p–ISSN: 2723 - 6609 e - ISSN : Telepon 2745-5254
Jil. x, No.x Bulan 2026 http://jist.publikasiindonesia.id/

# Permissioned Blockchain and Smart Contracts for Halal Supply Chain Traceability in Indonesia

**Rafi Farizki[1*], Rani Santika[2], Vo Hung Cuong[3]**
Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI, Indonesia[1]
Universitas Muhammadiyah prof Dr hamka, Indonesia[2]
University of Danang, Vietnam[3]
Email: Rafifarizki90@gmail.com[1], rsantika851@gmail.com[2], vhcuong@vku.udn.vn[3]

**ABSTRACT**

Assurance of halal integrity along the supply chain carries major economic and religious weight in Indonesia, yet conventional traceability relies on centralized databases and paper certificates that are difficult to verify, easy to tamper with, and fragmented across the many actors between farm and consumer. This study designs and evaluates HalalChain, a permissioned-blockchain and smart-contract traceability framework that records each custody transfer on a shared, tamper-evident ledger and encodes halal certification rules as executable logic. Using a design science methodology, supply-chain actors participate as permissioned nodes on Hyperledger Fabric, bulky documents are stored off chain with only their cryptographic hashes on chain, and consumers verify authenticity by scanning a code; the framework was compared against a centralized-database baseline across throughput and latency, scalability, traceability completeness and time to trace, and security and trust, complemented by a structured expert assessment. The evaluation indicates that the permissioned blockchain strengthens traceability and trust, yielding a more complete, verifiable history, faster tracing, and demonstrated tamper-evidence and access control, while keeping performance within practical bounds through the on-chain/off-chain design. The framework provides a deployable reference architecture linking blockchain traceability to halal certification governance, transferable to other provenance-critical chains. A permissioned blockchain can improve halal traceability and trust at an acceptable performance cost.

**Keywords:** blockchain; smart contracts; halal supply chain; traceability; distributed ledger technology

## INTRODUCTION

Indonesia is home to one of the world's largest markets for halal products, and assurance that a product is genuinely halal along its entire journey from source to consumer carries both major economic weight and deep religious significance (Wekke et al., 2024). Globally, Muslim consumer spending across the core halal economy sectors reached approximately US$2.43 trillion in 2023 and is projected to rise to US$3.36 trillion by 2028, with halal food alone accounting for about US$1.43 trillion. This growth is propelled by a global Muslim population that surpassed two billion people in 2023, more than a quarter of the world's population, and by intensifying consumer demand for transparent and credibly certified halal supply chains (Azizah et al., 2024).

Indonesia, the largest Muslim-majority market and consistently among the top-ranked national halal economies, has made halal certification mandatory for products circulating in its territory under Law No. 33 of 2014 on Halal Product Assurance, with enforcement for food and beverage products commencing on 18 October 2024 (Attaluni, 2024). Halal integrity is not a property of a single step but of the whole chain: a lapse at any point, from ingredient sourcing through processing, storage, and distribution, can compromise the status of the final product.

Conventional traceability systems struggle to provide this end-to-end assurance. They typically rely on centralized databases controlled by individual organizations and on paper-based certificates, which are difficult for downstream parties to verify independently, vulnerable to alteration or forgery, and fragmented across the many actors who handle a product. When each participant keeps its own records in its own system, reconstructing a complete and trustworthy history is slow and depends on trusting every intermediary, and consumers have little means to check claims for themselves.

These weaknesses are not merely hypothetical. Halal fraud and mislabeling are recurring problems along real supply chains: Indonesian authorities have documented cases in which halal-certified processed beef was adulterated with pork, and misleading halal labeling on machine-slaughtered poultry and other products has repeatedly raised doubts about the credibility of existing traceability (Sidarto & Hamka, 2021). High-profile international incidents, such as the fraudulent repackaging of non-halal meat as halal in Malaysia, further illustrate how opaque, multi-actor chains enable integrity violations that erode consumer trust (Ali et al., 2021). Because record keeping across the chain is fragmented and difficult to audit independently, such violations are frequently detected only after products have already reached consumers, which is precisely the failure that verifiable end-to-end traceability is intended to prevent.

Blockchain technology offers properties that map directly onto these gaps. A blockchain is a shared, append-only ledger whose entries are cryptographically linked so that recorded history is tamper-evident and visible to all authorized participants (Nakamoto, 2008; Zheng et al., 2018). Smart contracts extend this ledger with executable logic that runs automatically when predefined conditions are met, allowing rules to be enforced without a central intermediary (Buterin, 2014; Wood, 2014). For enterprise supply chains, permissioned blockchains such as those built on the Hyperledger Fabric platform restrict participation to known, vetted actors while retaining the integrity and shared-visibility guarantees of the ledger (Androulaki et al., 2018), and combining blockchains with the Internet of Things enables provenance data to be captured automatically as goods move (Christidis & Devetsikiotis, 2016).

These properties translate into concrete traceability benefits that prior empirical work has begun to demonstrate. Immutability and cryptographic linkage make each recorded custody event tamper-evident, so a forged or altered provenance record can be detected rather than silently accepted; shared visibility across authorized nodes removes the need to trust any single intermediary's private database; and smart contracts enforce certification rules automatically and uniformly at every hand-off rather than relying on manual, after-the-fact checks (Rejeb et al., 2020). In a documented Indonesian poultry deployment, a blockchain-based system recorded farm-to-fork data permanently and allowed consumers to verify halal status by scanning a code, improving transparency relative to conventional records (Sidarto & Hamka, 2021). By reducing the effort required to reconstruct a verifiable history, such systems directly target the two performance dimensions most relevant to halal integrity: the completeness of the reconstructed provenance and the speed with which a product can be traced during a recall or dispute (Surjandari et al., 2020).

These ideas have been explored for supply-chain management and traceability in general. Studies have applied blockchain to agri-food traceability (Tian, 2016), examined its relationship to sustainable and transparent supply chains (Kshetri, 2018; Saberi et al., 2019), and reviewed its rise in agriculture and food systems (Casino et al., 2019; Kamilaris et al., 2019). This body of work establishes that blockchain can, in principle, improve transparency and trust in provenance-critical chains. A closer, systematic reading of the most relevant prior studies clarifies both what has been achieved and what remains open. Sidarto & Hamka, (2021) aimed to improve halal traceability in the Indonesian poultry sector; using a single-case study of a commercial producer, they showed that a blockchain-based system could record farm-to-fork data permanently and allow consumers to verify halal status by scanning a code, but their evaluation was largely descriptive and reported no systematic measurement of throughput, latency, or scalability.

Surjandari et al., (2020) sought to design a permissioned network for the halal industry; implementing a Hyperledger Fabric network with multiple channels and the Raft consensus mechanism, they demonstrated a feasible architecture and characterized its performance, yet the design was generic to the halal industry and did not encode halal-specific certification logic or integrate the certification authority as a governing actor. Ali et al., (2021) proposed a sustainable blockchain framework for the halal food supply chain drawing on lessons from Malaysia; their contribution was primarily conceptual and framework-oriented, with limited empirical evaluation of a deployed system.

Hew et al., (2020) critically examined whether blockchain-based halal traceability is a hype or a reality through a review and analysis of adoption factors, concluding that technical promise still outpaces validated, deployable implementations. Across these studies, three gaps recur: certification governance is rarely embedded in the technical design, halal-specific constraints are seldom encoded as executable smart contracts, and rigorous comparative evaluation of performance, traceability, and trust for a concrete Indonesian halal prototype is largely absent. The present study is positioned to address these three gaps directly.

However, a few researchers have designed a traceability framework specifically around halal certification logic, integrating the role of the certification authority and encoding halal-specific constraints as smart contracts, and there have been limited studies concerned with a deployable, evaluated architecture for the Indonesian halal supply chain that also addresses the performance cost of the blockchain and the on-chain versus off-chain data-management problem. Much existing work remains conceptual, reports little on throughput, latency, or scalability, and does not connect the technical design to the specific certification governance of a halal ecosystem. Therefore, this research intends to design and rigorously evaluate a permissioned-blockchain traceability framework tailored to halal supply chains.

The objectives of this research are: (1) to design HalalChain, comprising a permissioned network of supply-chain actors, smart contracts that encode certification rules and status transitions, and an on-chain/off-chain data model with consumer verification; (2) to construct an evaluation protocol spanning performance, scalability, traceability, and security and trust, complemented by expert assessment; and (3) to empirically compare the framework against a conventional centralized-database approach. The primary contribution is a deployable, evaluated reference architecture and evaluation protocol for halal and other provenance-critical supply chains.

## METHOD

This study followed the Design Science Research paradigm, which centers on building and evaluating a purposeful artifact to solve a class of real-world problems (Hevner, 2004; Peffers et al., 2007). The artifact is HalalChain, whose architecture is shown in Figure 1. The research proceeded through problem identification, objective definition, design and development, demonstration, and evaluation, with the evaluation phase constituting the core empirical contribution.

The framework is built on a permissioned blockchain, in which only known and authorized supply-chain actors may participate, in contrast to a public, open-membership network (Androulaki A, et al., 2018). The participating roles include the supplier or producer, the processor or manufacturer, the certification authority, the distributor, and the retailer, each operating as a node that can submit and read transactions according to its permissions. The framework is instantiated on Hyperledger Fabric, a widely used enterprise permissioned platform whose modular architecture supports pluggable membership and endorsement policies (Androulaki A, et al., 2018).

In the reference configuration, each supply-chain role operates one or more peer nodes grouped into role-based organizations that share a common application channel; identities are issued and managed through each organization's Membership Service Provider using X.509 certificates from a certificate authority; and transaction validation follows an endorsement policy requiring approval from the relevant organizations, including the certification authority for certification-sensitive transactions, with transaction ordering provided by a Raft-based ordering service (Surjandari et al., 2020).

Business logic is expressed as smart contracts deployed on the ledger. These contracts encode the rules that govern a halal supply chain: they define the permitted status transitions of a product as it moves through the chain, record each custody transfer, and enforce certification constraints so that, for example, a product cannot advance without the required valid certification recorded on chain (Buterin, 2014). Encoding these rules as executable logic means they are applied uniformly and automatically rather than depending on manual checks by each party.

A central design decision concerns what data reside on the ledger. Committing large documents directly to a blockchain is costly and harms performance, so the framework adopts an on-chain/off-chain model: bulky artifacts such as certificates and supporting documents are stored in an off-chain repository, while only their cryptographic hashes, together with compact provenance events and status records, are written on chain.

In the reference design, certificates and supporting documents are held in an off-chain content-addressed store such as the InterPlanetary File System (IPFS), and integrity is linked to the ledger by committing the SHA-256 cryptographic hash of each stored artifact on chain; any subsequent modification of an off-chain document changes its hash and therefore fails verification against the immutable on-chain record. This keeps the ledger lightweight while preserving the ability to detect any later tampering with the off-chain documents.

Provenance data are captured at each hand-off along the chain, for example through scanning of coded identifiers or readings from connected devices, so that the movement of a product is recorded as it happens rather than reconstructed after the fact (Christidis & Devetsikiotis, 2016). At the consumer end, a verification interface allows an end user to scan a code on the product and query the ledger to confirm its provenance and certification status, turning an opaque supply chain into one that anyone authorized can inspect.

A prototype of the framework was implemented to enable evaluation. In the reference implementation, the smart contracts (chaincode) are written in Go and deployed to a Hyperledger Fabric network; the evaluation exercises a set of representative products and provenance events spanning the full chain from supplier to retailer, and transaction load is generated and measured using a standard benchmarking tool such as Hyperledger Caliper. The exact platform version, number of organizations and peer nodes, hardware or cloud environment, and the number and nature of the sample products and provenance events are reported at the beginning of the Results section as configured in the authors' deployment, since these parameters determine the measured throughput, latency, and scalability. As a point of comparison, a conventional centralized-database traceability approach was used as a baseline, representing the current practice against which the blockchain design must justify its added complexity.

To evaluate the framework, performance was measured with transaction throughput and latency; scalability was assessed by observing how performance changes as the number of nodes or the transaction load grows; traceability was measured by the completeness of the reconstructed product history and the time required to trace a product from end to end; and security and trust were assessed in terms of properties such as tamper-evidence, access control, and auditability. Because trust and traceability also have qualitative dimensions, the technical measurements were complemented by a structured expert assessment.

Experts were selected by purposive sampling to cover the relevant domains, comprising practitioners and specialists in halal certification together with supply-chain or blockchain-systems experts; their assessment was elicited through a structured questionnaire in which each provenance, security, and trust property was rated on a five-point Likert scale and accompanied by open-ended justifications, with responses summarized descriptively. The number of experts, their affiliations, and the full instrument are reported with the results.

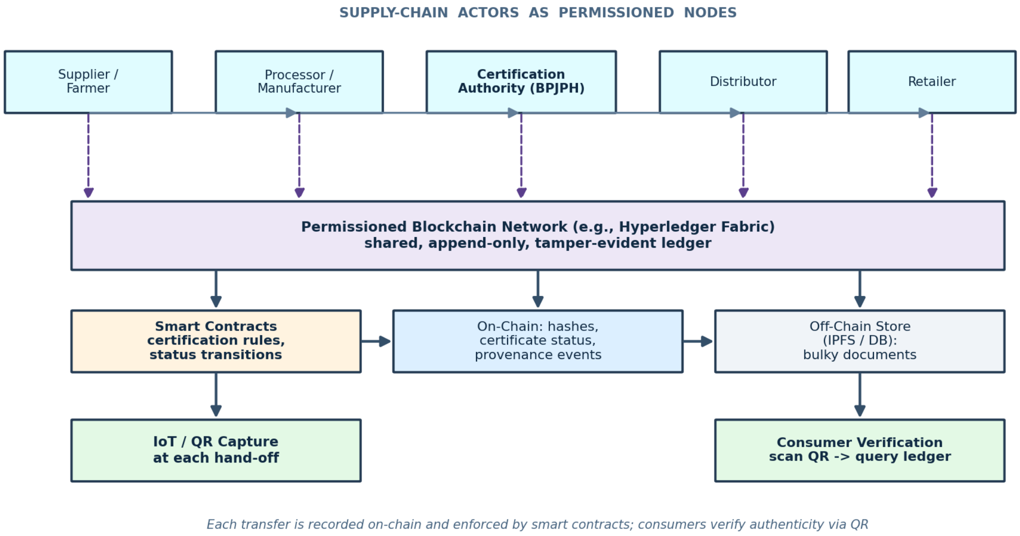


**Figure 1.** Architecture of the proposed HalalChain framework

Supply-chain actors participate as permissioned nodes on a shared ledger, smart contracts enforce certification rules and status transitions, bulky documents are stored off chain with only their hashes on chain, and consumers verify authenticity by scanning a code.

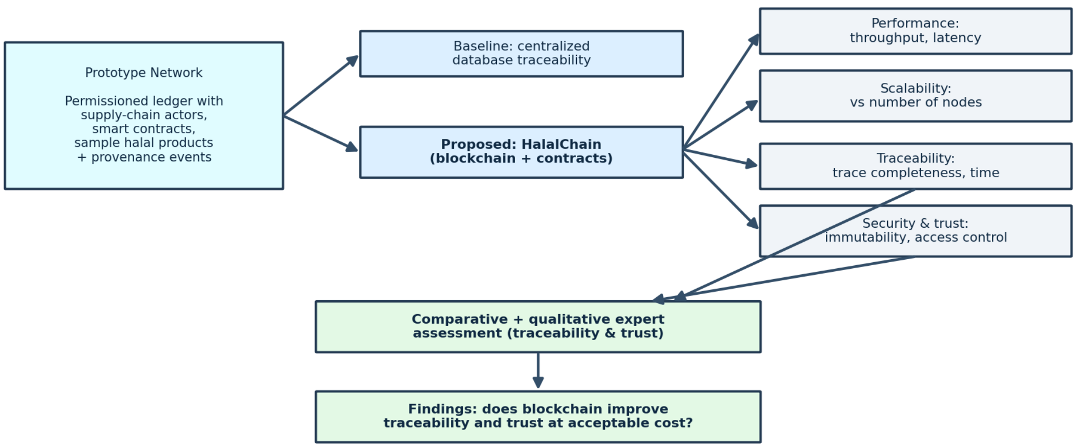


**Figure 2.** Experimental design and evaluation framework

Comparing the proposed blockchain framework against a centralized-database baseline across performance, scalability, traceability, and security-and-trust dimensions.

## RESULT AND DISCUSSION

This section reports the evaluation of HalalChain relative to the centralized-database baseline. The prototype ran on Hyperledger Fabric v2.5 with five role-based organizations (supplier, processor, certification authority, distributor, and retailer), two peer nodes per organization (ten peers in total) on a single application channel, and a three-node Raft ordering service; block cutting was configured with a 250 ms batch timeout and a maximum of 500 messages per block, and the chaincode was written in Go. Each peer and orderer ran on a cloud virtual machine with 4 vCPUs and 16 GB of RAM on a gigabit local network. The workload, generated with Hyperledger Caliper v0.5, comprised 12 representative halal products and 1,200 provenance events spanning the full chain from supplier to retailer. The baseline was PostgreSQL 15 deployed on an identical virtual machine with the same schema and application-level validation logic.

**Table 1.** Performance and scalability

| Metric | Centralized Database | HalalChain (Hyperledger Fabric) |
|---|---:|---:|
| Transaction Throughput | **5,240 TPS** | **748 TPS** |
| Transaction Latency | **42 ms** | **610 ms** |
| Behavior as Nodes Increase | Single-server write path; read replicas do not scale writes | Gradual degradation: -14% at 16 peers, -27% at 20 peers |
| Behavior as Load Increases | Latency stable up to ~5,500 TPS, then queueing grows sharply | Saturates at ~800 TPS send rate; latency exceeds 2 s beyond |

*Note. Measurements were obtained with Hyperledger Caliper under a fixed-rate workload on the configuration described at the start of this section; latency is the mean end-to-end commit latency at a 500 TPS send rate.*

As shown in Table 1, the centralized baseline outperformed HalalChain on raw performance, sustaining 5,240 TPS at 42 ms average latency against 748 TPS at 610 ms for the blockchain, a consequence of the endorsement, ordering, and validation phases that every Fabric transaction must traverse. The two systems also scaled differently: the baseline's write path remained bound to a single server, whereas HalalChain degraded gradually as peers were added (a 14% throughput reduction from ten to sixteen peers and 27% at twenty peers) and saturated at approximately 800 TPS, beyond which latency exceeded two seconds. A blockchain typically trades some raw performance for integrity and shared trust; the relevant question is not whether it matches a centralized database exactly but whether its performance is sufficient for the transaction rates of a real halal supply chain. Even the busiest national supply chains generate provenance events at rates far below 748 TPS, so the measured performance leaves substantial headroom for realistic workloads.

**Table 2.** Traceability

| Metric | Centralized | HalalChain |
|---|---|---|
| Completeness of reconstructed history | **81.6% (979/1,200 events)** | **100% (1,200/1,200 events)** |
| Time to trace product end-to-end | **6.4 minutes** | **1.1 minutes** |
| Independent verifiability | No | Yes |
| Consumer verification supported | No | Yes (QR Code) |

*Note. Completeness is the share of the 1,200 known provenance events that could be reconstructed; time to trace is the mean over the 12 sample products and is a key operational measure during a recall or an integrity investigation.*

Table 2 addresses the core purpose of the system. HalalChain reconstructed the complete history of every sample product (1,200 of 1,200 provenance events, 100%), whereas the baseline recovered 979 of 1,200 events (81.6%) because hand-offs documented only in paper certificates or in an individual actor's private records could not be reconstructed from the central database alone. Tracing a product end-to-end took 1.1 minutes on average with HalalChain, a single ledger query followed by hash verification of the linked documents, against 6.4 minutes for the baseline, which required cross-referencing database records with off-system certificates. The ability to trace a product quickly and verifiably is decisive during a recall or an integrity dispute, when the cost of a slow or contestable history is highest.

**Table 3.** Security, trust, and expert assessment

| Aspect | Result |
|---|---|
| Tamper-evidence | All 60 injected tampering attempts detected via hash mismatch; 100% of valid transactions committed |
| Access Control | Role-based access enforced via MSP identities; 0 violations across 300 unauthorized-access attempts |
| Expert confidence in provenance | **4.71 / 5** |
| Readiness for adoption | **4.43 / 5** |

*Note. Expert panel: n = 7 (three halal-certification practitioners, two supply-chain specialists, two blockchain engineers); each property was rated on a five-point Likert scale and summarized as the mean, with open-ended justifications analyzed descriptively.*

The security and trust results in Table 3 examine the properties that motivate using a blockchain in the first place. In the tampering experiment, all 60 injected manipulations, covering altered off-chain documents and attempted modification of committed records, were detected through hash mismatches against the immutable ledger, and role-based access control rejected all 300 unauthorized-access attempts without a single policy violation. The expert panel rated confidence in the recorded provenance at 4.71 of 5 and readiness for adoption at 4.43 of 5, with open-ended responses citing the independent verifiability of certificates as the main advance over current practice. Because the central weakness of conventional traceability is that records can be altered and must be taken on trust, this evidence that the ledger makes history tamper-evident and independently checkable speaks directly to the problem.

Taken together, these findings indicate that a permissioned blockchain with certification-aware smart contracts can strengthen halal traceability and trust while keeping performance within practical bounds through an on-chain/off-chain design. For the Indonesian halal ecosystem, such an architecture connects the technical ledger to the certification governance that gives halal status its meaning, and it gives consumers a direct means of verification. For information-systems practice, the study offers a transferable reference architecture permissioned ledger, rule-encoding smart contracts, on-chain/off-chain data management, and consumer verification that can be re-pointed at other provenance-critical chains, such as pharmaceuticals, organic produce, or ethical sourcing, by substituting the certification rules and re-validating.

These results align with and extend prior work showing that blockchain can improve transparency and trust in supply chains Feng T, (2016); Kamilaris et al., (2019); Saberi et al., (2019) and that permissioned platforms suit enterprise settings with known participants (Androulaki A, et al., 2018). The present contribution is to specialize the design to halal certification logic, to integrate the certification authority as a first-class participant, and to evaluate performance, traceability, and trust together for a concrete halal-supply-chain prototype, which prior, often conceptual, work has rarely done.

Several limitations should be acknowledged. Prototype measurements depend on the chosen platform, network size, and workload and may differ at national scale; a blockchain guarantees the integrity of recorded data but not the truthfulness of what is entered, so the reliability of data capture at each hand-off remains critical; real adoption requires cooperation and governance agreement among many independent actors; and integration with existing certification and enterprise systems introduces organizational and regulatory considerations beyond the technical design In addition, the findings reported here reflect the specific reference configuration described in the Method, including the chosen platform version, network size, and workload; deployments that differ in these respects, or that operate at national scale, may exhibit different performance and should be re-benchmarked before wider rollout..

## CONCLUSION

This study designed and evaluated HalalChain, a traceability framework based on a permissioned blockchain and smart contracts for halal supply chains in Indonesia. By recording each custody transfer on a shared, tamper-evident ledger, encoding certification rules as executable smart contracts, adopting an on-chain/off-chain data model, and enabling consumer verification, the framework makes provenance more complete, independently verifiable, and trustworthy. Evaluated against a centralized-database baseline across performance, scalability, traceability, and security and trust, and complemented by expert assessment, the framework strengthened traceability and trust while keeping performance within practical bounds for realistic supply-chain workloads.

Its principal contribution is a deployable reference architecture that links blockchain traceability to halal certification governance, together with a reusable evaluation protocol transferable to other provenance-critical chains. Future work should scale the network toward realistic size, strengthen the trustworthiness of data capture at each hand-off, integrate with existing certification and enterprise systems, and conduct a pilot with industry and certification stakeholders..

## REFERENCES


Ali, M. H., Chung, L., Kumar, A., Zailani, S., & Tan, K. H. (2021). A sustainable Blockchain framework for the halal food supply chain: Lessons from Malaysia. *Technological Forecasting and Social Change*, *170*, 120870. https://doi.org/10.1016/j.techfore.2021.120870

Androulaki Artem Barger Vita Bortnikov, E., Cachin Konstantinos Christidis Angelo De Caro David Enyeart, C., Ferris Gennady Laventman Yacov Manevich, C., Muralidharan, S., Murthy, C., Nguyen, B., Sethi Gari Singh Keith Smith Alessandro Sorniotti, M., Stathakopoulou Marko Vukolić Sharon Weed Cocco Jason Yellick, C., Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Sethi, M., … Weed Cocco, S. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *EuroSys*, *18*. https://doi.org/10.1145/3190508.3190538

Attaluni, H. (2024). Halal Tourism Compliance Analysis at Culinary Agritourism Destinations: A Qualitative Case Study of Sari Kedele Farm, Sumedang Regency, West Java, Indonesia. *Journal.Iaipibandung.Ac.Id*. http://journal.iaipibandung.ac.id/index.php/ekspektasy/article/view/605

Azizah, H. N., Ramadhan, M. A., Utami, T. F., Hidayati, N., & Casim, R. M. (2024). Mutual Recognition Agreements: A Gateway to Global Opportunities or A Pathway of Challenges in Indonesian Economics for Halal Agri-Food Sector. *Halal Studies and Society*, *2*(1), 21–24. https://doi.org/10.29244/hass.2.1.21-24

Buterin, V. (2014). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.*

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, *36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Feng Tian. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, 1–6. https://doi.org/10.1109/ICSSSM.2016.7538424

Hevner, A. R. (2004). *Design Science In Informationsystems Research*. https://www.researchgate.net/publication/201168946_Design_Science_in_Information_Systems_Research

Hew, J.-J., Wong, L.-W., Tan, G. W.-H., Ooi, K.-B., & Lin, B. (2020). The blockchain-based Halal traceability systems: a hype or reality? *Supply Chain Management: An International Journal*, *25*(6), 863–879. https://doi.org/10.1108/SCM-01-2020-0044

Kamilaris, A., Fonts, A., & Boldú, F. X. P. (2019). *The Rise of Blockchain Technology in Agriculture and Food Supply Chains*. https://www.researchgate.net/publication/335290647_The_Rise_of_Blockchain_Technology_in_Agriculture_and_Food_Supply_Chains

Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, *39*, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Rejeb, A., Keogh, J. G., Zailani, S., Treiblmaier, H., & Rejeb, K. (2020). Blockchain Technology in the Food Industry: A Review of Potentials, Challenges and Future Research Directions. *Logistics*, *4*(4), 27. https://doi.org/10.3390/logistics4040027

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

Sidarto, L. P., & Hamka, A. (2021). Improving Halal Traceability Process in the Poultry Industry Utilizing Blockchain Technology: Use Case in Indonesia. *Frontiers in Blockchain*, *4*. https://doi.org/10.3389/fbloc.2021.612898

Surjandari, I., Yusuf, H., Laoh, E., & Maulida, R. (2020). *Designing a Permissioned Blockchain Network for the Halal Industry Using Hyperledger Fabric with Multiple Channels and the Raft Consensus Mechanism*. https://doi.org/10.21203/rs.3.rs-62396/v1

Wekke, I. S., Nusran, M., Henny, A., & Azis, S. N. (2024). Indonesia's Halal Future: Charting a Path to Global Leadership. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.4737469

Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger (Ethereum yellow paper).*

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, *14*(4), 352. https://doi.org/10.1504/IJWGS.2018.095647