

Revolutionizing Payment Systems: Integrating RSA-Encrypted NFTs in Blockchain for Cash-on-Delivery Transactions

L. K. Bang[1], P. H. T. Trung[1(✉)], T. P. Nghiem[1], D. P. N. Trong[1], N. T. K. Ngan[2], L. T. Nhi[1], N. H. Kha[1], and T. N. Anh[1]

[1] FPT University, Can Tho City, Vietnam
banglkce160155@fpt.edu.vn, trungpht@fe.edu.vn
[2] FPT Polytecnic, Can Tho City, Vietnam

Abstract. In the e-commerce fields, our approaches consider to address the enhance security, trust, and transparency issues in cash-on-delivery (COD) systems. Handling the traditional risks and inefficiencies of current COD processes (e.g., cross-border transactions between the shipper and buyer/purchaser), this paper present an encryption-powered (i.e., RSA encryption) with Non-Fungible Tokens (NFTs) within a blockchain platform. This approach not only benefits the decentralized, immutable, and transparent as a nature of blockchain-supported technology but also protects the sensitive info with the added security layer of RSA encryption. The NFTs usages ensure the uniqueness and irreplaceability of each transaction, thereby offering a system that is secure, private, and efficient compared to the central-based storage in the current system. This paper represents a our effort in digital payment systems, providing a comprehensive solution that responds to the evolving challenges in e-commerce and sets new benchmarks for digital transaction security, privacy, and efficiency.

Keywords: RSA-Encrypted · Blockchain · cash-on-delivery (COD) · NFT · Smart contract

1 Introduction

In the upgrading of the e-commerce approach to address the traditional limitation, the blockchain-exploited technology has become an important factor, addressing the steps in which transactions are processed [14]. In particular, smart contracts usage as well as decentralized-based consideration are considered to handle some challenges and problems regarding payment processes, for example, trust, transparency, and security [13]. In the same benefit, our proposed model refines payment systems via blockchain-baed techniques, moreover to protect the personal information in the transaction the RSA-powered on Non-Fungible

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
O. Gervasi et al. (Eds.): ICCSA 2024 Workshops, LNCS 14815, pp. 125–141, 2024.
https://doi.org/10.1007/978-3-031-65154-0_8

Tokens (NFTs) release layer to enhance both the security and efficiency of Cash on Delivery (COD) transactions is the necessary consideration. This means that our paper is an effort for the preparation step in addressing both privacy concerns and operational challenges in e-commerce platforms before considering the blockchain-deployed system in the real environment.

The basis of our research is built on the effort presented in prior work. In practice, Son et al. [15] and Le et al. [9] have deployed a framework for secure transactional ecosystems using blockchain technology in the initial steps. These systems protect the interests of sellers in COD transactions by proposing several roles of the stakeholder via the definition of rules and responsibilities through smart contracts. Although these studies have improved transactional transparency and privacy (i.e., based on the role/permission definition) some personal information is still released to the unexpected stakeholders. To this end, our approach changes the focus from not only the transparency of the transaction among the users (e.g., shipper vs buyers/purchasers) to the privacy of sensitive user data through RSA encryption, addressing a key shortfall in previous frameworks which often place the security of transactional details above the protection of personal information.

Furthermore, our research expands upon the ideas presented by Ha et al. [5] and Quoc et al. [12], who have explored decentralized marketplace mechanisms and the challenges in cross-border e-commerce exchanges. Additionally, the other approaches build on ideas from several aspects (e.g., Ha et al. [5]; Quoc et al. [12]) that have examined decentralized marketplace mechanisms as well as the challenges of cross-border e-commerce exchanges. While these studies provide robust solutions for maintaining integrity and fostering trust in transactions, our work goes a step further. We implement a multi-platform blockchain deployment strategy, assessing and comparing the suitability of various EVM-supported blockchain environments for our e-commerce solution. This methodology provides a comprehensive analysis of each platform's strengths and limitations, allowing for a more informed choice of blockchain technology tailored to specific e-commerce requirements. We apply not only a multi-platform blockchain deployment strategy to evaluate and compare different EVM-supported blockchain environments for our e-commerce solution but also analysis of each platform's strengths and weaknesses as the original approach of [3].

For the encryption-based approaches on the blockchain platform, sensitive info sharing is not a strong point consideration in traditional e-commerce systems. In fact, the background section, in this paper, summarized the traditional considerations that focus on transparency, decentralization, and immutable improvement by applying the blockchain characteristic technique. By ensuring that personal and sensitive information is encrypted and secure via RSA strategy, we address an important issue that has previously been somewhat neglected in blockchain-based e-commerce solutions [13]. The use of RSA-encrypted NFTs stored on IPFS networks ensures that transaction details remain transparent and immutable, while personal and sensitive data are kept confidential and secure.

The rest of our paper is structured as follows: the first two sections provide background on traditional approaches and review existing literature on blockchain applications in e-commerce. The sections on system architecture and implementation, detailed in Sect. 4 and Sect. 5, outline our methodology and the implementation points for our proposed model. The evaluation of our system, including performance, cost, and efficiency, is discussed in Sect. 6. The discussion section explores the implications of our findings and potential directions for future research. Finally, the conclusion highlights our key contributions and the potential impact of our work in this paper.

2 Background

2.1 The Traditional Approach - Post-office Transportation

The traditional model for COD transactions is a sequential, five-step process encompassing activities from the seller's preparation of the package to the final delivery and payment collection by the buyer. This model serves as the foundation for understanding the subsequent integration of RSA-Encrypted NFTs in blockchain technology (Fig. 1).

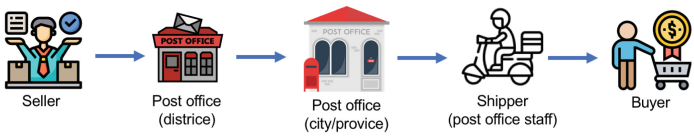

Fig. 1. The post-office case for transporting goods

Step 1 - Seller Preparation: The COD process commences with the seller preparing the item for dispatch. This initial step involves meticulous packaging and the completion of all necessary documentation to ensure the item's security and provide clear delivery instructions. This meticulous preparation is essential to mitigate potential delays or complications in the later stages of the delivery process.

Step 2 - District Post Office Handling: Following the seller's preparation, the package is transferred to the district-level post office. Here, postal workers assume responsibility for the package, processing it in accordance with postal regulations. Activities in this stage include sorting based on destination, address verification, and logging the package into the postal tracking system. The district post office acts as an intermediary, preparing the package for its onward journey to a city or provincial-level facility.

Step 3 - City/Provincial Post Office Processing: The package, upon reaching the city or provincial post office, undergoes additional sorting. These larger

facilities are equipped to handle greater volumes, enabling efficient sorting based on the final delivery areas. At this juncture, packages are grouped according to their destinations, and logistics for the last part of the delivery are organized to guarantee timely and efficient delivery.

Step 4 - Delivery by Postal Staff: In the fourth stage, the postal delivery staff, often referred to as shippers, are tasked with the final delivery. They ensure the package is loaded onto the delivery vehicle and transported to the recipient's address. This phase is critical, as it tests the postal service's reliability and timeliness, with shippers navigating various routes to deliver the package safely.

Step 5 - Buyer Receives Package: The delivery process culminates with the buyer receiving the package. In COD transactions, the buyer pays the postal delivery staff the owed amount upon delivery. This exchange marks the completion of the transaction, with the buyer confirming receipt in satisfactory condition, and the seller's obligation considered fulfilled following successful delivery and payment.

The traditional model for cash-on-delivery transactions, when viewed through the lens of a shipping company's involvement, presents a comprehensive and multi-faceted process. This integrated approach marries the detailed steps of seller preparation, postal handling, and delivery with the logistical prowess of a transportation company.

2.2 The Traditional Approach - Transportation Company Case

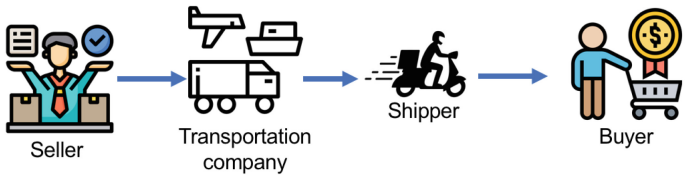

Fig. 2. The transportation company case for transporting goods

Step 1 - Seller's Preparation: The process begins with the seller preparing to package the product and prepare it for shipping through the shipping service. This preparation is based on the product packaging steps, depending on the size and material the seller will package them differently. For example, the steps involved include selecting appropriate packaging materials to protect the item during shipping and preparing the necessary documents to provide to the partner, such as shipping labels, pricing, etc. name, destination and delivery address or customs form for long-distance orders (e.g. international orders). After the sealing and labeling stage, the package is ready for pickup, and the seller selects

the shipping company to deliver the goods to the buyer. Depending on the needs as well as the price, the companies are chosen (Fig. 2).

Step 2 - Transportation Company's Involvement: Once the shipping company takes care of the package, they will begin a journey that may include multiple forms of transportation by different means, e.g., motorbike, truck, plane, or ship. Depending on the distance, the shipper's vehicle will change accordingly. The key requirement at this stage is to use a tracking system (e.g. GPS) to provide updates and assurance to both sellers and buyers, thereby instilling customer confidence. This advanced tracking feature builds on traditional postal services, providing delivery reliability and consistency. Taking advantage of transportation through traditional postal systems also contributes to the benefits of this approach. Specifically, as the package moves through different stages, especially when it is close to the recipient's location, messages will be sent including the time and location of delivery.

Step 3 - Shipper's Role: The final delivery phase is managed by a shipper, a dedicated individual responsible for the last segment of the package's journey. Their role, navigating through local terrains, is a testament to the adaptability and customer-centric focus of the delivery process. Here, the traditional postal approach and modern shipping methodologies converge, ensuring the package reaches its intended recipient efficiently and securely.

Step 4 - Buyer's Receipt: The culmination of this integrated process is marked by the buyer receiving the package. This final interaction, whether it includes a cash-on-delivery transaction or simply a confirmation of receipt, is a critical touchpoint in the logistics chain. It signifies the successful collaboration between traditional postal services and modern transportation logistics, wrapping up the delivery process with customer satisfaction as the ultimate goal.

3 Related Work

3.1 Smart Contract-Based Solutions for Cash on Delivery (COD) and E-Commerce

In the realm of Cash-on-Delivery (COD) transactions, blockchain technology and smart contracts are paving the way for secure and efficient processes. Son et al. (2019) developed a blockchain-based payment system that safeguards sellers by enforcing a predefined set of transaction rules through smart contracts [15]. This system ensures transparency and minimizes risk by requiring adherence to agreed delivery times, places, and costs. Similarly, Le et al. (2019) propose a multi-shipper mechanism using blockchain and smart contracts to instill trust and prevent fraud in decentralized markets, demonstrating the practicality of their approach with case studies and open-source code for community enhancement [9].

Further advancing COD security, Le et al. (2019) introduce a framework involving double smart contracts to mitigate fraudulent transactions. This innovative approach, leveraging Ethereum blockchain, requires both buyers and shippers to place a mortgage, ensuring reliability and imposing penalties for any breaches of contract [10]. Ha et al. (2020) contribute to the field with DEMCOD, a decentralized marketplace mechanism designed to promote integrity and robustness in COD transactions through smart contracts, enhancing participant trust and privacy while offering a comprehensive code solution for adoption and improvement [5]. These studies collectively highlight the transformative impact of blockchain and smart contracts in enhancing the security and efficiency of COD transactions.

3.2 Security, Trust, and Transparency in E-Commerce and Delivery Systems

Ha et al. [6] scrutinize the existing decentralized blockchain approaches, identifying key areas needing improvement for efficiency and completion in COD systems. The paper highlights the lack of motivation for honest participation among sellers, buyers, and shippers, and the over-reliance on a trusted third party or arbitrator. To address these issues, they propose a novel solution using Hyperledger Composer to protect merchant rights and smart contracts to eliminate the need for any third party or arbitrator. This approach aims to enhance trust and transparency in the transaction process, mitigating the risks associated with dishonesty and disputes.

Duong et al. [3], on the other hand, tackle the operational inefficiencies in COD systems, particularly in handling multiple delivery sessions. They observe that existing models support only a single delivery session at a time, leading to inefficiencies when buyers are unavailable to receive goods. To overcome this challenge, they propose a multi-session mechanism that leverages blockchain technology, smart contracts, and the hyperledger fabric platform. This mechanism ensures distributed and transparent operations across multiple delivery sessions in decentralized markets, significantly improving the efficiency of the delivery process. The authors also release their source codes to encourage further development and reproducibility in this field.

3.3 Decentralized Marketplaces and Peer-to-Peer E-Commerce

Quoc et al. [12] introduce the Safe Seller Safe Buyer (SSSB) system, an innovative approach utilizing blockchain technology and smart contracts to insure cross-border exchanges. They identify key challenges in traditional commercial systems, such as transportation issues, information latency, and reliability, which affect the overall trading process. The SSSB system addresses these issues by storing all relevant information about packages and orders in a distributed ledger, allowing both sellers and buyers to access necessary data about their transactions. This system significantly differs from traditional international trading systems by reducing the need for a middleman or arbitrator in conflict resolution.

The authors also implement the SSSB system on various platforms supporting Ethereum's ERC20, like Ethereum, BNB Smart Chain, and Fantom, and provide an analysis of the implementation costs on these platforms, encouraging further research in this area.

Dragomir et al. [2] focus on the logistics aspect of online second-hand marketplaces, particularly the pickup and delivery problem (PDP) with alternative locations and overlapping time windows. They aim to facilitate transportation providers in expanding their services by addressing the complexities of serving a fleet of vehicles to multiple roaming pickup and delivery locations. The proposed solution approach is based on a multi-start, adaptive, large neighborhood search with specific operators tailored to solve the PDP with alternative locations. By examining different scenarios based on real data from an Austrian logistics provider, Dragomir et al. demonstrate that increased flexibility and convenience for customers can lead to significant cost savings for carriers, up to 30% in some cases.

3.4 Revolutionizing Cash-on-Delivery Systems: The Transformative Role of Blockchain and Smart Contracts

The integration of blockchain technology and smart contracts into various sectors is revolutionizing traditional processes, enhancing security, efficiency, and trust. Son et al. (2019) proposed a novel payment system based on smart contracts implemented on blockchain technology to protect sellers' interests in cash-on-delivery transactions, showcasing the use of Hyperledger to minimize risks for parties involved [15]. Similarly, Le et al. (2019) introduced double smart contracts to assure non-fraudulent transactions in cash-on-delivery systems, presenting a framework that prevents fraud by shippers and buyers [10]. Hasan and Salah (2018) proposed a decentralized solution for the proof of delivery of digital assets using blockchain and smart contracts, leveraging Ethereum to provide immutable, tamper-proof logs, and accountability [7]. To address security concerns, Mohammed et al. (2023) developed a secure smart contract based on blockchain to prevent the non-repudiation phenomenon, focusing on enhancing transaction security [11]. Ahmadieh and El Madhoun (2023) explored the potential of NFTs in online trading and transaction cancellation, demonstrating how smart contracts can facilitate the creation, trading, and ownership transfer of digital artworks [1]. Jha et al. (2023) proposed a blockchain-based transaction system using smart contracts to eliminate the need for bank and third-party verification in transactions, thereby improving the speed and security of payments [8]. Lastly, Elghaish et al. (2020) integrated project delivery with blockchain in the construction industry, developing an automated financial system that leverages smart contracts for financial transactions, which could significantly improve project delivery outcomes [4]. These studies collectively highlight the transformative potential of blockchain and smart contracts across various domains, from ensuring secure and efficient transactions to revolutionizing digital marketplaces and project delivery systems.

4 Approach

We present the traditional model as well as the analysis in appendix A. In the ever-evolving landscape of digital transactions, the need for more secure, transparent, and efficient systems is paramount, especially in the context of cash-on-delivery (COD) operations. This proposed architecture aims to revolutionize COD transactions by enhancing security, ensuring authenticity, and fostering trust among all stakeholders. In the realm of modern logistics and supply chain management, the integration of RSA-Encrypted Non-Fungible Tokens (NFTs) into blockchain technology represents a revolutionary stride, especially in the context of cash-on-delivery transactions. This approach involves a multi-step process that seamlessly combines traditional logistics with cutting-edge blockchain technology, offering unprecedented levels of transparency, security, and efficiency. It is shown in Fig. 3.

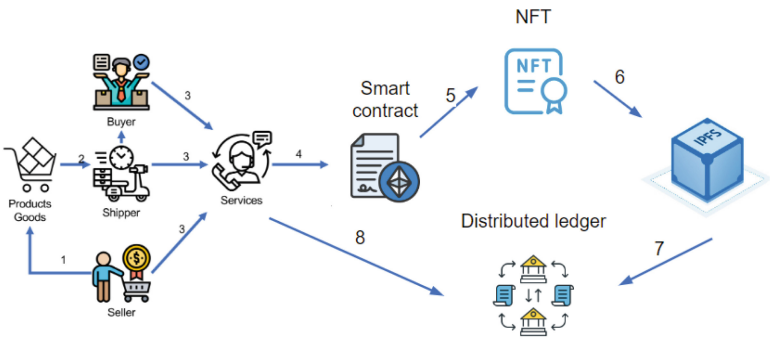

Fig. 3. The process of transporting goods based on blockchain technology, smart contract, NFT and IPFS

The Seller's Pivotal Role: The journey of a product in this innovative system commences with the seller. Beyond merely selling the product, the seller interacts with a sophisticated service system, marking the transaction's completion. This interaction is crucial, as it involves the seller using the system interface to register the product information, subsequently transforming it into an NFT. This step is not just a digital representation of the product but a significant leap in ensuring its uniqueness, security, and traceability. The initiation of a smart contract on the blockchain at this point is pivotal, setting in motion the delivery chain that is both transparent and immutable.

The Journey of Products/Goods: Once the transaction is completed and the product information is securely embedded in the blockchain, the physical goods embark on their journey. This transition from a digital entry to physical

logistics is where the model integrates traditional shipping methods. The product, now linked to its digital counterpart, is handed over to shipping personnel, maintaining a tangible connection between the physical item and its digital representation.

The Interplay of Shipper and Buyer: The shipper plays a crucial role in this ecosystem. Upon receiving the product from the seller, the shipper updates the order status through the same system interface, ensuring every step of the delivery process is transparently recorded on the blockchain. This transparency extends to the buyer, who actively participates by tracking the progress of the order through the system interface. The culmination of this process is marked by the buyer confirming the receipt of the goods. In scenarios involving cash-on-delivery, this step is also recorded and confirmed through the interface, adding an extra layer of security and trust to the transaction.

The Central Role of Smart Contracts and NFTs: The smart contract, embedded within the blockchain, is the backbone of this model. It automates the transaction terms and executes only when predefined conditions, such as the buyer's confirmation of receipt, are met. The representation of each product or good as an NFT is a game-changer. It ensures the product's uniqueness and irreplaceability, further solidifying the process's security and authenticity. This digital representation also plays a vital role in verifying ownership, a crucial aspect in cash-on-delivery transactions.

The Distributed Ledger: A Record of Transparency: Every interaction, from the issuance of the NFT to updates made by the seller, shipper, or buyer, is meticulously recorded on a distributed ledger. This ledger forms an immutable and fully transparent record of the entire product delivery process. The immutability of this ledger means that once a transaction is recorded, it cannot be altered, providing a trustworthy and transparent account of the entire process.

The Service Interface: The Unifying Element: At the heart of this model lies the service component, represented by the system interface. This interface is integral to the service and supply chain management system, offering tools for tracking, confirming, and managing order information. It is through this interface that all stakeholders - the seller, the buyer, and the shipper - interact. From updating the order status to confirming the delivery, every interaction is facilitated through this interface, ensuring a seamless and integrated experience for all parties involved.

The second phase of our proposed approach introduces a sophisticated (Fig. 4, secure transaction process within the blockchain environment, leveraging the power of RSA encryption and Non-Fungible Tokens (NFTs). This phase is centered around ensuring the security and integrity of the transaction between the seller and buyer, facilitated through a smart contract.

The process begins with the seller, who is integral to initializing the transaction. The seller possesses a unique identifier in the form of a public key, hereafter

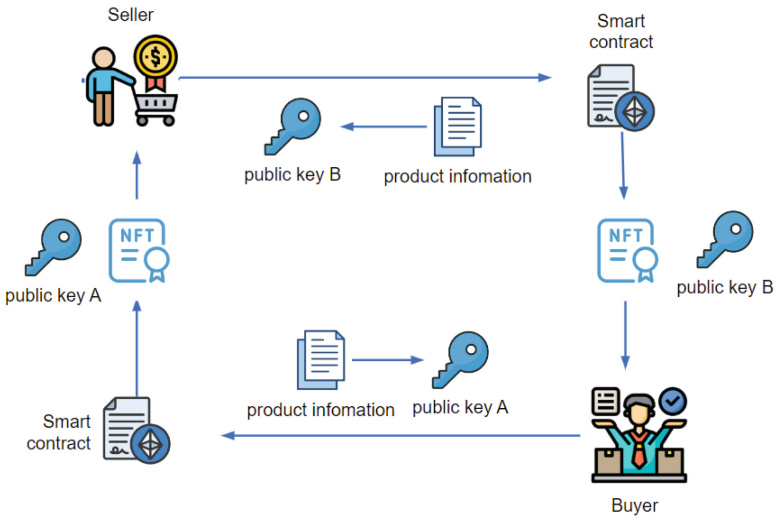

Fig. 4. RSA Encryption Model for Secure NFT Transactions

referred to as public key A. When the seller decides to create an NFT that represents a product, the product's information, including details like description, price, and ownership data, is first encrypted using public key A. In step 2, the smart contract in our architecture plays a pivotal role in facilitating the transaction. Upon receiving the encrypted product information from the seller, the smart contract securely stores this data. It is designed to interact with potential buyers who express interest in purchasing the product. When a buyer steps into the transaction process, they engage with the smart contract using their distinct public key, referred to as public key B. This interaction is a key element of our architecture, as it enables a secure and direct communication channel between the buyer and the smart contract.

After that, the encrypted product information is transferred to them via this smart contract. This transfer ensures that the integrity and confidentiality of the product information are maintained, as only the holder of the private key corresponding to the public key used for encryption (in this case, the buyer) can decrypt and access this information. Finally, the buyer's role in this phase is not just limited to expressing interest in the product but also extends to the decryption and verification of the product information. Using their public key B, the buyer receives the encrypted product information from the smart contract.

5 Implementation

This section presents the implementation process of our proposed model which exploits the RSA-encrypted for the NFTs (called the proof-of-delivery) as well

as stores in the IPFS. The next four steps will detail our implementation in the proof-of-concept.

Figure 5 illustrates the benchmarking of NFT-related operations in a testing environment (step 1). It specifically highlights the time efficiency of two critical operations: minting the NFT, which is completed in 2151 ms, and decrypting the NFT's URI, which takes 3329 milliseconds. The tests are conducted to assess the performance and reliability of the NFT creation and retrieval process, which is fundamental to ensuring a seamless COD system. The sub-7-s total time for completing all tests indicates a swift execution conducive to real-world applications where transaction speed is essential.

In second step, Fig. 6 delves into the technical implementation of the minting function. The code snippet shows a JavaScript function utilizing asynchronous execution to handle the NFT creation process. The data structure includes various fields such as product information, price, weight, and transaction details. This structured data is essential for creating a comprehensive and descriptive NFT. Moreover, the metadata options specify the file name "COD_RSA.json", suggesting the NFT's metadata will be in a format compatible with the RSA encryption scheme, further underpinning the security aspect of the NFT.

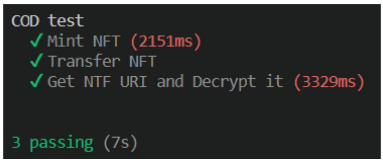

Fig. 5. NFT Minting and Decryption Test Benchmarks



Fig. 6. Minting NFT Function Implementation

Figure 7, we see the Pinata cloud interface, which is used for hosting the NFT data (step 3). The file "COD_RSA.json" appears to have been successfully uploaded to the IPFS through Pinata, as indicated by its presence in the files list. The use of Pinata suggests an intention to leverage decentralized storage solutions for maintaining the NFT metadata, which not only provides redundancy and persistence but also aligns with the decentralized nature of blockchain technology.

Finally, Fig. 7 showcases the actual encrypted data as it is stored on the IPFS, retrieved via a specific IPFS gateway. The data is displayed as an encrypted

string, representing the secure storage of the NFT's content. This level of encryption is critical to protect sensitive transaction data from unauthorized access, and it requires the corresponding private key for decryption, ensuring that only authorized participants can access the transaction's details (Fig. 8).

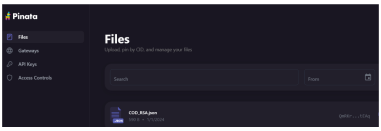

Fig. 7. Pinata Cloud Storage Interface

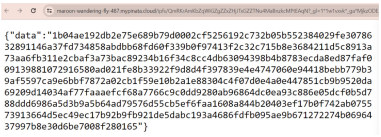

Fig. 8. Encrypted NFT Data Retrieval from IPFS

The detailed analysis of the performance and the secure handling of data through encryption and storage reveals a system designed with security and efficiency at its core. The time taken for minting and decrypting NFTs demonstrates the feasibility of integrating such a system into real-world COD transactions, where the balance between security measures and performance is critical. The implementation of RSA encryption within this context not only safeguards against potential data breaches but also ensures the privacy and integrity of the transactions, thus addressing two of the most significant concerns in e-commerce today. This intricate process, from minting to encryption and secure storage, forms a comprehensive solution poised to enhance the COD payment landscape significantly.

6 Evaluation

6.1 Performance Evaluation of RSA-Encrypted NFT Framework

The evaluation of our work involved a thorough analysis of the performance of RSA encryption and decryption in two distinct scenarios: encryption of a 120 KB image and encryption of the text presented in Fig. 6 The experiments were structured into three stages: Generating the RSA key, Encrypting, and Decrypting. The outcomes are elucidated in a structured format below.

For the image encryption scenario, the process times across ten trials showed notable consistency and variation in performance. The average time taken for generating the RSA key was approximately 2,461 ms, highlighting a relatively high computational demand in the key generation phase. This duration is crucial as it underpins the security of the RSA algorithm, with longer key generation times often correlating with increased security strength. The encryption times averaged around 1,156 ms, indicating a faster process compared to key generation. This quicker encryption process is beneficial in real-world applications where rapid response times are desired. Decrypting the image, however, took an

average of 3,442 ms, the longest duration among the three stages. This longer decryption time is attributed to the computational complexity involved in the RSA decryption process, underscoring the trade-off between security and computational efficiency (Table 1).

Table 1. Time Analysis for RSA Processes in Image Data Encryption and Decryption 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, similar patterns were observed. The RSA key generation time averaged around 2,413 ms, aligning closely with the image encryption scenario and reaffirming the computational intensity of this stage. Encrypting the text (Fig. 6) took an average of 1,167 ms, comparable to the image encryption, suggesting that the RSA encryption algorithm maintains a consistent performance regardless of the data type. The decryption time for the text averaged around 3,561 ms, slightly higher than that for the image decryption. This increment might be due to variations in the data structure of the text compared to the image, affecting the decryption complexity (Table 2).

Table 2. Evaluation of RSA Key Generation, Encryption, and Decryption Timings for Text Data Scenario

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 the performance, it is evident that the RSA encryption process is relatively efficient and consistent across different data types. However, the key generation and decryption processes are computationally intensive, a characteristic inherent to RSA due to its high security standards. The decryption time, being the longest, highlights the computational costs associated with secure data retrieval in RSA-encrypted systems. This trade-off between security and efficiency is a critical consideration in the deployment of RSA-encrypted systems in real-world applications, especially in e-commerce scenarios where both security and speed are paramount.

In conclusion, the evaluation demonstrates that while the RSA encryption method in our proposed system ensures a high level of security, it does so at

the expense of increased computational time, especially in key generation and decryption phases. This insight is essential for optimizing and balancing the security and efficiency of payment systems in e-commerce, particularly in scenarios demanding rapid transaction processing without compromising data security.

6.2 Economic Efficiency of Smart Contract Deployment for RSA-Encrypted NFTs

Smart Contract Deployment on EVM-Compatible Platforms. In the quest to revolutionize payment systems, we explored the deployment of smart contracts on four eminent Ethereum Virtual Machine (EVM)-compatible platforms. Binance Smart Chain (BNB Smart Chain), Polygon, Fantom, and Celo were selected due to their prominence and innovative contributions to the blockchain ecosystem. These platforms, while ensuring compatibility with Ethereum, offer distinct advantages and cost structures, making them suitable candidates for our implementation.

Our research involved deploying and examining the performance of smart contracts-specifically their transaction creation, NFT minting, and transfer capabilities-within real-estate transaction scenarios on these platforms, ensuring the integrity and functionality of our RSA-encrypted NFT framework.

Comparative Transaction Fee Analysis. The operational costs associated with blockchain technologies are a critical factor, especially in the adoption of smart contracts for commercial applications like cash-on-delivery transactions. We conducted a meticulous analysis of the transaction fees required for deploying smart contracts and executing their functions on each platform, as shown in Table 3. This assessment was vital for understanding the financial feasibility of our proposed payment system across different blockchain networks.

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)

The findings from our examination revealed Fantom as the optimal platform for deploying our smart contract for RSA-encrypted NFTs, particularly considering the economic efficiency. The transaction fees on Fantom, as detailed in Table 3, were substantially lower compared to the other platforms. Such cost-effectiveness, paired with robust functionality, positions Fantom as a leading

choice for our application, which demands frequent and economically feasible smart contract interactions. The reduced costs of NFT minting and transfer on Fantom are conducive to the broad-scale implementation of blockchain solutions in payment systems, particularly in the real estate sector where multiple, frequent transactions are the norm.

This comparative analysis underscores our commitment to not only enhancing the security and efficiency of COD transactions but also ensuring the economic viability of our solutions in real-world applications. By selecting a platform that aligns with our performance and cost-efficiency criteria, we lay the groundwork for a more accessible and practical adoption of blockchain technology in the transformation of payment systems.

7 Discussion

In discussing the validity of our study on integrating RSA-Encrypted NFTs in blockchain for cash-on-delivery transactions, it's crucial to acknowledge the inherent limitations and potential threats to the validity of our proposed model. One of the primary concerns is the computational demand of RSA encryption, which, while providing a high level of security, imposes a significant processing overhead. This could potentially limit the scalability of our system, especially in scenarios with a high volume of transactions or where rapid transaction processing is required.

Another threat to validity is the assumption of consistent network conditions. The performance evaluation was conducted in a controlled environment, which may not accurately reflect the real-world conditions where network latency and varying loads could affect the transaction times. Additionally, the deployment of smart contracts across multiple blockchain platforms may encounter unforeseen challenges due to platform-specific constraints or incompatibilities, which could hinder the practical implementation of our model.

Furthermore, the ever-present risk of evolving security threats, particularly in the realm of blockchain and encryption technologies, cannot be overlooked. Our system's reliance on RSA encryption may be robust against current threats, but the development of quantum computing and other advanced cryptographic attack methods could pose significant risks in the future. This necessitates ongoing research and updates to our encryption mechanisms to maintain the integrity and security of the transactions.

The economic feasibility of deploying our model is also subject to the volatile nature of transaction fees within the blockchain ecosystem. The cost-effectiveness of our approach today might be challenged by fluctuating transaction fees, affecting the overall sustainability of the model. As such, continuous monitoring of the economic landscape and the integration of adaptive fee management strategies are essential for the long-term viability of the proposed system.

Lastly, the adoption of our RSA-Encrypted NFT framework depends heavily on the end-user acceptance and the perceived complexity of the system. Despite its technical merits, the practical deployment may face resistance due to the

technology's complexity and the potential reluctance of users to transition from traditional payment systems to a blockchain-based model.

Addressing these threats to validity and acknowledging the limitations of our deployment strategy is critical for the refinement and successful implementation of our proposed model. Future work will need to focus on optimizing the encryption process for better performance, designing robust systems capable of adapting to changing network conditions and security landscapes, and ensuring economic and user-centric feasibility to facilitate widespread adoption.

8 Conclusion

The research presented a pivotal advancement in the landscape of digital payment systems. By intricately combining RSA encryption with NFTs in a blockchain-based environment, this paper addresses the critical challenges of traditional COD systems, offering a solution that is not only secure and transparent but also efficient. This innovative approach transcends the limitations of existing payment systems, particularly in securing and streamlining cross-border transactions. The integration of advanced cryptographic techniques with blockchain technology in our model sets a new standard in the realm of e-commerce transactions, emphasizing security, privacy, and transactional integrity. This contribution is poised to have a substantial impact on the future of digital transactions, potentially revolutionizing the way COD transactions are conducted and perceived in the digital era. It is a forward-looking solution that signals a new era of trust and reliability in e-commerce, catering to the dynamic needs of a rapidly evolving digital economy.

References

1. Ahmadieh, E., El Madhoun, N.: Artwork NFTS for online trading and transaction cancellation. In: 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA), pp. 235–239 (2023)
2. Dragomir, A.G., Van Woensel, T., Doerner, K.F.: The pickup and delivery problem with alternative locations and overlapping time windows. Comput. Oper. Res. **143**, 105758 (2022)
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. Elghaish, F., Abrishami, S., Hosseini, M.: Integrated project delivery with blockchain: an automated financial system. Autom. Constr. **114**, 103182 (2020)
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., Le, T.H., Phan, T.T., Nguyen, H.H.D., Vo, H.K., Duong-Trung, N.: Scrutinizing trust and transparency in cash on delivery systems. In: Wang, G., Chen, B., Li, W., Di Pietro, R., Yan, X., Han, H. (eds.) SpaCCS 2020. LNCS, vol. 12382, pp. 214–227. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-68851-6_15

7. Hasan, H.R., Salah, K.: Proof of delivery of digital assets using blockchain and smart contracts. IEEE Access **6**, 65439–65448 (2018)
8. Jha, A., Dubey, S., Kumar, H.U.: Transaction system based on blockchain technology using smart contract. Int. J. Sci. Res. Eng. Manag. (2023)
9. Le, H.T., et al.: Introducing multi shippers mechanism for decentralized cash on delivery system. Int. J. Adv. Comput. Sci. Appl. **10**(6) (2019)
10. 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)
11. Mohammed, N.S., Dawood, O., Sagheer, A., Nafea, A.A.: Secure smart contract based on blockchain to prevent the non-repudiation phenomenon. Baghdad Sci. J. (2023)
12. Quoc, K.L., et al.: SSSB: an approach to insurance for cross-border exchange by using smart contracts. In: Awan, I., Younas, M., Poniszewska-Marańda, A. (eds.) MobiWIS 2022. LNCS, vol. 13475, pp. 179–192. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-14391-5_14
13. Raj, P.V.R.P., Jauhar, S.K., Ramkumar, M., Pratap, S.: Procurement, traceability and advance cash credit payment transactions in supply chain using blockchain smart contracts. Comput. Ind. Eng. **167**, 108038 (2022)
14. Sikder, A.S.: Blockchain-empowered e-commerce: Redefining trust, security, and efficiency in digital marketplaces in the context of Bangladesh. Blockchain-empowered e-commerce. Int. J. Imminent Sci. Technol. **1**(1), 216–235 (2023)
15. Son, H.X., et al.: Towards a mechanism for protecting seller's interest of cash on delivery by using smart contract in hyperledger. Int. J. Adv. Comput. Sci. Appl. **10**(4) (2019)