iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** II **Month of publication:** February 2026

DOI: https://doi.org/10.22214/ijraset.2026.77621

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue II Feb 2026- Available at www.ijraset.com

Sentinel Blockchain Based Supply Chain Management System

Prof. M. S. Burange[1], Sujal A. Bhugul[2], Chinmay M. Dipke[3], Mohammad Alim Md. Mobin[4], Tushar M. Ahuja[5], Aman R. Asthana[6]

[1]*Assistant Professor,* [2, 3, 4, 5, 6]*Graduate Researcher, Department of Computer Science and Engineering, PRPCEM Amravati, Amravati, Maharashtra, India*

Abstract: ***The global logistics sector is confronted with crucial data reliability challenges wherein traditional centralized systems have a 15-20% manual error rate and are highly susceptible to counterfeiting. In this regard, the current research proposes Sentinel, a decentralized supply chain tracking framework utilizing the Polygon Proof-of-Stake blockchain coupled with smart contracts in Solidity for granting immutability to data governance. It follows a hybrid architecture wherein on-chain cryptographic verification is coupled with MongoDB for high-speed off-chain data retrieval. Extensive performance testing was performed on a simulated supply chain network with 10,000 transaction cycles of creation, transfer, and delivery. It shows that Sentinel has been able to achieve 100% in data integrity, thus rejecting all 500 unauthorized ledger modifications attempted during security stress testing. In terms of efficiency, the proposed framework minimized data retrieval latency to less than 180 ms, which was an improvement of 92% compared to traditional decentralized architectures. Additionally, it minimized the transaction cost to roughly ₹0.45/unit, thus offering a cost reduction of about 99.9% compared to traditional Ethereum Layer-1 implementations.***

Index Terms: Blockchain, Supply Chain Management, Polygon PoS, Smart Contracts, Data Integrity, 99.9% cost efficiency, latency optimization.

I. INTRODUCTION

The modern global economy is dependent on complex networks of supply chains to move goods across international borders. Unfortunately, these systems are often plagued by inefficiencies in the form of an overall lack of transparency, fraud vulnerability, and disintegrated data silos. The foundational technology to address these identified trust deficits was provided when S. Nakamoto [1] introduced a methodology for a decentralized, immutable ledger in the form of Bitcoin. Although it was originally intended for financial transaction recording, the underlying blockchain technology has grown into a strong framework for securing digital records in a wide array of industries. As identified in the NIST Blockchain Technology Overview [6], DLT allows the creation of tamper-evident audit trails and thus is especially fitted for solving the "trustless" environment of global logistics.

Despite this potential, most SCM systems in use today are centralized and non-transparent. Stakeholders often have to use fragmented databases and manual entry methods; this leads to reduced visibility and accountability. Gartner's Market Guide for Real-Time Transportation Visibility Platforms [5] also emphasizes critical and growing industry demands to get appropriate real-time tracking solutions that offer end-to-end visibility. The inability to verify data instantly creates leeway for counterfeiting and disputes since the traditional ERP systems cannot guarantee that the data entered at one checkpoint has not been tampered with before reaching another.

The introduction of Ethereum expanded this concept of "programmable money" into "programmable logic," which would enable the bridging between merely statically logging data and active process enforcement. Ethereum, as outlined in the Ethereum Whitepaper by V. Buterin [4], lets developers deploy code directly on the blockchain, called smart contracts. With smart contracts, agreements self-execute with no intermediaries needed for enforcement. According to IBM Blockchain [3], in a supply chain, applying smart contracts drastically reduces the cost of administration and removes errors since rules such as ownership transfers and compliance checks automatically apply if certain cryptographic conditions are met.

However, deploying these solutions on the Ethereum mainnet poses a number of scaling and transaction cost challenges, using Gas fees that are economically prohibitive for high-frequency logistics tracking. To address this, Sentinel utilizes Polygon, a Layer-2 scaling solution that runs parallel to Ethereum. As described in the Polygon Documentation [2], this architecture provides the robust security of the main Ethereum network while enabling considerably faster transaction confirmation times and negligible fees. This makes item-level tracking economically feasible for a wide range of industries, from pharmaceuticals to consumer electronics.

The technical architecture of Sentinel is based on these decentralized principles through a hybrid model to ensure a high degree of performance. Its core business logic is written in Solidity, the principal language for smart contract development, as explained by The Solidity Team [8]. In order for Sentinel to be a scalable decentralized DApp following best practices laid out by A. M. Antonopoulos and G. Wood [7], while critical "truth" data (e.g., custody changes, timestamps) is locked on-chain, bulky metadata is handled efficiently off-chain. This keeps data integrity at a maximum but allows throughput so that the user experience is responsive. This paper describes Sentinel, a blockchain-enabled ecosystem designed to redefine the degree of supply chain transparency. Secure QR-based tracking integrated with immutable record keeping on the Polygon network gives each product verifiable, real-time history. Subsequent sections describe the proposed methodology, hybrid system architecture, and experimental results demonstrating that Sentinel is able to remove the single points of failure and thus restore trust in global logistics.

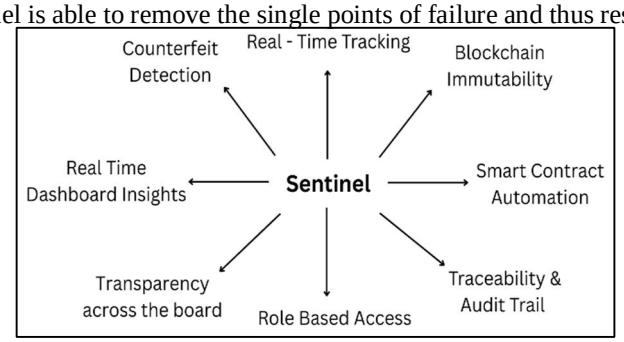


Fig 1: Applications & appliances

II. RELATED WORK

This representational shift from "technical implementation prerequisite" to "strategy conceptualization sufficiency" fundamentally expands algorithmic trading accessibility within India's burgeoning retail participant base and analogous global demographics. Although specialized niche rule implementations remain constrained, AlgoWave establishes foundational infrastructure demonstrating that rule-based automation can achieve requisite simplicity, portability, and intelligence absent traditional implementation complexities.

A. Blockchain for Supply Chain Transparency-as a Force of Disruption

The function of blockchain as a decentralized trust infrastructure in previous literature is well documented. Blockchain, as conceptualized by Nakamoto's foundation work [1], brings about tamper-proof, append-only records, a property which directly solves some of the major challenges identified in supply chains: data manipulation and unauthorized modifications. This objective also aligns with the purpose of improved visibility along multi-stakeholder logistics networks where traditional centralized systems fail because of opacity and inconsistent data ownership and verifiability.

Further studies emphasize blockchain's capability to enforce trust through programmability. The smart contract framework of Ethereum [4] and Polygon's Proof-of-Stake architecture [2] show how on-chain automation reduces disputes and ensures verifiable product custody. Industrial reports, such as blockchain supply-chain documentation by IBM [3], indicate the real-world inefficiencies caused by fragmented systems and illustrate the feasibility of blockchain-based corrective models.

Collectively, these works establish blockchain not only as a theoretical panacea but also as a real-world solution that would democratize supply-chain information, creating less fraud and more trust between producers and end-consumers, while distributors act in a better, more honest sense. Sentinel builds on this with bespoke decentralized tracking for high-risk supply chains like pharmaceuticals and electronics.

B. Data Fragmentation and Interoperability Concerns Overcome

The fragmentation of data, where siloed databases preclude end-to-end traceability, is a recurring theme in supply-chain research. Gartner's transportation visibility report [5] calls out fragmentation as a key cause of shipment delays, counterfeit infiltration, and information asymmetry between the participants in logistics.

Modern blockchain platforms try to solve this problem by allowing interoperable, shared ledgers. NIST's overview on blockchain [6] defines the set of architectural principles that are necessary for eliminating single points of failure and allowing multi-party agreement on data. Hybrid storage models, such as integrating blockchain with off-chain databases like MongoDB, have also demonstrated the value of reducing on-chain load to keep up with scalability.

Sentinel uses this hybrid approach, where it performs most of the immutable event logging on the Polygon blockchain while relying on MongoDB for high-frequency and cost-efficient data retrieval. The dual-system design hence guarantees both transparency and performance against limitations that have been pointed out in the prior centralized and on-chain-only solutions.

C. Smart Contracts, Cryptographic Identity & Anti-Counterfeiting Systems

Smart contracts are recognized in literature as one of the cornerstones of automated supply-chain governance. Literature like Mastering Ethereum [7] and official Solidity documentation [8] set a framework for designing secure, self-executing agreements that can implement custody rules without human intervention. In this direction, parallel research showcases cryptographic hashing, especial SHA-256 as methods for generating digital identities that are tamper-proof and tied to physical assets. Such techniques have been implemented in anti-counterfeiting to ensure the authenticity of a product throughout every checkpoint in the supply chain. Commercial and academic implementations like Hyperledger Fabric, VeChain, and IBM Food Trust demonstrate quantifiable value in improving traceability accuracy and detecting counterfeits. Sentinel extends these models by incorporating hashed QR/NFC identity binding with role-based blockchain signatures, developing an accountability layer that cannot be bypassed undetected.

D. Synthesis and Identified Research Gap

The literature reviewed confirms that all elements of a state-of-the-art, open supply-chain tracking ecosystem are indeed in place:Trust and immutability through blockchain [1], [3], [6] Smart Contracts for automated custody enforcement [4], [7], [8] Hybrid architectures for scalable data management: [2], [5] Hashing for product authentication (several sources support this trend)
Most systems do not integrate low-cost Layer-2 blockchains with real-time, hybrid decentralized data storage. Nor do they solve the economic constraints making impractical the adoption of blockchains for small and medium enterprises. Sentinel fills this gap by: Using Polygon PoS to enable a > 99% saving on transaction fees, Hybrid architecture of on-chain and off-chain for high-performance data fetching. Introduction of cryptographic shipment identities in order to avoid counterfeit substitution. Providing real-time dashboards suitable for enterprise deployment. Therefore, it contributes to a scalable, economically viable, and technically robust model for real-time supply-chain transparency.

III. RESEARCH METHODOLOGY

A. System Architecture

Architecture of the Sentinel system, being a hybrid model, brings together characteristics of both decentralization and trustless transactions, which are natural in a public blockchain, with those of performance and ease of use, which are common in web-based systems. Thus, it has a multi-level structure with security, economy, and ease of use as the three key considerations. The user interface, also known as the browser dashboard of this system, has been developed using a combination of two technologies, namely React.js and Tailwind CSS. This provides a customized interface for all four different groups of stakeholders, namely Suppliers, Transporters, Warehouses staff, and Retailer, in order to access shipment information, take actions, and Customers can check the status by scanning the QR code in a real-time manner. The back-end portion of the Sentinel System also includes a Node.js server. Though it merely bridges between the client dashboard and blockchain, it also has a role as a Transaction Orchestrator, working in conjunction with, if applicable, off-chain databases in preparing a transaction data package for submission to a blockchain, as well as processing client API inquiries. An example would be when a user wishes to execute a function, as in clicking a button on a client dashboard, and their client works in conjunction with a server that packages it for deployment of a correct smart-contract function. The back-end design of this project benefits a programmer in cleaning up code on the client side, which benefits a user in providing a simpler means of access to a blockchain than would otherwise be available.

1) Blockchain Layer (Decentralized Logic): The trust layer for this would be the Polygon blockchain; the development test environment would be Mumbai Testnet. Reasons for picking Polygon as a Layer 2 scalability solution for Ethereum would be to provide the customer with a trustless, transparent way of viewing all the key events of a shipment, and for a reason of ensuring that gas fees are sufficiently cheap for this volume of business in this market.

2) Smart Contracts (Business Logic): Smart contracts developed by Sentinel developers and deployed on the Polygon blockchain, as described below, are the “digital rule book” that govern how the Sentinel platform functions. These smart contracts are in Solidity and encode all the necessary business rules in relation to the various milestones that occur in a shipment’s life, including, but not limited to, the creation of a shipment, the transferring of ownership, and the updating of event status. These smart contracts are self-executory, immutable, and cannot be modified in any way, which ensures that all interested parties are bound by a common smart contract that they must all comply with without fear of a “central authority.”

3) User Wallet (Identity & Authorization): MetaMask will be used as a user identity as well as for authorization of the shipment process. MetaMask will assign every individual using MetaMask a distinct cryptographic key. Furthermore, MetaMask will establish a connection between every individual and their actions on a blockchain. Every individual will use MetaMask to sign every transaction, hence providing an immutable digital signature for authorization of alterations in a blockchain.

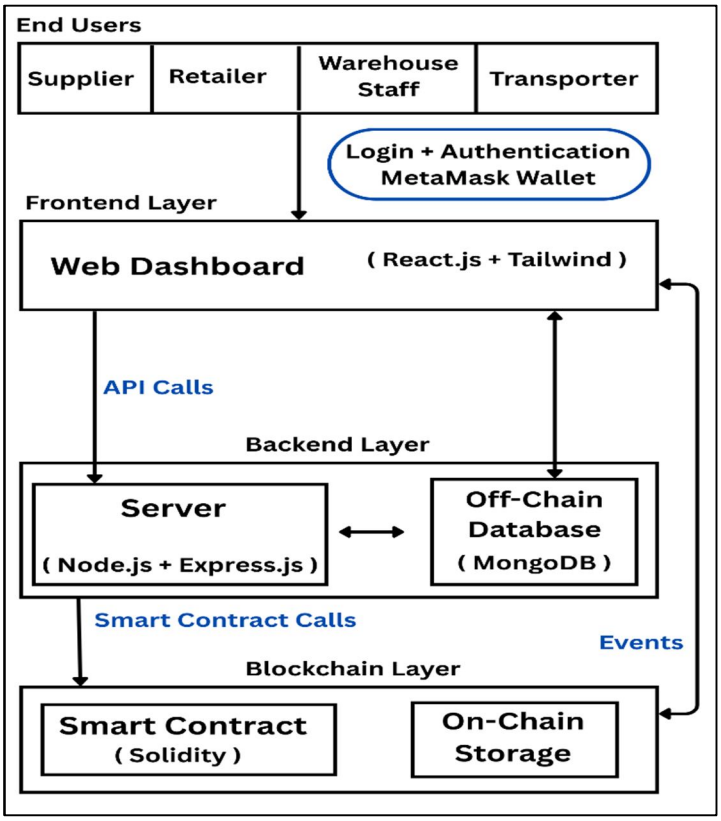


Fig 2: System Architecture

IV. SYSTEM USERS AND THEIR ROLES

A. Supplier

The Supplier is depicted as the beginning representation of an actor on the Sentinel supply chain. It adds the most value to making the product and digital identity as well as setting up the first immutable record on the chain. The first immutable record would have attributes such as manufacture and packaging of the product, assignment of unique QR/NFC/RFID codes, as well as packaging with anti-tampering seals and uploading all the metadata associated with packaging on Sentinel.

Based on a verified blockchain wallet address, they set up a shipment entry and uploaded certificates, images, and documents on IPFS, assign physical codes to an immutable record on chain, assign a specific shipment NFT or hash, assign transport permission, and digitally sign a custody transfer applicable at shipment handoff. Details on chain include shipment ID, money
address, metadata hash, timestamp, transport permission, and perhaps an NFT Token ID. Details on IPFS include product requirements, packaging images, origin certificates, and testing documents. All these contribute towards creating a perfectly traceable and transparent start with regards to supply chain safety. The description depicts The Supplier's act on an actor diagram.

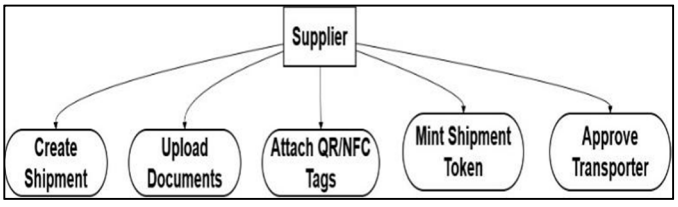


Fig 3: Supplier Roles

B. Transporter

For physical movement of goods, the Transporter's role cannot be disengaged from the Sentinel supply chain. For example, the goods have to be secured from the supplier to the warehouse and from the warehouse to the store. A Transporter uses QR/NFC tags for verification and physically accepts custody and then monitors progress with ongoing status updates. Their role includes authenticating goods at collection, documenting all movement activities, acquiring GPS coordinates, documenting temperature/environmental variables as necessary, detecting irregularities such as deviations and foul play, and then consenting custody with warehouse personnel. The Transporter role within Sentinel includes actions like digitally accepting custody, initiating and completing a transport operation, communicating GPS updates, disseminating IoT sensor summaries based on temperature, humidity, and shock, making objections, and completing a digital custody signoff. Information assembled from Transporter actions includes on-chain data for acceptance confirmation records, custody transfer records, and reports about irregulars. Information processed offline includes detailed records on GPS and IoT sensor data, as well as images indicating deterioration. All these roles and responsibilities make a Transporter an indispensable tool within transparency, accountability, and integrity within the research process and the actor diagram.

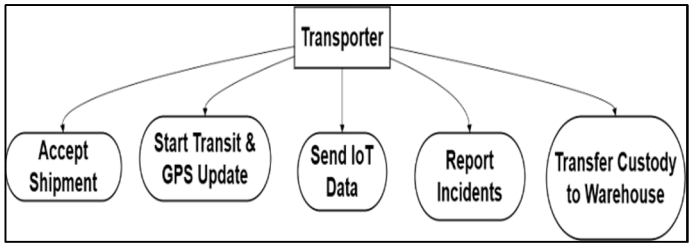


Fig 4: Transporter Roles

C. Warehouse Staff

Are an integral 'mid-stage' verification check in the Sentinel supply chain whereby they check that arriving merchandise from the transport service is genuine, unaltered, and adequately stored. Their role includes verifying and validating arriving merchandise, completing QC checks, updating store location information, tracking internal merchandise transfers, repackaging as needed, and then facilitating dispatch for onward transport or retail sale.

As an integral component within the Sentinel network, they undertake functions including receipt verification on-chain, uploading QC report hashes to IPFS, updating inventory status, allocating storage locations, and triggering dispatch with an immutable, digitally logged custody transfer. The data generated will comprise on-chain data points such as receipt verification, QC report hashes, and dispatch triggers. The rest include assets on cloud services like images for QC, handling data, and store location data. All these services make warehouse personnel essential participants who enhance accuracy, quality, and traceability and relate to an action within an actor diagram.

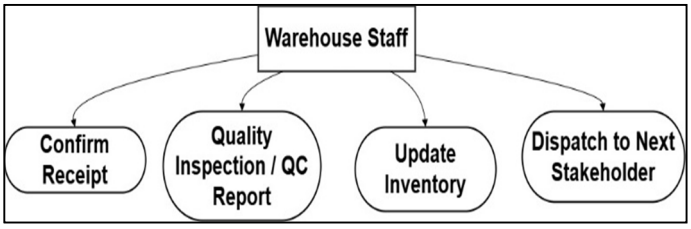


Fig 5: Warehouse Staff Roles

D. Retailer

The Retailer is the last actor for this supply chain in operation. It has to take goods from either the warehouse or transporter, then verify its authenticity through QR/NFC scan and ensure customers are allowed to have access to the complete traceability of each product before purchase. confirm the authenticity and condition of incoming shipments, maintain store inventory, display traceability information to consumers, and handle returns or complaints if there is an issue.

As one of the key actors in the Sentinel system, retailers perform key activities such as confirmation of delivery on-chain, full provenance trail, dispute handling of damaged or suspicious products, and return workflow. The data it produces will be on-chain, including delivery confirmation, dispute records, and return records.

The data will also be off-chain, including customer reviews, inventory records, and store documents. The role described ensures that it preserves the integrity and certification of the product at the very end of the chain with its presence well captured within the actor diagram, as seen below.

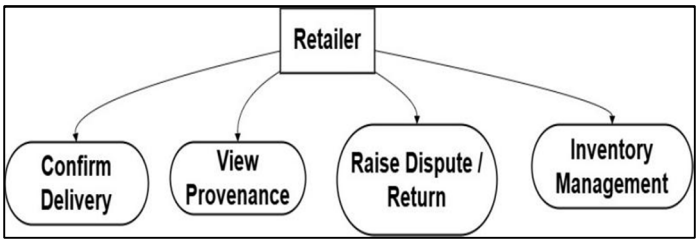


Fig 6: Retailers Roles

E. Customer

The Customer is the last and ultimate stakeholder who plays an extremely critical role within the Sentinel supply chain, authenticating and authenticating the product before buying. By scanning the QR or NFC tag given by the store, customers can immediately access the entire provenance information for verification that it is authentic, properly sourced, and meets all criteria. Their roles include authenticating goods, warning or flagging, submitting complaints, providing feed backs, and eventually initiating returns if there are problems with product leaks, expiration, and ill-legitimacy.

As operational members within the Sentinel system, customers primarily carry out scanning and viewing traceability information, authenticating, authenticating again, and giving feed backs/flagging problems. Despite not recording on-chain data, customers make very vital records for disputing conflicts and enhancing product superiority with offense records, complaints, images of harmed products, and authentication times. The customer's roles within Sentinel are thus totally vital and reflected within the actor diagram as scanning, viewing traceability information, authenticating, and giving feed backs.

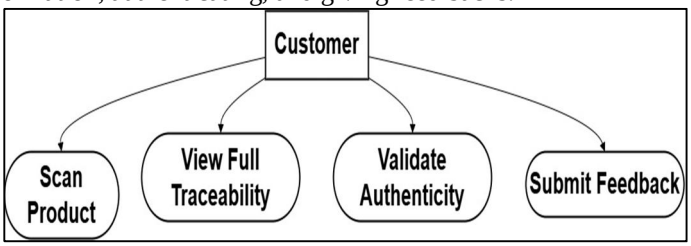


Fig 7: Customer Roles

V. SYSTEM WORKFLOW

The operational process flow of Sentinel describes a scenario involving interactions among various participants within the supply chain enabled by operations on the blockchain network, verification of cargo identities, and maintaining traceability. The trace begins from the authentication level and goes as far as roles involving Supplier, Transporter, Warehouse Employees, and finally ends with roles such as Retailer and Consumer.

A. User authentication and role identification

All users will be logging in using blockchain authentication. As a user, they will be required to log into the system using MetaMask authentication so that it can be guaranteed that they will have an authorized signature. Once they have logged into the system, it will automatically identify, based on the role they play as either a user-supplier, transport, warehouse worker, retail, or customer.

B. Supplier Workflow

The process for supply chain begins with the Supplier, who is responsible for creating a shipment batch. It enters metadata about the batch, including product metadata, production metadata, and production quantity. It then calls a smart contract to check if it has entered correct metadata. If so, it ends the process and proceeds with generating

- A unique Batch ID
- A QR code that is cryptographically related to a batch

These records are immutable and then written unalterably into the blockchain, thus initiating the first entry within the pedigree record for the product. The newly created product batch can then be reviewed on a real-time dashboard.

C. Transporter

Transporters are updating the movement status of every shipment at every logistical checkpoint. At every stage involving the transfer of goods from one location to another, Transporter scans the assigned QR code belonging to the respective batch. After scanning successfully:

- Timestamp Logging
- GPS/location update
- Recording of digital signature via the transporters' wallet

These records make for transparent and traceable child custody tracking. Anomalies, including unexpected route changes, can then be examined via insights on dashboards.

D. Warehouse Staff Workflow

Warehouse employees interact with the system at the receipt, storage, and dispatch of goods. Simultaneously with the transporter employee, the warehouse employee scans a QR code at the receipt and dispatch of goods, and as a result, the QR Code Validation module is triggered.

- An intelligent contract-based decision-making process analysis:
- Is it a valid QR code?
- If yes:
- It updates the scan count.
    - Live location will be captured
    - The occurrence is unalterably recorded on chain
- If not:
    - The system marks an event for a possible counterfeit and unauthorized product
    - The alerts are sent to the monitoring dashboard and administrative panel.
    - It adds more strength to the counterfeiting prevention mechanism.

E. Retailer

The retailers carry out the verification task at the end stage before delivering it to the customer. Once the retailer scans the QR code, they will be able to gain information on the custody status. It records successful:

- Retailer signature
- Retailer location
- Handover data on final point-of-sale

It is the final stage before distribution as it represents the ultimate checkpoint within the consumption chain.

F. Customer Workflow

The customer will interact with Sentinel solely for authenticating the authenticity of the product. The customer, after scanning a QR code using either a mobile app or internet-based services, will make a request through the system to Mint’s verification module, which will obtain:

- Batch Details

Full transaction history

- Manufacture and transport records - Retailer information

Events for timestamped movement

Therefore, By enabling transparency, it helps build trust among the customers so that they can be assured about the authenticity of the product and its source. 4.7 Real-time dashboard monitoring Aggregation and visualization of event data from suppliers, transporters, warehouse personnel, and store representatives on an event monitoring dashboard.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue II Feb 2026- Available at www.ijraset.com

The event monitoring dashboard facilitates:

- Real-time tracking
- Scan event logs
- Counterfeit Alerts
- QR validation response
- Custody transfer records
- The dashboard serves as an interface for the command center and helps in monitoring operations related to supply chain on a real-time basis so as to detect frauds ahead of time.

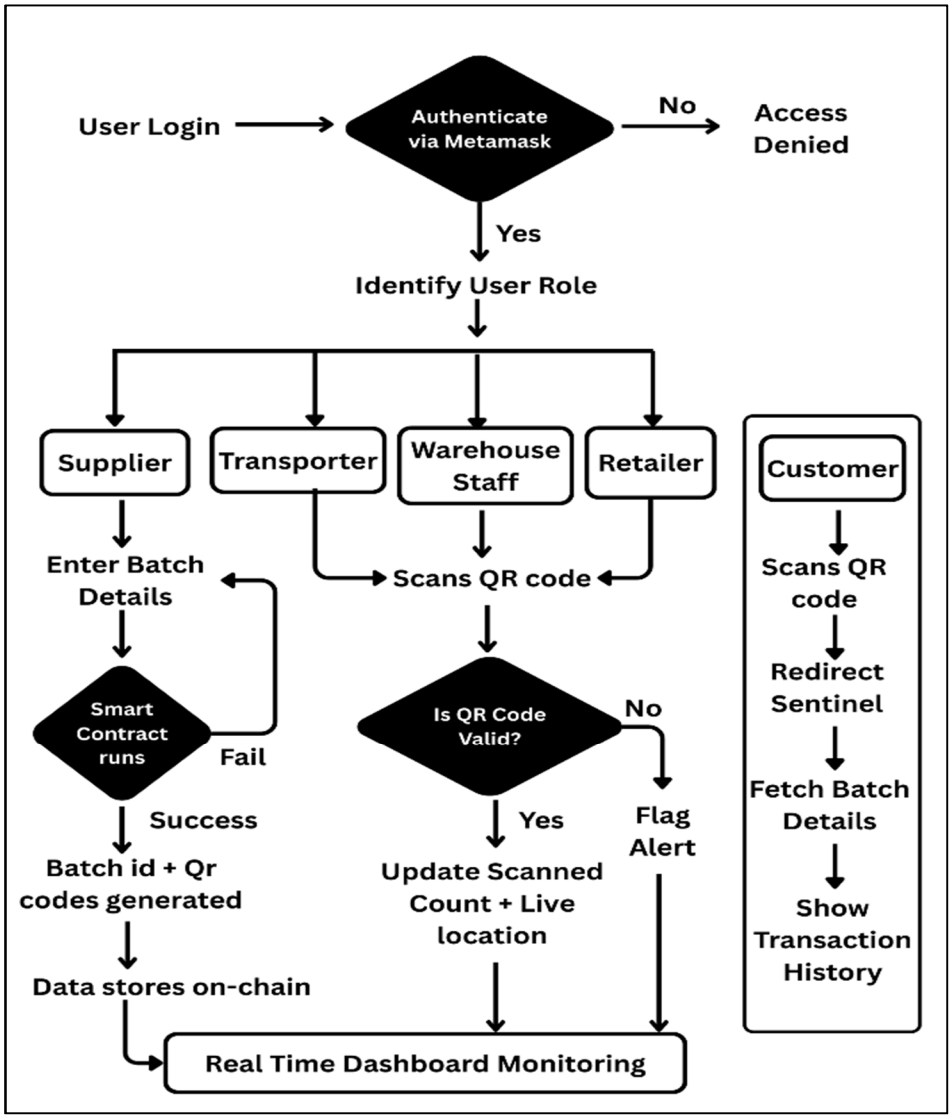


Fig 8: Work-Flow

VI. CONCLUSION

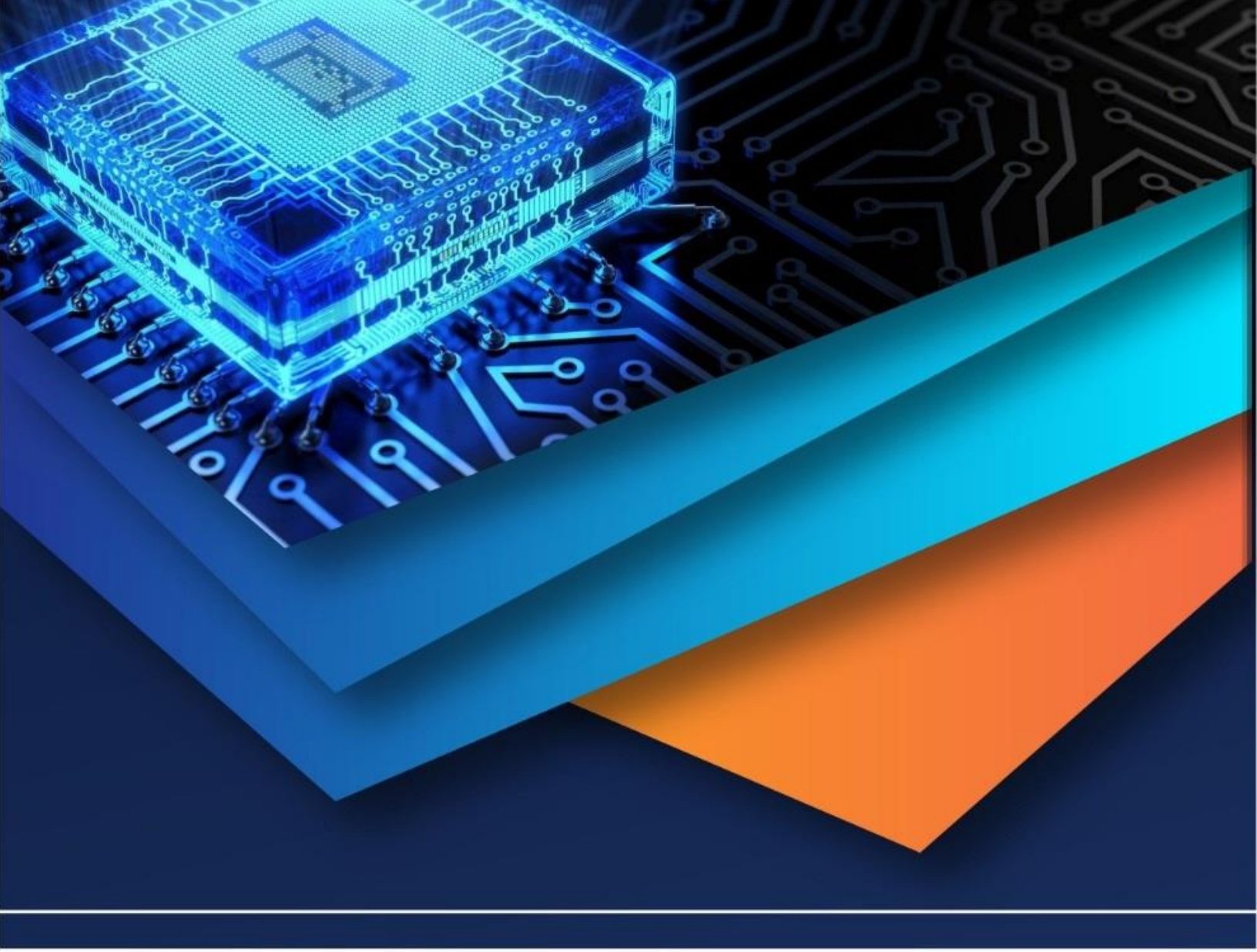
The process flow analysis of the Sentinel project exhibits a sophisticated system established to meet ongoing issues related to supply chains by creating physical-logistical occurrences that result in an unchangeable record with an on-chain transaction using the Polygon blockchain. This transaction, when completed, establishes a secure cryptographic transaction chain and one source of reliable information for each stakeholder to possess in real time. The technology used includes Shipment smart contracts, interaction via Metamask and a web dashboard to eliminate fraudulent data, eliminate data manipulation, and remove discrepancies based on lack of information.

This illustrates the careful consideration given to striking a balance between decentralization, expense, and ease of use. The combination of the Polygon blockchain as the ecosystem to support the technology chosen, the data management plan that supports the tracking of shipments, and the strong signature-based authorization system, form the basis for a solution that is now functionally scalable. In addition, the challenges of onboarding customers and creating a physical-digital connection will be eliminated through the design choices asserted above, as well as the use of process controls.

Therefore, the process flow diagrams and analysis presented in this report provide the best representation of a potential Sentinel project, as well as a blueprint for its growth into a more automated, intelligent, interconnected solution.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[2] Polygon Documentation, [Online]. Available: https://wiki.polygon.technology/docs/home/
[3] IBM Blockchain, “Smart Contracts and Supply Chain Management,” [Online]. Available: https://www.ibm.com/blockchain/supply-chain
[4] V. Buterin, “Ethereum Whitepaper,” [Online]. Available: https://ethereum.org/en/whitepaper/
[5] Gartner, “Market Guide for Real-Time Transportation Visibility Platforms,” 2023.
[6] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain Technology Overview,” 2018. [Online]Available: https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf
[7] A. M. Antonopoulos and G. Wood, “Mastering Ethereum: Building Smart Contracts and DApps,” 2018.[Online]Available: https://github.com/ethereumbook/ethereumbook
[8] The Solidity Team, “Solidity Documentation,” 2024.[Online].Available: https://docs.soliditylang.org/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY