Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer
Vol. 24, No. 1, November 2024, pp. 105∼116
ISSN: 2476-9843, accredited by Kemenristekdikti, Decree No: 200/M/KPT/2020
DOI: 10.30812/matrik.v24i1.4337

Blockchain-Based Traditional Weaving Certification and Elliptic Curve Digital Signature

Pradita Dwi Rahman , Heri Wijayanto , Royana Afwani , Melki Jonathan Andara , Wirama Wesdawara , Ahmad Zafrullah Mardiansyah
Universitas Mataram, Mataram, Indonesia

Article Info

Article history:

Received July 31, 2024
Revised October 21, 2024
Accepted November 05, 2024

Keywords:

Blockchain
Digital Signature
E-Certificate
Non-Fungible Token

ABSTRACT

Traditional weaving in West Nusa Tenggara was essential to the region's cultural heritage. Many local micro, small, and medium enterprises continued to practice traditional weaving using natural materials. However, the rise of synthetic materials threatened this tradition, making distinguishing between natural and synthetic woven fabrics difficult. This study aimed to develop a blockchain-based self-certification system to enhance traceability, security, and efficiency using Non-Fungible Tokens. The research method leveraged the Elliptic Curve Digital Signature Algorithm for user authentication and smart contracts to mint Non-Fungible Tokens, ensuring the authenticity and origin of each product. Each product's metadata was signed with a digital signature that anyone could authenticate, and the outcome and the product metadata became a certificate. This study resulted in a web prototype with an easy-to-use interface that allowed artisans to create certificates and sell their registered works. This solution aimed to ensure the authenticity of traditional woven products by offering secure and transparent blockchain technology.

Copyright ©2024 The Authors.
This is an open access article under the CC BY-SA license.

Corresponding Author:

Heri Wijayanto,
Department of Informatics Engineering, Faculty of Engineering,
Universitas Mataram, Mataram, Indonesia,
Email: heri@unram.ac.id.

How to Cite:
P. Rahman, H. Wijayanto, R. Afwani, W. Wesdawara, and A. Mardiansyah, "Blockchain-Based Traditional Weaving Certification and Elliptic Curve Digital Signature", *MATRIK: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer*, Vol. 24, No. 1, pp. 105-116, November, 2024.
This is an open access article under the CC BY-SA license (https://creativecommons.org/licenses/by-sa/4.0/)

1. INTRODUCTION

The craft of weaving is a traditional art form and skill that has existed for centuries. It is an essential part of culture related to its knowledge, cultural heritage, beliefs, and social organization systems [1]. In West Nusa Tenggara, weaving is an essential part of the local cultural heritage, with traditional motifs reflecting the values and identity of the Sasak community [2]. This traditional craft boasts a variety of patterns from different regions, adding to its uniqueness. Many artisans in the region still rely on hand tools instead of modern machinery, adding a personal touch to their craftsmanship. Today, woven fabric artisans in West Nusa Tenggara are primarily Micro, Small, and Medium Enterprises (MSMEs). These enterprises face limitations in production power and funds compared to larger companies. Moreover, the widespread use of synthetic materials in woven fabric production poses a significant risk to these MSMEs. The similarity between synthetic and natural woven fabrics makes it difficult for customers to distinguish between the two.

Blockchain technology holds great potential to address this issue. Recent advancements in blockchain have opened new avenues for ensuring authenticity and provenance. Blockchain is an immutable data structure formed by a series of data blocks connected linearly in time-ordered [3]. Blockchain offers numerous benefits, such as receiving, validating, and providing trusted data, offers numerous benefits, such as secure ownership and copyright applications [4]. Its potential to revolutionize industries by ensuring data integrity and increasing stakeholder trust is significant [5]. As a decentralized database network, it serves as a master ledger, recording every transaction [6]. Blockchain also streamlines business processes using smart contracts. It is computerized protocols that automatically execute contract clauses [7]. Due to the various technologies it integrates, blockchain applications are safe and transparent. In the blockchain world, there is a technology called non-fungible tokens (NFT). It is a unique digital asset representing ownership of physical items such as art, images, movies, and music [8]. Each NFT has a unique identity based on metadata recorded on distributed ledgers. This metadata is usually stored in the InterPlanetary File System (IPFS). It is a decentralized storage and transfer protocol for data sharing [9]. It operates as a peer-to-peer (P2P) distributed file system, aiming to connect all computing devices using a standard file system. IPFS is a content-addressable, peer-to-peer hypermedia distribution protocol, where nodes in the network publish [10]. IPFS allows files to be stored permanently, traceably, immutably, and uniquely [11]. Furthermore, to increase trust in the information provided, digital signatures can be utilized to verify the authenticity and integrity of the information. A digital signature is a mathematical scheme that allows someone with a public and private key pair to authenticate a digital message [12]. There are several algorithms for implementing a digital signature, and in this study, we use the Elliptic Curve Digital Signature Algorithm (ECDSA). It is an efficient version of the Digital Signature Algorithm (DSA) that uses operations on elliptic curves. ECDSA offers improved efficiency over DSA by replacing modulo prime arithmetic with operations over an elliptic curve. It can achieve a level of cryptographic security equivalent to DSA but with a much smaller key size. It makes ECDSA more resource-efficient, enabling faster digital signatures and reducing the need for storage space and bandwidth [13]. It is widely used in web security technologies such as DNSSec and TLS, as well as in cryptocurrencies such as Bitcoin and Ethereum [14].

Several recent studies have explored and integrated Blockchain technologies in innovative ways. Hasan et al. [15] proposed a unique approach to managing Digital Twins (DTs) ownership using NFTs, providing proof of delivery for physical assets, and using IPFS for storage. They have addressed the challenge of accessing and managing DTs after asset movements or sales due to centralized systems. Their solution, which integrates NFTs, establishes a decentralized, secure, and traceable ownership management and delivery-proof system, ensuring transparent and verified ownership records. In contrast, Cruz et al. [16] propose the development of a decentralized health marketplace that utilizes blockchain technology, specifically NFT (Non-Fungible Tokens) and DeFi (Decentralized Finance). In this platform, patients can sell their data anonymously through NFTs to researchers. Blockchain offers a transformational medical record data management solution by enhancing data security, privacy, interoperability, and transparency. This technology also reduces dependence on central authorities, reducing the risk of data leaks and unauthorized access. On the other hand, Jamal et al. [17], explores blockchain technology as a decentralized approach to managing personal identity data, addressing issues such as identity theft and unauthorized access. Using blockchain technology, the system ensures that personal records are stored securely and can only be accessed by authorized entities. It offers a decentralized platform where users control who can access their information, thereby reducing the risks associated with traditional centralized systems. This system can be used across various sectors, increasing security, transparency, and efficiency, especially in environments prone to data breaches. Besides, Pawar et al. [18], developed a blockchain-based system for creating and verifying e-certificates. This system utilizes blockchain technology and the Interplanetary File System (IPFS) to generate tamper-resistant digital certificates. In their approach, blockchain stores the certificate's hash uploaded by educational institutions to IPFS. Each certificate is issued with a unique hash stored on the blockchain, ensuring the certificate data remains immutable and secure-furthermore, Chen et al. [19] introduced blockchain technology to strengthen ownership verification mechanisms in AI Generative Content (AIGC). Challenges addressed include data leaks, model replay attacks, and copyright protection. Proposed solutions include model watermarking, reputation-based worker selection, effective incentive mechanisms, and blockchain for decentralized and tamper-resistant ownership recording. These studies collec-

tively contribute to the existing body of knowledge by addressing various aspects of NFTs, from economic implications and security challenges to interoperability, environmental impact, and cultural significance.

Based on the literature above, blockchain technology has been applied in various fields, such as academic credentials, AI-generated content, and digital asset management. However, a significant research gap remains in applying blockchain technology to preserve cultural heritage, especially traditional weaving crafts. Unlike previous studies that mainly discuss the use of blockchain for digital assets or academic credentials certificates, our study introduces a new approach by integrating blockchain technology, NFTs, Elliptic Curve Digital Signature Algorithm (ECDSA), and IPFS into a certification system designed explicitly for traditional weaving crafts. This unique approach utilizes NFT as a digital representation of assets and digital signatures to authenticate and preserve the culture of woven products. Furthermore, our study addresses traditional artisan's challenges by providing a blockchain-based solution that enhances woven fabric's traceability, security, and authenticity. By developing a blockchain-based certification system that utilizes NFT and IPFS for metadata storage and digital signatures for authenticity, our study fills the gap in utilizing blockchain to protect traditional weaving crafts.

The contributions of this research are as follows: First, we developed a web platform to validate authenticity using NFT technology, e-certificates, and digital signatures, where each NFT's metadata is signed and displayed on an e-certificate. Additionally, it is a platform for artisans to sell their woven art as NFTs using ERC-721, enabling token ownership transfer to other users. Furthermore, the research introduces a digital signature verification system to increase system transparency and enable users to verify certificates. These innovations aim to introduce blockchain technology to the Lombok weaving craft sector, ensuring authenticity and supporting artisans.

The rest of the paper is organized as follows: Section 2 presents the Research Method. Section 3 presents the results and analysis of the proposed blockchain-based solution, followed by the implementation details and algorithms. Section 4 presents the conclusion from everything discussed previously. Section 5 acknowledges. Section 6 presents declarations that state the author's contribution, funding statement, and competing interests.

2. RESEARCH METHOD

This section outlines the methodological approach used in our study to develop a blockchain-based certification system for traditional Lombok weaving. We employed a structured workflow to guide our research process, ensuring a systematic and comprehensive approach to addressing the challenges faced by traditional artisans. The following subsections detail our research's specific steps and techniques, including the project workflow, purpose Architecture, verification mechanism, sequence diagrams, and testing procedures.

2.1. Project Workflow

In this research, we have adopted a carefully structured workflow, illustrated in Figure 1, to simplify and coordinate activities effectively. A workflow can be defined as a set of steps comprising a work process, often repeated [20]. This structured workflow is a reliable guide for our researchers and ensures that each phase of the research process is executed carefully. By implementing this systematic approach, we significantly improve our project management capabilities, thereby reducing the risk of delays or omissions. Automating task organization and progress tracking through a dedicated workflow management system is essential in maintaining a smooth project flow. This automation reduces the likelihood of errors, increases efficiency, and allows for timely adjustments throughout the project life cycle. By following this structured workflow, we aim to achieve higher productivity levels and maintain tight control over our research efforts.

In our blockchain-based certification system, each traditional Lombok weaving is represented as a digital asset in the form of a non-fungible token (NFT). Data related to the weaving is stored in two locations: the blockchain (on-chain) and the off-chain InterPlanetary File System (IPFS). Information in IPFS includes the weaving name, description, price, image URL, creator's digital signature, and creator's blockchain address. On-chain data stores the unique token ID, current owner's address, seller's address, price in ether, sale status, NFT creation timestamp, and ownership history. Our project began with problem identification, followed by a literature review on application development and product authenticity verification methods. Then, we designed the system and determined the architecture, technology, features, and program flow. We developed features using JavaScript with the React framework for the front end and Solidity with Hardhat for blockchain development during implementation. We conducted system testing, especially unit testing, to ensure component reliability. If the test fails, we return to the design stage; if successful, we proceed to documentation. In the documentation phase, we store important information about the project on GitHub to support future development and facilitate easier access and management of the project.

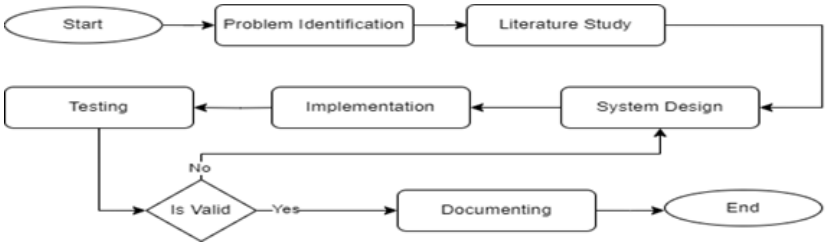

Figure 1. Project Workflow

2.2. Purpose Architecture

We have developed a self-certification system that combines e-certificates with blockchain technology for traditional Lombok weaving. The system uses Non-Fungible Tokens (NFTs) to manage and transfer ownership of woven products, with NFT metadata serving as e-certificates. To ensure the authenticity of the information in the metadata, we implemented the Elliptic Curve Digital Signature Algorithm (ECDSA), which significantly increases trust and transparency by verifying that the information comes directly from legitimate artisans. At the blockchain level, our system uses a peer-to-peer (P2P) network with two main types of nodes: artisans and customers. Smart contracts are implemented to automate the business process between the two parties, increasing efficiency and reducing human error potential. In our system, each artisan and customer confirm every transaction they make themselves. This process actively involves artisans and customers in validating the data, ensuring the registered information is accurate and legitimate. This approach results in a more secure, transparent, and efficient system than traditional certification methods while providing better protection against counterfeiting and facilitating more accurate tracking of product origins.

Our proposed scheme, outlined in Figure 2, begins with a first step, where users store their artwork metadata, including name, description, photo, and other details. In the second step, users digitally sign the information provided. The information is created into a certificate as in the third step. In the fourth step, the data in the certificate, including the digital signature and other relevant information, is uploaded to IPFS. Next, in the fifth step, the NFT is created through a smart contract that acts as an intermediary. Once the NFT is successfully created, its data is stored on the blockchain, as illustrated in the sixth step. At this point, the NFT is officially published. For customers, they can view the certificate data stored off-chain, as described in the seventh step. Afterward, users can verify whether the information is genuine and whether it comes directly from the artisans. Once verified, the customer can proceed with the purchase and complete the payment, as detailed in the ninth step. Ownership is then transferred via the smart contract in the tenth step, and the updated ownership data is stored back on-chain, as explained in the sixth step. Finally, the marketplace smart contract pays the sale proceeds to the artisans.

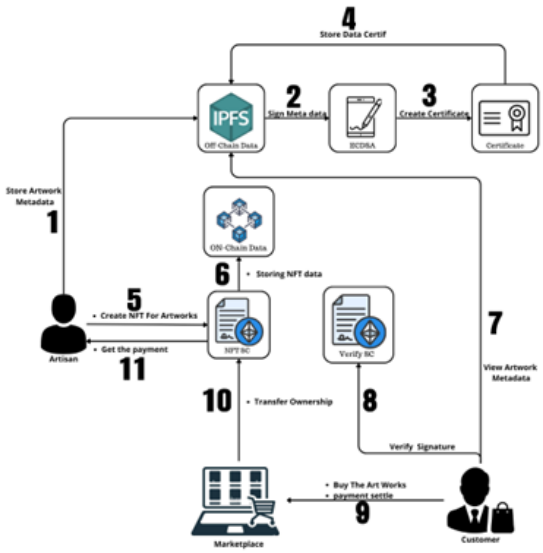

Figure 2. Purpose Architecture

2.3. Verification Mechanism

Figure 3 illustrates the general scheme of the digital signature process, showing the steps of creating and verifying a digital signature, as discussed by Farid Lalem et al. [21]. On the other hand, The implementation of sales, purchases, and verification is depicted in Figure 2. The explanation of Figure 3 is as follows: First, the artisan hashes the product data they own. Next, the artisan signs the resulting hash using their private key, as shown in the specific section. This process produces a signature hash and metadata. For the verification process that begins in step 5, verification uses the artisan's public key as depicted in Figure 6, which can be obtained from the information in the product metadata. After verification, the resulting digest is compared with the hash digest of the original data in step 8.

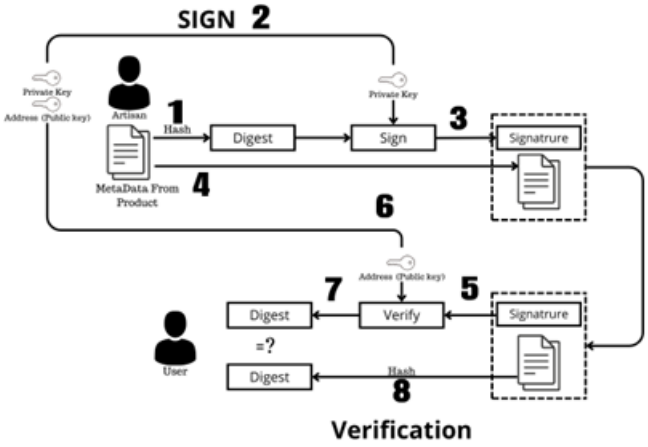

Figure 3. Sign and Verification

2.4. Create NFT

Figure 4 explains the process of creating a Non-Fungible Token (NFT). The process begins when the artisan initiates the creation of the token. Next, the front end handles the minting process by interacting with a smart contract. Once the minting is successful, the NFT is stored securely on the blockchain. Finally, the front end displays the results of the NFT creation, allowing customers to view the newly minted token. This process ensures transparency and security for the artisan and the customer.

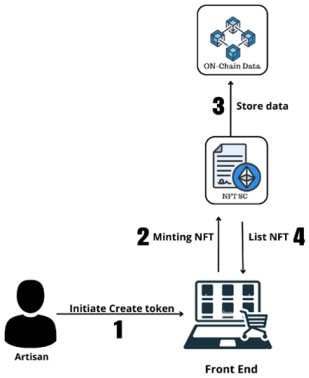

Figure 4. Asset Creation

2.5. Purchase Asset

As shown in Figure 5, the artwork purchase process leverages Non-Fungible Token (NFT) technology as the primary mechanism for transferring ownership. The process begins when the customer initiates the purchase of the artwork. Following this, the marketplace triggers a request to transfer ownership through a smart contract. Once the request is processed, the smart contract

updates the ownership information on the blockchain, ensuring transparency and security. The smart contract also manages the distribution of proceeds, sending the sale amount directly to the artisan. Finally, the marketplace updates the current owner's information, completing the transaction seamlessly and transparently for all parties involved.

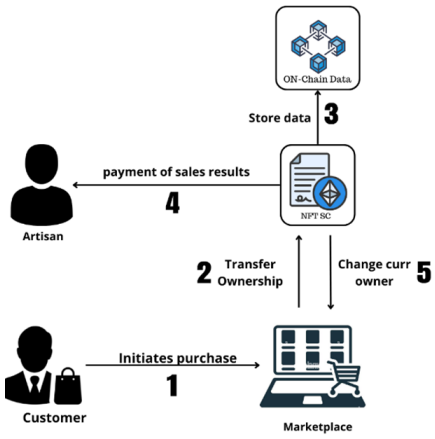

Figure 5. Purchase Asset

2.6. Verify Asset

Figure 6 illustrates how a user performs signature verification in the system. First, the user initiates the process by requesting secure metadata in IPFS, a decentralized storage solution. After reaching step 3, the user is required to input the required data into the smart contract to verify the product metadata, ensuring the authenticity of the information. Next, the smart contract executes its verification protocol by comparing the submitted data with the stored parameters and validation rules. Finally, the smart contract processes all the information and produces a result indicating whether the submitted data is valid or not, then communicates it back to the user for confirmation.

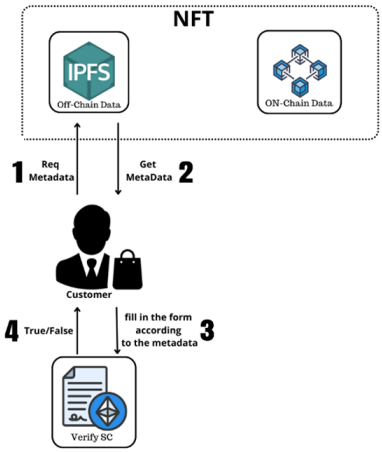

Figure 6. Verification Signature

2.7. Testing Design

In this project, the testing phase focuses on unit testing. This technique determines if software program code is efficient and error-free [22]. In software development, situations are expected to occur where the developed code could be more effective or used. Unit testing helps identify such inefficient code and measures the overall effectiveness of the software. Additionally, developers use unit testing to detect errors and defects that may not be apparent during program execution. Concentrating on unit testing ensures

the reliability and correctness of individual components of the blockchain-based certification system. This thorough testing phase is crucial for building a secure and trustworthy system for verifying the authenticity of woven fabrics. Each component's reliability and performance contribute to the overall integrity and robustness of the solution.

3. RESULT AND ANALYSIS

3.1. Implementation

To register a craft and create a certificate, they must complete all the necessary details as specified in the form shown in Figure 7. These details form the artwork metadata, which is then used to create a certificate. Once the form is filled, the metadata is stored securely in IPFS, ensuring that it remains accessible and verifiable in the future. This stored metadata acts as a digital certificate for the artwork, allowing it to be easily referenced and validated. Once everything is filled in correctly, the user only needs to press the list nft button.

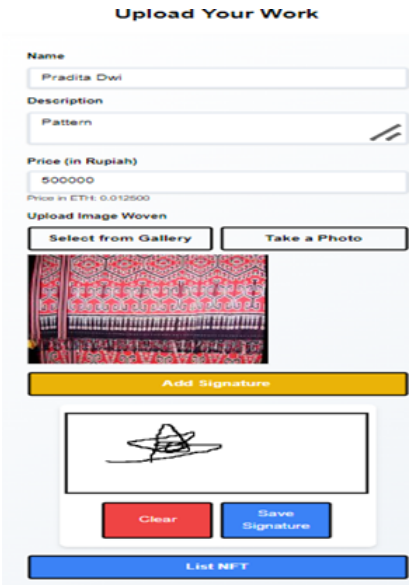

Figure 7. Form NFT Listing Page

As depicted in Figure 8, users must sign specific metadata before creating an NFT. Using MetaMask, users provide a digital signature on the certificate. This signature ensures that anyone can verify the authenticity of the certificate. The metadata includes essential information about the woven product. This signature makes it more transparent, and buyers can know whether the artisan made the information in the certificate.

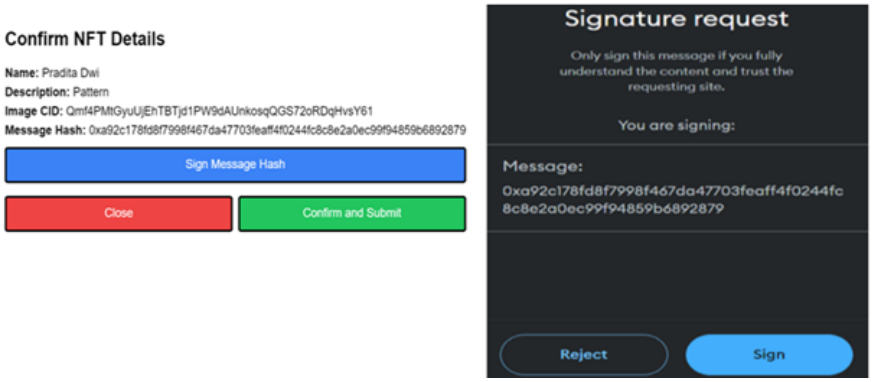

Figure 8. Sign Modal

Figure 9 illustrates the process following the completion of metadata signing by the user. At this stage, MetaMask prompts the user to confirm the creation of the Non-Fungible Token (NFT), providing a detailed breakdown of the associated gas fees. This confirmation step is crucial to ensure the minting process is executed correctly. Once the user confirms the transaction, the NFT is securely recorded on the blockchain, ensuring its authenticity and permanence. The marketplace platform then allows potential buyers to view, verify, and purchase authentic woven products, with detailed listings that include information about the item, its origins, and the artisans, ensuring a transparent and secure purchasing experience.

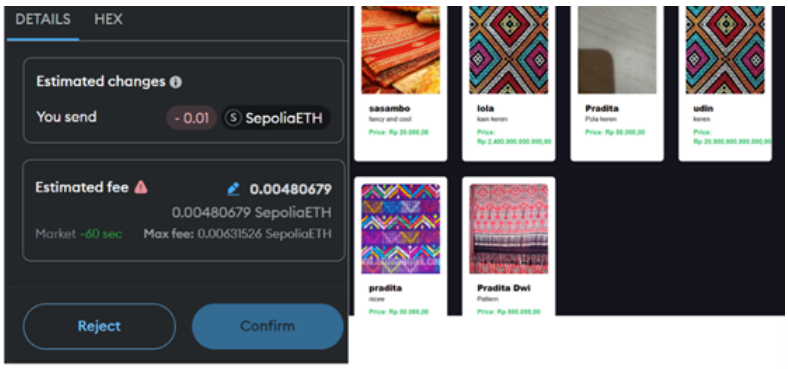

Figure 9. Mint NFT and Marketplace

In Figure 10, you can see the details of the created work, where users can view the details of the work and the certificate and verify the certificate. On this website, the ”current owner” refers to the work’s current owner, while the ”seller” is the party who wants to sell the work. If a seller decides to resell their work, they must first initiate the transfer process through the platform. When a seller wants to resell the work, the ownership of the work is temporarily transferred to the system to ensure security during the transaction process. This system acts as an intermediary in the sales transaction between the seller and the buyer, providing a trustworthy platform for both parties to complete their transaction safely.

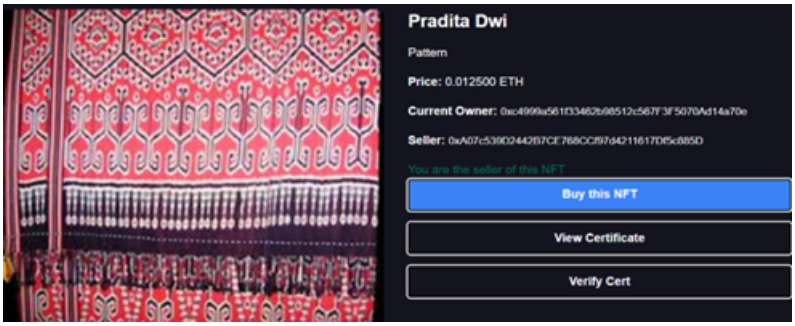

Figure 10. Detail Weave

Figure 11 illustrates how NFT metadata is presented as a certificate with different information, such as the creator’s name, description, address, signature, and CID. Each piece of information displayed in the certificate plays a crucial role in establishing the artwork’s authenticity. To confirm the accuracy of the data and validate that it originates from the correct creator, users can input the data from the certificate into the signature verification form and click the trigger button. The system then processes this information through its verification protocols to ensure the data matches the original records stored in the blockchain. This action then shows the verification result, indicating whether the information is true or false, providing users with confidence in the artwork’s authenticity.

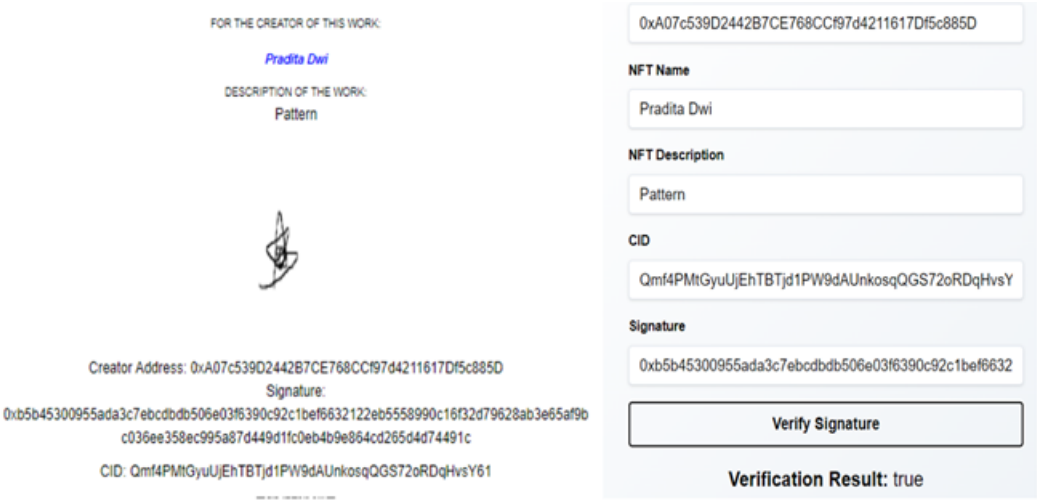

Figure 11. Certificate and Form Verification

When users are interested in purchasing woven products from the marketplace, they can verify the authenticity of the product's certificate, which assures its legitimacy. Once the user has decided to purchase, they must click the "Buy This NFT" button, as illustrated in Figure 12. At this point, MetaMask prompts the user to confirm the purchase. The transaction is processed following the confirmation, and ownership of the NFT is transferred to the buyer. This process ensures that the buyer acquires the NFT and, consequently, the rights associated with the woven product in a secure and verifiable manner. If the user wants to resell it, they simply press the "Resell" button, and the ownership is temporarily transferred to the marketplace or system that acts as an intermediary for the sale.

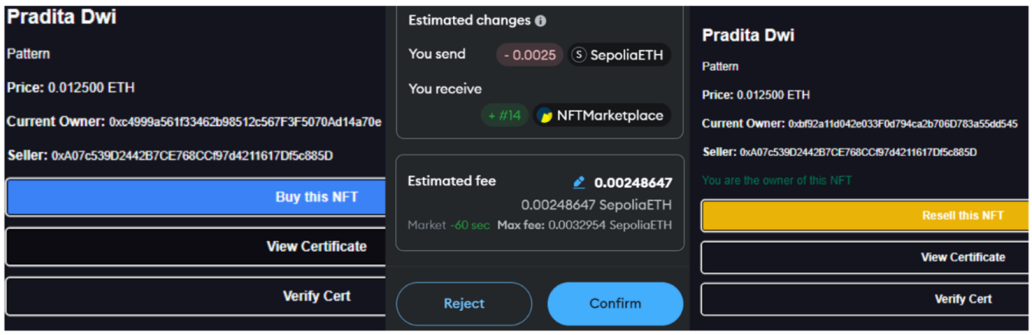

Figure 12. NFT Buying Prosses

3.2. Testing

In this test, we use unit testing as a basis for ensuring that all functions in the smart contract operate correctly. Table 1 shows that all tested functions run as expected. Furthermore, Table 1 illustrates the successful completion of tests for each function within the smart contract, confirming its integrity and proper implementation. These functions include setting the listing price by the contract owner, which allows users to add their work to the web, and creating NFT tokens, which generate a unique token for each registered work executing sales transactions. Enabling users to buy and transfer NFTs through the platform, retrieving all NFTs listed on the marketplace, which allows users to view the entire collection available, and obtaining specific NFTs associated with a user, ensuring they can easily access and manage their tokens. Each function was tested thoroughly, demonstrating that the processes work smoothly and as anticipated.

Table 1. NFT Marketplace Testing

Function Name	Description	Status	Notes
update Listing Price	Updates the price of an item	Passed	Price updated as expected
create Token	Creates an NFT token	Passed	NFT token was created successfully with correct data.
executeSale	Executes the buying and selling process	Passed	Transaction successful, all data valid
getAllNFT	Retrieves the list of all registered NFTs	Passed	All registered NFTs are displayed correctly.
getMyNFT	Retrieves NFTs owned by the user	Passed	The list of owned NFTs is displayed correctly.

Every process operates smoothly and as expected, underscoring the integrity of the smart contract implementation. As shown in Table 2, all tests passed successfully, confirming that the unit testing was effective. The critical functions tested include the "Get message hash," which converts a message into a hash the user can sign off-chain, and the "Verify" function, which checks whether the signing address corresponds to the correct individual. These successful tests highlight the robustness and reliability of the smart contract's functionalities.

Table 2. Verify Testing

Function Name	Description	Status	Notes
get Message Hash	Converts a message into a hash for off-chain signing	Passed	Hash generated correctly for user verification.
Verify	Checks if the signing address corresponds to the correct individual	Passed	Verification successfully matches the expected signer

3.3. Discussion

This research's findings include developing a certification system using blockchain technology that integrates NFTs as a mechanism for managing ownership, IPFS for decentralized storage, and the Elliptic Curve Digital Signature Algorithm (ECDSA) to verify the authenticity of information contained in the certificates. This approach ensures that each woven fabric product is securely documented, stored, and verifiable, preserving its cultural value and authenticity.

Several recent studies have explored the use of blockchain technology across different sectors, such as Hasan et al. [15] and Cruz et al. [16], used blockchain for managing digital assets, emphasizing secure and decentralized management in domains like digital and health-related assets. Jamal et al. [17], focused on enhancing transparency and trust by replacing centralized verification systems with decentralized alternatives. Additionally, Pawar et al. [18], examine the performance of an e-certificate generation and verification system using blockchain and IPFS, showing that this integration improves efficiency, security, and scalability in the digital certification process. In contrast, our study applies blockchain technology to certifying physical cultural products, specifically traditional woven fabrics. We integrate NFTs for ownership management, IPFS for secure storage, and ECDSA to verify the authenticity of creators and data within certificates. This comprehensive approach ensures the crafts' authenticity and facilitates easy ownership transfer, providing practical benefits to artisans while preserving cultural heritage through a secure, verifiable system.

This study paves the way for a foundation for future research in this area. There is significant potential for further development, including integrating artificial intelligence for pattern recognition, which could significantly enhance the system's capabilities and extend its applications to other traditional crafts and cultural heritage initiatives.

4. CONCLUSION

The conclusion that can be drawn from the results of our study is that we have successfully integrated e-certificates with several blockchain technologies, such as Non-Fungible Tokens (NFTs) to manage and transfer ownership of woven products, where NFT metadata functions as an e-certificate. To ensure the authenticity of the information in the metadata, we apply the Elliptic Curve Digital Signature Algorithm (ECDSA), which anyone can operate. This study also introduces the buying and selling process of using blockchain technology. However, there are several limitations. This study only covers traditional woven fabrics from Lombok, and the scalability of the NFT-based system in a broader market context is still uncertain, especially in terms of blockchain transaction costs and energy consumption. The current implementation is still a prototype and has not included large-scale or commercial testing. For future research, we plan to explore other ways to lower transaction costs and improve system efficiency in handling more users. Further research also focuses on improving the user interface to make it easier to use, especially for those less familiar with this technology, as well as expanding the use of this system to other fields that require similar solutions for certificate authentication.

5. ACKNOWLEDGEMENTS

We thank Mataram University for its support through internal funding, which enabled the timely completion of this research.

6. DECLARATIONS

AUTHOR CONTIBUTION

Pradita Dwi Rahman: coding, testing, writing, and editing. Heri Wijayanto: conceptualization, methodology, writing review, editing, and validation, Royana Afwani: writing review, and validation, Melki Jonathan: writing review, Wirama Wesdawara: writing a review, and validation, Ahmad Zafrullah Mardiansyah: writing review, and validation.

FUNDING STATEMENT

Universitas Mataram funds this research.

COMPETING INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] N. Hidayani, "Cultural Heritage Preservation: The Art of Traditional Weaving is Applied Not Only in Clothing," *Jurnal Impresi Indonesia*, vol. 3, no. 2, pp. 128–138, Feb. 2024, https://doi.org/10.58344/jii.v3i2.4636.

[2] D. Rahayu and F. Yanis, "Tourism Communication Model Based on Local Wisdom on Lombok Island, West Nusa Tenggara," *Eduvest - Journal of Universal Studies*, vol. 3, no. 9, pp. 1608–1616, Sep. 2023, https://doi.org/10.59188/eduvest.v3i9.883.

[3] I. Afrianto, A. Heryandi, and S. Atin, "Blockchain-based Trust, Transparent, Traceable Modeling on Learning Recognition System Kampus Merdeka," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 22, no. 2, pp. 339–352, Mar. 2023, https://doi.org/10.30812/matrik.v22i2.2780.

[4] J. Lin, W. Long, A. Zhang, and Y. Chai, "Blockchain and IoT-based architecture design for intellectual property protection," *International Journal of Crowd Science*, vol. 4, no. 3, pp. 283–293, Jun. 2020, https://doi.org/10.1108/IJCS-03-2020-0007.

[5] S. Ruoti, B. Kaiser, A. Yerukhimovich, J. Clark, and R. Cunningham, "Blockchain technology: what is it good for?" *Communications of the ACM*, vol. 63, no. 1, pp. 46–53, Dec. 2019, https://doi.org/10.1145/3369752.

[6] I. Afrianto, T. Djatna, Y. Arkeman, I. Sukaesih Sitanggang, and I. Hermadi, "Disrupting Agro-industry Supply Chain in Indonesia With Blockchain Technology: Current and Future Challenges," in *2020 8th International Conference on Cyber and IT Service Management (CITSM)*. Pangkal Pinang, Indonesia: IEEE, Oct. 2020, pp. 1–6, https://doi.org/10.1109/CITSM50537.2020.9268872.

[7] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019, https://doi.org/10.1109/TSMC.2019.2895123.

[8] A. Pereira, P. Ferreira, and D. Quintino, "Non-Fungible Tokens (NFTs) and Cryptocurrencies: Efficiency and Comovements," *FinTech*, vol. 1, no. 4, pp. 310–317, Oct. 2022, https://doi.org/10.3390/fintech1040023.

[9] T. V. Doan, Y. Psaras, J. Ott, and V. Bajpai, "Toward Decentralized Cloud Storage With IPFS: Opportunities, Challenges, and Future Considerations," *IEEE Internet Computing*, vol. 26, no. 6, pp. 7–15, Nov. 2022, https://doi.org/10.1109/MIC.2022.3209804.

[10] M. Alizadeh, K. Andersson, and O. Schelen, "Efficient Decentralized Data Storage Based on Public Blockchain and IPFS," in *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*. Gold Coast, Australia: IEEE, Dec. 2020, pp. 1–8, https://doi.org/10.1109/CSDE50874.2020.9411599.

[11] Y.-J. Su, C.-H. Chen, T.-Y. Chen, and C.-W. Yeah, "Applying Ethereum blockchain and IPFS to construct a multi-party used-car trading and management system," *ICT Express*, vol. 10, no. 2, pp. 306–311, Apr. 2024, https://doi.org/10.1016/j.icte.2023.12.007.

[12] A. K. Rai, M. Singh, H. C. Sudheendramouli, V. Panwar, N. A. Balaji, and R. Kukreti, "Digital Signature for Content Authentication," in *2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*. Chennai, India: IEEE, May 2023, pp. 1–6, https://doi.org/10.1109/ACCAI58221.2023.10200472.

[13] Z. Wu, R. Liu, and H. Cao, "ECDSA-Based Message Authentication Scheme for BeiDou-II Navigation Satellite System," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 4, pp. 1666–1682, Aug. 2019, https://doi.org/10.1109/TAES.2018.2874151.

[14] J. Doerner, Y. Kondi, E. Lee, and A. Shelat, "Threshold ECDSA from ECDSA Assumptions: The Multiparty Case," in *2019 IEEE Symposium on Security and Privacy (SP)*. San Francisco, CA, USA: IEEE, May 2019, pp. 1051–1066, https://doi.org/10.1109/SP.2019.00024.

[15] H. R. Hasan, M. Madine, I. Yaqoob, K. Salah, R. Jayaraman, and D. Boscovic, "Using NFTs for ownership management of digital twins and for proof of delivery of their physical assets," *Future Generation Computer Systems*, vol. 146, pp. 1–17, Sep. 2023, https://doi.org/10.1016/j.future.2023.03.047.

[16] G. Cruz, T. Guimarães, M. F. Santos, and J. Machado, "Decentralize Healthcare Marketplace," *Procedia Computer Science*, vol. 231, pp. 439–444, 2024, https://doi.org/10.1016/j.procs.2023.12.231.

[17] A. Jamal, R. A. A. Helmi, A. S. N. Syahirah, and M.-A. Fatima, "Blockchain-Based Identity Verification System," in *2019 IEEE 9th International Conference on System Engineering and Technology (ICSET)*. Shah Alam, Malaysia: IEEE, Oct. 2019, pp. 253–257, https://doi.org/10.1109/ICSEngT.2019.8906403.

[18] M. K. Pawar, P. Patil, R. Sawhney, P. Gumathanavar, S. Hegde, and K. Maremmagol, "Performance Analysis of E-Certificate Generation and Verification using Blockchain and IPFS," in *2022 International Conference on Inventive Computation Technologies (ICICT)*. Nepal: IEEE, Jul. 2022, pp. 345–350, https://doi.org/10.1109/ICICT54344.2022.9850830.

[19] C. Chen, Y. Li, Z. Wu, M. Xu, R. Wang, and Z. Zheng, "Towards Reliable Utilization of AIGC: Blockchain-Empowered Ownership Verification Mechanism," *IEEE Open Journal of the Computer Society*, vol. 4, pp. 326–337, 2023, https://doi.org/10.1109/OJCS.2023.3315835.

[20] C. Negru, G. Musat, M. Colezea, C. Anghel, A. Dumitrascu, F. Pop, C. De Maio, and A. Castiglione, "Dependable workflow management system for smart farms," *Connection Science*, vol. 34, no. 1, pp. 1833–1854, Dec. 2022, https://doi.org/10.1080/09540091.2022.2083078.

[21] A. Ghofar, M. Hardi, M. N. Firdaus, and G. F. Shidik, "Digital signature based on PlayGamal algorithm," in *2017 International Seminar on Application for Technology of Information and Communication (iSemantic)*. Semarang: IEEE, Oct. 2017, pp. 58–65, https://doi.org/10.1109/ISEMANTIC.2017.8251844.

[22] M. A. Kosim, S. R. Aji, and M. Darwis, "Pengujian Usability Aplikasi Pedulilindungi dengan Metode System Usability Scale (SUS)," *Jurnal Sistem Informasi dan Sains Teknologi*, vol. 4, no. 2, pp. 1–7, Aug. 2022, https://doi.org/10.31326/sistek.v4i2.1326.