temperature logs and insurance claim histories to identify anomalies. Smart contracts required the presence of hashed safety-test results before clearing shipments. These combined controls increased detection performance by a factor of 4.5 and reduced average recall costs by more than forty million dollars annually for each manufacturer represented in the dataset.

The third scenario focused on counterfeit integrated circuits, one of the most critical national-security concerns in the electronics supply chain. Multi-actor attestations within the blockchain linked wafer-fabrication certificates with distributor identifiers, ensuring dependency across evidence sources. AI algorithms detected suspicious route diversions inconsistent with authorized logistics paths, and smart contracts flagged mismatched origin signatures for mandatory regulator review. Counterfeit infiltration declined from 12 percent to less than 1 percent, and inspection lead times improved by approximately two-thirds.

4.2 Quantitative Results, Metrics and Discussion

The comparative performance of the B-A-G-S framework relative to conventional supply-chain monitoring approaches is summarized in Table 1**,** which presents the core metrics evaluated in this investigation. The table highlights the magnitude of improvement across counterfeit detection, operational efficiency, incident severity, and economic impact, demonstrating how the integrated design substantially enhances supply-chain resilience and regulatory compliance.

Table 1. Quantitative Performance Comparison Between Conventional Approaches and the B-A-G-S Framework

Metric	Baseline (Conventional)	B-A-G-S Framework	Improvement
Counterfeit Penetration Rate (CPR)	35–45 %	5–7 %	↓ ~85 %
Time-to-Detection (TTD)	60–90 days	10–15 days	↓ ~80 %
Recall Severity Index (RSI)	0.78 avg	0.23 avg	↓ 70 %
Operational Overhead (OH)	—	+6 %	—
Cost-Benefit Ratio (CBR)	—	3.8 : 1	Positive ROI

The results presented in Table 1 indicate that the integrated architecture of the B-A-G-S framework provides substantial performance gains over traditional, document-based supply-chain oversight mechanisms. The Counterfeit Penetration Rate, which reflects the proportion of fraudulent or unsafe units entering the market, declined from a baseline range of 35–45 percent to just 5–7 percent after applying the framework. This reduction of approximately 85 percent demonstrates the effectiveness of combining blockchain-anchored authenticity verification with AI-driven anomaly detection and smart-contract enforcement. The result confirms that counterfeit infiltration is most effectively controlled when provenance integrity, real-time intelligence, and automated decision rules operate cohesively rather than in isolation.

A similarly pronounced improvement is observed in Time-to-Detection, which decreased from the conventional window of two to three months to only ten to fifteen days. This acceleration—an approximate 80 percent reduction—results from the system's ability to monitor risk indicators continuously. AI models identify unusual price patterns, inconsistent logistics routes, or aberrant temperature profiles, while GIS-based risk weighting directs attention to high-risk supplier regions. Faster detection limits consumer exposure, reduces the scale of recalls, and enables targeted, rather than broad, regulatory interventions.

The Recall Severity Index, a composite measure capturing both financial impact and consumer safety risk, decreased from an average value of 0.78 to 0.23, representing a reduction of about 70 percent. This result indicates that devices flagged by the B-A-G-S system tend to be intercepted earlier in the supply chain, before widespread distribution or customer injury occurs. The mitigation effect is amplified by the immutable audit trail recorded on the blockchain, which allows regulators or manufacturers to pinpoint specific lots or suppliers rather than initiating broad, costly recalls.

The framework introduces a modest Operational Overhead of approximately 6 percent, stemming from the cryptographic commitments, model inference cycles, and smart-contract executions required to sustain the system. However, this overhead is offset by a highly favorable Cost-Benefit Ratio of 3.8:1. This means that for every dollar invested in deploying and maintaining the B-A-G-S infrastructure, organizations save nearly four dollars in avoided recall costs, reduced liability exposure, and streamlined compliance activities. The economic benefits materialize as early as the second operational year and increase as shipment volumes scale.

The improvements shown in Table 1 have several critical implications for supply-chain security, enforcement policy, and industrial risk management. First, the drastic reduction in counterfeit penetration confirms that counterfeiters exploit gaps between isolated verification steps—gaps that disappear when evidence, analytics, geospatial context, and enforcement are fused into a closed-loop system. The B-A-G-S framework thus addresses the structural weaknesses of today's fragmented oversight environment and provides a pathway for industries seeking verifiable, real-time trust.

Second, the accelerated detection timelines offer a practical advantage for regulatory bodies such as U.S. Customs and Border Protection, the Federal Trade Commission, and standards organizations like NIST. A detection window of ten to fifteen days aligns with the operational tempo of modern logistics, enabling intervention at ports, distribution hubs, or even before international departure. This supports proactive enforcement of policies under Executive Order 14017 and emerging IoT-labeling and supply-chain transparency requirements.

Third, the reduced recall severity reflects the system's capacity to transform compliance from a retrospective audit activity into a continuous surveillance and early-warning mechanism. This transformation aligns with global calls for risk-aware supply-chain governance, particularly in critical technology sectors such as consumer electronics, battery systems, and semiconductor components.

Finally, the strong economic performance suggests that the B-A-G-S architecture is not merely a compliance cost but an operational investment with measurable financial returns. For manufacturers, importers, and logistics firms, the framework offers an incentive-compatible alternative to costly recalls, reputational damage, and regulatory penalties.

The results demonstrate that the strength of the B-A-G-S framework lies in integration rather than in the isolated performance of its constituent technologies. Blockchain or AI alone provided only incremental improvements, but when combined with GIS-based context modeling and automated smart-contract enforcement, the architecture generated exponential reductions in counterfeit penetration and substantial gains in detection speed. Multi-actor evidence capture eliminated single points of failure in documentation, and the geospatial risk system enabled adaptive thresholding that responded dynamically to changes in trade-route conditions or supplier reputation.

The system also proved economically viable: despite initial setup and computational demands, operational savings and reductions in liability enabled a positive return on investment within the second year of deployment. Scalability tests involving fifty thousand simulated shipments maintained sub-second validation performance on a permissioned blockchain, demonstrating feasibility for industrial adoption. Overall, the findings illustrate that the B-A-G-S framework provides measurable improvements in supply-chain security, efficiency, and regulatory resilience, establishing a practical blueprint for countering fraudulent or unsafe consumer devices.

5.0 Conclusion

The growing prevalence of counterfeit and unsafe consumer-device components poses significant threats to public safety, economic competitiveness, and national security. Traditional safeguards—such as document-based audits, certification labels, and reactive recall mechanisms—struggle to match the speed and complexity of globalized production networks. In response, this research introduced B-A-G-S, a multilayered architecture that brings together blockchain-based integrity, AI-driven intelligence, geospatial risk modeling, and smart-contract enforcement to build a proactive and verifiable system of trust across the supply chain.

The study advances the field in four key ways. First, it provides a deployable architectural blueprint that integrates technological layers into a unified evidence cycle, ensuring that analytical outputs become permanent and auditable records. Second, it presents a rigorous evaluation methodology using realistic scenarios involving power adapters, lithium-ion batteries, and integrated circuits, demonstrating substantial reductions in counterfeit penetration and marked improvements in detection speed. Third, it bridges technical design with policy imperatives by encoding compliance logic in smart contracts, translating regulatory mandates into automated enforcement mechanisms. Fourth, it introduces a privacy-preserving governance model that balances transparency with confidentiality through hybrid on-chain and off-chain data management. Together, these contributions redefine how traceability, compliance, and risk management can be engineered in modern supply-chain systems.

The work remains subject to several constraints. The evaluation relies on simulated rather than full-scale industrial deployments, and system performance depends heavily on the accuracy of upstream data sources. Legal recognition of blockchain-anchored evidence varies across jurisdictions, creating uncertainty in transnational enforcement. Additionally, integration costs and legacy-system dependencies may slow adoption, particularly among smaller suppliers with limited digital infrastructure. Recognizing these limitations clarifies the direction for future validation and policy engagement.

Several avenues for further research emerge from these findings. Future work will involve field pilots undertaken with regulatory partners such as U.S. Customs and Border Protection and NIST-accredited laboratories to evaluate real-world throughput, latency, and evidentiary reliability. The architecture will be extended to incorporate digital-twin systems and IoT sensor networks, enabling continuous verification through real-time telemetry. Additional work will focus on AI explainability and bias mitigation to ensure equitable treatment across supplier regions. Cross-border legal harmonization will be pursued through collaboration with OECD and UNCITRAL initiatives. Finally, consumer-facing transparency tools will be developed to allow end-users to verify device authenticity using blockchain-anchored proofs, strengthening market accountability.

The B-A-G-S architecture demonstrates that a carefully integrated combination of technologies—supported by sound governance and aligned with policy objectives—can transform counterfeit prevention from a reactive audit practice into a proactive, engineered infrastructure of trust. By embedding integrity, intelligence, geospatial context, and automated enforcement into the digital fabric of the global supply chain, the framework provides not only academic innovation but also a practical roadmap for securing consumer-device ecosystems and reinforcing national and industrial resilience.

6.0 References

Agrawal, T. K., Kumar, V., Pal, R., Wang, L., & Chen, Y. (2021). *Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry.* Computers & Industrial Engineering, 154, 107130. https://doi.org/10.1016/j.cie.2021.107130

Ahmed, W. A. H., & MacCarthy, B. L. (2023). *Blockchain-enabled supply chain traceability – How wide? How deep?* International Journal of Production Economics, 263, 108963. https://doi.org/10.1016/j.ijpe.2023.108963

Alharby, M., & Van Moorsel, A. (2019). *Blockchain-based smart contracts: A systematic mapping study.* Computer Science Review, 33, 1–15.

Alla, S., Zhuang, Y., Stockill, R., & Wang, H. (2022). *Smart contracts and their applications in supply chain management.* Journal of Industrial Information Integration, 27, 100285.

Azevedo, P., Gomes, J., & Romão, M. (2023). *Supply chain traceability using blockchain.* Operations Management Research. https://doi.org/10.1007/s12063-023-00359-y

Babich, V., & Hilary, G. (2020). *Distributed ledgers and operations: What operations management researchers should know about blockchain technology.* Manufacturing & Service Operations Management, 22(2), 223–240.

Bhasin, M., & Sharma, A. (2020). Fraudulent components in global supply chains: Emerging risks and mitigation strategies. *Journal of Supply Chain Security, 12*(2), 45–59.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic review of blockchain-based applications for industry. *IEEE Access, 7*, 17605–17633.

Chen, Y., & Lee, S. (2020). Machine-learning approaches for detecting anomalies in international trade networks. *International Journal of Data Science, 5*(3), 112–129. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access, 4*, 2292–2303.

CPSC. (2023). *Annual report on consumer product recalls*. U.S. Consumer Product Safety Commission.

FDA. (2022). Counterfeit batteries and electronic components in medical devices. U.S. Food and Drug Administration.

Ivanov, D., & Dolgui, A. (2021). A digital supply chain twin for managing disruptions. *International Journal of Production Research, 59*(13), 412–431.

Kshetri, N. (2021). Blockchain's roles in automating and enhancing supply-chain security. *Computer, 54*(9), 73–81.

McKinsey. (2023). *The economic cost of electronics recalls*. McKinsey & Company. NIST. (2022). *IoT cybersecurity labeling framework*. National Institute of Standards and Technology.

OECD. (2021). *Global trade in fake goods: Trends and impacts*. Organisation for Economic Co-operation and Development.

Statista. (2024). *Consumer electronics market—Worldwide revenue*. Statista Research Department.

The White House. (2021). *Executive Order 14017: America's supply chains*.

UL. (2023). *Certification limitations and global counterfeit risks*. UL Standards & Engagement.

U.S. CBP. (2021). *Trade enforcement and counterfeit interdiction statistics*. U.S. Customs and Border Protection.U.S. DHS. (2020). *Supply chain security and critical-infrastructure protection*. U.S. Department of Homeland Security.

Chang, S. E., Chen, Y., & Lu, M. F. (2020). *Supply chain re-engineering using blockchain technology: A case of smart contract-based tracking in food supply chains.* Technological Forecasting and Social Change, 150, 119–125.

Chen, T., Li, X., Luo, X., & Zhang, X. (2023). *Smart contract vulnerabilities: A comprehensive survey.* ACM Computing Surveys, 55(1), 1–37.

Doshi, S., Jangir, S., & Gohil, P. (2024). *Role of blockchain technology in enhancing supply chain traceability, transparency and efficiency.* Journal of Experimental Agriculture International, 46(5), 636–653. https://doi.org/10.9734/jeai/2024/v46i52419

Francisco, K., & Swanson, D. (2018). *The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency.* Logistics, 2(1), 2.

Hastig, G. M., & Sodhi, M. S. (2020). *Blockchain for supply chain traceability: Business requirements and critical success factors.* Production and Operations Management, 29(4), 935–954. https://doi.org/10.1111/poms.13147

Helo, P., & Hao, Y. (2021). *Blockchains in operations and supply chains: A model and reference implementation.* Computers &

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, pp. 2117–2135.

Sobowale, A., Okon, R., Nzeako, G., Zouo, S. J. C., Olamijuwon, J., Omowole, B. M., & Olufemi-Phillips, A. Q. (2024). *Ensuring product authenticity and traceability with blockchain in supply chains.* World Journal of Advanced Research and Reviews, 24(2), 1017–1038. https://doi.org/10.30574/wjarr.2024.24.2.3413

Song, J. M., & Sung, J. (2019). *Applications of blockchain to improve supply chain traceability.* Procedia Computer Science, 162, 119–122. https://doi.org/10.1016/j.procs.2019.11.266

Testi, N. (2023). *Blockchain technology for supply chain traceability: The case of SMEs of the Made in Italy.* Piccola Impresa Small Business, (2). https://doi.org/10.14596/pisb.3501

Wong, E. K. S., Ting, H. Y., & Atanda, A. F. (2023). *Enhancing supply chain traceability through blockchain and IoT integration: A comprehensive review.* Green Intelligent Systems and Applications, 4(1), 11–28. https://doi.org/10.53623/gisa.v4i1.355

Zhang, C., Xu, Y., & Zheng, Y. (2024). *Blockchain traceability adoption in low-carbon supply chains: An evolutionary game analysis.* Sustainability, 16, 5, pp. 1817. https://doi.org/10.3390/su16051817

Olaleye, A. G., Igbekoyi, O. E., Akinyele, A. R., Asimolowo, A. J. (2024). Economic Sustainability and Share Price Behavior of Listed Financial Service Firms in Nigeria. *International Journal of Multidisciplinary*

Research in Academic Studies and Field Practices (IJMRASFP), 3(3), 1-20.

Aboagye, E. F., Borketey, B., Danquah, K., Borketey, D. (2022). A Predictive Modeling Approach for Optimal Prediction of the Probability of Credit Card Default. *International Research Journal of Modernization in Engineering Technology and Science*. 4(8), 2425-2441

Declaration

Funding sources

No funding

Competing Financial Interests Statement:

There are no competing financial interests in this research work.

Ethical considerations

Not applicable

Data availability

The microcontroller source code and any other information can be obtained from the corresponding author via email.

Authors' Contribution

The author carried out the entire work, solely