

ChainGuards: Verification of Sensed Data using Permissioned Blockchain Technology

Sara Aguincha*

INESC-ID, Instituto Superior Técnico,
Universidade de Lisboa, Portugal.
sara.aguincha@tecnico.ulisboa.pt

Samih Eisa

INESC-ID, Instituto Superior Técnico,
Universidade de Lisboa, Portugal.
samih.eisa@inesc-id.pt

Emanuel Nunes

Sensefinito,
Lisbon, Portugal.
emanuel.nunes@sensefinito.com

Miguel L. Pardal

INESC-ID, Instituto Superior Técnico,
Universidade de Lisboa, Portugal.
miguel.pardal@tecnico.ulisboa.pt

Abstract

Sensor technologies have evolved to a point where it is now convenient to monitor products along the supply chain. The collected data can even be stored in a decentralized way using blockchain technology. However, ensuring the reliability of sensed data is a challenge as we need to trust the data.

We propose ChainGuards, a decentralized system that uses product-specific rules to verify data collected across the supply chain, with particular focus on sensor-derived information to issue warnings and trigger audits when anomalies are detected. We evaluated it with data from a real world supply chain deployment. The implemented solution is able to correctly detect data discrepancies and inconsistencies and provides reliable verification of supply chain data with low performance overhead.

CCS Concepts

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

Keywords

Sensors, Sensed Data, Safety, Internet of Things, Supply Chain.

ACM Reference Format:

Sara Aguincha, Emanuel Nunes, Samih Eisa, and Miguel L. Pardal. 2026. ChainGuards: Verification of Sensed Data using Permissioned Blockchain Technology. In *The 41st ACM/SIGAPP Symposium on Applied Computing (SAC '26)*, March 23–27, 2026, Thessaloniki, Greece. ACM, New York, NY, USA, 2 pages. <https://doi.org/10.1145/3748522.3779980>

1 Introduction

A supply chain consists of multiple *trading partners* that are involved in the production and distribution of goods, yet recent scandals such as one involving mislabeled meat products [13] reveal weaknesses in current safety measures. Existing mechanisms rely on audits and labeling, which do not always ensure accuracy.

*Corresponding author



This work is licensed under a Creative Commons Attribution 4.0 International License. SAC '26, Thessaloniki, Greece

© 2026 Copyright held by the owner/author(s).

ACM ISBN 979-8-4007-2294-3/2026/03

<https://doi.org/10.1145/3748522.3779980>

Although sensors enhance monitoring, they also risk faulty readings or manipulation. Reliable information therefore requires verification based on defined data-checking rules. Assigning this role to a central authority would undermine transparency and resilience, making blockchain technology [10] a suitable decentralized environment for collective and deterministic verification. We introduce ChainGuards, a chaincode library for Hyperledger Fabric [3] that applies verification rules to data recorded in the ledger. The system evaluates entries, flags inconsistencies and can turn unverified claims into facts agreed upon by all participants.

2 Related Work

Sensor data is inherently error-prone with common issues such as outliers, drift, noise and others [14]. Addressing these problems often relies on *preprocessing* to remove noise and inconsistencies through cleaning, integration and transformation [2]; *error detection* to identify anomalies [16]; and *analysis* to extract insights or support decision-making, sometimes through multi-sensor fusion to achieve more reliable signals [15].

Various blockchain-based solutions have been applied to traceability across industries, including food [4, 6, 7, 12] and pharmaceuticals [8, 11], demonstrating its versatility for immutable data storage in supply chain scenarios.

Our work focuses on rule-based verification using *business rules* – formal, event-driven policies that define how sensor data and operational claims should be checked [1, 5, 17]. When combined with intra- and inter-organizational cross-validation in a blockchain environment, these rules enable detection of sensor errors and support consensus on the validity of recorded claims.

3 Proposed Solution

ChainGuards is designed to improve trust in supply-chain sensor data by applying collaboratively defined, product-specific rules. Its design is grounded in expert requirements – focusing on provenance, environmental conditions, shipment integrity and support for audits and recalls – and aims to validate data coming from multiple organizational contexts. The supply-chain model includes: *Journeys*, representing a product's lifecycle; *Steps*, capturing business phases such as storage or transport; and *Points*, containing granular sensor readings.

ChainGuards considers three classes of data sources: single-source data (SSoD), multi-source data within an organization (MSoD)

and diverse sources across organizations (DSoD). SSoD ensures basic checks when only one device is available; MSoD performs redundancy-based cross-validation and configurable sensor fusion; and DSoD compares independent records from different stakeholders, supporting provenance checks and discrepancies at handoff events. Verification rules are modular and parameterized through policy files, covering thresholds, geofencing, route deviation, hand-off timing and shipment duration. These rules are evaluated at the Step or Journey levels depending on context, enabling localized checks (e.g., temperature within a phase) and lifecycle-wide verification (e.g., consistent custody).

Processing follows a structured pipeline: incoming events are parsed; sensor data is cleaned through outlier detection (IQR for 1D, speed-based filtering for GPS) and smoothed with Kalman filtering; multi-sensor fusion for MSoD uses reliability weights derived from Mahalanobis distance. Warnings and alerts are issued, providing an auditable trail for anomaly investigation and supporting transparent, multi-stakeholder trust in supply-chain data.

4 Evaluation

Evaluation combined controlled synthetic tests with data from the Fundão Cherry supply chain pilot. Synthetic traces – generated with a custom EPCIS toolkit and OSRM [9] – enabled systematic validation of all verification rules, including geofence, backtrack, thresholds, multi-sensor fusion (MSoD) and cross-stakeholder discrepancy checks (DSoD). These tests confirmed that the system reliably detects abnormal situations. The synthetic dataset generation toolkit allowed complete coverage of all rule types.

The pilot offered real-world validation in a cherry supply chain with PGI (Protected Geographical Indication) certification. It involved farms, processing factory and regional depot. Data was collected using newly deployed technology, covering field production, factory reception, palletization and downstream logistics. ChainGuards successfully verified farm-to-factory routes, confirmed geofence and timing compliance and detected discrepancies in product attributes and lineage between the sensor provider and factory systems. These mismatches exposed real data-quality issues, illustrating the value of rule-based cross-verification for resolving inconsistent claims.

Performance tests on Hyperledger Fabric (v2.5.9) showed approx. ~1% overhead for storing parsed objects and stable verification latency even with thousands of events. Multi-source preprocessing added negligible cost and granular point storage enables parallel ingestion, significantly reducing processing time. The system also scales reliably across multi-organization networks.

5 Conclusion

ChainGuards introduces a rule-driven verification layer that connects sensor outputs with blockchain records. Events are processed on Hyperledger Fabric and checked through single-, multi- and cross-stakeholder verification, while the underlying object model unifies sensor traces with business steps and full journeys. Tests using both real data and anomaly-injected synthetic events confirmed that the system reliably identifies environmental deviations, route issues and process discrepancies. These results show that

ChainGuards improves supply-chain transparency by validating data automatically and consistently across organizations.

Acknowledgments

Work supported by national funds through Fundação para a Ciência e a Tecnologia, I.P. (FCT) under projects UID/50021/2025 and UID/PRR/50021/2025 (INESC-ID) and Project Blockchain.PT – Decentralize Portugal with Blockchain Agenda, (Project no 51), WP 1: Agriculture and Agri-food, Call no 02/C05-i01.01/2022, funded by the Portuguese Recovery and Resilience Program (PRR), The Portuguese Republic and The European Union (EU) under the framework of Next Generation EU Program.

References

- [1] Vivek Acharya. 2012. *Oracle BPM Suite 11g Developer's Cookbook*. Packt Publishing Ltd.
- [2] Suad A Alasadi and Wesam S Bhaya. 2017. Review of data preprocessing techniques in data mining. *Journal of Engineering and Applied Sciences* 12, 16 (2017), 4102–4107.
- [3] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, et al. 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth EuroSys conference*. 1–15.
- [4] Kamanashis Biswas, Vallipuram Muthukkumarasamy, and Wee Lum Tan. 2017. Blockchain based wine supply chain traceability system. In *Future Technologies Conference (FTC) 2017*. The Science and Information Organization, 56–62.
- [5] Jérôme Boyer and Hafedh Mili. 2011. Agile business rule development. In *Agile Business Rule Development: Process, Architecture, and JRules Examples*. Springer, 49–71.
- [6] Fran Casino, Venetis Kanakaris, Thomas K Dasaklis, Socrates Moschuris, Spiros Stachtiaris, Maria Pagoni, and Nikolaos P Rachaniotis. 2021. Blockchain-based food supply chain traceability: a case study in the dairy sector. *International journal of production research* 59, 19 (2021), 5758–5770.
- [7] Luisanna Cocco, Katiusia Mannaro, Roberto Tonelli, Lorena Mariani, Matteo B. Lodi, Andrea Melis, Marco Simone, and Alessandro Fanti. 2021. A Blockchain-Based Traceability System in Agri-Food SME: Case Study of a Traditional Bakery. *IEEE Access* 9 (2021), 62899–62915. <https://doi.org/10.1109/ACCESS.2021.3074874>
- [8] Xinlai Liu, Ali Vatankhah Barenji, Zhi Li, Benoit Montreuil, and George Q Huang. 2021. Blockchain-based smart tracking and tracing platform for drug supply chain. *Computers & Industrial Engineering* 161 (2021), 107669.
- [9] Dennis Luxen and Christian Vetter. 2011. Real-time routing with OpenStreetMap data. In *Proceedings of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (GIS '11)*. ACM, New York, NY, USA, 513–516. <https://doi.org/10.1145/2093973.2094062>
- [10] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Satoshi Nakamoto* (2008).
- [11] Ilhaam A Omar, Mazin Debe, Raja Jayaraman, Khaled Salah, Mohammad Omar, and Junaid Arshad. 2022. Blockchain-based supply chain traceability for COVID-19 personal protective equipment. *Computers & Industrial Engineering* 167 (2022), 107995.
- [12] Pratyush Kumar Patro, Raja Jayaraman, Khaled Salah, and Ibrar Yaqoob. 2022. Blockchain-based traceability for the fishery supply chain. *Ieee Access* 10 (2022), 81134–81154.
- [13] Jagadeesan Premanandh. 2013. Horse meat scandal—A wake-up call for regulatory authorities. *Food control* 34, 2 (2013), 568–569.
- [14] Hui Yie Teh, Andreas W Kempa-Liehr, and Kevin I-Kai Wang. 2020. Sensor data quality: A systematic review. *Journal of Big Data* 7, 1 (2020), 11.
- [15] Athina Tsanousa, Evangelos Bektsis, Constantine Kyriakopoulos, Ana Gómez González, Urko Leturiondo, Ilias Gialampoukidis, Anastasios Karakostas, Stefanos Vrochidis, and Ioannis Kompatsiaris. 2022. A review of multisensor data fusion solutions in smart manufacturing: Systems and trends. *Sensors* 22, 5 (2022), 1734.
- [16] Sai Xie and Zhe Chen. 2017. Anomaly detection and redundancy elimination of big sensor data in internet of things. *arXiv preprint arXiv:1703.03225* (2017).
- [17] Michael Zur Muehlen and Marta Indulska. 2010. Modeling languages for business processes and business rules: A representational analysis. *Information systems* 35, 4 (2010), 379–390.