A STUDY ON AN INTEGRATED FRAMEWORK FOR COPYRIGHT PROTECTION ON NFT

Hye-Young Kim

Department of Games, Hongik University, Sejong-si, Korea

ABSTRACT

NFT (Non-Fungible Token) has considerable potential in the field of intellectual property. It can not only improve the efficiency of copyright registration but also promote the improvement of transaction transparency and liquidity. However, existing copyright protection schemes of NFT image relied on the NFTs itself minted by third-party platforms. Also, the widespread use of NFTs has introduced new complexities to copyright protection due to their unique nature. Therefore, we have proposed a multi-layered blockchain security framework to resolve security vulnerabilities by protecting users from threats such as illegal copying, intellectual property rights infringement, and malware infection that may occur during the process of acquiring NFT assets through analysis of smart contracts, metadata, and digital assets that constitute NFTs.

KEYWORDS

Blockchain, Non-Fungible Token, copyright protection, smart contract

1. INTRODUCTION

Blockchain technology is increasingly being used in a wide range of industrial sectors, including financial services, games and entertainment, logistics and distribution, digital identity verification, public services, and healthcare. Non-fungible token (NFT), a digital asset verification system based on blockchain technology, is becoming a pivotal element of the new digital economy [1-4]. However, the fast expansion of the NFT market is accompanied by new security problems. According to OpenSea, the world's largest NFT trading platform, approximately 80% of NFTs generated using its NFT creation tool were verified as either plagiarized or forged collections [2].

By assigning weights based on the importance and risk level of each validation item, we enabled a more precise evaluation of NFTs. For example, higher weights were assigned to direct security threats such as malware detection, while relatively lower weights were given to indirect threat factors like the properties of content assets in metadata. This enables users to quantitatively assess the overall security level of NFTs and make informed purchase decisions based on risk levels.

Additionally, this framework mitigates the risk of malware infection that may arise during the downloading or trading of NFTs while ensuring the secure storage and use of digital assets. It aims to safeguard users from diverse security risks, such as unauthorized duplication, copyright infringement, and malware, while also promoting the growth of a dependable NFT ecosystem.

David C. Wyld et al. (Eds): COMIT, AISO, CRBL, WIMNET, EDUPT– 2025
pp. 77-82, 2025. CS & IT - CSCP 2025 DOI: 10.5121/csit.2025.151206

Therefore, we have proposed an integrated framework for aims to enhance the dependability of the digital asset market and provide a robust trading environment through the practical implementation of the NFT security framework.

2. PROPOSED SCHEME

In this paper, we have proposed a comprehensive framework enabling users to easily verify the quality and security of NFTs. This framework comprehensively analyses the three fundamental components of NFTs: smart contracts, metadata, and digital assets. In this study, rather than making simple Pass/Fail judgments on the key validation functions proposed above, we implemented a weight-based evaluation system.

Figure 1 illustrates the proposed framework for intellectual property protection of NFTs proposed in this study. The framework comprises a collecting unit that gathers NFT block data, metadata, and digital asset information, and an API service provider that performs validation and security assessments on proposed NFTs and reports the outcomes of these evaluations.

The following formatting rules must be followed strictly. This (.doc) document may be used as a template for papers prepared using Microsoft Word. Papers not conforming to these requirements may not be published in the conference proceedings.

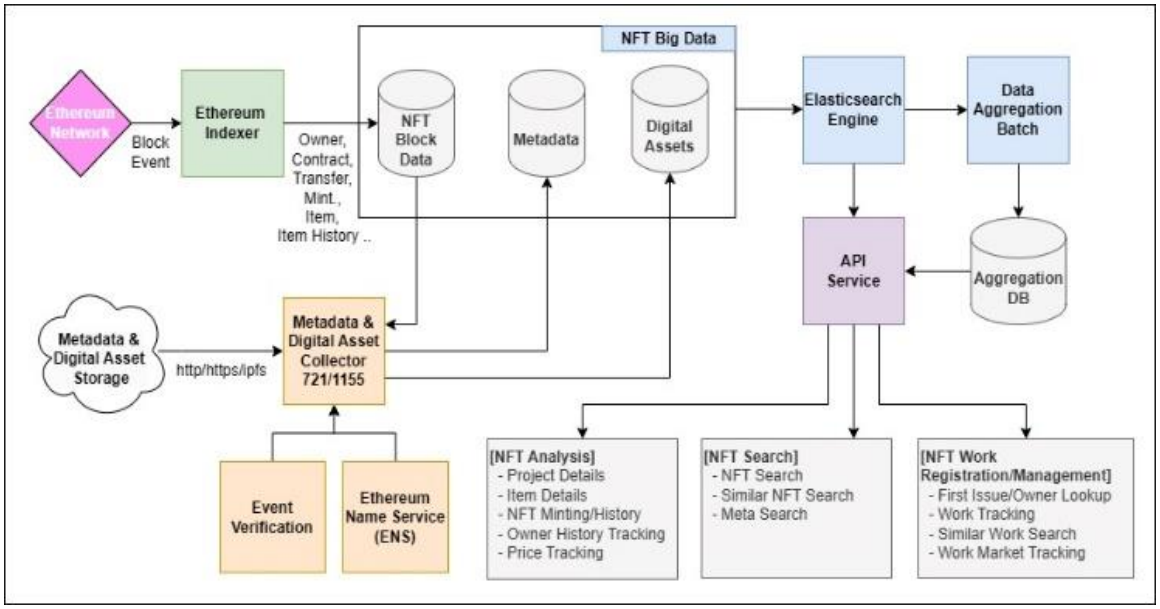

Figure 1. Framework for the protection of intellectual property rights related to NFTs

2.1. Blockchain Indexing

A technology for indexing data from blockchains such as Ethereum, Flow, Polygon, Solana, and Klaytn into an analysis database is developed [5]. This technology enables the fast retrieval and analysis of blockchain data stored in the analysis database [6].

If relevant to the collection target, embed and store TransactionReceipt based on transaction data. To reduce the index size, use blockNumber as the index and blockNumber + transactionIndex as

the unique index. Only the data required by the NFT framework are loaded. Gather all contract deployments.

2.2. Validation Check

The legitimacy of digital assets associated with NFT tokens is verified, and the results are presented [7]. In addition to validity, it also assesses accessibility, reliability, security, and persistence. Additionally, we assign appropriate weights to each validation item, calculate these weights upon verification requests, and deliver the corresponding results.

Table 1. items for validation checks

Classification	Primary Validation Items	Weight
Contract	Compliance with the ERC-721 standard	5
	Compliance with the ERC-1155 standard	5
	The registration status of the contract code on Etherscan	5
	The acquisition status of the token URI based on the contract address and token ID	3
Metadata	Compliance of ERC-721 with the expanded OpenSea standard	3
	Compliance of ERC-1155 with the expanded OpenSea standard	3
	The acquisition status of metadata via token URI	4
	Verify the response time to the metadata request	2
	Verify the location of metadata storage (centralized, decentralized)	3
	Verify if the access URL protocol is HTTPS if the metadata is of a centralized type	4
Content	Compliance with specifications for content asset attributes (e.g., image, animation_url) in metadata	3
	Verify that the information may be connected to tangible assets	4
	Verify that the actual asset information adheres to standards	3
	The availability of asset information (e.g., image, image data, animation_url, youtube_url)	4
	Verify response time to the asset information request	2
	Verify the asset storage locations (e.g., centralized, decentralized, image, image data, animation_url, youtube_url)	3
	Verify that the access URL protocol is HTTPS if the asset is of a centralized type	4
	Whether the external URL is accessible within 10 s	2

2.3. Security Check

Table 2. secure assessment items

Classification	Primary Validation Items	Weight
Contract	Verify if the NFT contract address has been reported as a scam	5
Metadata	Conduct a security assessment to check whether the metadata access URL is a secure host	5
	Verify the inclusion of Javascript code in the metadata URL response	5
Content	Conduct a security assessment to check whether the URLs of the asset information attributes originate from a secure host	5
	Conduct a malware assessment for the asset downloaded via the URLs of the asset information attributes	5
	Verify the inclusion of HTML/Javascript if the asset information attribute is SVG	5

Malware and URL assessments for NFT digital assets are conducted, and the findings to determine the safety of the NFT are provided. As with the validation items, weights were also assigned to security inspection items.

3. PERFORMANCE ANALYSIS

we implemented the proposed framework to validate the tokens that were sold on OpenSea. In figures 2, we show an inspection results, respectively. (Note: Original Korean interface text is shown with English translations for reference).

This study systematically validated the compliance of NFTs with the standard for smart contracts. The verification items were categorized as mandatory and optional requirements.

In terms of mandatory requirements, we confirmed the implementation of the ERC-721, ERC-165, and ERC-721TokenReceiver interfaces. More specifically, the verification included the implementation of the Transfer, Approval, and ApprovalForAll.

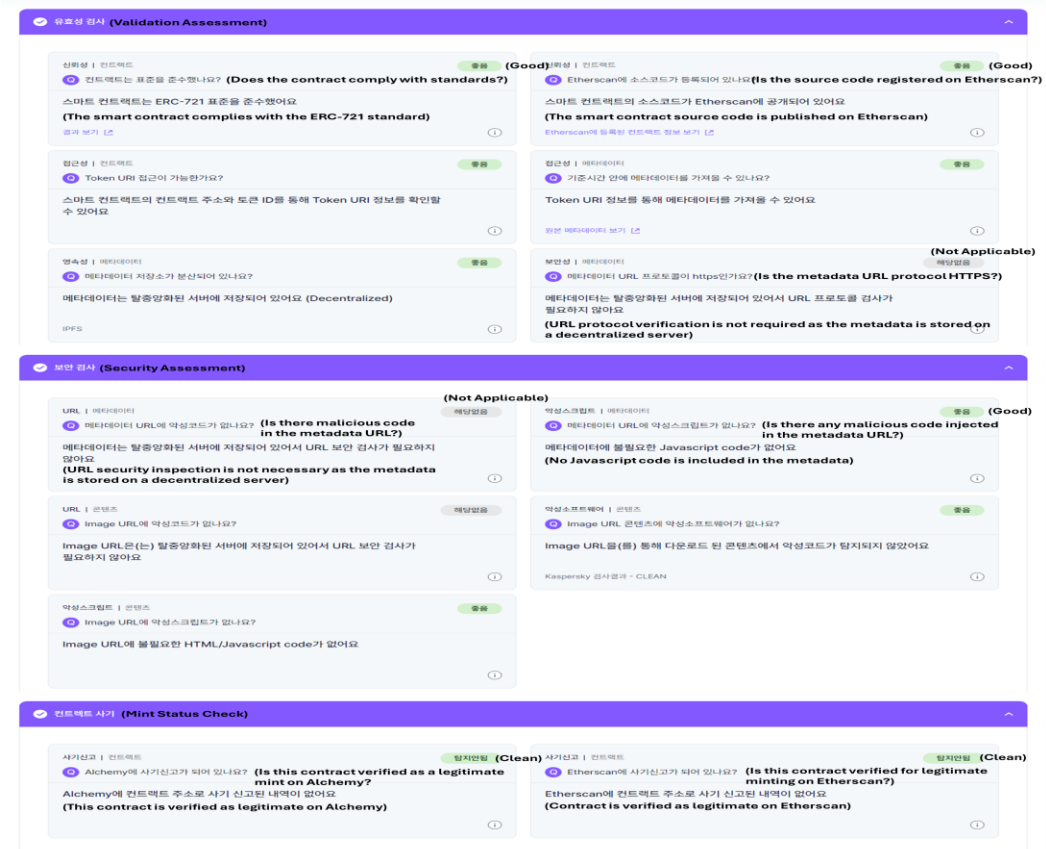

Figure 2. Test Results

In terms of optional requirements, we verified the implementation of the ERC-721Metadata and ERC-721Enumerable interfaces. The implementation of name (token name), symbol (token symbol), and tokenURI (token metadata URI) was verified as a metadata-related function.
The verification confirmed that the assessed NFT fulfilled all the required criteria, and it was also determined that the metadata interface, an optional requirement, was flawlessly implemented.

This indicates that the NFT adheres strictly to the Ethereum network's standards and allows for secure transactions and ownership management.

This comprehensive verification process is crucial because it provides objective standards for NFT buyers to assess the technological stability of the asset [8].

Furthermore, this study introduced a weight-based evaluation system to enhance the objectivity and accuracy of verification by reflecting the importance of each inspection item. The items were categorized into security and validation assessments, evaluated independently. While the current phase only displays binary (pass/fail) results for each item, the system internally computes weighted scores for both assessments. Future iterations will implement the display of these weighted evaluation results.

4. CONCLUSIONS

We developed an innovative security verification framework to improve the reliability of the rapidly growing NFT market. Our proposed framework implements a multi-tiered verification system that includes smart contracts documented on the blockchain, metadata from distributed storage, and actual digital content. Specifically, it identifies potential risk factors using security vulnerability analysis for each layer and provides objective assessment information on the current state and security level of NFTs.

ACKNOWLEDGEMENTS

This study was supported by the Culture, Sports and Tourism R&D Program through the Korea Creative Content Agency grant funded by the Ministry of Culture, Sports, and Tourism in 2024 (Project Name: Global Talent Training Program for Copyright Management Technology in Game Contents, Project Number: RS-2024-00396709, Contribution Rate: 100%).

REFERENCES

[1] Dipanjan Das, Priyanka Bose, Nicola Ruaro, Christopher Kruegel, and Giovanni Vigna. 2022. Understanding security issues in the NFT ecosystem. In *ACM SIGSAC Conference on Computer and Communications Security*. 667–681.

[2] Oleg Wlasinsky. 2023. Literature review on the most popular of NFTs types. *Int. J. Educ. Technol. Artif. Intell.* 2, 1 (2023), 8–12.

[3] Statista, "NFT Market share," accessed Jul. 2024. [Online]. Available: https://www. Statista.com/outlook/fmo/digital-assets/nft/worldwide.

[4] "Treatment episode data set: discharges (TEDS-D): concatenated, 2006 to 2009." U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, Office of Applied Studies, August, 2013, DOI:10.3886/ICPSR30122.v2.

[5] Nguyen, T., "The Role of AI in Vietnam's Digital Transformation", Vietnam Technology Review, 2023.

[6] Choi, D., "Copyright Challenges in AI-Based Industries", Journal of Content Protection, 2022.

[7] C. Pungila, D. Galis, V. Negru, A new high-performance approach to approximate pattern-matching for plagiarism detection in blockchain-based non-fungible tokens (NFTs). Computer Science, (2022).

[8] [8] Bamakan, S.M.H.; Motavali, A.; Bondarti, A.B. A survey of blockchain consensus algorithms performance evaluation criteria. Expert Syst. Appl. **2020**, 154, 113385.

AUTHOR

Hye-Young Kim works at Hongik University of South Korea as a Full Professor since March 2007. She had developed a network protocol for 9 years while she was working at Hyundai Electronics as a senior researcher. Her research interests include traffic modeling, load balancing scheme and copyright technology for digital content on blockchain and web3.