VOL. 10. NO. 3 FEBRUARY 2025
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480 /jitk.v10i3.6010

JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

OPTIMIZING MSME PRODUCT AUTHENTICITY VERIFICATION IN DECENTRALIZED MARKETS USING BLOCKCHAIN

Adnan Zulkarnain[1*]; Mukhlis Amien[2]

Information Systems[1], Informatics[2]
Sekolah Tinggi Informatika & Komputer Indonesia, Malang, Indonesia[1, 2]
https://stiki.ac.id[1, 2]
adnan.zulkarnain@stiki.ac.id[1*], amien@stiki.ac.id[2]

(*) Corresponding Author
(Responsible for the Quality of Paper Content)

Abstract— *Blockchain technology offers a solution for ensuring product authenticity in decentralized digital marketplaces. However, Micro, Small, and Medium Enterprises (MSMEs) face barriers such as limited infrastructure, high costs, and data interoperability challenges. This study develops a hybrid blockchain-based application architecture tailored to MSME needs, integrating on-chain and off-chain storage. Critical security data, such as product hashes, is stored on-chain, while non-sensitive data, like product descriptions, is managed off-chain using a cloud-based MySQL database. This design reduces storage costs and computational load while maintaining data integrity. Ethereum smart contracts manage product registration and verification, linked to QR code-based authentication for end-users. A realistic simulation environment using server-based infrastructure and cloud databases evaluated system performance, including transaction throughput, latency, resource utilization, and scalability. The results show significant improvements compared to conventional centralized methods, achieving a transaction throughput of 391 TPS for 1 million transactions while maintaining low latency and resource efficiency. This research addresses a theoretical gap by optimizing blockchain for small-scale decentralized markets, tackling resource limitations and interoperability issues unique to MSMEs. Practically, it provides a scalable and cost-effective solution for product authenticity verification, enhancing consumer trust and reducing counterfeiting in MSME digital markets. While real-world testing remains a limitation, the findings underline the system's potential to support sustainable MSME digital marketplaces and build consumer confidence.*

Keywords: *blockchain, decentralized market, hybrid storage, MSMEs, product verification.*

Intisari— *Teknologi blockchain menawarkan solusi untuk memastikan keaslian produk di pasar digital yang terdesentralisasi. Namun, Usaha Mikro, Kecil, dan Menengah (UMKM) menghadapi hambatan seperti keterbatasan infrastruktur, biaya tinggi, dan tantangan interoperabilitas data. Studi ini mengembangkan arsitektur aplikasi berbasis blockchain hibrida yang disesuaikan dengan kebutuhan UMKM, yang mengintegrasikan penyimpanan on-chain dan off-chain. Data keamanan penting, seperti hash produk, disimpan on-chain, sementara data yang tidak sensitif, seperti deskripsi produk, dikelola off-chain menggunakan basis data MySQL berbasis cloud. Desain ini mengurangi biaya penyimpanan dan beban komputasi sambil mempertahankan integritas data. Kontrak pintar Ethereum mengelola pendaftaran dan verifikasi produk, yang ditautkan ke autentikasi berbasis kode QR untuk pengguna akhir. Lingkungan simulasi realistis menggunakan infrastruktur berbasis server dan basis data cloud mengevaluasi kinerja sistem, termasuk throughput transaksi, latensi, pemanfaatan sumber daya, dan skalabilitas. Hasilnya menunjukkan peningkatan yang signifikan dibandingkan dengan metode terpusat konvensional, mencapai throughput transaksi sebesar 391 TPS untuk 1 juta transaksi sambil mempertahankan latensi rendah dan efisiensi sumber daya. Penelitian ini mengatasi kesenjangan teoritis dengan mengoptimalkan blockchain untuk pasar terdesentralisasi berskala kecil, mengatasi keterbatasan sumber daya, dan masalah interoperabilitas yang unik bagi UMKM. Secara praktis, penelitian ini menyediakan solusi yang dapat diskalakan dan hemat biaya untuk verifikasi keaslian produk, meningkatkan kepercayaan konsumen, dan mengurangi pemalsuan di pasar*

VOL. 10. NO. 3 FEBRUARY 2025
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i3.6010

digital UMKM. Meskipun pengujian di dunia nyata masih menjadi keterbatasan, temuan ini menggarisbawahi potensi sistem untuk mendukung pasar digital UMKM yang berkelanjutan dan membangun kepercayaan konsumen.

***Kata Kunci**: blockchain, pasar terdesentralisasi, penyimpanan hibrida, UMKM, verifikasi produk.*

INTRODUCTION

Blockchain has become an increasingly widely used solution in addressing product authenticity issues, especially in the context of a decentralized digital marketplace [1]. The technology offers transparency, security, and tamper-resistant properties, enabling end-to-end product tracking without relying on a centralized third party [1][2][3][4]. Blockchain technology has also proven to be a reliable solution for combating counterfeiting by reducing dependency on centralized systems and ensuring tamper-proof product authenticity [5] For instance, hybrid on-chain and off-chain storage strategies can enhance both scalability and cost-efficiency, which are critical for MSMEs operating in digital marketplaces [5] In the context of MSMEs, verification of product authenticity is a big challenge because often MSMEs do not have adequate infrastructure to guarantee the authenticity of their products in the digital market [6]. Blockchain enables MSMEs to ensure that their products are authentic and provide more trust to consumers in an increasingly competitive e-commerce environment [1]. Recent studies have shown that decentralized blockchain systems can improve transaction efficiency and the reputation of market participants by creating an automated and distributed trust system [7]. This research is highly relevant to the growing demand for blockchain-based solutions to address the problem of product counterfeiting and guarantee authenticity in digital marketplaces [8].

Despite the growing recognition of blockchain's potential, its application for verifying the authenticity of MSME products remains underexplored. Most existing studies focus on blockchain's use in large-scale applications, such as supply chain management and IoT [9][10][11], without emphasizing its optimization for decentralized MSME markets. This represents a theory gap, wherein current research does not provide a conceptual or theoretical framework specifically tailored to address the unique constraints faced by MSMEs—such as limited resources, smaller transaction volumes, and the need for cost-effective integration with existing systems. In other words, while large enterprises have been studied extensively in terms of blockchain adoption and scalability, the theoretical underpinnings and guiding principles that explain how blockchain can be effectively adapted, scaled down, and financially optimized for MSMEs remain insufficiently explored [12]. MSMEs face unique challenges such as limited resources, high implementation costs, and the complexity of data interoperability, making the adoption of blockchain systems impractical for many [13][14][15].

To address these gaps, this study develops a hybrid blockchain-based application architecture tailored to MSME needs, integrating on-chain and off-chain storage. Critical security data, such as product hashes, is stored on-chain, while non-sensitive data, such as product descriptions and manufacturer details, is managed off-chain using a cloud-based MySQL database. This approach reduces blockchain storage costs by 50% compared to fully on-chain methods while maintaining data security. Ethereum smart contracts are utilized to manage product registration and verification, linked to QR code-based authentication for end-users. A realistic simulation environment was implemented using server-based infrastructure and cloud databases to evaluate system performance, including transaction throughput, latency, resource utilization, and scalability. Compared to conventional centralized methods, the results demonstrate significant improvements in speed and cost efficiency, achieving a transaction throughput of 391 TPS for 1 million transactions while maintaining low latency and efficient resource utilization [16][17][18].

Unlike traditional blockchain solutions, which often focus on large-scale enterprises, this study provides a practical and resource-efficient system specifically designed for MSME needs**.** This system empowers MSMEs by enabling affordable product authenticity verification, reducing counterfeit risks, and fostering greater consumer trust in digital marketplaces.

This research contributes to the literature in two key ways. Theoretically, it advances the understanding of blockchain applications for MSMEs by addressing the theory gap in blockchain optimization for small-scale decentralized markets [19]. Practically, it provides a cost-effective and scalable solution to minimize product counterfeiting and improve consumer trust, enriching the body of knowledge on blockchain adoption for digital marketplaces [20]. Cost-

effectiveness is achieved by reducing the computational and storage overhead associated with purely on-chain operations. By employing a hybrid on-chain and off-chain storage strategy, where static data (such as product authenticity certificates) is stored on-chain while dynamic transactional data is placed off-chain, the system reduces transaction fees and network load. Scalability is demonstrated through the ability to maintain stable transaction throughput and low latency even as the number of transactions grows, ensuring the system can accommodate increasing market demands without significant resource inflation.

However, this research does not include direct testing with consumers or an evaluation of the economic impact on MSMEs due to limitations in time and resources. Future research will involve pilot implementations with MSMEs to test the system's usability, scalability, and real-world impact on consumer trust and operational costs. Additionally, an economic analysis, including cost-benefit assessments and total cost of ownership calculations, will provide insights into the financial viability and long-term sustainability of blockchain solutions for MSMEs [21].

MATERIALS AND METHODS

Research Design

This research uses a simulation experiment method to test the performance of a blockchain architecture specifically designed to support the authenticity verification of MSME products in decentralized digital markets. This simulation is done through modeling QR Code transactions that represent the product authenticity verification process. Each transaction is simulated through a program code that automatically executes the product verification procedure in the blockchain, without involving direct user interaction. The main objective of this simulation is to evaluate the transaction speed (throughput), response time (latency), CPU and memory utilization during transaction processing (resource consumption), and the ability of the system to handle large scale (scalability) when facing transaction scenarios with varying numbers and nodes.

Simulation Environment and Tools Used

To ensure the reliability, performance, and scalability of the blockchain application used in this study, the simulation was conducted on a robust server infrastructure. This setup was meticulously designed to handle the high transaction volumes and complex computational requirements inherent to decentralized blockchain applications. By leveraging multiple servers with specific roles, including main servers for transaction processing, a dedicated database server for off-chain storage, and a load balancer to manage the distribution of network traffic, the simulation environment provides a high-performance and scalable solution for product authenticity verification.

The main servers were responsible for processing the bulk of blockchain transactions and managing communication between the frontend and backend systems. Meanwhile, the database server ensured that non-sensitive data was efficiently stored and accessed, thus reducing the computational overhead of blockchain operations. The load balancer played a crucial role in distributing incoming transactions evenly across the main servers, preventing performance bottlenecks and ensuring the system's responsiveness during high-volume scenarios.

In addition to the server infrastructure, the simulation environment utilized various software tools and libraries that facilitated smooth integration and communication between the system components. These tools included programming languages, blockchain frameworks, and off-chain storage systems that worked in synergy to deliver reliable performance. Further details of the server infrastructure and tools utilized in this simulation are outlined in Table 1 below.

Table 1. Simulation Environment and Tools Specifications

No	Component	Specifications
1	Main Servers (2 units)	Processor: 16-core CPU RAM: 16GB Storage: 60GB SSD
2	Database Server (1 unit)	Processor: 16-core CPU RAM: 16GB Storage: 60GB SSD
3	Load Balancer (1 unit)	Processor: 16-core CPU RAM: 16GB Storage: 60GB SSD
4	Server Environment	Deployed in a cloud environment running Ubuntu 20.04 LTS for stability and support for blockchain software.
5	Programming Language	JavaScript with Node.js platform to ensure good integration between frontend, backend, and blockchain.
6	Blockchain Framework	Ethereum network with smart contracts developed using Solidity on Sepolia Testnet.
7	Off-chain Storage	MySQL used for storing non-sensitive product data (product name, description, manufacturer ID).

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

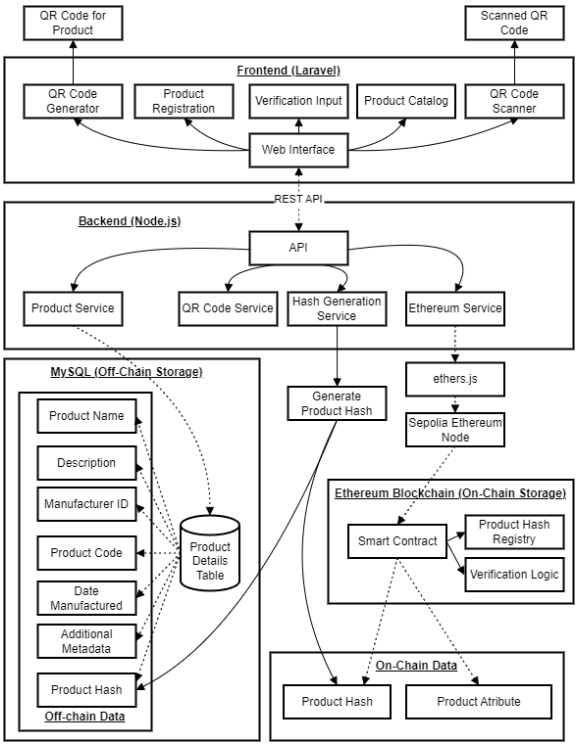
VOL. 10. NO. 3 FEBRUARY 2025
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i3.6010

No	Component	Specifications
8	Supporting Libraries	Ether.js for managing interactions with the Ethereum network. Express.js for building a RESTful API connecting frontend and blockchain.

Source: (Research Results, 2024)

Architecture

To solve the problem of counterfeit product verification, we propose a hybrid architecture that combines blockchain and off-chain storage. This approach ensures data security by storing product hashes on the blockchain, while other information is stored in an off-chain database for efficiency, as described in Figure 1.



Source: (Research Results, 2024)

Figure 1. Hybrid Architecture for Product Authenticity Verification Using Blockchain Technology

The architecture of the product authenticity verification system is designed using a hybrid approach, combining both on-chain and off-chain data storage to ensure efficiency and security. This system comprises three main components: the frontend, the backend, and a hybrid storage mechanism involving a MySQL database and the Ethereum blockchain. Each component operates synergistically to support the processes of product registration and verification in a secure and reliable manner.

The frontend, developed using the Laravel framework, provides the user interface for two key functionalities: product registration and product verification. Manufacturers can input product data such as the product name, description, and manufacturer ID through a web interface. Once the product data is successfully entered, the system generates a unique QR code linked to the product's information. End-users, such as consumers, can scan the QR code using this interface to verify the authenticity of the product.

On the backend side, Node.js serves as the primary platform for managing communication between the frontend and the blockchain, as well as handling various essential services. The Product Service oversees the registration of products and stores product data in the MySQL database as part of the off-chain storage. Additionally, the QR Code Service is responsible for generating QR codes that serve as the identification keys for the products. The system also leverages the Hash Generation Service, which generates a hash from the registered product data. This hash acts as a unique representation of the product and is stored on the blockchain via the Ethereum Service, which utilizes smart contracts to store and retrieve the product hashes.

This hybrid storage approach uses the MySQL database to store non-sensitive product information, such as product names and descriptions, off-chain. Off-chain storage is selected to reduce the costs associated with blockchain storage while still allowing quick access to product data. On the other hand, the hash of the product data is stored on the Ethereum blockchain as proof of the product's authenticity. This approach ensures that product data remains secure, as any modification to the product attributes will result in a different hash, which can be verified against the blockchain.

The product registration process begins when the manufacturer inputs product data via the frontend interface. Once the data is stored in the MySQL database, the system generates a hash of the product attributes and stores it on the blockchain via a smart contract. The generated QR code is then provided to the manufacturer as a product identifier that can be used by consumers for verification. The verification process is carried out by end-users who scan the product's QR code. The backend retrieves the product data from the MySQL database, recalculates the hash, and compares it to the hash stored on the blockchain. If the hashes match, the system confirms the product's authenticity.

This hybrid approach offers several advantages, including cost efficiency and improved performance. By storing only the hash on the blockchain, the system reduces the typically high

costs associated with blockchain storage while maintaining data security. Furthermore, storing product data in the MySQL database allows for faster access compared to storing the entire dataset on the blockchain. The system is also easily scalable, as only security-relevant data is stored on-chain, while other product information is managed off-chain.

Test Network Used

The simulation uses Sepolia Testnet, one of Ethereum's testnets, to run smart contracts and process Hash Based Verification based transactions via QR Code scanning. Sepolia Testnet provides a testing environment similar to the Ethereum mainnet, but with lower gas costs and without the risks associated with using real assets. Sepolia was chosen because it supports the Ethereum ecosystem with the Proof of Stake (PoS) protocol, provides greater efficiency in experimentation, and enables transaction validation and smart contract execution in a secure scenario.

Data Sources

The data for this study was obtained through a series of simulations conducted by emulating various transaction scenarios, as detailed in Table 2: Transaction Testing Scenarios. Each scenario represents a different transaction volume, designed to evaluate the robustness and scalability of the blockchain architecture.

Table 2. Transaction Testing Scenario

Transaction Scenario	Number of Transactions	Description
Scenario 1	10	Validate system performance baseline for small transactions
Scenario 2	100	Testing for medium transactions, measuring the baseline efficiency of the system
Scenario 3	1000	Large transaction scale simulation to test performance in larger scenarios
Scenario 4	10000	Simulation of large transactions to test the system's capabilities in real markets
Scenario 5	100000	Validating the system at a larger market level with multiple users
Scenario 6	1000000	Test the scalability of the system in handling very large transaction volumes

Source: (Research Results, 2024)

Data Collection Techniques

During the simulation, the performance metrics, as outlined in Table 3: Blockchain Performance Metrics and Their Functions, are systematically collected.

Table 3. Blockchain Performance Metrics and Their Functions

Metrics Collected	Function
Transaction Throughput	Number of transactions processed per second (TPS). This metric shows the speed at which the system can process transactions in each scenario.
Latency	The time taken to complete a transaction, calculated from initiation to verification completion. This response time is expressed in milliseconds (ms).
Resource Consumption	CPU and memory utilization during transaction processing. This metric measures the efficiency of the system in utilizing computing resources.
Scalability	The ability of the system to remain efficient and responsive as the number of transactions increases. Scalability is tested by increasing the transaction volume from small to large scenarios.

Source: (Research Results, 2024)

Simulation Procedures

The simulation is run in a distributed computing environment based on the Ethereum network, which mimics the real conditions of a decentralized digital marketplace. The process of verifying the authenticity of the product is done using Hash-Based Verification through QR Code scanning, which stores the same hash of the product as the hash stored on the blockchain. This verification is done using smart contracts that manage and automate the authenticity checking process. The simulation procedure was carried out as follows:

1. Transaction initiation

Each entity (MSME or consumer) scans the QR Code of the product which contains a unique hash of the product. This hash is a digital representation of the product data stored on the blockchain. After the scan, a verification request is sent to a smart contract present on the Ethereum network. In the context of simulation, this process will be carried out through program code simulation.

2. Execution of the smart contract

After receiving the verification request, the smart contract on Ethereum is activated. The smart contract retrieves the hash of the product that has been stored on the blockchain and compares it with the hash submitted by the user through scanning the QR Code. This process confirms whether the

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 10. NO. 3 FEBRUARY 2025
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i3.6010

submitted product hash matches the hash previously stored on the blockchain.

3. Product verification (Hash-Based Verification)
The validator node processes the transaction to verify the hash match. If the hash contained in the QR Code and the hash on the blockchain match, the product is declared genuine. Otherwise, the product is considered not genuine or the data has been altered.

4. Performance metrics collection
During the simulation, key performance metrics such as transaction throughput (number of transactions processed per second), latency (time taken to complete verification), resource consumption (CPU usage and memory), and hash verification time are recorded at each stage of the verification process. This is done to assess the efficiency and capability of the blockchain system in performing hash-based verification.

5. Scalability testing
Scalability was tested by incrementally increasing the number of transactions and hash verification requests. Although the number of validator nodes was not explicitly changed, the increased transaction volume was tested to see the impact on throughput and latency, especially when the transaction load was high.

Data Analysis

The data collected from the simulations were analyzed using descriptive statistics and performance evaluation methods. The analysis steps performed include:

1. Transaction Throughput Analysis
Measures throughput in each scenario, then compares results between scenarios to assess how quickly the system processes increased transaction volumes.

2. Latency Analysis
Analyzes the average time taken to complete transactions in each scenario, to determine if the response time increases as the number of transactions increases.

3. Resource Consumption Evaluation
Evaluates CPU and memory usage during simulation. Resource usage is calculated to ensure the system remains efficient as the transaction load increases.

4. Scalability Analysis
Assesses the performance of the system when the transaction volume increases exponentially. This test is conducted to determine whether throughput remains high and latency remains low when transactions reach one million.

RESULTS AND DISCUSSION

This research examines the performance of a blockchain architecture designed to support authenticity verification of MSME products in a decentralized digital marketplace using the Ethereum network, smart contracts, and hybrid data storage that utilizes a combination of on-chain and off-chain data storage. In this research, data that is important for verification and security is stored on-chain, while large non-critical data is stored off-chain to reduce costs and improve storage efficiency. This method aims to optimize Transaction Throughput, Latency, Resource Consumption, and Scalability.

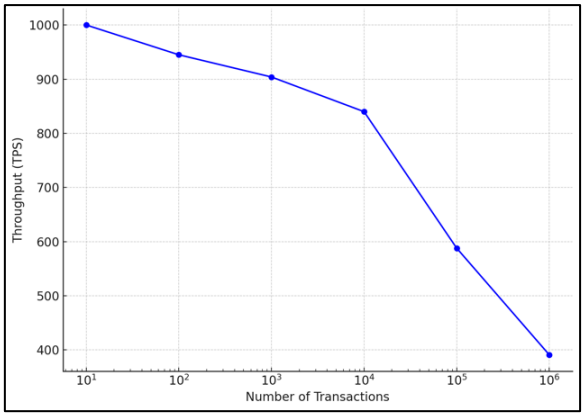
Transaction Throughput

Transaction Throughput measures the speed at which a system can process transactions per second (TPS) and is one of the key metrics for assessing the scalability and efficiency of blockchain-based systems. The combination of on-chain and off-chain storage plays an important role in maintaining high throughput, especially in large transaction scenarios, as storing data directly on the blockchain (on-chain) is usually expensive and slow. In this approach, only data hashes are stored on the blockchain to ensure integrity, while the full data is stored off-chain.

The observed improvements in throughput align with the theoretical framework that emphasizes reducing blockchain network congestion through hybrid architectures. This approach leverages the strengths of both on-chain immutability and off-chain efficiency, as suggested in prior studies [22] [23].

Figure 2 shows the throughput testing results based on various transaction scenarios. The simulation reveals that although there is a slight decrease in throughput at higher transaction volumes, the hybrid storage approach maintains competitive throughput. For instance, in a scenario with 1 million transactions, the throughput was recorded at 391 TPS, a significant improvement compared to systems relying solely on on-chain storage. This value vastly outperforms Ethereum Mainnet's typical throughput of 15-30 TPS, underscoring the effectiveness of hybrid solutions

in managing large-scale transaction volumes [22] [23].



Source: (Research Results, 2024)
Figure 2. Throughput Testing Results Based on Transaction Scenario

The results are consistent with SlimChain's findings, which demonstrate up to a 15.6x increase in throughput compared to traditional on-chain systems [24]. However, unlike SlimChain, which focuses on general throughput, our research emphasizes applications requiring high data integrity verification. By storing data hashes on-chain and utilizing off-chain storage for larger datasets, the system ensures efficient processing without compromising security.

These findings substantiate the theoretical proposition that hybrid architectures not only enhance scalability but also preserve data integrity. This balance is critical for applications in sensitive domains such as finance, logistics, and healthcare, where both trust and efficiency are paramount. The research extends existing blockchain theories by demonstrating that hybrid storage solutions can adapt to the specific needs of resource-constrained environments like MSMEs.

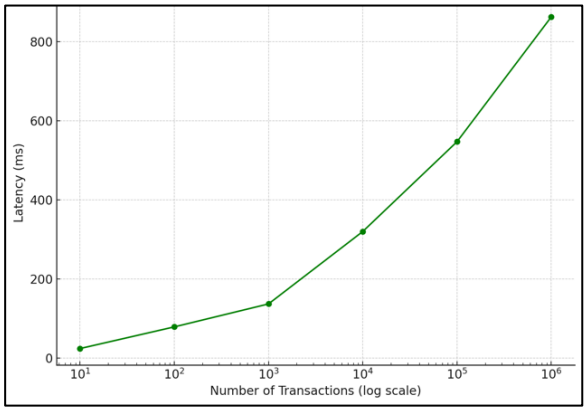
By leveraging efficient off-chain storage and reducing the transaction load on the blockchain, the system accommodates large transaction volumes while maintaining data integrity in a more affordable and scalable manner. These results provide practical evidence for the theoretical claims that hybrid storage enables decentralized solutions to meet the demands of high-throughput applications in various industries.

Latency

Latency is a metric that measures the time taken to complete a transaction from initiation to final confirmation. With the use of hybrid data storage, heavier data is processed off-chain, while hash and metadata verification is done on-chain. This division of tasks is central to improving efficiency in blockchain systems while maintaining data integrity.

The observed latency trends are consistent with the theoretical understanding that increasing transaction volumes lead to higher processing times in blockchain systems. Validator nodes experience greater computational loads as the transaction queue grows, which aligns with prior studies emphasizing the importance of off-chain solutions to mitigate latency issues [25].

Figure 3 illustrates the latency testing results across different transaction scenarios. In the large transaction scenario, latency increased from 23.75 ms in the 10 transaction scenario to 862.40 ms in the 1,000,000 transaction scenario. This increase reflects the expected behavior of blockchain systems under heavy transaction loads. However, the hybrid storage approach significantly mitigates latency for big data processing tasks, as only hashes and metadata are stored on-chain, while full data is processed off-chain.



Source: (Research Results, 2024)
Figure 3. Latency Testing Results Based on Transaction Scenario

These results align with MSTDB research, which demonstrates that hybrid architectures effectively reduce latency in high-transaction scenarios through off-chain processing [25]. While our study observed latency increases under higher transaction volumes, the results remain far more efficient than traditional on-chain systems like Ethereum Mainnet, which lacks hybrid optimization.

The findings reinforce the theoretical proposition that hybrid architectures can balance blockchain security and scalability. By maintaining on-chain hashes for data integrity and utilizing off-chain processing for larger datasets, this approach provides a scalable and secure solution. These results extend existing theories by demonstrating

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 10. NO. 3 FEBRUARY 2025
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i3.6010

the practical application of hybrid solutions in scenarios requiring both high throughput and low latency.

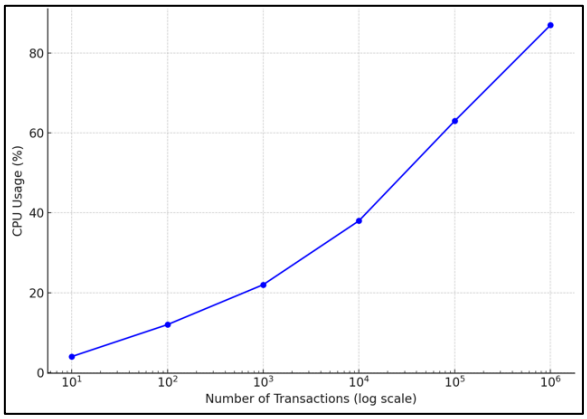
This study offers practical insights for blockchain applications in industries where both data integrity and performance are critical, such as finance, logistics, and healthcare. The hybrid approach provides a more efficient alternative for handling large-scale transactions without compromising the security and trust inherent in blockchain systems.

This balance between security and efficiency exemplifies the hybrid architecture's potential to address real-world challenges, making it a viable solution for resource-constrained environments that require robust, scalable transaction systems.

Resource Consumption

The Resource Consumption evaluation focuses on CPU and memory utilization, which are critical metrics for assessing the efficiency of system resources in handling transaction loads. The use of hybrid data storage has been shown to reduce resource requirements in large transaction scenarios, as large data is not stored directly on the blockchain but instead utilizes more resource-efficient off-chain solutions.

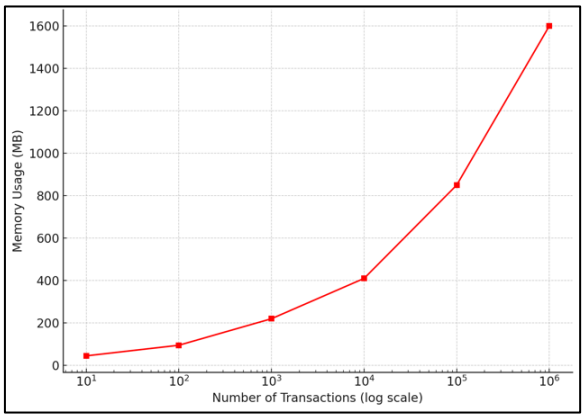
These findings align with the theoretical framework emphasizing that hybrid storage can reduce the computational and storage demands on blockchain networks [24]. By offloading large datasets to off-chain storage, the system alleviates on-chain resource constraints, which is critical for scalability in resource-constrained environments.



Source: (Research Results, 2024)

Figure 4. CPU Usage Based on Number of Transactions

The trends of CPU and memory utilization based on transaction volumes are visualized in Figure 4 and Figure 5. CPU utilization increases progressively from 4% for 10 transactions up to 87% for 1,000,000 transactions (Figure 4). Similarly, memory usage rises from 45 MB for 10 transactions to 1.6 GB for 1,000,000 transactions (Figure 5). These results indicate that while resource usage increases with transaction volume, the system maintains high efficiency due to the off-chain storage approach.



Source: (Research Results, 2024)

Figure 5. Memoy Usage Based on Number of Transactions

These results are consistent with SlimChain's findings, which show significant reductions in on-chain storage [24]. Unlike SlimChain, which achieves up to a 97% reduction in on-chain storage, our research prioritizes resource efficiency while preserving on-chain data integrity for product authentication applications. This dual focus ensures the system remains efficient and secure, even in high-throughput scenarios.

These findings contribute to blockchain theories by demonstrating that hybrid architectures effectively balance resource efficiency and data integrity. The high CPU and memory efficiency observed in the 1 million transaction scenario validates the theoretical proposition that off-chain storage can significantly alleviate network congestion while ensuring robust performance.

By optimizing resource consumption, this approach ensures that the system remains scalable and efficient, making it particularly suitable for applications requiring high data integrity and throughput. These findings have practical significance for industries such as supply chain, finance, and healthcare, where resource efficiency is critical for managing large-scale transactions.

The high resource efficiency achieved through hybrid storage underscores the system's capability to handle large transaction volumes while maintaining scalability and security. This approach aligns with prior blockchain research advocating hybrid solutions as a pathway to achieving both

resource optimization and data integrity in decentralized applications.

Scalability

Scalability refers to the system's ability to handle an increasing number of transactions without significant performance degradation. By utilizing hybrid storage and optimized smart contracts, the system demonstrates the capacity to handle large transaction volumes with better performance than systems relying solely on on-chain storage.

Scalability is a fundamental challenge in blockchain systems, as noted in prior research, where increasing transaction volumes often lead to performance bottlenecks [24]. Hybrid architectures have been theoretically proposed to mitigate these issues by offloading non-critical data to off-chain storage, thereby reducing on-chain computational loads [25].

Table 4 illustrates the throughput and latency performance under various transaction scenarios. In the 1,000,000 transaction scenario, the system maintains a throughput of 391 TPS with latency reaching 862.4 ms. Although throughput decreases as transaction volume increases—1000 TPS for 10 transactions to 391 TPS for 1,000,000 transactions—the results remain significantly higher than traditional on-chain blockchain systems, which typically achieve only 15-30 TPS [24].

Table 4. Result throughput and latency performance Based on Transaction Scenario

Number of Transactions	Throughput (TPS)	Latency (ms)
10	1000 TPS	23.75 ms
100	945 TPS	78.52 ms
1000	904 TPS	136.6 ms
10000	840 TPS	319.73 ms
100000	588 TPS	546.81 ms
1000000	391 TPS	862.4 ms

Source: (Research Results, 2024)

These findings align with the MSTDB study, which demonstrates that hybrid architectures enhance scalability by reducing on-chain storage load [25]. However, unlike MSTDB, which primarily focuses on general throughput improvements, this study emphasizes product authentication applications. By integrating on-chain hashes, the system maintains data integrity while efficiently managing large transaction volumes.

These results substantiate the theoretical proposition that hybrid architectures can balance scalability and security. The consistent performance across high transaction volumes demonstrates the feasibility of hybrid blockchain systems for decentralized applications requiring both high throughput and robust data integrity.

The study highlights the hybrid system's ability to manage large-scale transactions securely and efficiently, making it highly suitable for industries such as MSME product authentication, finance, and logistics. The integration of on-chain hashes ensures data authenticity, addressing the common trade-off between scalability and data integrity seen in traditional blockchain systems.

By leveraging off-chain storage to reduce blockchain network load while maintaining on-chain data integrity, the system enables scalable and secure handling of high transaction volumes. These results provide a practical foundation for developing blockchain applications that require high throughput, data authenticity, and resource efficiency in real-world scenarios.

Discussion

This research differs from previous studies as it focuses on a specific application for MSME product authentication in digital markets, which require high efficiency for large transaction volumes. The proposed hybrid system not only maintains high throughput (391 TPS for 1 million transactions), but also preserves data integrity by storing hashes on-chain. This ensures that data stored off-chain can still be securely verified, without significantly burdening the blockchain network. Unlike studies such as SlimChain, which focus on improving general throughput [24], this research is specifically designed to meet the security and scalability needs in MSME market scenarios.

The MSTDB study also shows that the hybrid approach can improve query efficiency by utilizing off-chain storage [25]. However, this research adds a new contribution by combining throughput efficiency, on-chain hash security, and relevance for product authentication applications. By leveraging on-chain hashes, our hybrid system provides a more comprehensive solution to address the specific needs of large digital markets involving large transactions and sensitive data.

Furthermore, this research addresses the limitations of previous studies by balancing the need for data integrity and scalability. With acceptable latency (862.4 ms for 1 million transactions) and high resource efficiency (87% CPU and 1.6 GB memory in the large transaction scenario), this study provides a practical solution that is relevant for blockchain applications in the MSME digital market.

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 10. NO. 3 FEBRUARY 2025
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i3.6010

CONCLUSION

This research successfully demonstrates that a blockchain-based hybrid system can provide an efficient solution for product authentication verification in MSME digital markets. By maintaining a throughput of 391 TPS for 1 million transactions, this system proves its ability to handle large transaction volumes with high efficiency. Unlike traditional fully on-chain approaches, this study introduces a new contribution through the integration of on-chain hashes that preserve data integrity while reducing the blockchain storage burden.

This research also makes a significant contribution by showing that the hybrid approach not only improves throughput and resource efficiency but also remains relevant for high-security applications, such as MSME product authentication. By combining throughput efficiency, acceptable latency, and data security, this study surpasses previous results like SlimChain and MSTDB, which tend to focus on general technical aspects without addressing the specific needs of blockchain-based applications.

However, this study has some limitations. All experiments were conducted in a simulated environment, and further testing is needed to validate performance in real-world scenarios. Additionally, scalability was only evaluated up to a volume of 1 million transactions. Future research could explore the integration of additional technologies such as sharding or cross-chain interoperability to further enhance the scalability of this system. Nevertheless, these findings pave the way for more cost-effective and scalable blockchain applications in large digital markets.

ACKNOWLEDGMENT

The authors would like to express their deepest gratitude to the Directorate of Research, Technology, and Community Service of the Ministry of Education, Culture, Research, and Technology of the Republic of Indonesia for their invaluable support and funding through the Regular Beginner Lecturer Research scheme with contract number: 108/SP2H/PT/LL7/2024. This research would not have been possible without their commitment to advancing technological innovation and research in Indonesia. Their encouragement and resources have significantly contributed to the success of this project and to the broader development of blockchain technology for MSME product authenticity verification. We are honored to have been a part of their mission to foster groundbreaking research that benefits society.

REFERENCE

[1] J. Ma, S.-Y. Lin, X. Chen, H.-M. Sun, Y.-C. Chen, and H. Wang, "A Blockchain-Based Application System for Product Anti-Counterfeiting," *IEEE Access*, vol. 8, pp. 77642–77652, 2020, doi: 10.1109/ACCESS.2020.2972026.

[2] N. T. Singh, Saurav, V. Sharma, A. Raizada, S. Sharma, and N. Pathak, "Identification of Fake Products using Blockchain Technology," *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 736–740, 2023, doi: 10.1109/ICSSIT55814.2023.10060998.

[3] M. Mhatre, H. Kashid, T. Jain, and P. Chavan, "BCPIS: Blockchain-based counterfeit product identification system," *Journal of Applied Security Research*, vol. 18, no. 4, pp. 740–765, 2023.

[4] R. R. Singh, R. R. Singh, A. Singh, and S. Vhatkar, "Comparative Analysis of Fake Product Identification System Using Blockchain Technology," *Journal of Electrical Systems*, vol. 20, no. 4s, pp. 470–477, 2024.

[5] T.-M. Choi and X. Ouyang, "Initial coin offerings for blockchain based product provenance authentication platforms," *Int J Prod Econ*, vol. 233, p. 107995, 2021.

[6] N. Vashistha, M. M. Hossain, M. R. Shahriar, F. Farahmandi, F. Rahman, and M. Tehranipoor, "eChain: A Blockchain-Enabled Ecosystem for Electronic Device Authenticity Verification," *IEEE Transactions on Consumer Electronics*, vol. 68, pp. 23–37, 2022, doi: 10.1109/tce.2021.3139090.

[7] N. Truong, G. M. Lee, K. Sun, F. Guitton, and Y. Guo, "A blockchain-based trust system for decentralised applications: When trustless needs trust," *Future Generation Computer Systems*, vol. 124, pp. 68–79, 2021.

[8] J. Liu and P. Jiang, "A blockchain-driven cyber-credit evaluation approach for establishing reliable cooperation among unauthentic MSMEs in social manufacturing," *Ind. Manag. Data Syst.*, vol. 121, pp. 724–749, 2020, doi: 10.1108/imds-05-2020-0295.

[9] L. Li *et al.*, "A Blockchain-Based Product Traceability System with Off-Chain EPCIS and IoT Device Authentication," *Sensors (Basel)*, vol. 22, 2022, doi: 10.3390/s22228680.

[10] H. Rathore, A. M. Mohamed, and M. Guizani, "A Survey of Blockchain Enabled Cyber-Physical

Systems," *Sensors (Basel)*, vol. 20, 2020, doi: 10.3390/s20010282.
[11] A. A.-N. Patwary, A. Fu, S. Battula, R. Naha, S. Garg, and A. Mahanti, "FogAuthChain: A secure location-based authentication scheme in fog computing environments using Blockchain," *Comput. Commun.*, vol. 162, pp. 212–224, 2020, doi: 10.1016/j.comcom.2020.08.021.
[12] H. M. Hussien, S. Yasin, N. Udzir, and M. I. H. Ninggal, "Blockchain-Based Access Control Scheme for Secure Shared Personal Health Records over Decentralised Storage," *Sensors (Basel)*, vol. 21, 2021, doi: 10.3390/s21072462.
[13] C.-H. Liao, H.-E. Lin, and S. Yuan, "Blockchain-Enabled Integrated Market Platform for Contract Production," *IEEE Access*, vol. 8, pp. 211007–211027, 2020, doi: 10.1109/ACCESS.2020.3039620.
[14] X. Yang, M. Li, H. Yu, M. Wang, D. Xu, and C. Sun, "A Trusted Blockchain-Based Traceability System for Fruit and Vegetable Agricultural Products," *IEEE Access*, vol. 9, pp. 36282–36293, 2021, doi: 10.1109/ACCESS.2021.3062845.
[15] M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang, "Blockchain-Based Decentralized Authentication Modeling Scheme in Edge and IoT Environment," *IEEE Internet Things J*, vol. 8, pp. 2116–2123, 2021, doi: 10.1109/JIOT.2020.3037733.
[16] Z. Cui *et al.*, "A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN," *IEEE Trans Serv Comput*, vol. 13, pp. 241–251, 2020, doi: 10.1109/TSC.2020.2964537.
[17] T. Choi and O. Xu, "Initial coin offerings for blockchain based product provenance authentication platforms," *Int J Prod Econ*, vol. 233, p. 107995, 2021, doi: 10.1016/j.ijpe.2020.107995.
[18] B. Shen, C. Dong, and S. Minner, "Combating Copycats in the Supply Chain with Permissioned Blockchain Technology," *Prod Oper Manag*, vol. 31, pp. 138–154, 2021, doi: 10.1111/poms.13456.
[19] J. Leng, M. Zhou, L. J. Zhao, Y. Huang, and Y. Bian, "Blockchain Security: A Survey of Techniques and Research Directions," *IEEE Trans Serv Comput*, vol. 15, pp. 2490–2510, 2022, doi: 10.1109/tsc.2020.3038641.
[20] X. Zhu, Y. Li, L. Fang, and P. Chen, "An Improved Proof-of-Trust Consensus Algorithm for Credible Crowdsourcing Blockchain Services," *IEEE Access*, vol. 8, pp. 102177–102187, 2020, doi: 10.1109/ACCESS.2020.2998803.
[21] X. Xu, M. Zhang, G. Dou, and Y. Yu, "Coordination of a supply chain with an online platform considering green technology in the blockchain era," *Int J Prod Res*, vol. 61, no. 11, pp. 3793–3810, 2023.
[22] R. Neiheiser, G. Inácio, L. Rech, C. Montez, M. Matos, and L. Rodrigues, "Practical Limitations of Ethereum's Layer-2," *IEEE Access*, vol. 11, pp. 8651–8662, 2023, doi: 10.1109/ACCESS.2023.3237897.
[23] Z. Guan, Z. Wan, Y. Yang, Y. Zhou, and B. Huang, "BlockMaze: An Efficient Privacy-Preserving Account-Model Blockchain Based on zk-SNARKs," *IEEE Trans Dependable Secure Comput*, vol. 19, pp. 1446–1463, 2020, doi: 10.1109/tdsc.2020.3025129.
[24] C. Xu, C. Zhang, J. Xu, and J. Pei, "SlimChain: Scaling Blockchain Transactions through Off-Chain Storage and Parallel Processing," *Proc. VLDB Endow.*, vol. 14, pp. 2314–2326, 2021, doi: 10.14778/3476249.3476283.
[25] E. Zhou *et al.*, "MSTDB: A Hybrid Storage-Empowered Scalable Semantic Blockchain Database," *IEEE Trans Knowl Data Eng*, vol. 35, pp. 8228–8244, 2023, doi: 10.1109/TKDE.2022.3220522.

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri