Innovating Letter-of-Credit Mechanisms: The Integration of RSA-Encrypted NFTs for Enhanced Security and Efficiency

Bang L. K.[1](*), Khanh H. V.[1], Triet M. N.[1], Hung N. N.[1], Vinh T. N.[2], Kha H. N.[1], Minh V. N.[1], and Ngan K. T. N.[2]

[1] FPT University, Can Tho city, Vietnam
[2] FPT Polytechnic, Can Tho city, Vietnam
banglkce160155@fpt.edu.vn

Abstract. This paper presents a groundbreaking approach to modernizing the Letter-of-Credit (L/C) process in trade finance by integrating RSA-Encrypted Non-Fungible Tokens (NFTs). Addressing the prevalent challenges of fraud, privacy concerns, and operational inefficiencies in traditional L/C mechanisms, our research proposes a robust, transparent, and efficient framework. Building upon the advancements in blockchain technology and smart contracts, we introduce a dual-layered security strategy combining RSA encryption with the unique characteristics of NFTs. This integration ensures the secure encryption of trade documents, accessible only to authorized parties, and leverages blockchain's immutability to create a transparent, tamper-evident record of document ownership and verification. Our approach not only enhances the security and privacy aspects of trade finance but also introduces significant improvements in efficiency through the automation of verification and settlement processes via smart contracts. This paper discusses how our innovative framework sets a new standard in international trade finance, promising a more secure, efficient, and reliable L/C transaction.

Keywords: International trade; Blockchain; Smart contract; RSA-Encrypted NFT, Ethereum; Fantom; BNB Smart Chain

1 Introduction

Trade finance is undergoing a transformative phase, propelled by advancements in blockchain technology and smart contracts. The need for secure, transparent, and efficient mechanisms in international trade, especially within the letter-of-credit (L/C) framework, has never been more pronounced. Current methodologies, while robust, present several challenges, including fraud risk, privacy concerns, and operational inefficiencies. In light of this, our paper titled "Innovating Letter-of-Credit Mechanisms: The Integration of RSA-Encrypted NFTs for Enhanced Security and Efficiency" seeks to address these challenges by introducing a novel integration of RSA-encrypted Non-Fungible Tokens (NFTs) into the L/C process.

Building on this narrative, Ha et al. [5] introduced a decentralized marketplace mechanism that negates the need for a trusted third party, thus enhancing the trust and privacy in commercial transactions. Their work is a testament to the potential of blockchain technology in mitigating privacy risks and points of failure associated with traditional intermediaries. In the broader context of e-commerce, the SSSB system proposed by Quoc et al. [13] addresses the problems of transportation reliability and information latency, while also providing dispute resolution mechanisms—an essential feature for cross-border trade.

The pursuit of efficiency and reliability in e-commerce and delivery systems has also been explored by Madhwal et al. [10], who delve into the use of smart contracts for the management of Proof of Delivery processes. Their insights on the potential for transaction cost reduction and the need for blockchain systems to handle off-chain transactions pave the way for our proposed solution, which aims to streamline the L/C process further. Drawing inspiration from these seminal works, our research contributes to the field by not only emphasizing the efficiency and transparency afforded by blockchain and smart contracts but also by significantly bolstering the security aspect. The integration of RSA-Encrypted NFTs in the L/C process ensures the confidentiality and integrity of trade documents, mitigating the risks of unauthorized access and document tampering. This dual-layered security approach—combining RSA encryption with the inherent benefits of NFTs on the blockchain—provides an innovative leap forward in the realm of trade finance, setting a new standard for security and privacy in international trade transactions.

Our contribution to the field of trade finance is a pioneering framework that enhances the Letter-of-Credit (L/C) process with the integration of RSA-Encrypted Non-Fungible Tokens (NFTs), targeting the enduring challenges of security and privacy. By employing RSA encryption, our model ensures that trade documents are securely encrypted, making them accessible solely to entities with the corresponding decryption keys, thus addressing privacy concerns. The encapsulation of these documents within NFTs leverages blockchain's immutability, providing a transparent and tamper-evident ledger of document verification and ownership. This integration not only fortifies the trustworthiness of the L/C process but also streamlines it, as smart contracts automate and expedite the verification and settlement stages.

2 Related work

2.1 Blockchain in Cash-on-Delivery Systems

The domain of smart contracts in trade finance has seen significant development aimed at enhancing transaction security and reliability. Son et al. [14] propose a blockchain-based smart contract mechanism to protect the seller's interests in cash-on-delivery systems, which are prevalent in cash-based economies [3]. Their system is designed to enforce specific delivery times, costs, and mortgage money, ensuring accountability for all parties. Similarly, Le et al. [9,9] introduce a double smart contract framework to assure non-fraudulent transactions

in cash-on-delivery scenarios, mitigating risks by requiring both shippers and buyers to place a mortgage. This approach prevents fraudulent activities and safeguards sellers' interests by imposing penalties to deter buyers from unjustly refusing commodities and shippers from tampering with goods in transit. Addressing the challenges of creating highly trustworthy cash-on-delivery systems, Ha et al. [5] present an innovative decentralized marketplace mechanism that incentivizes honest behavior without a trusted third party and incorporates access control protocols to protect user privacy. Ngamsuriyaroj [12] and Hasan [7] further enhance COD systems and package delivery by leveraging blockchain technology to improve data integrity and user verification through decentralized proof of delivery systems using Ethereum smart contracts, offering tamper-proof solutions for tracking the delivery of physical assets and ensuring accountability and integrity throughout the delivery process. These studies collectively contribute to the development of secure and reliable trade finance mechanisms via smart contracts, reflecting a shift towards more decentralized, transparent, and accountable commercial transactions.

2.2 Blockchain and smart contracts in E-commerce

In the realm of e-commerce and delivery systems, security, trust, and transparency are paramount. Quoc et al. [13] introduce the Safe Seller Safe Buyer (SSSB) system, a smart contract-based approach that leverages blockchain technology to address issues like transportation reliability and information latency in cross-border trade transactions. The SSSB framework establishes clear rules and policies during order and package creation, aiding in dispute resolution and enforcing penalty fees for contract violations. Ha et al. [6] further scrutinize trust and transparency in cash-on-delivery systems, proposing a blockchain-based system using Hyperledger Composer to eliminate the need for a trusted third party and reduce costs. Madhwal et al. [10] extend blockchain technology to Proof of Delivery (PoD) processes, developing an open-source system to enhance delivery efficiency and reliability, applying Transaction Costs theory to highlight potential cost reductions. Collectively, these studies underscore the potential of blockchain and smart contracts to enhance e-commerce and delivery system trustworthiness and efficiency. Our work advances this field by incorporating RSA encryption with NFTs to fortify the Letter-of-Credit process against fraud and privacy breaches, addressing crucial security gaps while maintaining transactional efficiency. The exploration of blockchain and smart contracts in e-commerce encompasses various dimensions and applications. Blockchain solutions to the letter-of-credit problem highlight innovations in trade finance, enhancing transparency and efficiency in e-commerce transactions [2]. A systematic literature review provides a comprehensive overview of existing applications, addressing identity verification and transaction management [8]. The impact of blockchain on e-commerce is assessed, showcasing its transformative potential in enhancing trust and operational efficiency [4]. In logistics, blockchain-based smart contracts offer significant improvements in transparency, security, and

sustainability, crucial for e-commerce supply chains [1]. Additionally, decentralized reputation systems enabled by smart contracts aim to mitigate fraudulent activities and build trust among stakeholders in e-commerce environments [11].

3 Approach

3.1 Letter-of-Credit (L/C) Traditional Model

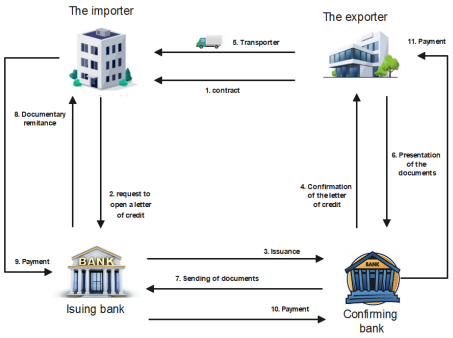

Fig. 1. Traditional Letter-of-Credit Transaction Process

Figure 1 presents a comprehensive depiction of the traditional letter-of-credit transaction process, which serves as a critical financial instrument in international trade. This process is designed to reduce the risk between trading partners or counterparts, namely the importer and exporter, and involves multiple steps facilitated primarily through two banking institutions.

At the inception of the transaction, we have the importer and exporter agreeing on a contract (1), signifying their intent to engage in the trade of goods or services. This contractual agreement lays the foundation for the subsequent financial interactions and is a pivotal point that necessitates a high level of trust between the two parties. Following the contract agreement, the importer initiates the process by applying for a letter of credit at their bank, known as the issuing bank (2). This application signifies the importer's request for the bank to guarantee payment to the exporter, provided that the terms stipulated in the letter of credit are met. Upon the importer's request, the issuing bank proceeds to open a letter of credit (3), which is then forwarded to the exporter's bank, referred to as the confirming bank. The confirmation of the letter of credit (4) by the confirming bank assures the exporter that payment will be received under the terms of the credit. This assurance is crucial as it mitigates the risk the exporter bears in sending goods to the importer without any guarantee.

Subsequently, the goods are dispatched by the exporter via a transporter (5), and upon shipment, the exporter presents the necessary shipping documents to

the confirming bank (6). These documents are evidence that the goods have been sent as per the agreement, and it is imperative that they match the terms of the letter of credit to ensure that the payment obligation is triggered. The confirming bank reviews the documents for compliance and, once satisfied, sends the documents to the issuing bank (7). This transfer is known as documentary remittance (8) and is a critical step in ensuring that the issuing bank has all the necessary paperwork to authorize payment. Upon receipt and verification of the documents, the issuing bank releases the payment to the confirming bank (9), which in turn makes the payment to the exporter (10). Finally, the exporter receives the payment (11), concluding the transaction. The letter-of-credit process not only facilitates the smooth execution of payment upon fulfillment of the contractual obligations but also instills confidence in the international trade ecosystem by reducing the risk of non-payment and non-receipt of goods. This traditional model, while effective, involves several intermediary steps and parties, each of which introduces potential delays and costs, highlighting the opportunity for innovation and improvement through technologies such as blockchain.

3.2 Phase 1: Contract Initiation and Digital Synchronization

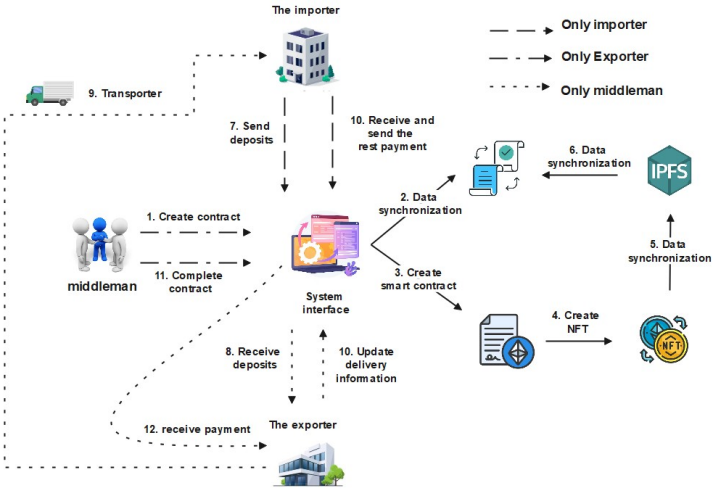

Fig. 2. Decentralized Trade Finance Model Utilizing Blockchain and NFTs.

The figure illustrates a cutting-edge decentralized model for trade finance that leverages blockchain technology, smart contracts, and Non-Fungible Tokens (NFTs) to streamline traditional processes. This proposed architecture offers a solution to the current system's inefficiencies by introducing a seamless, transparent, and secure mechanism for conducting trade transactions.

In this model, the initiation of a trade deal commences with the creation of a digital contract by the intermediary, which is subsequently synchronized with the system interface (1, 2). This synchronization ensures that all parties, including the importer and the exporter, have real-time access to the contract terms. The creation of a smart contract (3) is pivotal as it encapsulates the trade agreement's conditions and executes automatically upon the fulfillment of predefined criteria, thereby minimizing the need for manual intervention and reducing the potential for disputes. Furthermore, the innovative use of NFTs to digitize trade documents (4) introduces an unparalleled level of security and authenticity to the transaction process. These NFTs, stored on the blockchain, are immutable and easily verifiable, ensuring that documents cannot be tampered with or replicated fraudulently. Data synchronization steps (5, 6) across the blockchain network facilitate the real-time updating and verification of transaction information, allowing all parties to monitor progress and maintain transparency.

The importer and exporter interact with the system through deposits and payments (7, 8, 10, 12), with the blockchain providing a secure and efficient medium for the transfer of funds. This minimizes the dependency on traditional banking channels, reducing transaction times and costs. The transporter, integral to the physical movement of goods, is also integrated into the system (9), with delivery updates reflected in the blockchain, thus enabling dynamic updating of delivery information (10). Upon the successful delivery and verification of goods, the smart contract triggers the final settlement (11, 12). This automated process ensures that the exporter receives payment swiftly and securely, closing the loop on the transaction. The entire process is underpinned by the IPFS, which provides a distributed storage solution to host the transaction data, enhancing accessibility and durability.

3.3 Phase 2: Secure Exchange of RSA-Encrypted NFT Mechanism

The figure 3 illustrates the sophisticated RSA-Encrypted NFT architecture, a significant component in the second phase of a blockchain-based trade finance solution. This phase encapsulates the secure exchange of contractual agreements between the importer and exporter, facilitated through a series of cryptographic transactions that ensure both the confidentiality and the integrity of the trade documents. At the core of this system lies the use of RSA encryption, a public-key cryptosystem that is widely recognized for its security, which encrypts the sale contract document. Public keys, labeled as A and B in the diagram, correspond to the respective parties—the importer and the exporter. When the sale contract is created, it is encrypted with the exporter's public key (public key B). This encrypted document can only be decrypted by the corresponding private key, which is securely held by the exporter, ensuring that only the intended recipient can access the sensitive contract details. Subsequent to the encryption, the sale contract is linked to an NFT, creating an indelible record of the contract's issuance and its terms on the blockchain. This NFT, acting as a digital certificate of authenticity, ensures that the contract cannot be altered without detection,

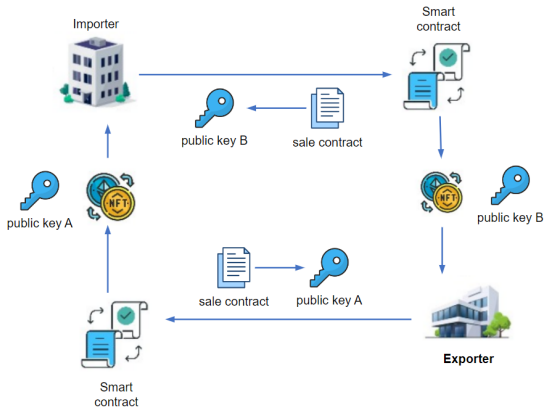

Fig. 3. Decentralized Trade Finance Model Utilizing Blockchain and NFTs.

as each modification would require a new transaction on the blockchain, which is a transparent and tamper-evident process.

The smart contract, which is another crucial element of the architecture, acts autonomously to facilitate, verify, or enforce the negotiation or performance of the contract. It carries out pre-programmed instructions dependent on certain conditions, such as the confirmation of payment or receipt of goods, and is instrumental in reducing the need for intermediaries, thereby streamlining the transaction process. Once the NFT representing the sale contract is created and stored on the blockchain, it undergoes a synchronization process with the smart contract. This synchronization ensures that the terms encoded in the smart contract reflect the agreement detailed within the NFT-encrypted sale contract. Through this mechanism, the smart contract is effectively 'aware' of the contractual obligations and can execute the respective clauses upon the satisfaction of the agreed-upon terms.

4 Evaluation

4.1 Evaluating of the RSA-Encrypted NFT Framework

To evaluate the performance of our RSA-Encrypted NFT framework, we conducted experiments focusing on three key processes: generating RSA keys, encrypting, and decrypting. The tests were performed for two different scenarios: encrypting a 120 KB image and encrypting the text "Hello, RSA encryption!" The results, presented in tables, provide insights into the efficiency and effectiveness of our encryption and decryption mechanism.

For the image encryption scenario, the time taken for generating RSA keys varied, with an average of approximately 2537 milliseconds (ms). The encryption process showed a faster performance, averaging around 1136 ms. However, the decryption process took the longest time, with an average of around 3387 ms.

The variation in times for key generation and decryption processes suggests that the complexity and size of the image significantly influence the performance.

Table 1. Performance Metrics for RSA Key Generation, Encryption, and Decryption in Image Processing Scenario

RSA with image(ms)	1	2	3	4	5	6	7	8	9	10
Generating RSA key	2330	2206	2750	2314	2480	2218	2526	3790	2773	2378
Encrypting image	1436	848	913	890	1141	1422	1025	1036	1397	1355
Decrypting image	3234	3946	3337	3796	3379	3360	2449	3174	3830	3267

In the text encryption scenario, the RSA key generation times were slightly more consistent, averaging around 2453 ms, showing a comparable performance to the image scenario. The encryption times for the text were generally faster, averaging around 1161 ms. The decryption times for text were also high (around 3480 ms), which is consistent with the trend observed in the image scenario.

Table 2. RSA Encryption Process Times for Text Data Across Multiple Trials

RSA with Text(ms)	1	2	3	4	5	6	7	8	9	10
Generating RSA key	2332	2257	2368	2259	2866	2736	2442	1947	2689	2151
Encrypting Text	1496	933	1363	1523	888	781	1483	825	1030	1520
Decrypting Text	3172	3810	3269	3218	4246	3483	4075	3228	3281	3329

Analyzing these results, it is evident that the RSA encryption process is more efficient for smaller data sizes, as seen in the text encryption scenario. However, the decryption process is consistently the most time-consuming step in both scenarios. This could be attributed to the computational complexity involved in decrypting data encrypted using RSA, which tends to increase with the size and complexity of the data. The key generation process, while relatively time-consuming, is a one-time process and does not significantly impact the overall efficiency of the system in real-world applications where keys can be reused. The encryption times are reasonably efficient, demonstrating the feasibility of our approach for real-time applications.

In conclusion, our RSA-Encrypted NFT framework shows promising results in terms of performance, particularly for smaller data sizes. The longer decryption times indicate a need for optimization, especially for larger data sets. However, considering the enhanced security and privacy this framework offers, the trade-off in decryption time could be acceptable in scenarios where security is of paramount importance. Future work could focus on optimizing the decryption process and exploring the scalability of the system for larger data sets to enhance its applicability in a broader range of trade finance scenarios.

4.2 Cost-Effectiveness in Deploying RSA-Encrypted NFTs

In our study, we evaluated the deployment of smart contracts on several leading Ethereum Virtual Machine (EVM)-compatible platforms known for their cost-effectiveness and blockchain prowess. Platforms such as Binance Smart Chain (BNB Smart Chain), Polygon, Fantom, and Celo were selected for their unique balance of compatibility, cost efficiency, and network innovation. These platforms provide an ideal testing ground for our RSA-encrypted NFT framework, specifically tailored for the nuanced requirements of Letter-of-Credit transactions in the global trade finance sector.

Our research primarily focused on the deployment of smart contracts and their subsequent operations, including transaction creation, NFT minting, and transfer processes, within the context of Letter-of-Credit transactions. Such operations are critical to the integrity and practical application of our encrypted NFTs in real-world trade finance scenarios.

Considering the economic implications is essential when integrating blockchain technologies into commercial applications, especially within the Letter-of-Credit framework. We conducted an exhaustive comparative analysis of the costs associated with deploying smart contracts and executing their primary functions across the selected blockchain platforms. This economic analysis is a cornerstone in evaluating the financial sustainability of implementing our RSA-encrypted NFT mechanism across various blockchain infrastructures. Through this metic-

Table 3. Transaction fee

	Contract Creation	Create NFT	Transfer NFT
BNB Smart Chain	0.027311 BNB ($8.33)	0.00109162 BNB ($0.33)	0.00056991 BNB ($0.17)
Fantom	0.0095767 FTM ($0.003)	0.000405167 FTM ($0.000127)	0.0002380105 FTM ($0.000075)
Polygon	0.0068405000328344 MATIC($0.01)	0.000289405001273382 MATIC($0.00)	0.000170007500748033 MATIC($0.00)
Celo	0.00709722 CELO ($0.004)	0.0002840812 CELO ($0.000)	0.0001554878 CELO ($0.000)

ulous evaluation, we identified Fantom as the most economically viable platform for our purposes (Table 3) . The transaction fees on Fantom were significantly lower than those on the other platforms, as detailed in our comparative findings. This economical advantage makes Fantom an attractive option for facilitating Letter-of-Credit transactions via our smart contract framework, given the need for frequent and cost-effective operations in trade finance.

5 Conclusion

In conclusion, our paper contributes in the field of trade finance. By integrating RSA-Encrypted NFTs into the L/C process, we address longstanding issues in security and privacy, bringing a much-needed transformation to traditional trade finance mechanisms. Our solution leverages the strengths of blockchain technology, including its transparency and immutability, and combines them with the

robust security offered by RSA encryption. The resultant framework not only secures sensitive trade documents but also enhances the overall efficiency and reliability of the L/C process. This innovative approach paves the way for a new era in trade finance, marked by heightened security, improved operational efficiency, and reinforced trust among international trade participants. Our work demonstrates the potential of combining cutting-edge technologies like blockchain and encryption to revolutionize traditional financial processes, setting a benchmark for future innovations in the domain of international trade finance.

References

1. Chauhdary, S.H., Saleem, S.: Use of blockchain-based smart contracts in logistics and supply chains. Electronics (2023)
2. Doe, J., Smith, J.: Blockchain solutions to the letter-of-credit problem. Journal of Blockchain Research (2023)
3. Duong-Trung, N., et al.: Multi-sessions mechanism for decentralized cash on delivery system. Int. J. Adv. Comput. Sci. Appl **10**(9) (2019)
4. Green, M., White, L.: The impact of blockchain on e-commerce. E-commerce Technology Review (2021)
5. Ha, X.S., et al.: Dem-cod: Novel access-control-based cash on delivery mechanism for decentralized marketplace. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). pp. 71–78. IEEE (2020)
6. Ha, X.S., et al.: Scrutinizing trust and transparency in cash on delivery systems. In: Security, Privacy, and Anonymity in Computation, Communication, and Storage: 13th International Conference. pp. 214–227. Springer (2021)
7. Hasan, H.R., Salah, K.: Blockchain-based proof of delivery of physical assets with single and multiple transporters. IEEE Access (2018)
8. Johnson, A., Brown, B.: A systematic literature review of blockchain and smart contract applications. International Journal of Blockchain Applications (2022)
9. Le, N.T.T., et al.: Assuring non-fraudulent transactions in cash on delivery by introducing double smart contracts. Int. J. Adv. Comput. Sci. Appl **10**(5), 677–684 (2019)
10. Madhwal, et al.: Proof of delivery smart contract for performance measurements. IEEE Access **10**, 69147–69159 (2022)
11. Miller, K., Clark, S.: Smart contract enabled decentralized reputation system for e-commerce. Journal of Decentralized Applications (2020)
12. Ngamsuriyaroj, S., et al.: Package delivery system based on blockchain infrastructure. 2018 Seventh ICT International Student Project Conference (ICT-ISPC) (2018)
13. Quoc, K.L., et al.: Sssb: An approach to insurance for cross-border exchange by using smart contracts. In: Mobile Web and Intelligent Information Systems: 18th International Conference. pp. 179–192. Springer (2022)
14. Son, H.X., et al.: Towards a mechanism for protecting seller's interest of cash on delivery by using smart contract in hyperledger. International Journal of Advanced Computer Science and Applications **10**(4) (2019)