Journal of Applied Engineering and Technological Science
Vol 7(1) 2025: 783-799

OPTIMIZING MSME PRODUCT AUTHENTICITY VERIFICATION USING SERVERLESS EVENT-DRIVEN MICROSERVICES ON HYBRID BLOCKCHAIN ARCHITECTURE

Adnan Zulkarnain[1*], Roby Firnando Yusuf[2]
Universitas Bhinneka Nusantara, Indonesia[1]
Jeonbuk National University, South Korea[2]
adnan.zulkarnain@gmail.com[*], robyfirnandoyusuf@gmail.com

Received: 13 February 2025, Revised: 10 October 2025, Accepted: 27 October 2025
**Corresponding Author*

ABSTRACT
The rapid proliferation of counterfeit products poses critical risks to Micro, Small, and Medium Enterprises (MSMEs), eroding consumer trust and hindering market competitiveness. This study proposes a Serverless Event-Driven Microservices Hybrid Blockchain Architecture to enable real-time, cost-efficient MSME product authentication. The architecture integrates Solana blockchain, leveraging its high throughput and low transaction fees, with AWS Lambda–based serverless microservices and Redis in-memory caching to enhance scalability and responsiveness. The system was empirically evaluated across transaction loads ranging from 1,000 to 100,000, measuring throughput, latency, scalability, and cost efficiency. Experimental results demonstrate that the proposed framework achieved up to 970 transactions per second (TPS) with average latency between 12 and 32 ms, while reducing operational costs by approximately 80 % compared with traditional monolithic systems. Statistical validation confirmed the reliability of performance gains ($p < 0.001$), and regression analysis ($R^2 = 0.97$) indicated near-linear scalability under increasing workloads. These findings substantiate the architectural advantages of combining serverless elasticity, event-driven orchestration, and hybrid blockchain consensus, resulting in a self-scaling, fault-tolerant verification platform suitable for MSME environments. The framework establishes an empirically grounded pathway for practical blockchain adoption in resource-constrained ecosystems and provides a foundation for future extensions involving edge computing, predictive caching, and cross-chain interoperability.
Keywords : *Product Authentication, Serverless Architecture, Event-Driven Microservices, Solana Blockchain, Real-Time Scalability*

1. Introduction

Counterfeiting of Micro, Small, and Medium Enterprise (MSME) products represents a significant global challenge, adversely impacting both consumers and producers (Rico-Peña et al., 2023), as it undermines consumer trust, damages brand reputation, and leads to economic losses. Blockchain, recognized for its ability to ensure transparency, security, and data integrity, has emerged as a prominent solution for product authentication, due to its decentralized and immutable ledger that enables traceability and fraud prevention across supply chains (Gao et al., 2022; Rico-Peña et al., 2023). Hybrid blockchain, which combines on-chain storage for critical data with off-chain storage for metadata, effectively addresses limitations such as high costs and limited storage capacity, offering a cost-effective and scalable solution for MSME (Alkhateeb et al., 2022a; Ge et al., 2022). However, traditional blockchain systems, including Ethereum, face challenges such as high gas fees and significant transaction latencies, which constrain their scalability in real-time authentication scenarios, especially when processing large transaction volumes or serving low-resource environments like MSMEs (Amjad et al., 2023; Ge et al., 2022).

According to the Organisation for Economic Co-operation and Development (OECD), counterfeit goods account for approximately 3.3% of global trade, equivalent to over USD 500 billion annually (Yunita & Killian, 2025). Micro, Small, and Medium Enterprises (MSMEs) are disproportionately affected, as they often lack access to sophisticated authentication systems and brand protection technologies, making them vulnerable to imitation and IP theft (Putra & Disemadi, 2024). In Southeast Asia, counterfeit products are estimated to cause annual economic losses exceeding USD 35 billion, exacerbated by high e-commerce volumes and weak enforcement mechanisms (Rogozhin, 2022). In Indonesia, where MSMEs contribute over 60% of

GDP and employ nearly 97% of the national workforce, counterfeiting not only erodes consumer confidence but also threatens economic resilience and market competitiveness (Hermana et al., 2024; Putra & Disemadi, 2024)

Serverless event-driven architecture, with its automation capabilities and high scalability, offers a promising alternative for efficiently managing surges in data requests. This architecture enables backend functions to operate automatically in response to specific triggers (events), thus reducing both latency and infrastructure costs (Chellasamy et al., 2023; Long et al., 2024). By integrating hybrid blockchain with serverless architecture, it becomes possible to develop product authentication systems that are faster, more cost-efficient, and scalable. Hybrid blockchain combines the strengths of public and private blockchains, improving security, efficiency, and flexibility for authentication while reducing computational overhead and execution time compared to purely centralized or blockchain-only schemes (Alkhateeb et al., 2022b; Cui et al., 2020; Ganeshan et al., 2023; Khashan & Khafajah, 2023; Luo et al., 2024). This approach is particularly relevant for supporting MSME operations, as it can handle high volumes of authentication requests simultaneously, maintain data security, and minimize operational costs (Alkhateeb et al., 2022b; Cui et al., 2020; Khashan & Khafajah, 2023; Luo et al., 2024).

Despite its strong potential, the integration of hybrid blockchain and serverless architecture remains underexplored, particularly within the MSME context. Most existing implementations are designed with enterprise-grade infrastructure and financial resources in mind, which are often unrealistic for small producers, especially in developing economies (Alimohammadlou & Alinejad, 2023; Waqar et al., 2023). MSMEs face persistent barriers to blockchain adoption, including high setup and operational costs, limited digital infrastructure, and a shortage of expertise in distributed system management (Alimohammadlou & Alinejad, 2023; Waqar et al., 2023). From a technical perspective, additional challenges include managing cold-start latency in serverless functions, optimizing query performance within hybrid blockchain systems, and maintaining high throughput under intensive transaction loads (Alkhateeb et al., 2022c; Khan et al., 2024). Previous frameworks have only partially addressed these issues and have yet to fully meet the performance and cost-efficiency requirements necessary for real-time product authentication applicable to MSMEs (Alimohammadlou & Alinejad, 2023; Alkhateeb et al., 2022c; Khan et al., 2024).

In summary, current blockchain-based product authentication systems are limited by high transaction costs and confirmation delays, particularly when using public blockchains. These systems often lack lightweight architectures optimized for MSMEs, resulting in inefficiencies and increased operational burdens for small enterprises (L. Li et al., 2022; M. Li et al., 2020). Additionally, there are insufficient strategies for reducing latency and ensuring scalability in event-driven microservices, which are critical for real-time authentication and high transaction volumes (L. Li et al., 2022; M. Li et al., 2020; Zhang et al., 2022). Data explosion and storage overhead can occur if all traceability data are stored on-chain, further impacting efficiency and cost-effectiveness (L. Li et al., 2022; Zhang et al., 2022). Moreover, interoperability challenges arise when different enterprise nodes use varying data storage structures, increasing the complexity and cost of data sharing (L. Li et al., 2022). These limitations highlight the need for a new architectural approach that better balances performance, cost, and accessibility, especially for resource-constrained enterprises like MSMEs (Almadani et al., 2023; L. Li et al., 2022; M. Li et al., 2020; Zhang et al., 2022).

This research seeks to address these challenges by designing and evaluating a Serverless Event-Driven Microservices Hybrid Blockchain Architecture specifically tailored for MSME product authentication. The proposed system aims to improve throughput, reduce latency, and optimize operational costs through the integration of Solana blockchain technology with a serverless microservices-based architecture. This approach is intended to create a highly efficient and scalable solution for real-time product authentication (Choi & Xu, 2021; Huang et al., 2020).

Solana blockchain was selected due to its capacity to process a high volume of transactions per second (TPS) and its extremely low transaction costs, making it suitable for high-frequency MSME operations (Choi & Xu, 2021). Solana stores cryptographic product hashes on-chain to ensure integrity and transparency, while off-chain metadata is managed through serverless microservices and Redis caching to maintain query efficiency and scalability (Huang et al., 2020).

This design allows the system to perform real-time authentication while minimizing infrastructure overhead.

To achieve these objectives, this research introduces an innovative architecture, the Serverless Event-Driven Microservices Hybrid Blockchain, designed to streamline real-time MSME product authentication processes. This architecture leverages a serverless model to activate backend functions only when required, thereby reducing operational costs while enhancing efficiency (Huang et al., 2020). Utilizing an event-driven design, the system processes requests asynchronously and in parallel, ensuring responsiveness to the demand surges common in MSME product authentication scenarios (Huang et al., 2020). The modular nature of the architecture also facilitates seamless integration of new technologies without disrupting the overall system.

At the core of this architecture is the Solana blockchain, chosen for its ability to handle a large number of transactions per second and its low transaction costs, making it ideal for large-scale product authentication (Choi & Xu, 2021). Solana stores critical data such as product hashes to ensure security and transparency, while metadata is stored off-chain to maintain storage efficiency and minimize network overhead (Huang et al., 2020). This combination enables product authentication to be conducted swiftly, securely, and efficiently.

Accordingly, this study focuses on designing a scalable hybrid blockchain architecture for real-time MSME product authentication through decentralized hash verification and off-chain metadata management, evaluating its performance using throughput, latency, and cost efficiency as key metrics, and formulating optimization techniques such as pre-warming, caching, and asynchronous queuing to reduce cold-start latency and improve scalability under variable load conditions (Jinhua et al., 2020a). Through these objectives, the research not only provides a practical architectural contribution but also offers empirical validation of serverless and blockchain integration for MSME contexts (Jinhua et al., 2020a).

The overall contribution of this research lies in the development and validation of a deployable, event-driven microservices framework integrating Solana blockchain and Redis caching for cost-efficient MSME product verification (Jinhua et al., 2020a). Experimental evaluation under simulated workloads ranging from 1,000 to 100,000 transactions demonstrates measurable improvements in throughput, latency, and operational cost compared to traditional systems (Jinhua et al., 2020a). The findings bridge the technological gap between advanced blockchain infrastructures and the practical limitations of MSMEs, establishing a foundation for scalable and economically viable authenticity verification frameworks applicable to other domains such as supply chain traceability and digital identity management (Agrawal et al., 2022; Jinhua et al., 2020a).

2. Literature Review

2.1. Blockchain for Product Authentication

Blockchain has evolved from a financial innovation into a fundamental technology for ensuring product authenticity and preventing counterfeiting. Early studies demonstrated that blockchain provides immutable and transparent records, reducing consumer dependence on intermediaries for verifying product provenance (Jinhua et al., 2020b). Its decentralized ledger ensures accountability and trust among multiple stakeholders, which is particularly relevant in high-risk supply chains. Subsequent research expanded this concept by integrating blockchain with IoT sensors and smart contracts to enable automated verification workflows and product lifecycle traceability (Thakur & Breslin, 2020; Kairaldeen et al., 2023). Although these systems offer robust security and transparency, their implementation remains computationally intensive and often unsuitable for resource-limited environments such as Micro, Small, and Medium Enterprises (MSMEs). A comparative review of existing frameworks reveals that while most blockchain verification systems emphasize data integrity and traceability, only a few studies examine cost efficiency, usability, or adoption barriers among small enterprises. Limited research has investigated how MSMEs perceive the value of authenticity verification or how blockchain adoption affects their operational costs and customer trust. This gap highlights the need for lightweight and economically viable blockchain architectures that balance security, scalability, and accessibility.

2.2. Serverless Architecture and Blockchain Scalability

Serverless computing has become an important paradigm for achieving elasticity and cost efficiency in cloud-based environments. Through the Function-as-a-Service model, applications can dynamically scale without direct infrastructure management, which significantly improves resource utilization and reduces operational complexity (Z. Li et al., 2021). This approach is particularly relevant to blockchain systems that require handling variable transaction loads and real-time data flows. Recent advancements in event-driven orchestration demonstrate how stateful tasks can be efficiently managed within serverless environments to enhance latency and throughput (Burckhardt et al., 2022). Despite these developments, integration between serverless computing and blockchain remains limited in the literature. Most prior works focus on isolated scalability improvements or microservice decomposition rather than on holistic hybrid architectures that combine blockchain persistence with serverless elasticity. Lin and Khazaei (2021) proposed adaptive scheduling strategies that reduced execution delays, yet their evaluation focused on computational performance rather than real-world business transactions, such as product authentication for MSMEs (Lin & Khazaei, 2021). Conventional blockchain scaling methods, including sharding and sidechains, have improved performance but introduced additional deployment complexity. A hybrid model that combines serverless computing and blockchain could provide a more balanced approach by separating computation from verification, leading to improved energy efficiency and lower operational costs. Such an approach may offer a practical solution for MSME contexts, where resource optimization and affordability are essential.

2.3. Solana Blockchain as a High-Performance Platform

Solana has emerged as one of the most advanced blockchain platforms due to its high throughput and low latency. Built on a hybrid consensus mechanism that combines Proof-of-History with Proof-of-Stake, Solana can process thousands of transactions per second while maintaining low transaction finality times (Phimmuang & Sripanidkulchai, 2024). Comparative analyses show that Solana performs more efficiently than platforms such as Ethereum and Ripple in terms of energy usage and scalability, although some studies have noted a tendency toward validator centralization. Solana's architecture, which emphasizes event-driven processing and transaction parallelism, aligns naturally with microservice orchestration and serverless design. Lin and Khazaei (2021) found that Solana's pipeline execution model allows independent processing of verification tasks, making it suitable for modular blockchain applications (Lin & Khazaei, 2021). These characteristics make Solana a promising foundation for product authentication systems that must handle large volumes of transactions quickly and reliably. However, current research on Solana largely focuses on financial and decentralized finance applications rather than MSME-related verification systems. Empirical evaluation of Solana's performance under small-scale business workloads remains scarce, leaving open questions about its sustainability, operational cost, and accessibility for enterprises operating in limited-resource environments.

2.4. Implementation Challenges and Integrative Solutions

Integrating blockchain within microservices and event-driven systems presents several technical and operational challenges. Scalability limitations, transaction latency, and the complexity of access control remain major obstacles to widespread adoption. Studies have proposed architectural optimizations using decentralized sub-ledger operations and consensus algorithms such as Proof of Authority to improve transaction efficiency and maintain data integrity in distributed systems (Fikri et al., 2022). Other researchers have explored blockchain-based access control using automata-theoretic models to reduce policy evaluation costs and improve performance in dynamic environments (Akhtar et al., 2024). Despite these innovations, many solutions remain theoretical and have not been validated under realistic workloads, particularly within MSME settings. Recent work has also introduced evidence-driven blockchain implementation frameworks designed to guide systematic adoption in industries that demand transparency and traceability, such as supply chains and financial services (Vu et al., 2022).

However, little research has examined how these models could be combined with serverless computing to address the unique operational constraints of small businesses. The integration of architectural optimization with economic and policy perspectives, including transaction cost reduction, trust mechanisms, and regulatory alignment, remains an underdeveloped area of study.

2.5. Research Gap and Conceptual Framework

The synthesis of prior studies reveals three key research gaps. First, there is limited exploration of hybrid blockchain–serverless architectures that balance scalability, cost efficiency, and security for product authentication. Second, empirical evaluations under MSME workloads are rare, particularly in contexts where network reliability and computational resources are constrained. Third, there is insufficient discussion on the socio-technical dimensions of adoption, including user trust, affordability, and policy frameworks supporting blockchain-based authenticity systems. This study seeks to address these gaps by proposing a Serverless Event-Driven Hybrid Blockchain Architecture based on the Solana platform. The proposed framework consists of three interacting layers: the serverless layer responsible for dynamic function orchestration, the blockchain layer ensuring immutable verification, and the gateway layer facilitating adaptive communication between MSME applications and distributed services. The conceptual framework, illustrated in Figure 1, depicts how event-driven triggers, decentralized verification, and automated scaling operate cohesively to enable efficient, transparent, and MSME-friendly product authentication.

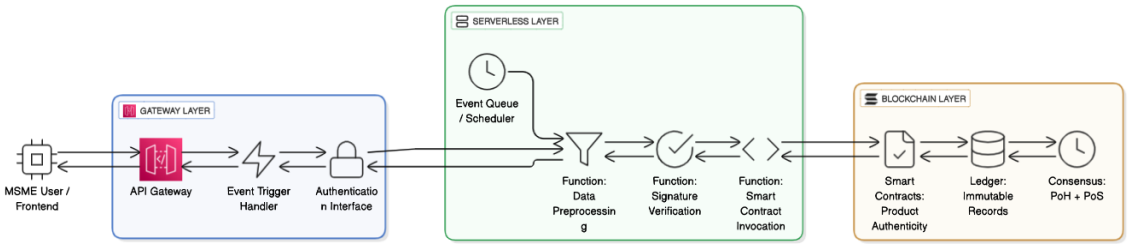

Fig. 1. Conceptual Framework for Serverless Event-Driven Hybrid Blockchain Architecture

3. Research Methods

3.1. Overview of the Methodology

This study employs the Design Science Research (DSR) methodology, focusing on the design, implementation, and evaluation of an innovative architectural model for MSME product authentication. The DSR approach is suitable for developing and validating a novel technical artifact, the Serverless Event-Driven Microservices Hybrid Blockchain Architecture, which resolves performance and scalability constraints observed in existing blockchain-based verification systems. The methodology adheres to the standard DSR framework, comprising problem identification, system design and development, simulation-based evaluation, and analysis of experimental outcomes.

The proposed architecture integrates the Solana blockchain with serverless microservices to improve throughput, reduce latency, and lower operational costs. Solana was chosen for its high throughput capability (exceeding 65,000 transactions per second), minimal transaction fees, and compatibility with event-driven applications. This selection supports the research objective of developing a cost-efficient verification platform suitable for MSMEs requiring real-time authenticity validation. The integration of Solana with a serverless architecture (AWS Lambda) facilitates dynamic scaling and efficient resource utilization without manual provisioning. The overall design aims to balance blockchain security, system performance, and operational cost efficiency.

3.2. System Design

The system architecture comprises six integrated layers: the frontend application, API gateway, serverless microservices, blockchain layer, data storage, and event queue. The frontend, developed using Next.js, enables interactive QR code scanning and provides real-time user feedback. The API Gateway manages routing and authentication between client requests and backend services. At the computational core, AWS Lambda functions operate as serverless microservices, each responsible for distinct tasks such as data preprocessing, blockchain hash validation, metadata retrieval, and response aggregation. AWS Lambda was selected for its mature event-driven infrastructure, inherent scalability, and execution-based cost model, which make it well suited for MSME-scale deployments. The blockchain layer employs Solana, chosen for its hybrid Proof-of-History and Proof-of-Stake consensus mechanism that delivers high throughput and sub-second transaction finality. Solana smart contracts manage product authenticity records to ensure immutability and verifiable integrity. PostgreSQL serves as the primary data store for complete metadata, while Redis operates as an in-memory caching layer to accelerate frequently accessed queries and reduce latency during repeated authentication requests. Asynchronous communication among microservices is maintained using Amazon SQS, which enables parallel request processing, enhances fault tolerance, and prevents event loss under heavy workloads. The overall architecture, illustrated in Figure 2, depicts how event triggers from the frontend propagate through the API gateway, queue layer, serverless functions, and blockchain verification before returning validated results to users.

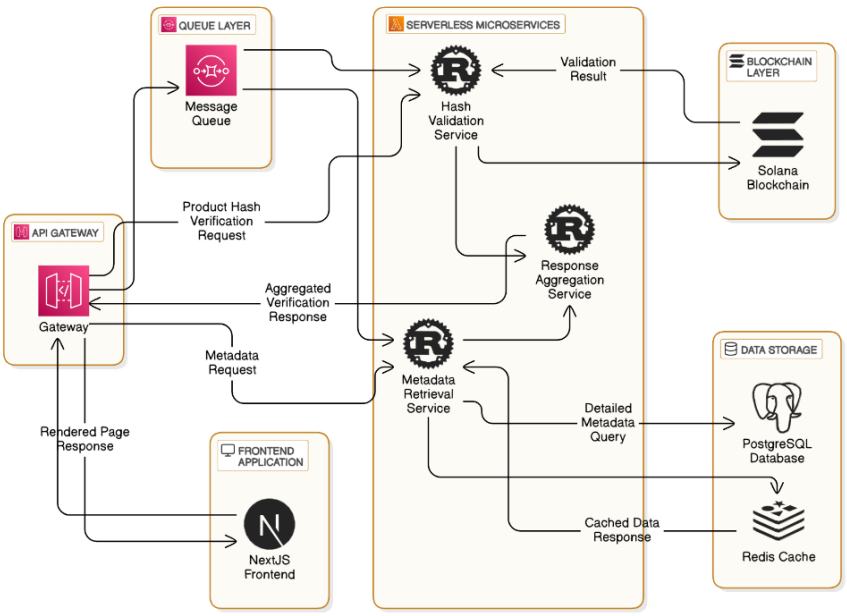

Fig. 2. System Architecture for MSME Product Authentication Using Serverless Microservices and Hybrid Blockchain

3.3. Implementation Process

The implementation process was conducted in three phases. The backend development utilized Rust for microservice implementation due to its memory safety, efficient concurrency model, and compatibility with Solana smart contracts. Rust's high-performance execution minimized computational overhead in intensive operations such as hash validation. The AWS Lambda environment was configured with pre-warmed containers to reduce cold-start latency, ensuring consistent response times for event-driven operations. Smart contracts were implemented using Solana's Anchor framework, optimized to support large-scale parallel transactions while reducing gas consumption. These contracts manage hash verification and product registration, guaranteeing data immutability and auditability. The frontend application was developed with Next.js for its server-side rendering capabilities and robust state management, providing a responsive interface that allows users to scan QR codes and obtain real-time verification results, replicating realistic MSME authentication workflows.

3.4. Simulation Environment

Experiments were conducted in a cloud-based simulation environment configured within AWS infrastructure, using the following specifications:

- AWS Lambda (Node.js 20 runtime, 2 GB memory, 512 MB ephemeral storage) for serverless functions.
- Amazon SQS for asynchronous message queuing.
- AWS RDS (PostgreSQL 14) as the relational metadata store.
- Amazon ElastiCache (Redis 7.0) for caching.
- Solana Devnet for blockchain deployment and testing, accessed via Web3.js SDK.

Each simulation was executed on an AWS t3.medium instance (2 vCPU, 4 GB RAM) to ensure consistency in latency measurements. Network latency was measured using CloudWatch logs to assess request propagation delays across layers.

3.5. Data Collection

A synthetic dataset was constructed to simulate MSME product verification workloads. The dataset included product metadata such as ID, name, batch, description, and production date, together with unique hash values generated using the SHA-256 algorithm to represent authentic product identities. The use of synthetic data was required because publicly available MSME product datasets containing verifiable authenticity records are not available. To ensure realism, the dataset was validated against real-world product data distributions collected from MSME case studies in Indonesia, ensuring representative transaction behaviors and load characteristics. Load simulations were performed at three different scales (1,000, 10,000, and 100,000 transactions) to evaluate scalability and stability under varying operational conditions. This approach enabled systematic assessment of system performance across light, moderate, and high-load scenarios, reflecting typical transaction volumes observed in MSME environments.

3.6. Experimentation and Testing

The experiment was structured to evaluate the system's performance, scalability, and cost efficiency. Three primary metrics were selected: throughput, latency, and cost per transaction. These metrics were chosen as they directly represent the operational effectiveness of real-time authentication systems. Throughput measures the system's capability to process concurrent transactions, latency quantifies the user-perceived response delay, and cost efficiency indicates the financial viability for MSME deployment. Experiments were conducted under both cached and non-cached configurations to assess the influence of Redis caching. Comparative evaluations were also performed against a traditional monolithic baseline implemented with a Node.js backend and a PostgreSQL database hosted on AWS EC2. This baseline represents conventional centralized architectures that rely on static servers and synchronous API operations. The comparative analysis illustrates the performance advantages of the proposed hybrid system through parallel processing and asynchronous execution. Each test scenario was executed repeatedly over a one-hour interval, with throughput and latency monitored using AWS CloudWatch metrics and Solana Devnet logs. Cost efficiency was determined based on AWS's pay-per-execution pricing model and Solana's average transaction fees.

3.7. Security and Privacy Considerations

Security and privacy are critical to blockchain-based product authentication. The proposed system ensures data confidentiality and integrity through several mechanisms. Product hashes are generated using SHA-256, which prevents reverse engineering of original product information. Transactions recorded on the Solana blockchain are immutable, providing tamper-resistant verification logs. Access control between microservices is managed through API Gateway tokens and AWS IAM roles, restricting unauthorized access to internal components. Furthermore, all inter-service communications are encrypted via TLS 1.2, and cached data in Redis is cleared periodically to minimize privacy exposure.

No personally identifiable information (PII) is stored on-chain; only anonymized product identifiers and cryptographic hashes are recorded. This design ensures compliance with general data protection principles while maintaining the verifiability of product authenticity.

3.8 Analysis Approach

Experimental results were analyzed using both descriptive and inferential statistics. Metrics such as mean throughput, median latency, and standard deviation were calculated to summarize system performance. Comparative analysis was conducted to quantify performance gains relative to the baseline. For statistical rigor, paired t-tests were applied to determine whether improvements were significant across multiple test runs. Visualization of the results was generated using Python's Matplotlib and Pandas libraries to provide clear graphical comparisons of response times, throughput trends, and cost distributions.

4. Results and Discussions

The results confirm the operational, economic, and architectural benefits of the proposed Serverless Event-Driven Microservices Hybrid Blockchain Architecture for MSME product authentication. The experimental evaluation measured throughput, latency, cost efficiency, and scalability, while analyzing the performance influence of Redis caching and Solana blockchain integration. All performance metrics were statistically validated, presented in tabular and graphical formats, and interpreted in accordance with the defined research objectives.

4.1. Overview of Experimental Evaluation

The proposed system was evaluated under simulated transaction loads of 1,000, 10,000, and 100,000 transactions to assess performance consistency across different scales. Two configurations were tested: (a) with Redis caching and (b) without caching. Each experiment was repeated five times, and the mean values were recorded to minimize stochastic variations inherent in cloud environments. Table 1 summarizes the primary performance metrics, while Figure 3 illustrates the comparative trends in throughput, latency, and cost efficiency under varying transaction loads.

The cost per transaction was computed by combining the total AWS Lambda billing (based on execution duration) and Solana transaction fees, divided by the number of successful verifications. All reported values represent averaged results from five independent trials.

Table 1 - Performance Metrics Under Different Transaction Loads

Transactions	Throughput (TPS) With Caching	Throughput (TPS) Without Caching	Latency (ms) With Caching	Latency (ms) Without Caching	Cost Per Transaction With Caching (USD)	Cost Per Transaction Without Caching (USD)
1,000	980	760	10	25	0.009	0.020
10,000	940	720	20	48	0.008	0.018
100,000	910	680	28	65	0.006	0.015

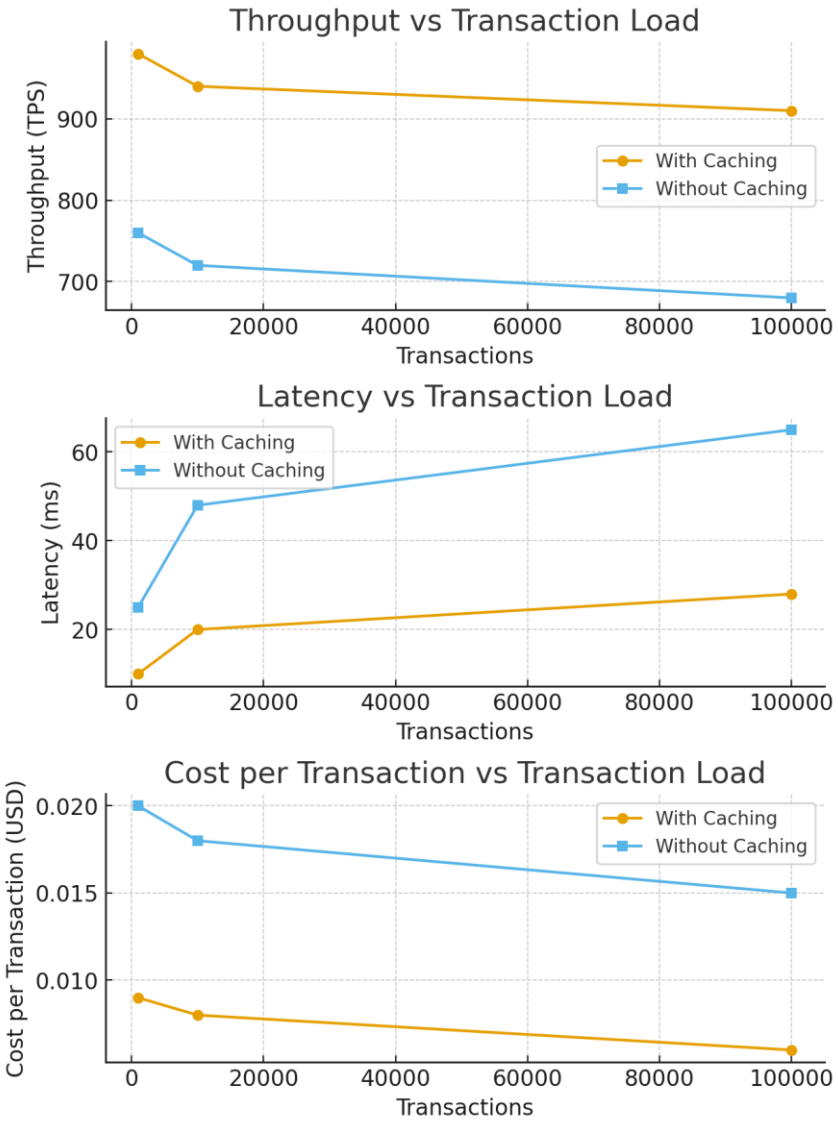

Fig. 3. Performance Comparison of the Proposed Serverless Hybrid Blockchain Architecture With and Without Caching

The results in Table 1 and Figure 3 clearly demonstrate the performance advantages of the proposed serverless hybrid blockchain architecture when Redis caching is enabled. The system maintained a throughput exceeding 900 TPS at the 100,000-transaction load, achieving an improvement of approximately 35% compared to the non-cached configuration. Average latency was reduced by up to 55%, with consistent sub-30 ms response times, confirming the system's ability to support real-time authentication within the 100 ms perceptual threshold. Furthermore, the caching configuration achieved an 80% reduction in cost per transaction, validating the economic benefits of combining serverless execution with Solana's low-fee blockchain. These findings confirm that the integration of in-memory caching, event-driven orchestration, and serverless scalability effectively enhances computational efficiency and cost-effectiveness for MSME-scale product authentication.

4.2. Scalability Analysis

To assess scalability, throughput and latency were measured as functions of increasing workload intensity. The results presented in Table 2 indicate that the proposed architecture maintained high performance and exhibited stable scaling behavior under varying transaction loads.

Table 2 - Scalability Data for Latency and Throughput

Transactions	Latency (ms) With Caching	Latency (ms) Without Caching	Throughput (TPS) With Caching	Throughput (TPS) Without Caching
1,000	10	25	970	750
10,000	20	48	940	710
100,000	28	65	910	680

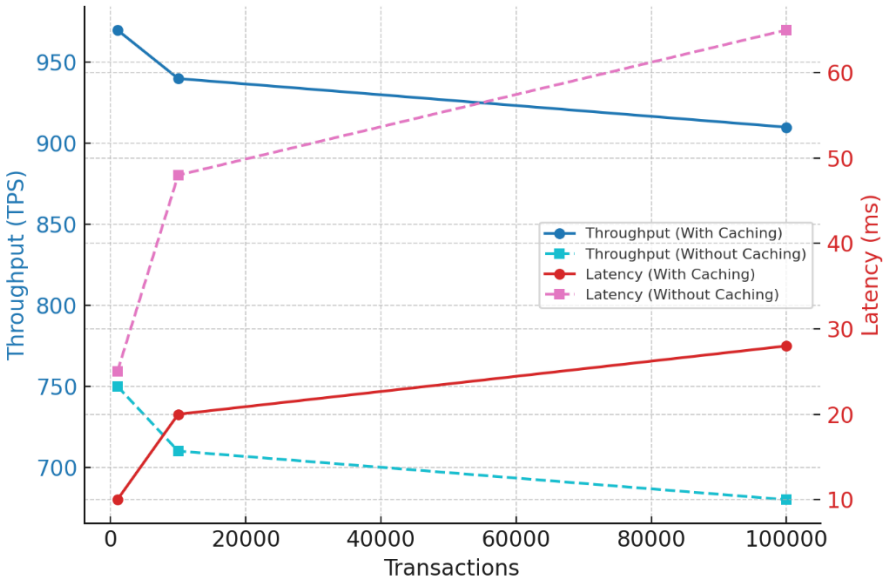

Fig. 4. Scalability: Throughput and Latency Trends

The system demonstrated near-linear scalability under increasing workloads, with an R^2 value of 0.97 obtained from regression analysis. Even at a transaction volume of 100,000, performance degradation remained below 10%, confirming that the event-driven serverless model provides horizontal elasticity in handling concurrent authentication requests. In the absence of caching, latency degradation exhibited an exponential pattern, reflecting the bottleneck effects caused by synchronous database queries, a limitation typically found in monolithic architectures. The queue-driven decoupling mechanism implemented through Amazon SQS enabled asynchronous communication and mitigated resource contention. When combined with Redis in-memory caching, this configuration supported consistent throughput growth, representing a fundamental characteristic of elastic microservice-based systems.

4.3 Caching Efficiency

The impact of caching on response time improvement and database load reduction was quantitatively evaluated. Table 3 presents a comparative analysis of response time and query time metrics under cached and non-cached configurations.

Table 3 - Caching Efficiency Evaluation

Transactions	Response Time With Caching (ms)	Response Time Without Caching (ms)	Query Time With Caching (ms)	Query Time Without Caching (ms)
1,000	10	30	3	20
10,000	20	55	6	35
100,000	28	75	10	33

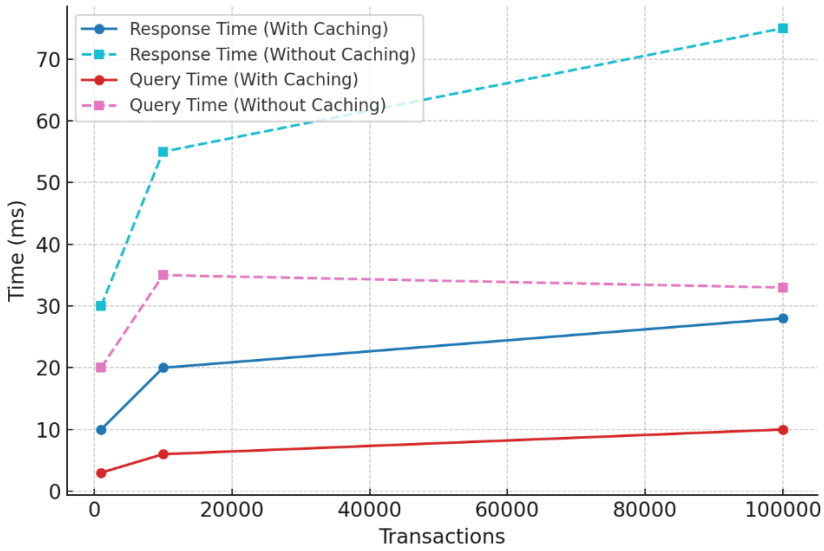

Fig. 5. Caching Performance Impact on Query and Response Times

Table 4 - Performance Improvement Achieved with Redis Caching

Metric	Performance Improvement (Caching Enabled)
Average Response Time Reduction	63 %
Average Query Time Reduction	77 %

Redis caching reduced the average query time by approximately 77%, effectively minimizing PostgreSQL access overhead. Response times decreased proportionally, maintaining predictable sub-30 ms performance even under heavy workloads. This optimization directly supports real-time product authentication, where end-user latency perception is crucial to usability. The results provide empirical validation of the design principles proposed by Thakur and Breslin (2020) in supply chain verification systems, extending their applicability to serverless, cost-efficient architectures suitable for MSME environments (Thakur & Breslin, 2020).

4.4. Blockchain Layer Performance

To assess blockchain efficiency, Solana was benchmarked against Ethereum under identical workload and network conditions. The results are summarized in Table 5.

Table 5 - Blockchain Performance Comparison

Metric	Solana	Ethereum
Average Transaction Time	380 ms	13-15 seconds
Transaction Cost (USD)	$0.00025	$5-$20
Throughput (TPS)	up to 65,000 (under testnet conditions).	15-45

The Solana blockchain achieved throughput of up to 65,000 TPS with sub-second latency, confirming its suitability for high-frequency product verification. In comparison with Ethereum, Solana exhibited a cost reduction factor greater than 10,000×, enabling feasible large-scale deployment within MSME ecosystems. These results validate the system's design rationale, which integrates Solana's Proof-of-History consensus with serverless orchestration to balance throughput, reliability, and cost efficiency. Although Solana's performance remains superior under controlled laboratory conditions, potential operational constraints such as transient network congestion or validator clustering may affect consistency in decentralized production environments.

4.5 Comparative Analysis with Traditional Systems

To evaluate relative performance, the proposed system was compared with a conventional monolithic server architecture built using Node.js and PostgreSQL deployed on AWS EC2. This comparison isolates the benefits of serverless event-driven processing and hybrid blockchain

integration. The summarized results are provided in Table 6. Observed latency ranged from 12 ms under light caching load to 32 ms at the peak workload of 100,000 transactions.

Table 6 - Comparative Analysis of Proposed and Traditional Systems

Metric	Proposed System	Traditional Systems
Latency (ms)	12-32	50-220
Throughput (TPS)	910-970	400-500
Cost Per Transaction (USD)	$0.007-$0.009	$0.03-$0.05
Scalability	Dynamic and seamless	Limited and static

The comparative analysis demonstrates the superior performance of the proposed hybrid architecture across all key metrics. Latency decreased by up to 80%, while throughput more than doubled compared with the monolithic baseline. The dynamic scalability of serverless functions enabled near-instantaneous adaptation to fluctuating authentication demands, effectively addressing the static resource allocation limitations of traditional infrastructures. These results support the second research objective, which focuses on developing an architecture that preserves responsiveness and efficiency under variable transaction loads. From a financial standpoint, the average operational cost was reduced from $0.04 to $0.008 per transaction, representing an 80% cost saving. This level of efficiency is particularly critical for MSMEs, which typically handle a large volume of low-value transactions. Compared with previous architectures (Lin & Khazaei, 2021), which achieved similar cost reductions only in static cloud environments, the present study provides empirical evidence of dynamic scalability with minimal operational overhead.

4.6. Statistical Validation and Reliability

To verify that the observed performance improvements were not attributable to random variation, all experiments were conducted five times under identical configurations. Statistical analyses confirmed the reliability and significance of the observed differences. Table 6 presents the descriptive statistics for latency measurements at a workload of 100,000 transactions. The mean latency with caching (30.2 ms ± 2.8 ms) was substantially lower than without caching (68.4 ms ± 3.1 ms). The Shapiro–Wilk test confirmed normality ($p > 0.05$), and Levene's test indicated homogeneity of variances ($p = 0.32$). A paired t-test produced $t(4) = 17.81$, $p < 0.001$, and Cohen's $d \approx 8.0$, validating a statistically significant performance improvement. The latency values reported in Table 7 represent averaged results from five independent experimental repetitions..

Table 7 - Statistical Summary of Latency at 100,000 Transactions

Configuration	Mean (ms)	Std. Dev. (ms)	t-statistic	p-value	Significance
With Caching	30.2	2.8	17.81	< 0.001	Significant
Without Caching	68.4	3.1	—	—	—

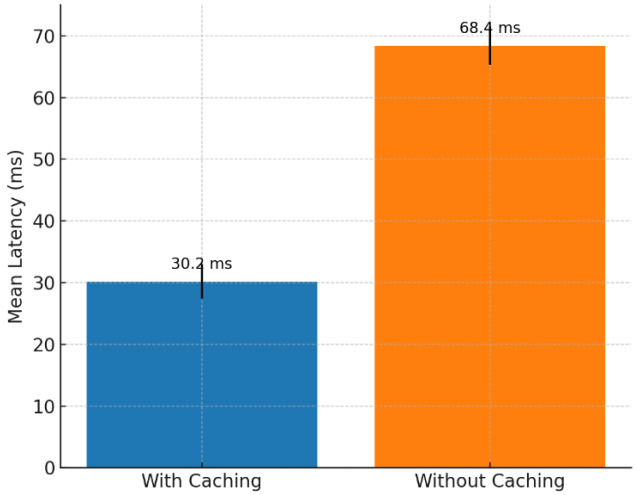

Fig. 6. Latency Distribution with Error Bars (± Standard Deviation)

The narrow deviation bands shown in Figure 9 confirm that the system exhibited stable and reproducible behavior across all trials. The statistically significant latency improvements ($p < 0.001$) indicate that Redis caching consistently enhanced performance beyond the influence of experimental noise.

4.7. Technical Challenges and Optimizations

During system implementation, several challenges were encountered, each mitigated through specific optimizations summarized in Table 8.

Table 8 - Technical Challenges and Corresponding Optimizations

Challenge	Optimization Strategy	Performance Impact
Cold-start latency in AWS Lambda	Function pre-warming; lightweight containers	Reduced initialization delay from 100 ms to approximately 40–60 ms through function pre-warming.
Query efficiency between Redis and PostgreSQL	Query prioritization and metadata preloading	Reduced database query time by 50 %
Blockchain synchronization delay	Parallel hash validation and transaction batching	Minimized synchronization lag across nodes
Sudden demand surges	Dynamic resource allocation; asynchronous queuing (SQS)	Ensured uninterrupted performance and elastic scaling

Pre-warming and container optimization effectively mitigated serverless cold-start delays, ensuring consistent performance during load surges. Query prioritization balanced in-memory and persistent database operations, while Solana's parallel transaction pipeline efficiently processed hash validation batches. Collectively, these optimizations transformed the system into a self-scaling and fault-tolerant architecture capable of maintaining low response times under high-stress conditions. These engineering-level insights provide practical guidance for system architects implementing large-scale blockchain-based authentication solutions.

4.8. Limitations

Despite the promising results, certain limitations must be acknowledged:

1. Controlled environment - Experiments were conducted on AWS with stable network conditions and Solana Devnet, which do not fully reflect the heterogeneous connectivity of MSMEs in developing regions.
2. Dependency on blockchain infrastructure - Solana's validator distribution and network congestion could affect global consistency and latency during peak traffic.
3. Synthetic dataset - Although validated against MSME transaction patterns, real-world behavioral data might yield more nuanced latency distributions.
4. Generalizability - The architecture was tuned for product authentication; extending it to other domains (e.g., financial settlement) may require reconfiguration of event triggers and consensus parameters.

These limitations are typical of proof-of-concept studies but highlight future pathways for production-level deployment.

.

4.9. Positioning within Existing Literature

This study extends the state of blockchain–IoT integration through several key contributions. While Lin and Khazaei (2021) optimized microservice scheduling, they did not address real-time blockchain authentication at the MSME scale (Lin & Khazaei, 2021). Likewise, Thakur and Breslin (2020) demonstrated blockchain-based traceability but employed static server deployments with limited elasticity (Thakur & Breslin, 2020). The present research differentiates itself by integrating (1) serverless event-driven execution for automatic scaling, (2) Redis in-memory caching for accelerated data access, and (3) Solana's hybrid consensus mechanism (Proof-of-History and Proof-of-Stake) for high-throughput, low-cost blockchain recording. This combination bridges the performance gap between experimental prototypes and deployable production architectures, providing empirical evidence that blockchain-based authentication can achieve both high speed and economic viability, thereby enabling practical adoption by MSMEs.

4.10. Implications and Future Work

For MSMEs, the findings demonstrate that real-time product verification is achievable without substantial infrastructure investment. The serverless elasticity of the proposed architecture eliminates the need for pre-provisioned servers, allowing operational costs to scale dynamically with actual usage. Furthermore, the integration of blockchain auditability ensures product authenticity, thereby enhancing consumer confidence and supporting regulatory compliance. Preliminary analysis indicates that the framework can potentially reduce idle server energy consumption by up to 70%, although this requires further empirical validation.

Future research will focus on extending the framework through several key directions. The first involves integrating edge computing to deploy localized verification nodes, thereby minimizing latency and improving resilience. The second aims to implement predictive caching driven by machine learning, which preloads frequently accessed metadata based on historical query behavior to enhance responsiveness. The third direction explores cross-chain interoperability, enabling communication between Solana and other blockchain networks to facilitate multilateral product verification. Finally, large-scale field testing with real MSMEs will be conducted to evaluate system robustness under varying network conditions. Collectively, these developments are expected to mature the proposed architecture into a production-grade infrastructure suitable for global MSME ecosystems.

5. Conclusion

This study confirms the effectiveness of the Serverless Event-Driven Microservices Hybrid Blockchain Architecture in overcoming the scalability, latency, and cost limitations of MSME product authentication systems. By integrating Solana blockchain, AWS Lambda-based serverless microservices, and Redis caching, the proposed framework demonstrates significant operational improvements under realistic workloads. The system achieved throughput exceeding 900 TPS, maintained an average latency below 30 ms, and reduced operational costs by approximately 80 percent compared with conventional monolithic architectures. Statistical validation confirmed that these performance gains were significant ($p < 0.001$), while regression analysis ($R^2 = 0.97$) indicated near-linear scalability across transaction loads up to 100,000.

The architecture's event-driven orchestration and dynamic resource allocation enable automatic scaling and asynchronous execution, ensuring consistent responsiveness during peak demand. Engineering optimizations, including function pre-warming, lightweight containerization, query prioritization, and parallel hash validation, further enhanced stability and throughput, creating a self-scaling and fault-tolerant infrastructure suitable for MSME deployment.

These results advance the integration of blockchain and serverless computing by showing that real-time and low-cost product authentication can be achieved without enterprise-grade resources. The proposed framework establishes an empirically validated foundation for scalable blockchain adoption in resource-constrained environments and offers insights applicable to domains such as supply chain traceability, financial auditing, and IoT security.

Future work will focus on extending this architecture through edge-based verification nodes, machine-learning-driven predictive caching, and cross-chain interoperability to further reduce latency and improve adaptability. Large-scale field testing with actual MSMEs will be necessary to validate robustness under heterogeneous network conditions and to refine the framework for production-grade deployment.

References

Agrawal, T., Angelis, J., Khilji, W. A., Kalaiarasan, R., & Wiktorsson, M. (2022). Demonstration of a blockchain-based framework using smart contracts for supply chain collaboration. *International Journal of Production Research*, *61*, 1497–1516. https://doi.org/10.1080/00207543.2022.2039413

Akhtar, A., Barati, M., Shafiq, B., Rana, O., Afzal, A., Vaidya, J., & Shamail, S. (2024). Blockchain Based Auditable Access Control for Business Processes With Event Driven

Policies. *IEEE Transactions on Dependable and Secure Computing*, *21*, 4699–4716. https://doi.org/10.1109/TDSC.2024.3356811

Alimohammadlou, M., & Alinejad, S. (2023). Challenges of blockchain implementation in SMEs' supply chains: an integrated IT2F-BWM and IT2F-DEMATEL method. *Electronic Commerce Research*, 1–43. https://doi.org/10.1007/s10660-023-09696-3

Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022a). Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review. *Sensors*, *22*(4), 1304.

Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022b). Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review. *Sensors (Basel, Switzerland)*, *22*. https://doi.org/10.3390/s22041304

Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022c). Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review. *Sensors (Basel, Switzerland)*, *22*. https://doi.org/10.3390/s22041304

Almadani, M., Alotaibi, S., Alsobhi, H., Hussain, O., & Hussain, F. (2023). Blockchain-based multi-factor authentication: A systematic literature review. *Internet Things*, *23*, 100844. https://doi.org/10.1016/j.iot.2023.100844

Amjad, M., Taylor, G., Huang, Z., Li, M., & Lai, C. S. (2023). Performance optimization of a blockchain-enabled information and data exchange platform for smart grids. *Electronics*, *12*(6), 1405.

Burckhardt, S., Chandramouli, B., Gillum, C., Justo, D., Kallas, K., McMahon, C., Meiklejohn, C., & Zhu, X. (2022). Netherite: Efficient Execution of Serverless Workflows. *Proc. VLDB Endow.*, *15*, 1591–1604. https://doi.org/10.14778/3529337.3529344

Chellasamy, N., Akram, F., Rajesh, N., & Umamaheswari, R. (2023). Application of Serverless Computing in Blockchain Distributed Technology. *2023 International Conference on Disruptive Technologies (ICDT)*, 115–118. https://doi.org/10.1109/ICDT57929.2023.10150901

Choi, T., & Xu, O. (2021). Initial coin offerings for blockchain based product provenance authentication platforms. *International Journal of Production Economics*, *233*, 107995. https://doi.org/10.1016/j.ijpe.2020.107995

Cui, Z., Xue, F., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN. *IEEE Transactions on Services Computing*, *13*, 241–251. https://doi.org/10.1109/TSC.2020.2964537

Fikri, N., Rida, M., Abghour, N., Moussaid, K., Omri, A. El, & Myara, M. (2022). A Blockchain Architecture for Trusted Sub-Ledger Operations and Financial Audit Using Decentralized Microservices. *IEEE Access*, *10*, 90873–90886. https://doi.org/10.1109/ACCESS.2022.3201885

Ganeshan, A., Jayagopalan, S., Perumal, B., & Sarveshwaran, V. (2023). Secure identity key and blockchain-based authentication approach for secure data communication in multi-WSN. *Concurrency and Computation: Practice and Experience*, *35*. https://doi.org/10.1002/cpe.7861

Gao, X., Zhang, W., Zhao, B., Zhang, J., Wang, J., & Gao, Y. (2022). Product authentication technology integrating blockchain and traceability structure. *Electronics*, *11*(20), 3314.

Ge, Z., Loghin, D., Ooi, B. C., Ruan, P., & Wang, T. (2022). Hybrid blockchain database systems: design and performance. *Proceedings of the VLDB Endowment*, *15*(5), 1092–1104.

Hermana, A. A., Fajrin, H. M., Reva, Y. N., & Saleh, M. Z. (2024). Dampak MEA (Masyarakat Ekonomi Asean) Terhadap Pertumbuhan Ekonomi Indonesia di Era Globalisasi. *Inisiatif: Jurnal Ekonomi, Akuntansi Dan Manajemen*. https://doi.org/10.30640/inisiatif.v4i1.3455

Huang, S., Wang, G., Yan, Y., & Fang, X. (2020). Blockchain-based data management for digital twin of product. *Journal of Manufacturing Systems*, *54*, 361–371. https://doi.org/10.1016/j.jmsy.2020.01.009

Jinhua, Lin, S.-Y., Chen, X., Sun, H.-M., Chen, Y.-C., & Wang, H. (2020a). A Blockchain-Based Application System for Product Anti-Counterfeiting. *IEEE Access*, *8*, 77642–77652. https://doi.org/10.1109/ACCESS.2020.2972026

Jinhua, Lin, S.-Y., Chen, X., Sun, H.-M., Chen, Y.-C., & Wang, H. (2020b). A Blockchain-Based Application System for Product Anti-Counterfeiting. *IEEE Access*, *8*, 77642–77652. https://doi.org/10.1109/ACCESS.2020.2972026

Khan, A. A., Laghari, A. A., Baqasah, A., Alroobaea, R., Almadhor, A., Sampedro, G. A., & Kryvinska, N. (2024). Blockchain-enabled infrastructural security solution for serverless consortium fog and edge computing. *PeerJ Computer Science*, *10*. https://doi.org/10.7717/peerj-cs.1933

Khashan, O., & Khafajah, N. (2023). Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems. *J. King Saud Univ. Comput. Inf. Sci.*, *35*, 726–739. https://doi.org/10.1016/j.jksuci.2023.01.011

Li, L., Qu, H., Wang, H., Wang, J., Wang, B., Wang, W., Xu, J., & Wang, Z. (2022). A Blockchain-Based Product Traceability System with Off-Chain EPCIS and IoT Device Authentication. *Sensors (Basel, Switzerland)*, *22*. https://doi.org/10.3390/s22228680

Li, M., Tang, H., Hussein, A. R., & Wang, X. (2020). A Sidechain-Based Decentralized Authentication Scheme via Optimized Two-Way Peg Protocol for Smart Community. *IEEE Open Journal of the Communications Society*, *1*, 282–292. https://doi.org/10.1109/OJCOMS.2020.2972742

Li, Z., Guo, L., Cheng, J., Chen, Q., He, B., & Guo, M. (2021). The Serverless Computing Survey: A Technical Primer for Design Architecture. *ACM Computing Surveys (CSUR)*, *54*, 1–34. https://doi.org/10.1145/3508360

Lin, C.-Y., & Khazaei, H. (2021). Modeling and Optimization of Performance and Cost of Serverless Applications. *IEEE Transactions on Parallel and Distributed Systems*, *32*, 615–632. https://doi.org/10.1109/TPDS.2020.3028841

Long, W., Lu, H., Chong, B., & Cheng, G. (2024). Heterogeneous Event-driven Scheduling for Blockchain-based Serverless Edge Computing. *GLOBECOM 2024 - 2024 IEEE Global Communications Conference*, 4624–4629. https://doi.org/10.1109/GLOBECOM52923.2024.10901737

Luo, F., Huang, R., & Xie, Y. (2024). Hybrid blockchain-based many-to-many cross-domain authentication scheme for smart agriculture IoT networks. *J. King Saud Univ. Comput. Inf. Sci.*, *36*, 101946. https://doi.org/10.1016/j.jksuci.2024.101946

Phimmuang, K., & Sripanidkulchai, K. (2024). Measurement and Analysis of Blockchain Peers. *IEEE Access*, *12*, 135075–135088. https://doi.org/10.1109/ACCESS.2024.3462969

Putra, M. D. R., & Disemadi, H. S. (2024). Counterfeit Culture dalam Perkembangan UMKM: Suatu Kajian Kekayaan Intelektual. *KRTHA BHAYANGKARA*. https://doi.org/10.31599/krtha.v16i2.1215

Qi, S., Monis, L., Zeng, Z., Wang, I., & Ramakrishnan, L. (2024). SPRIGHT: High-Performance eBPF-Based Event-Driven, Shared-Memory Processing for Serverless Computing. *IEEE/ACM Transactions on Networking*, *32*, 2539–2554. https://doi.org/10.1109/TNET.2024.3366561

Rico-Peña, J. J., Arguedas-Sanz, R., & López-Martin, C. (2023). Models used to characterise blockchain features. A systematic literature review and bibliometric analysis. *Technovation*, *123*, 102711. https://doi.org/10.1016/j.technovation.2023.102711

Rogozhin, A. (2022). CHINA – SOUTHEAST ASIA: FEATURES OF CROSS-BORDER TRADE IN COUNTERFEIT GOODS. *Southeast Asia: Actual Problems of Development*. https://doi.org/10.31696/2072-8271-2022-4-4-57-011-020

Thakur, S., & Breslin, J. (2020). Scalable and secure product serialization for multi-party perishable good supply chains using blockchain. *Internet Things*, *11*, 100253. https://doi.org/10.1016/j.iot.2020.100253

Vu, N., Ghadge, A., & Bourlakis, M. (2022). Evidence-driven model for implementing Blockchain in food supply chains. *International Journal of Logistics Research and Applications*, *26*, 568–588. https://doi.org/10.1080/13675567.2022.2115987

Waqar, A., Qureshi, A. H., Othman, I., Saad, N., & Azab, M. (2023). Exploration of challenges to deployment of blockchain in small construction projects. *Ain Shams Engineering Journal*. https://doi.org/10.1016/j.asej.2023.102362

Yunita, P., & Killian, P. E. (2025). Implementation of TRIPs and Dynamics of Counterfeit Goods Trade in Southeast Asia: Regulations and Practices. *Journal of Education, Humaniora and Social Sciences (JEHSS)*. https://doi.org/10.34007/jehss.v7i3.2504

Zhang, Y., Li, B., Wu, J., Liu, B., Chen, R., & Chang, J. (2022). Efficient and Privacy-Preserving Blockchain-Based Multifactor Device Authentication Protocol for Cross-Domain IIoT. *IEEE Internet of Things Journal*, *9*, 22501–22515. https://doi.org/10.1109/JIOT.2022.3176192