JIKO (Jurnal Informatika dan Komputer) Accredited KEMDIKTISAINTEK, No.0173/C3/DT.05.00/2025
Vol. 8, No. 3, Desember 2025, pp. 188-195 p-ISSN: 2614-8897
DOI: 10.33387/jiko.v8i3.10606 e-ISSN: 2656-1948

# IMPLEMENTING SHA-256 IN BLOCKCHAIN FOR SECURE AND TRUSTED ONLINE TRANSACTIONS OF MSMEs

**Matthew Luis [1], Rico Wijaya Dewantoro [2], Andrian Reinaldo Crispin[3], Adya Zizwan Putra[4], Abdi Dharma[5], Celine Chrysia[6], Cherry Piya Vagga[7]**

[1,2,3,4,5,6,7]Teknik Informatika, Fakultasi Teknologi dan Ilmu Komputer, Universitas Prima Indonesia, Medan, 20118, Indonesia
[*]Email: [1]matthewluisss@gmail.com, [2]rico@unprimdn.ac.id, [3] andrianreinaldocrispin@unprimdn.ac.id, [4]putrazizwanadya@gmail.com, [5]abdidharma@unprimdn.ac.id, [6]celine52572@gmail.com, [7]cherrypivavagga@gmail.com

(Received: 7 August 2025, Revised: 19 August 2025, Accepted: 25 September 2025)

**Abstract**

The advancement of information technology has driven digital transformation in various sectors, including Micro, Small, and Medium Enterprises (MSMEs), which are vital to Indonesia's economy. However, local MSMEs still face challenges in online transactions, especially related to data security and low consumer trust. Issues like data manipulation, lack of transparency, and weak security systems hinder optimal digitalization. This study implements the SHA-256 cryptographic algorithm in a blockchain system to enhance security and trust in local MSMEs' online transactions. SHA-256 is chosen for its ability to produce unique, permanent, and tamper-resistant hashes. The system adopts a decentralized blockchain model, where transactions are recorded in encrypted, chronologically linked blocks. The testing results show that the SHA-256-based blockchain system functions effectively in maintaining data integrity and preventing manipulation. Black Box Testing confirmed that the system operates correctly from the user's perspective, including login validation, transaction recording, manipulation detection, and transaction history retrieval. White Box Testing validated the internal logic of the system, proving the correct implementation of SHA-256 hashing, block linking, Proof of Work (PoW), and transaction validation mechanisms. All test cases passed successfully, demonstrating that the system is stable, functional, and secure.

**Keywords**: *Blockchain, SHA-256, MSMEs, Data Security*



**Corresponding Author: Rico Wijaya Dewantoro*

## 1. INTRODUCTION

The development of information technology has had a significant impact on various aspects of life, including the digital economy sector [1]. One of the rapidly growing forms of digital transformation is online buying and selling, which has now become a primary alternative for business actors, including local Micro, Small [2], and Medium Enterprises (MSMEs) [3]. MSMEs play a vital role in the national economy but still face various challenges in optimizing the use of digital platforms, particularly in terms of transaction security and consumer trust [4].

Trust issues remain one of the main obstacles in online transactions, especially when dealing with businesses that lack a strong reputation or adequate security systems [5]. Numerous cases of fraud, transaction data manipulation, and a lack of transparency in recording sales make potential buyers hesitant to conduct online transactions with MSME [6].

Blockchain technology emerges as a potential solution to address these issue [7]. Blockchain is a decentralized digital recording system that enables data to be recorded transparently, permanently, and immutably [8]. One of the key components of blockchain is the use of cryptographic algorithms such as SHA-256 (Secure Hash Algorithm 256-bit), which serves to secure and uniquely identify data blocks [9][10]. With this algorithm, each transaction is encoded into a hash that cannot be manipulated, thereby enhancing data integrity and security [11][12].

Blockchain technology has been widely applied across various sectors due to its advantages in transparency, security, and decentralization [13]. For example, a study by Rissal Efendi et al. [14] integrated blockchain and data security to improve the efficiency and transparency of the global logistics system, while research by Felicia et al. [15] highlighted that blockchain presents both challenges and opportunities in the Digital Era, particularly in the areas of data security and digital transactions. However, most previous studies have focused on large corporations and the technical aspects of blockchain implementation. The application of blockchain—specifically the SHA-256 algorithm—in the context of online transactions for local MSMEs is still rarely the main focus of research [16]. Yet, MSMEs are the backbone of Indonesia's economy and require secure, efficient technological solutions that align with their capacity and limitations.

Several recent studies have further supported the effectiveness of SHA-256 in digital transaction security. A study by Fajrin, A.M. et al. [9] compared the performance of SHA-256 and BLAKE2b in a blockchain context, showing that SHA-256 excels in efficiency and security, making it the preferred choice for maintaining data integrity in digital transactions. Another study by Rabtsani et al. [17] revealed that combining SHA-256 with AES-256 significantly enhances data security in digital payment applications. Additionally, research by Suryani et al. [18] demonstrated how blockchain improves security, efficiency, and financial transparency, reducing fraud risks and increasing trust in digital payment systems. Ilyas Mahfud et al. [19] showed that integrating SHA-256 with REST APIs is highly effective for ensuring data integrity and authentication between clients and servers. Lastly, a study by Prateek Baranwal et al. [20] discussed the use of SHA-256 in managing Non-Fungible Tokens (NFTs) on the Ethereum blockchain, illustrating its role in ensuring the authenticity and security of digital assets.

## 2. RESEARCH METHOD

the research method that will be carried out can be seen in Figure 1.

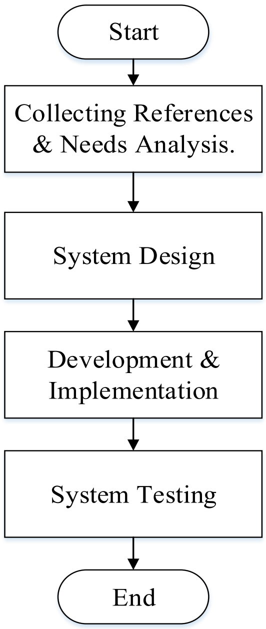


Figure 1. Stages of Research Methods

### 2.1 Collection References & Needs Analysis

This initial stage is crucial as it lays the foundation for the entire research and development process. It begins with an in-depth literature review to collect and study various references related to blockchain technology, the SHA-256 cryptographic algorithm, and security mechanisms for digital transactions, especially in the context of Micro, Small, and Medium Enterprises (MSMEs). Sources include scientific journals, books, case studies, and previous research projects. The purpose is to gain a comprehensive understanding of how blockchain and cryptography work, the challenges in online transactions, and the potential solutions offered by these technologies.

Simultaneously, a needs analysis is conducted by engaging with a selected local MSME to understand their specific pain points and expectations when conducting online transactions. This involves interviews or surveys with business owners and stakeholders to identify critical issues such as transaction fraud, lack of transparency, and system inefficiencies. The analysis helps to align the system being developed with real-world problems faced by MSMEs, ensuring that the solution is not only theoretically sound but also practically useful.

### 2.2 System Design

In this phase, the overall system architecture is designed based on the findings from the needs analysis. The goal is to build a user-centric solution tailored to the operational model of a local MSME. The system is broken down into several key components:

1. Frontend Design: Utilizing Flutter, a modern UI toolkit for building natively compiled applications across mobile and web platforms. The interface is designed to be simple, intuitive,

and accessible even for users with minimal technical knowledge.

2. Backend Development: The backend is constructed using Laravel, a robust PHP framework known for its scalability and security. This component handles user authentication, transaction logic, database management, and communication with the blockchain layer.
3. Blockchain Structure: A lightweight, customized blockchain model is designed, where transaction data is stored in blocks. Each block contains a hash of the previous block, a timestamp, and the hashed transaction data using SHA-256. This structure ensures chronological order and immutability of transaction records.

Clear data flows and security mechanisms are also defined during this phase, including how data is hashed, how blocks are chained, and how validation occurs within the system.

### 2.3 Development & Implementation

This stage involves translating the design into a working application through systematic development. The development process includes:

1. Building the Frontend and Backend: Writing the actual code using Flutter and Laravel based on the designs created. The application includes modules for transaction entry, user authentication, and a dashboard to track transactions and hash values.
2. Applying SHA-256 Hashing: The SHA-256 algorithm is implemented to convert each transaction's data into a fixed-length hash string. This hash acts as a digital fingerprint of the data, making it impossible to alter the information without being detected.
3. Constructing the Blockchain: Each hashed transaction is placed into a block, which also contains a reference (hash) to the previous block, forming a continuous, tamper-resistant chain. New blocks are added sequentially, and the system checks the integrity of the chain during every operation.
4. Integration: All components—frontend, backend, and blockchain—are integrated into a unified platform that can be accessed by MSME users to perform and verify transactions.

This phase ensures that the blockchain application is functional, user-friendly, and aligned with the technological capabilities of small business users.

### 2.4 System Testing

System testing is a critical phase to evaluate the reliability, performance, and security of the application. Several types of tests are conducted:

1. Functional Testing: Ensures that all system features work as intended, including user registration, transaction processing, and data hashing.
2. Hashing Validation: Verifies the accuracy of the SHA-256 algorithm in generating consistent and tamper-proof hashes for the same input, and differing hashes for altered input, thus confirming data integrity.
3. Blockchain Integrity Check: The system is tested to ensure that the chain structure is preserved, with no broken links between blocks. Any attempt to tamper with data in a block should result in a mismatch in the hash values, immediately flagging an integrity issue.
4. Black Box and White Box Testing: Black Box testing focuses on evaluating the system's functionality from the user's perspective without examining the internal code, ensuring that all inputs produce the expected outputs. In contrast, White Box testing analyzes the internal logic, algorithms, and code structure to detect hidden vulnerabilities, optimize performance, and ensure secure data flow within the blockchain system.

The results of these tests determine whether the system is ready for real-world use. If issues are found, the development team iterates the design until all benchmarks for functionality, security, and user experience are met.

## 3. RESULT AND DISCUSSION

This research resulted in an online buying and selling transaction system based on blockchain technology, implemented using the SHA-256 hash algorithm.

### 3.1 Collection References & Needs Analysis Result

The initial stage of the research involved collecting relevant references and conducting a needs analysis to identify the core problems faced by local MSMEs in conducting online transactions. Through a comprehensive literature review, various studies and publications related to blockchain technology, SHA-256 cryptographic algorithms, and digital transaction security were analyzed. These references provided valuable insights into how blockchain can enhance data integrity, ensure transparency, and prevent unauthorized manipulation in transaction systems.

In addition to theoretical references, a field study was conducted with a selected local MSME operating in the retail sector. Interviews and informal discussions were held with the business owner to better understand their daily operational challenges. The results revealed several key issues:

1. Lack of Consumer Trust: Many potential customers hesitate to transact online due to concerns about fraud and data manipulation.
2. Weak Transaction Records: The current transaction system used by the MSME lacked transparency and proper data tracking.
3. Limited Digital Knowledge: The business owner had minimal experience with advanced

technologies, highlighting the need for a user-friendly solution.

4. Desire for Efficiency: There was a strong desire to simplify transaction recording and enhance customer confidence without requiring large investments or complex infrastructure.

These findings confirmed the relevance of blockchain as a potential solution and guided the development of a system that is not only secure and reliable but also easy to use and tailored to the needs of small business owners. The implementation of SHA-256 within a simplified blockchain structure was identified as the most suitable approach, balancing security and simplicity for practical use by MSMEs

### 3.2 System Design Result

The system design developed to ensure the accuracy, transparency, and security of transaction data between sellers and buyers is shown in Figure 2 below.

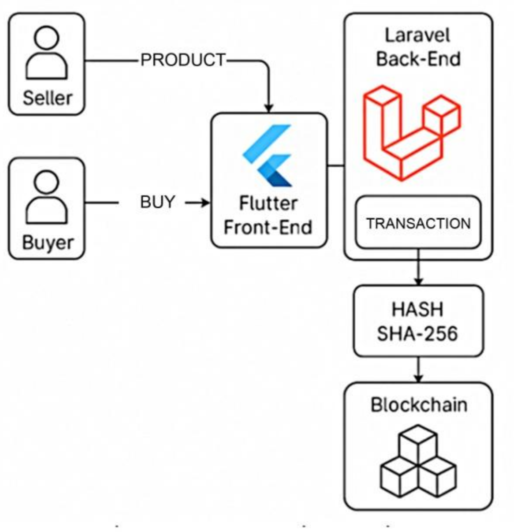


Figure 2. System Design Result

As shown in Figure 3, the developed system aims to enhance the security and integrity of online transaction data for local MSMEs through the implementation of the SHA-256 algorithm within blockchain technology. The mobile application was built using Flutter, with Laravel as the backend for data management. Each transaction performed by the user is processed to generate a unique hash using SHA-256, which is then stored in a block chain structure (blockchain). This hash serves as a permanent identifier of the transaction data, allowing the system to detect any tampering through hash value discrepancies. Thus, the system ensures transparency, authenticity, and resilience of the data against modification.

### 3.3 Development & Integration Result

The development of this system was carried out in the form of a mobile application designed to assist local MSMEs in conducting online transactions with a higher level of security using Blockchain technology based on the SHA-256 algorithm. The application was built using a modular approach to allow easy integration with existing systems used by MSMEs, such as transaction recording systems or inventory systems. The main focus of the development is to ensure data security, transaction authenticity, and to increase trust between business actors and customers in a digital environment. The following Figure 3 shows the initial view of the application in the form of a login screen.


Figure 3. Login Form Display

The login screen is used as the initial authentication for buyers to access the system. After a successful login, the home screen is displayed where buyers can purchase MSME products and add them to the shopping cart, as shown in Figure 4.

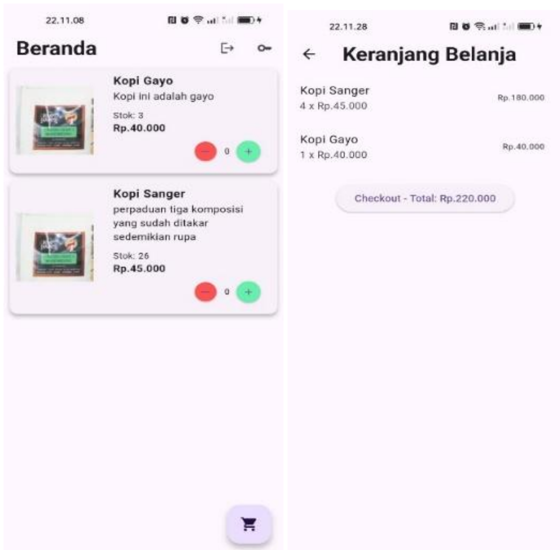


Figure 4. Home and Shopping Card Display

If the transaction is successfully completed, each transaction is recorded into the blockchain network, where 1 block represents 1 transaction. Figure 5 below shows the blockchain network in the developed application.

s

### 3.4 System Testing Result

The testing conducted aims to evaluate the effectiveness of the SHA-256 algorithm implementation in maintaining data integrity within the developed blockchain system. The main focus of the testing is on how the block chain structure (blockchain) is able to detect data changes in a single block and the impact of those changes on the entire chain

#### 3.4.1 Transaction Recording and Manipulation Detection Testing Results

The testing was carried out in a complete scenario that reflects the process of transaction recording and how the system responds in the event of data manipulation. Each recorded transaction generates one block containing the transaction number, transaction date, buyer and seller names, total price, previous block hash, nonce value, current hash result, and the actual or valid hash, which should match the current hash. Figure 6 below shows the transaction information stored in a single blockchain block


Figure 6. Transaction Information Stored in a Single Blockchain Block

All of these elements are combined and processed using the SHA-256 algorithm to generate a hash. The result will be used as the previous hash in the next block, creating a chained relationship that cannot be altered without affecting the subsequent structure.

1. Normal process.

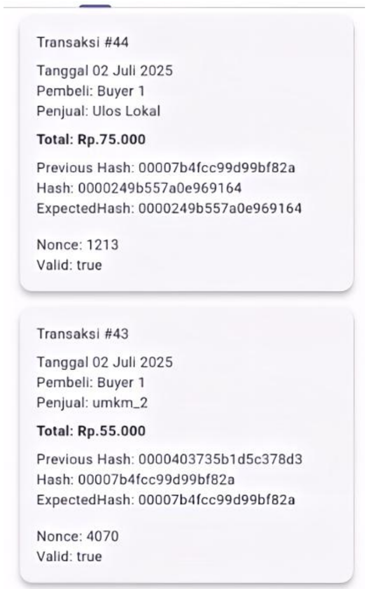


Figure 7. Normal Transaction Visualization

Under normal conditions, the system records two transactions sequentially, as visualized in Figure 3.3. Each block has a valid hash and is connected in a sequential chain. The Proof of Work process is carried out with a low difficulty level (two leading zeros in the hash), and the time required ranges from 1.2 to 2.5 seconds. For example, Transaction #43 generates the hash 00007b4fcc99d99bf82a. This hash value is then used as the previous hash for Transaction #44, which produces the hash 0000249b557a0e969164. The linkage between these blocks is visualized in Figure 7.

2. Manipulation process.


Figure 8. Transaction Information of the Manipulated Block

To test the system's resilience to changes, one of the blocks—specifically Transaction #41—was manipulated. The total transaction price was changed from Rp 90,000 to Rp 50,000. This alteration caused the hash calculation to differ from the original.

Expected Hash : **bd276003758e75166826**
Hash : **000087e5222a80850b6a**

Since the new hash does not match the expected hash, the system marks this block as invalid, as shown in Figure 8. The system displays an error message: Change detected in: total 90.000 to 50.000.

3. Transaction process with different buyer and different seller data.

Four transactions were carried out sequentially with different buyer and seller data to simulate dynamic recording in the blockchain system. Each transaction generates a new block that stores information such as transaction number, buyer and seller identities, total price, and transaction time. The data is hashed using the SHA-256 algorithm, then validated through the Proof of Work mechanism and linked sequentially using the previous hash property.

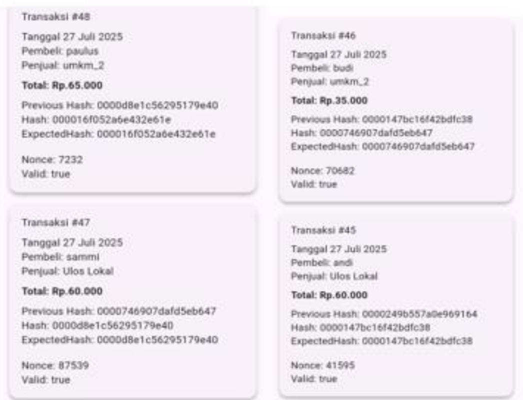


Figure 9. Transaction Information of Block with Different Data

### 3.4.2 Blockchain Visualization and Structure Testing Results

The developed blockchain structure can be described as a linear chain where each block is directly connected to the previous block through the hash value. Figure 10 illustrates the block-to-block relationship structure as a simple graph network.

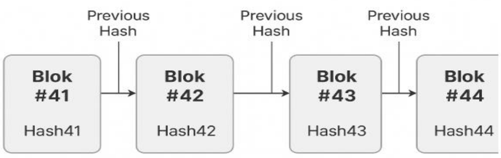


Figure 10. Block Chain Structure (Blockchain) with Hash Relationships Between Blocks

If one of the blocks is altered—for example, Block #41—then the entire chain that follows will be broken because the previousHash no longer matches. This demonstrates the fundamental principle of blockchain, which is immutability, meaning the inability to change data without breaking the chain.

Simply put, the way blockchain works is similar to a receipt book. Every time a transaction occurs, it is written on a page. At the end of each page, you write a unique code from the previous page. So, if a previous page is altered, all the following pages become incorrect. Blockchain works the same way. Each transaction is stored in a block. Every block has a unique code (called a *hash*), which is generated from the transaction data. This hash is like a "digital fingerprint." If someone changes the data, the hash also changes, and the next block becomes invalid. Because all the blocks are interconnected, anyone trying to alter even a single piece of data will break the entire chain. This is why blockchain is very difficult to manipulate. This structure is also referred to as a graph network because it forms a mathematically connected network of blocks

### 3.4.3 Blockchain Structure and Security Analysis Testing Results

The test results indicate that SHA-256 is effective in generating unique hash values and is highly sensitive to any changes in the data. The blockchain structure, which connects blocks through the previous hash attribute, has proven capable of maintaining data integrity. Furthermore, the system can automatically detect data manipulation, demonstrating its reliability in ensuring transparency and security in transactions. The Proof of Work process also runs efficiently for MSME-scale applications, with relatively short hash computation times and an adjustable difficulty level, making it well-suited for practical implementation.

### 3.4.4 Black Box and White Box Testing Results

To ensure that the developed system functions according to the requirements and specifications, testing was carried out using two methods: Black Box Testing and White Box Testing. The results of Black Box Testing are presented in Table 1.

Based on Table 1, the Black Box testing results indicate that the system functions as expected for all key test cases. For fundamental functionalities like

Tabel 1. Black Box Testing Results

| No | Test Case | Input / Action | Expected Output | Actual Output | Result |
|---|---|---|---|---|---|
| 1 | Login with valid credentials | Valid username & password | Successfully logged into the system (home screen displayed) | As expected | Pass |
| 2 | Login with invalid credentials | Incorrect username/password | Error message “Login failed” appears | As expected | Pass |
| 3 | Add product to cart | Select product → click “+” | Product added to shopping cart list | As expected | Pass |
| 4 | Make a purchase transaction | Select product → checkout → confirm payment | Transaction recorded in blockchain (1 block created) | As expected | Pass |
| 5 | Manipulate transaction data | Modify total price in 1 block | System detects changes → block marked invalid | As expected | Pass |
| 6 | View transaction history | Click “History” menu | All transactions displayed in sequential block order | As expected | Pass |

login, the system successfully validates user credentials, both valid and invalid, by providing the correct responses. The ability to add products to the cart and make a purchase transaction also worked flawlessly, with the system successfully recording each transaction onto the blockchain. More crucial tests, focusing on data security and integrity, also showed satisfactory results. When transaction data was manipulated, the system successfully detected the change and flagged the block as invalid, confirming that the blockchain's security mechanisms are working properly. Finally, the functionality to view transaction history also worked correctly, displaying all data in sequential block order. Overall, all test cases passed, showing that the system is stable, functional, and secure from a user's perspective.

The results of White Box Testing are presented in Table 2.

Tabel 1. White Box Testing Results

| No | Test Case | Testing Focus | Expected Behavior | Actual Behavior | Result |
|---|---|---|---|---|---|
| 1 | Hash generation function | Transaction data processed with SHA-256 function | Generates a unique 64-character hash | As expected | Pass |
| 2 | Block linking | New block stores previousHash of the prior block | Chain formed without error | As expected | Pass |
| 3 | Proof of Work | Mining continues until hash begins with 2 zeros | Average time 1.2 – 2.5 seconds | As expected | Pass |
| 4 | Manipulation detection | If data modified → hash changes → block invalid | System flags block as invalid | As expected | Pass |
| 5 | Transaction validation | Transaction data validated before entering blockchain | Only valid transactions recorded | As expected | Pass |

Based on Table 2, the White Box testing results indicate that the internal structure and code logic of the blockchain system are functioning correctly. This testing focused on the core mechanisms, starting with the hash function. The results confirmed that the function consistently generates a unique 64-character hash using the SHA-256 algorithm, which is crucial for data integrity. Following that, the block linking test successfully proved that each new block records the hash of the preceding block (previousHash), ensuring the formation of a complete and unbroken chain. For the Proof of Work (PoW) aspect, the test validated that the "mining" process works as intended—finding a hash that meets a specific criterion (starting with two zeros) within the expected timeframe (1.2–2.5 seconds). This indicates that the PoW mechanism is well-implemented and efficient. Finally, the transaction validation test proved that the system only accepts valid transaction data into the blockchain, preventing the recording of unauthorized information. Overall, all these White Box testing results show that the blockchain system's code architecture and implementation are robust, meeting the fundamental functional and security requirements.

### 3.5 Discussion

This research was motivated by the low consumer trust in the security of digital transaction data in MSMEs, as well as the potential for data manipulation in conventional systems that lack decentralized validation mechanisms. This issue highlights the need for a technology that can automatically and transparently maintain data integrity. The implementation results show that the SHA-256 algorithm within the blockchain system successfully generates unique hashes that are highly sensitive to changes. The system is capable of detecting data manipulation in a single block because such changes cause the hash to no longer match the following block, thereby breaking the chain. This proves that the hash structure and inter-block linkage effectively preserve data integrity [13]. These findings are consistent with previous literature that highlights the effectiveness of blockchain in maintaining data integrity and system transparency, particularly in sectors such as finance, logistics, and supply chains. For example, research by Lanzini et al. [21] stated that the adoption of blockchain by SMEs is greatly influenced by organizational maturity and management support to ensure successful technology implementation at the micro-organizational level. In addition, a study by Ramachandran et al. [22] explained that blockchain provides key benefits such as trust-building, traceability, transaction automation, and data transparency in multi-stakeholder environments like digital supply chains. Research by Wang, Han et al. [23] also supported that the decentralized structure of blockchain is highly effective in strengthening trust and auditability of transaction data in modern supply chains. However, its application in the context of local MSMEs has rarely been studied. Through this research, the implementation of blockchain is extended to the micro scale, demonstrating that the system can also be applied to MSMEs as a form of protection for digital transactions. Practically, this system can be used by MSMEs to increase customer trust, provide a permanent digital footprint, and serve as a foundation for business transparency. In an educational context, the system has the potential to become a learning medium for technology-based entrepreneurship. From a policy perspective, it opens opportunities to serve as a reference in the development of future digital MSME policies.

To comprehensively evaluate the system's performance, both Black Box and White Box testing methodologies were employed. The results from the Black Box testing (Table 1) confirm that the system's functional requirements are met from an end-user perspective. Tests for core functionalities, such as user login, adding products to a cart, and completing purchase transactions, all passed successfully. Most importantly, the system's ability to detect data manipulation and display transaction history worked as expected, proving that the system is stable, functional, and secure from a user's viewpoint.

The White Box testing (Table 2) provided deeper insights into the system's internal mechanisms, validating the integrity of the code's logic and structure. This stage of testing was crucial for confirming the correct implementation of the blockchain's core principles. The hash generation function consistently produced unique, 64-character hashes, affirming the correct use of the SHA-256 algorithm. The block linking test proved that the previousHash attribute was correctly stored in each new block, ensuring the formation of a secure and unbroken chain. Furthermore, the Proof of Work (PoW) mechanism was validated to function within an efficient timeframe, and the transaction validation logic was shown to correctly filter out invalid data before it could be added to the blockchain.

Collectively, the successful results from both testing approaches provide a strong basis for the system's reliability. The Black Box tests confirmed the system's usability and external behavior, while the White Box tests guaranteed the soundness of its internal architecture and security protocols. This dual validation approach demonstrates that the system is not only functional for its intended users but also robust and secure at a foundational, technical level.

## 4. CONCLUSION

Based on the implementation and testing results, it can be concluded that the SHA-256 algorithm has been effectively applied within the blockchain system to enhance data security in online transactions for local MSMEs. This algorithm generates unique, irreversible hashes that are highly sensitive to data changes, thereby ensuring the integrity of each block in the transaction chain. The blockchain structure, which links each block through the previous hash, creates a system that is difficult to manipulate, enhancing transparency and user trust. This represents a significant added value for local MSMEs that are adapting to the digital era and require a secure, reliable, and traceable transaction system.

However, this research has several limitations that must be acknowledged. First, the system developed is a prototype and has not been tested in real-world MSME conditions. As such, its performance and scalability under heavy transaction loads remain to be evaluated. Second, the success of a broader implementation would be challenged by the existing levels of digital literacy and technological infrastructure within the MSME community.

For future research, it is recommended to expand this prototype into a full-scale application. This could involve integrating smart contracts to automate key business processes, implementing digital tokens for new payment models, and establishing connections to broader payment systems to facilitate wider adoption. Furthermore, a long-term study on the practical adoption and impact of this system on MSME business growth and customer trust would provide valuable empirical data

## 5. REFERENCES


[1] D. R. Barus, J. S. Simangunsong, S. Engelika, B. Ginting, and S. Saragih, “Pengaruh Perkembangan Teknologi Informasi Terhadap Pasar Global The Influence Of Information Technology Developments On Global Markets,” pp. 495–500, 2024.

[2] A. B. Mokodaser, M. Maramis, and C. Tooy, “Dampak Digitalisasi Perdagangan Usaha Mikro Kecil Menengah Dari Offline Menjadi Online Selama Masa Pandemi Covid-19,” *Lex Priv.*, vol. 10, no. 4, pp. 1–14, 2022.

[3] Putri Salsabila Indrawan Lubis and Rofila Salsabila, “Peran UMKM (Usaha Mikro, Kecil, Dan Menengah) Dalam Meningkatkan Pembangunan Ekonomi Di Indonesia,” *MUQADDIMAH J. Ekon. Manajemen, Akunt. dan Bisnis*, vol. 2, no. 2, pp. 91–110, 2024, doi: 10.59246/muqaddimah.v2i2.716.

[4] N. Ramadhani, A. I. Sugesti, D. N. Sagita, and E. Purwanto, “Pemanfaatan Marketplace Digital dalam meningkatkan Kinerja UMKM melalui Sarana Komunikasi di Era Digital,” vol. 2, no. 2, pp. 1–20, 2025.

[5] K. Dan, K. Transaksi, D. A. N. Inovasi, and P. Digital, “Kemudahan dan keamanan transaksi e-commerce dan inovasi pembayaran digital,” vol. XXI, no. 1, pp. 24–32, 2024.

[6] P. Online and K. Digital, “MENINGKATKAN KESADARAN DIGITAL DALAM PENCEGAHAN PENIPUAN ONLINE UNTUK,” vol. 1, pp. 56–63, 2024.

[7] A. Info, “Eksplorasi Faktor Penerimaan Blockchain oleh Pengusaha UMKM,” vol. 1, no. 1, pp. 13–17, 2025.

[8] H. Zakiah, F. I. Lestari, A. S. Gea, F. Al-qowim, and N. Fitriana, “Implementasi Sistem Informasi Berbasis Blockchain untuk Pengelolaan Kas dan Keuangan Rumah Sakit : Studi Kasus pada Layanan Rawat Jalan,” vol. 02, no. 04, pp. 982–986, 2025.

[9] A. M. Fajrin and F. Baharuddin, “Analisis Performa Algoritma BLAKE2b dan SHA-256 pada Implementasi Blockchain,” vol. 6, no. 2, pp. 451–460, 2025.

[10] N. I. Septiani, A. Sediyono, and A. Rochman, “Perancangan Web Defacement Monitoring Dengan Menggunakan Metode Komparasi Nilai Hash1,” *JIKO (Jurnal Inform. dan Komputer)*, vol. 5, no. 2, pp. 150–155, 2022, doi: 10.33387/jiko.v5i2.4852.

[11] R. Welekar, B. Balkhande, T. Jadhav, V. Khetani, B. R. Singh, and A. Shukla, "Leveraging Blockchain for Enhanced Data Integrity and Security in Information Systems," *J. Inf. Syst. Eng. Manag.*, vol. 10, pp. 416–428, 2025.

[12] Andi, C. Juliandy, Robet, and O. Pribadi, "Securing Medical Records of COVID-19 Patients Using Elliptic Curve Digital Signature Algorithm (ECDSA) in Blockchain," *CommIT J.*, vol. 16, no. 1, pp. 87–96, 2022, doi: 10.21512/COMMIT.V16I1.7958.

[13] Andi, R. Purba, and R. Yunis, "Application of Blockchain Technology to Prevent The Potential Of Plagiarism in Scientific Publication," 2019, doi: 10.1109/ICIC47613.2019.8985920.

[14] T. Sistem and L. Global, "Jurnal JTIK ( Jurnal Teknologi Informasi dan Komunikasi ) Integrasi Blockchain dan Keamanan Data untuk Meningkatkan," vol. 9, no. June, pp. 461–466, 2025.

[15] J. Felicia1*, Elvilie2, Calista3, Sebastian Areen Chic4, Muhammad Fardian Bilqisthi5, "Tantangan dan Peluang Blockchain di Era Digital dalam Bidang Keamanan Data dan Transaksi," *Αγαη*, vol. 15, no. 1, pp. 37–48, 2024.

[16] W. Safitri and M. Huda, "Adoption of Blockchain Technology in Indonesian MSME Supply Chain Management (SCM).," *Ekonika J. Ekon. Univ. Kadiri*, vol. 8, no. 2, pp. 308–326, 2023, doi: 10.30737/ekonika.v8i2.3374.

[17] M. Rais Rabtsani, A. Triayudi, and G. Soepriyono, "Combination of AES (Advanced Encryption Standard) and SHA256 Algorithms for Data Security in Bill Payment Applications," *SAGA J. Technol. Inf. Syst.*, vol. 2, no. 1, pp. 175–189, 2024, doi: 10.58905/saga.v2i1.250.

[18] R. M. Handoko, B. Aulyansyah, A. Trisna, and R. Delon, "Implementasi Blockchain Untuk Keamanan Sistem Pembayaran Digital dan Optimasi Transaksi Keuangan ( Studi Kasus Industri Fintech di Indonesia )," vol. 4, pp. 64–74, 2024.

[19] I. Mahfud and P. Hadi Utomo, "Implementasi Sistem Kriptografi RSA Signature dengan SHA-256 pada Mekanisme Autentikasi REST API," *Pros. Semin. Nas. Teknoka*, vol. 6, no. 2502, pp. 84–92, 2022, doi: 10.22236/teknoka.v6i1.431.

[20] P. Baranwal, R. Katiyar, P. Kundu, and M. Yadav, "Implementation of SHA256 for NFT Management Using Blockchain," pp. 51–57, 2024.

[21] F. Lanzini, J. Ubacht, and J. De Greeff, "Blockchain adoption factors for SMEs in supply chain management," *J. Supply Chain Manag. Sci.*, vol. 2, no. 1, pp. 47–68, 2021, doi: 10.18757/jscms.2021.5624.

[22] G. S. Ramachandran *et al.*, "Blockchain in Supply Chain: Opportunities and Design Considerations," *Springer Optim. Its Appl.*, vol. 194, pp. 541–576, 2022, doi: 10.1007/978-3-031-07535-3_17.

[23] Y. Wang, J. H. Han, and P. Beynon-Davies, "Understanding blockchain technology for future supply chains: a systematic literature review and research agenda," *Supply Chain Manag.*, vol. 24, no. 1, pp. 62–84, 2019, doi: 10.1108/SCM-03-2018-0148.