SafeNFT Mart: A DSR Approach to a Secure NFT Marketplace

Ashok Kasthuri[a], Aseem Pahuja[b], Zhiling Guo[c], Lingxiao Jiang[a], Richard Banach[b]

[a]Singapore Management University

[b] University of Manchester

[c]University of North Texas

Contact: ashokk.2022@phdcs.smu.edu.sg; aseem.pahuja@manchester.ac.uk; zhiling.guo@unt.edu; lxjiang@smu.edu.sg; richard.banach@manchester.ac.uk;

Abstract

NFT marketplaces have witnessed exponential growth. The unique attributes of NFTs, encapsulated by the acronym CRAVED (concealable, removable, available, valuable, enjoyable, disposable), make them susceptible to multifaceted thefts. In response, we introduce "SafeNFT Mart," an NFT marketplace architecture devised to thwart counterfeiting and uphold both asset and ownership integrity. We leverage Zero Knowledge Proofs (ZKPs) for ownership verification and integrate a stringent punishment protocol to deter illicit activities. Our design draws from the design science research (DSR) approach. Expert interviews were conducted to fortify our findings, focusing on relevance, adaptability, and technological viability in tandem with real-world and strategic implications. An initial analytical model is provided to gauge the efficacy of our punitive mechanism. This research culminates with future work, outlining the further development and refinement of the proposed marketplace solution.

Keywords: Blockchain, NFT Marketplace, ERC 721, ZKP

Introduction

The meteoric rise of the NFT marketplace has been accompanied by considerable security challenges, most notably in the realms of cyber and intellectual theft. Esteemed platforms, including OpenSea and Rarible—pillars of the emerging crypto economy—aren't immune; counterfeit NFTs are believed to comprise a staggering 80% of OpenSea's complimentary listings (Jacobs, 2022). High-profile cases, such as the doxing of the Bored Ape Yacht Club NFT creators (Macaulay, 2022) and the theft of Seth Green's NFTs (Binder, 2022), underscore the magnitude of the problem.

Theft in the NFT domain predominantly manifests in two guises: **Cyber Theft**, where malicious actors hack digital wallets to appropriate NFTs; **Intellectual Theft**, where original content is replicated, leading to the minting and sale of fraudulent NFTs.

Central to their vulnerability is the inherent alignment of NFTs with the CRAVED attributes (Clarke RV, 1999): ***Concealable***: Unless explicitly encrypted, NFTs are not concealable as public blockchains like Ethereum allow access to anyone running a node or a blockchain explorer. NFTs are distinctly ***Removable*** as they can be effortlessly transferred between digital wallets. Once an unauthorized transfer occurs, despite the transaction's transparency, reclaiming ownership can be a formidable challenge. Their perpetual ***Available*** status on the blockchain leaves them continuously exposed, heightening the risk of targeted breaches. Their intrinsic ***Valuable & Enjoyable*** nature is underscored by their ability to encapsulate diverse digital phenomena, from art to virtual real estate, augmenting their allure for both legitimate users and malicious actors. ***Disposable***: Malicious actors can take advantage of the quick and convenient selling process to create counterfeit NFTs, tricking buyers into purchasing non-authentic or stolen assets.

In response to the escalating threats, we propose SafeNFT Mart, a safe marketplace design engineered to fortify the security and authenticity of NFT ownership. Its novelty resides in a comprehensive strategy that amalgamates Zero Knowledge Proofs (ZKPs), a robust punishment policy, and an address abstraction technique—a three-pronged approach dedicated to enhancing the security and privacy of the NFT marketplace. Our SafeNFT Mart design integrates advanced technologies, which brings along some complexities while integrating them with underlying blockchain infrastructure. Central to the design is the incorporation of Zero Knowledge Proofs (ZKPs), which demands an in-depth comprehension of foundational mathematical and cryptographic concepts. This includes proof generation, data encryption, and commit schemes backed by cryptographic hash functions like SHA-256, Merkle trees, and random function generators for unpredictable challenges. These elements, combined with the need for interoperability with existing blockchain infrastructures, render our design non-trivial.

Theoretical Background

The existing research on NFTs has primarily focused on the creation and purchase motivations of NFTs (Haried and Murray 2022; Pawelzik and Thies 2022), the effect of NFT collectibles on the sales of physical collectibles (Kanellopoulos et al. 2021), applications of NFT to event ticketing (Regner et al. 2019), and the metaverse (Brown Sr et al. 2022). Of interest to us is research on NFT Marketplaces (NFTMs), which is still in its nascent stages. Pawelzik and Thies (2022) and White et al. (2022) present qualitative and quantitative analyses of the NFTMs, respectively.

Major NFTMs such as OpenSea and Rarible are centralized in that even though they use blockchain to transfer the ownership of the NFT, user identity management and listing are done on central servers (Das et al. 2022). NFT fraud has been studied by Kshetri N (2022).

Centralization presents a risk of being hacked and not only revealing user identities but also their asset ownership and past transaction history. This is because once the connection between real-life identity and blockchain wallet is revealed, transparency of the blockchain enables anyone to query account balances, asset ownership, and transaction history of the affected wallets (Tschorsch and Scheuermann 2016).

Analysis of NFT markets reveals ongoing challenges related to cyber and intellectual property theft (Yoder, 2022). Counterfeiters not only replicate NFT digital art but also create fake URLs and listing names. Research by Das et al. (2022) found that approximately 24.4% of listing URLs on OpenSea were counterfeit, reflecting a longstanding issue in the digital goods space (Jaisingh, 2009; Sundararajan, 2004). One specific concern is the tampering of NFT metadata, discussed by Wang et al. (2021) and Das et al. (2022). To address these issues, Das et al. (2022) propose a URL comparison method for mitigation. Additionally, concerns about asset ownership, as highlighted by Bellagarda et al. (2022) and Avrilionis (2022), persist in the NFT ecosystem. Motivated by this, we propose a solution that employs Zero-Knowledge Proofs (ZKP) to ensure metadata integrity, following the work of Blum et al. (1988). We also introduce a punishment policy to address counterfeit problems.

General Deterrence Theory (GDT) (Peace et al. 2003) suggests that as malicious actors fear losses due to punishments, punishments can help curb these thefts. To operationalize the punishments in a decentralized NFTM we draw from the PnR (Punishment Not Reward) Blockchain Architecture and propose two punishments: public listing of malicious wallets and permanent ban. We account for these factors in our economic evaluation that follows expert evaluations.

Design Science Research Methodology

Following Peffers et al. (2007)'s design science approach, we started with **Problem Identification and Motivation**, recognizing the rampant NFT theft and counterfeiting in the prevalent ecosystem. Moving to **Define the Objectives of a Solution**, our goal was to craft a secure NFT marketplace that could deter these threats. For the **Design and Development** phase, we merged technical elements, like using address abstraction techniques and Zero-Knowledge Proofs (ZKP) for ownership and content verification of the NFTs, with social elements, like the punishment policy against malicious actors. Our methodology culminated in **Demonstration & Evaluation**, where an NFT marketplace design was showcased at our university. Here, feedback from experts paired with economic analysis provided a preliminary assessment of our solution's impact and feasibility. Due to paucity of space we are unable to delve deeper into each process of DSRM.

Components of the Marketplace

Interplanetary File System (IPFS): IPFS provides a decentralized, secure, and reliable way to store and distribute NFT content. Users can trust that the associated content is genuine, unaltered, and accessible with the help of transparent, immutable log records.

NFT Metadata: NFT metadata contains unique attributes such as NFT's name, description, location, datatype (audio, video, image), creation process, and technical source. The NFT metadata is created to identify the asset with an asset URL with an integrated content identifier (CID) value. CID is created by combining the SHA-256 hash of the asset and the asset URL. This is embedded within the metadata to ensure the integrity of the asset with its storage location.

Zero-Knowledge Proofs:

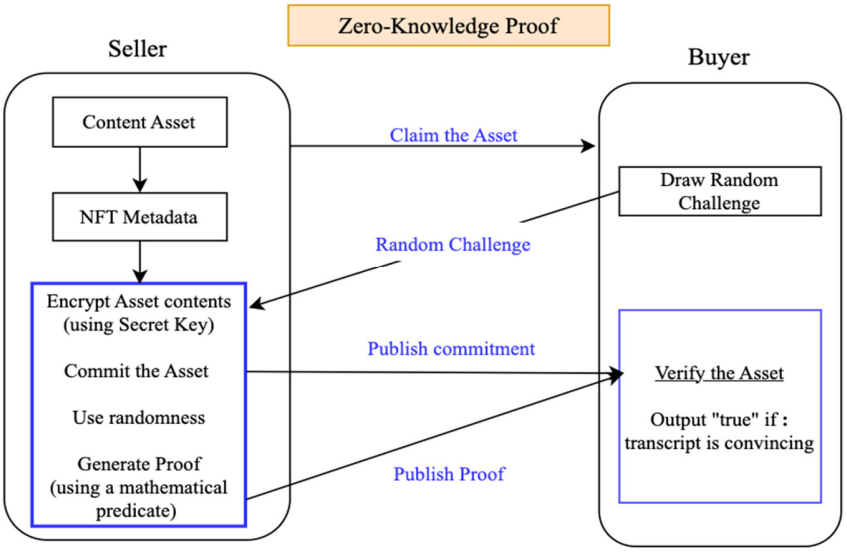

Figure 1. ZKP Overview

We took motivation from well-known zero-knowledge blockchain architectures (such as zCash (Hopwood et al. 2016)) and the DSR approach (Hevner et al. 2004) to create a safe NFT marketplace. The primary objective of the ZKP solution is to ensure integrity between the owner and the content.

The existing marketplaces encounter various issues, including tampering with metadata, specifically the image URL link (Das et al., 2022), which is a common method used to deceive buyers. When metadata tampering occurs, it results in the buyer not receiving the expected asset associated with the NFT, and there's also a potential risk of compromising the buyer's wallet's private keys when dealing with a corrupted NFT. These challenges undermine the integrity of NFTs within the marketplace.

Commitment, Binding, and Verification: To tackle the tampering issue, we propose a 'commit and bind' scheme using Zero-Knowledge Proofs (ZKP), as illustrated in Figure 1. Additionally, to combat counterfeiting, we have implemented a robust punishment policy. In the commitment phase, the NFT's metadata undergoes cryptographic commitment by hashing its contents with its

digital signature, generating a commitment value that binds the content and ownership integrity. This commitment ensures the metadata remains unaltered during the verification process. For privacy protection, the asset's content is encrypted using an RSA public-private keypair (Rivest et al. 1978) generated using a unique key stored in a Trusted Execution Environment (such as Intel SGX), limiting access to authorized parties. The core of the verification process revolves around "proof generation (Bowe 2020)." ZKP plays a critical role in constructing a robust predicate, a mathematical expression used to verify the truth of a statement, leading to the creation of ZKP circuits. These circuits, comprising computations and constraints, produce a proof statement shared with the buyer for verification.

During the binding phase, the content committed by the seller in the commitment phase must align with what the buyer receives. A successful buyer verification and satisfaction match can lead to trade approval, while discrepancies trigger the enforcement of the punishment policy. To address scalability concerns related to ZKP, we intend to incorporate efficient ZKP libraries such as zk-SNARKs, Plonks, or Sonic, which offer faster proofs with reduced computational overhead.

Marketplace Operations

As illustrated in Figure 2, the foundation of the architecture lies in smart contracts deployed on Ethereum using interfaces ERC721 or ERC-1155, which define the rules and logic governing NFT creation, ownership transfer, verification, and security mechanisms.

User Onboarding and Identity Management: To ensure the legitimacy of users and compliance with KYC/AML regulations, users are required to provide their credentials.

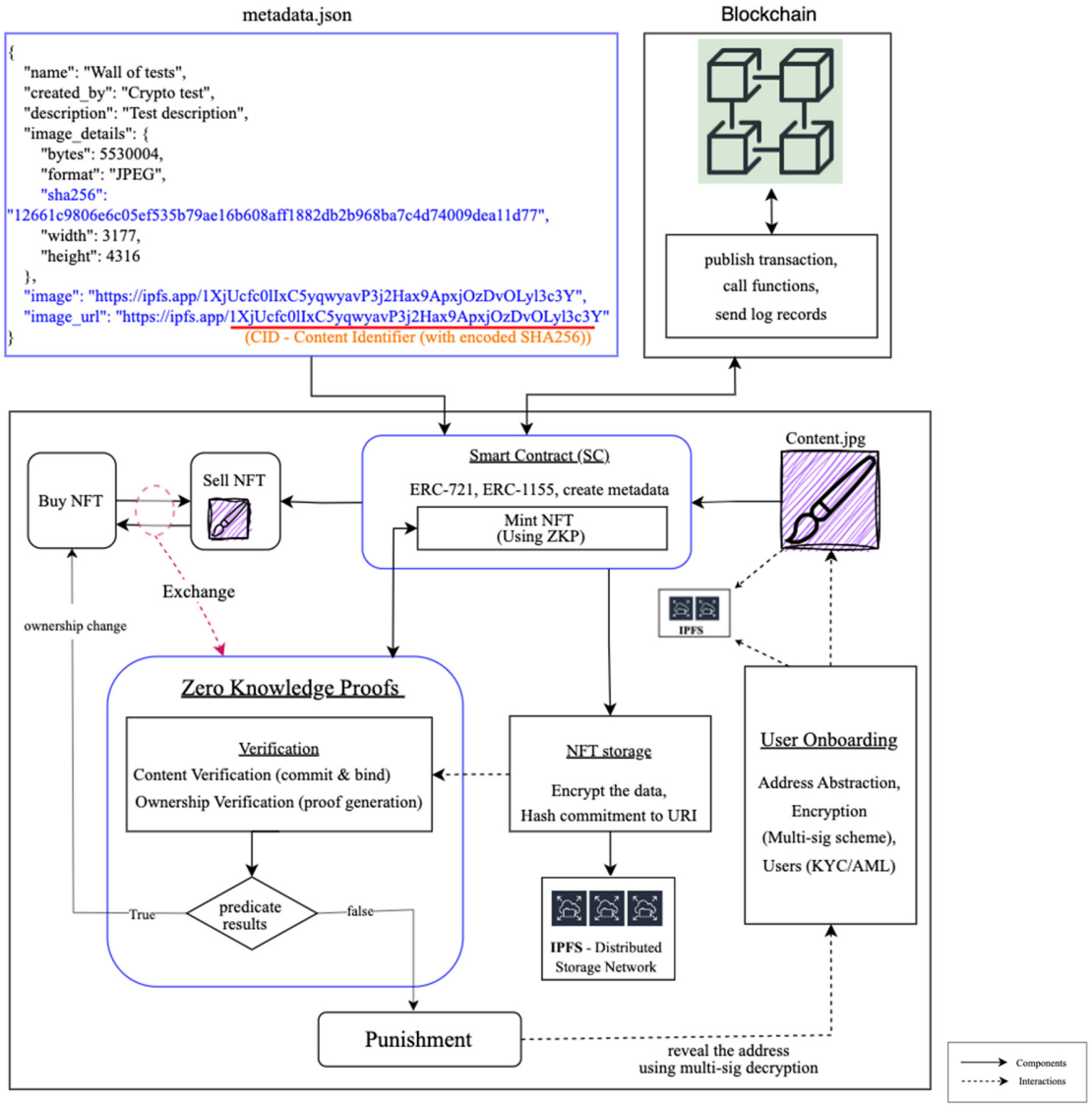

Figure 2. Proposed NFT Marketplace Design

The provided sensitive data is encrypted using a multi-signature scheme in a decentralized manner. The secure keys are not controlled by a central party, instead, keys are contributed by multiple parties, which decentralizes the control with enhanced transparency. We propose an account abstraction to provide anonymity to the users. Abstraction turns every user account into a logical contract that serves as proxies for user actions and interactions. These contracts act as intermediaries between users and the blockchain. Therefore, adds an extra layer of privacy by

masking the actual user identity by assigning a unique identifier (such as a cryptographic key). Using this identifier users initiate actions by interacting with proxy contracts.

At SafeNFT Mart, we require KYC/AML procedures, which bolster the effectiveness of our punishment policy compared to other marketplaces. An additional advantage of employing Zero-Knowledge Proofs (ZKP) is that it enhances NFT security by limiting accessibility. After all, one cannot view what they cannot access, thereby reducing the exposure of desirable attributes (CRAVED).

NFT Lifecycle: As shown in Figure 2, first, an artist creates some digital content and mints an NFT on Ethereum, using a deployed smart contract. Second, the creator may choose to list the NFT on an NFT Marketplace, such as OpenSea or Rarible, to sell. Potential buyers can purchase the NFT if their bid is successful.

ZKP Verification & Punishment Policy: ZKPs are utilized to verify the integrity and ownership of NFT as explained in Section 4. In case the verification process fails, and the output of the predicate is false, the platform's punishment policy is triggered to reveal the actual address of the user using a multi-signature decryption scheme.

The punishment policy is inspired by the Punishment-Not-Reward (PnR) blockchain architecture (Banach 2021). In PnR, rather than rewarding appropriate behavior with payments of cryptocurrency, which is the usual way of motivating good behavior on the blockchain, and which brings its problems of temptation to defraud the blockchain by illicitly acquiring the said cryptocurrency, disincentives are introduced to dissuade participants from unruly behavior. Drawing from Banach (2021), we propose two main punishment mechanisms: public listing of malicious wallet addresses and permanent bans from the NFTM. Punishment policy can be

invoked during the purchase process or upon a user reporting suspicious seller activity. If subsequent investigations confirm the seller's malicious actions, the punishments are applied.

Public listing through anonymity revocation implies that pseudo-identities are used in the NFTM and the corresponding blockchain, and a permanent ban implies that real identities are also involved (so that bad actors cannot simply re-enroll under a new, self-invented pseudonym). It is worth noting this is in line with the procedures of the US Office of Foreign Assets Control (OFAC), which maintains a list of cryptocurrency addresses that are sanctioned.

Expert Evaluations

We engaged five experts in the fields of cryptography, blockchain, and cryptocurrency, along with two novices, to evaluate the secure NFT marketplace's design. Our methodology was based on the guidelines by Rosemann and Vessey (2008). The majority of the participants agreed that the proposed marketplace design fosters trust and protects the genuine content creator. One expert provided a positive insight, stating: "*… the seamless integration of various components within the artifact, including user onboarding, marketplace smart contract interactions, ZKP verification, and the punishment policy, is based on evidence and structured arguments that addresses critical security and vulnerability challenges."* However, raising concerns, another expert noted "*On the negative side, privacy concerns may arise due to the use of ZKPs, potentially inviting regulatory scrutiny such as compromising KYC/AML regulations. Balancing privacy with transparency and addressing any unintended consequences will be crucial to ensure stakeholders' trust and long-term success*."

One of the experts responded about the artifact design that "*The artifact incorporates engineering principles of problem-solving, drawing from empirical evidence that has shown*

practical efficacy. In this work, following the DSR methodology, a critical analysis of definitions and arguments is carried out to identify and rectify potential errors".

When asked about the design's impact on the CRAVED aspects, an expert highlighted that "*the proposed NFT marketplace reduces the "CRAVED" attributes of NFTs. Through address abstraction, ownership privacy is maintained while deterring malicious tracing attempts. This design mitigates concealability through ownership verification. Counterfeit accountability is achieved through blockchain and IPFS integration, challenging the removability of fraudulent transactions. By discouraging counterfeiting via a punishment policy, value preservation is addressed, and an enjoyable user experience is upheld, supporting reliable disposal and trading of NFTs".* In sum, SafeNFT Marts' design introduces measures to deter intellectual and cyber theft, enhancing the overall trustworthiness of the NFT marketplace.

Economic Evaluation of Punishment Policy

As mentioned before, our punishment policy encompasses two punitive measures: public denouncement and a subsequent permanent ban. The initial transgression results in a public denouncement, which involves the revocation of anonymity and the inclusion of the offender's address into a registry of malicious actors. If another offense follows, a permanent ban is instituted (refer to the figure below for further elucidation).

To evaluate this policy, in line with Becker (1968), we develop a stylized analytical model representing the interactions of the NFTM and the malicious actor. In each period, the malicious actor decides on the level of illegal activity (denoted by a) and the NFTM decides on the effort in reviewing and reprimanding fake or stolen NFTs (denoted by b). *The Malicious Actor's Problem:*

$$v_c^f = (1 - p_r)u_c + p_r(u_o + (1 - p_r)u_{rc} + p_r u_o). \quad (1)$$

Equation 1 shows the value function of the malicious actor. The malicious actor's problem is to maximize his value function. He gets reported and reprimanded with the probability $p_r = \frac{ab}{1+ab}$. The functional form of p_r ensures that higher levels of counterfeiting as well as a higher level of effort from the NFTM increases the probability of getting reprimanded in a non-linear way. It also ensures that the probability is strictly less than 1, implying that the detection technology is imperfect. If he is not caught $(1 - p_r)$, he earns the utility $u_c = a^{\frac{2}{3}}$. We assume that $a \epsilon [1, a_o]$ such that the malicious actor's utility is concave in his effort, and he exerts effort between one and a_o . However, if he is sanctioned by public listing his utility falls to zero for that period ($u_o = 0$). In the next period, if he is reprimanded again, he is permanently banned ($u_o = 0$). However, if he is not reported and reprimanded again, he earns positive but reduced utility owing to a public denouncement in the previous period ($u_{rc} = a^{1/3}$). Please note that $u_c \geq u_{rc} > u_o$ since $a \geq 1$.

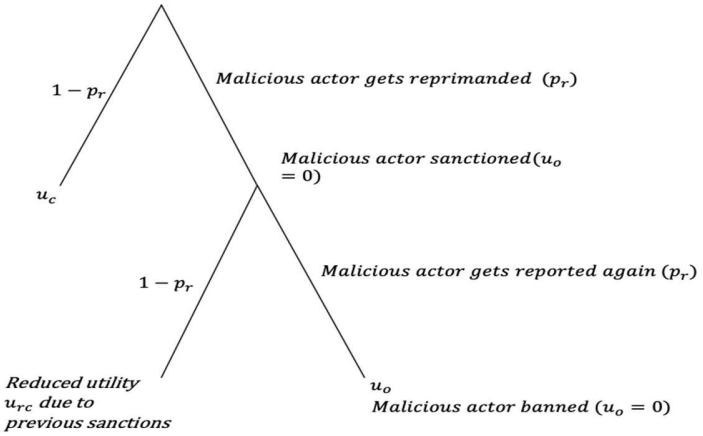

Figure 3. The sequence of punishment policy

NFT Marketplace's Problem:

$$v_m^f = -\frac{a^4}{b^2} - \frac{k_p^8}{k_c^8} b^2 \quad (2)$$

Equation 2 shows the loss function of the NFTM. We posit that the effort exerted by the NFTM lies within a positive range, denoted by $b \in [b_{min}, b_{max}]$. The first term of the value function presents the loss in the value of the platform due to malicious activity. Notably, the loss increases the level of malicious activity and decreases the efforts of the platform in reviewing NFTs and reprimanding the malicious actors. It is also worth highlighting that even when the malicious actors are caught and penalized, the NFTM still incurs a loss. This is because these malicious actors have already enacted their malicious deeds (such as theft or counterfeiting) in that period, regardless of their subsequent apprehension.

The efforts of the NFTM come at the cost of $\frac{k_p^8}{k_c^8} b^2$ where k_p is the marginal cost of the NFTM's effort. The marginal cost drops by a factor of k_c^8 if the community is active in reporting malicious activity such as fake NFTs. We note that the analytical formulations of the utility functions are only indicative and are chosen to get closed-form solutions, however, the results can be generalized to other functions. The NFTM's problem is to maximize its value function.

The Equilibrium analysis: To solve the maximization problem laid out in Equation (1), we differentiate v_c^f w.r.t a to get the first-order condition. Assuming positive effort, a similar procedure is followed to solve the maximization problem in Equation (2). We get $a^* = \frac{2}{b^*}$ and $b^* = \frac{k_c^2}{k_p^2} a^*$. As the results indicate, a malicious actor is thwarted by increasing levels of NFTM's efforts and NFTM's efforts increase with an increased level of malicious activity or decreased

level of community involvement (low k_c). Solving the system of best-response simultaneous equations we obtain the following optimal solution: $a^* = \frac{\sqrt{2}k_p}{k_c}, b^* = \frac{\sqrt{2}k_c}{k_p}$.

At equilibrium, the value lost by the NFTM is $\frac{4\,k_p^6}{k_c^6}$. Comparing this to the scenario where NFTM exert minimal effort ($b = b_{min}$), the value lost by the NFTM is $\frac{16}{b_{min}^6} + \frac{b_{min}^2 k_p^8}{k_c^8}$. Therefore, it is safe to say that implementing the punishment policy prevents a loss of $\frac{16}{b_{min}^6} + \frac{b_{min}^2 k_p^8}{k_c^8} - \frac{4\,k_p^6}{k_c^6}$.

Conclusion, Limitations, and Suggestions for Future Work

Our research explores the design of an NFTM that verifies ownership and content using ZKPs, and IPFS and suppresses cyber and intellectual thefts through a punishment policy. The punishment policy comprises the public denouncement of malicious actors, and permanent bans as the punishments. Also, by leveraging address abstraction for user anonymity, the marketplace enhances the integrity, authenticity, and user experience of NFT transactions. The combination of these features makes NFTs less CRAVED, reducing the risk of theft, unauthorized access, and manipulation. The paper has shown promising results, demonstrating the potential of the proposed marketplace to foster a secure and thriving NFT ecosystem. The preliminary evaluation of the punishment policy indicates that the optimal efforts of the NFTM and the level of malicious activities are inversely related.

The paper does have certain limitations that should be acknowledged. Firstly, the effectiveness of the punishment policy hinges on real-world implementation and cooperation from platform users, which may pose challenges in ensuring full compliance. Secondly, while Zero-Knowledge Proofs (ZKPs) enhance privacy, their adoption may demand additional computational

resources, potentially impacting transaction speeds and scalability. Additionally, the success of the marketplace relies on user adoption and participation, requiring effective marketing and community-building efforts.

Moreover, when it comes to content moderation, the choice between an automated image-matching tool (cost-effective but potentially less accurate) and a human-moderated system (highly accurate but costly) presents a trade-off. Lastly, we have not addressed the complexity of the reporting process, which is a critical aspect. Simplifying the reporting process may make it more vulnerable to misuse by competitors, whereas a cumbersome process could discourage reporting and result in underreporting of counterfeit items.

To address these limitations, future research may involve conducting comprehensive user feedback surveys and focus groups to gather valuable insights for ongoing improvements and user-centric enhancements. We intend to work on these aspects of the NFTM design for the journal paper.

References*:*

Avrilionis, D. and Hardjono, T., 2022. From trade-only to zero-value nfts: The asset proxy nft paradigm in web3. *arXiv preprint arXiv:2205.04899*.

Banach, R. (2021). "Blockchain Applications Beyond the Cryptocurrency Casino: The Punishment Not Reward Blockchain Architecture," *Concurrency and Computation: Practice and Experience* (33:1), pp 1 – 23.

Becker, G. S. (1968). Crime and punishment: An economic approach. Journal of Political Economy, 76(2), 169-217.

Bellagarda, J. and Abu-Mahfouz, A.M., 2022. Connect2NFT: A web-based, blockchain enabled NFT Application with the Aim of Reducing Fraud and ensuring authenticated social, non-human verified digital identity. *Mathematics*, *10*(21), p.3934.

Binder, M. (2022). "Seth Green's Bored Ape Was Stolen. Now He Can't Make His N.F.T. Show.", from https://mashable.com/article/seth-green-stolen-bored-ape-nft-show

Blum, M., Feldman, P., and Micali, S. (1988). "Non-Interactive Zero-Knowledge and Its Applications," in: *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*. Chicago, Illinois, USA: Association for Computing Machinery, pp. 103–112.

Bowe S, Chiesa A, Green M, Miers I, Mishra P, Wu H. Zexe: Enabling decentralized private computation. In2020 IEEE Symposium on Security and Privacy (SP) 2020 May 18 (pp. 947-964). IEEE.

Brown Sr, R., Shin, S.I., and Kim, J.B. (2022). "Will Nfts Be the Best Digital Asset for the Metaverse?," *SAIS 2022 Proceedings*, pp. 1 – 6.

Cao Z, Zhen Y, Fan G, Gao S. TokenPatronus: a decentralized NFT anti-theft mechanism. arXiv preprint arXiv:2208.05168. 2022 Aug 10.

Clarke RV, Webb B. Hot products: Understanding, anticipating and reducing demand for stolen goods. London: Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate; 1999 Nov 18.

Das, D., Bose, P., Ruaro, N., Kruegel, C., and Vigna, G. (2022). "Understanding Security Issues in the Nft Ecosystem," in: *ACM Conference on Computer and Communications Security 2022*. Pp. 1 – 17.

Haried, P., and Murray, J. (2022). "Understanding Non-Fungible Token (NFT) Purchase Motivations," in: *AMCIS 2022*. Pp. 1 – 5.

Hevner, Alan R., Salvatore T. March, Jinsoo Park, and Sudha Ram. "Design Science in Information Systems Research." *MIS Quarterly* 28, no. 1 (2004): 75–105. https://doi.org/10.2307/25148625.

Hopwood, D., Bowe, S., Hornby, T., and Wilcox, N. (2016). "Zcash Protocol Specification." pp. 1 - 217.

Jacobs, H. (2022). "The Counterfeit N.F.T. Problem Is Only Getting Worse." from https://www.theverge.com/22905295/counterfeit-nft-artist-ripoffs-opensea-deviantart

Jaisingh, J. (2009). "Impact of Piracy on Innovation at Software Firms and Implications for Piracy Policy," *Decision Support Systems* (46:4), pp 763-773.

Kanellopoulos, I.F., Gutt, D., and Li, T. (2021). "Do Non-Fungible Tokens (N.F.Ts) Affect Prices of Physical Products? Evidence from Trading Card Collectibles," in: *ICIS 2021 Proceedings*. pp. 1 - 9.

Kshetri N. Scams, Frauds, and Crimes in the Non-Fungible Token Market. Computer. 2022 Apr 11;55(4):60-4.

Macaulay, T. (2022). "'Doxxing' of Bored Ape Founders Exposes Web3's Transparency Issues." from https://thenextweb.com/news/bored-app-founders-doxxing-web3-transparency-privacy-issue

Pawelzik, L., and Thies, F. (2022). "Selling Digital Art for Millions-a Qualitative Analysis of N.F.T. Art Marketplaces," *ECIS 2022 Research Papers* (0:0), pp 1 - 16.

Peace, A.G., Galletta, D.F., and Thong, J.Y. (2003). "Software Piracy in the Workplace: A Model and Empirical Test," *Journal of Management Information Systems* (20:1), pp 153-177.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77.

Petrossian, G.A. and Clarke, R.V., 2014. Explaining and controlling illegal commercial fishing: An application of the CRAVED theft model. *British Journal of Criminology*, *54*(1), pp.73-90.

Pfeffers K, Tuunanen T, Gengler CE, Rossi M, Hui W, Virtanen V, Bragge J. The design science research process: A model for producing and presenting information systems research. In Proceedings of the First International Conference on Design Science Research in Information Systems and Technology (DESRIST 2006), Claremont, CA, USA 2006 Feb (pp. 83-106).

Rehman W, e Zainab H, Imran J, Bawany NZ. NFTs: Applications and challenges. In2021 22nd International Arab Conference on Information Technology (ACIT) 2021 Dec 21 (pp. 1-7). IEEE.

Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM* 21, no. 2 (1978): 120-126.

Rosemann, M.; and Vessey, I. Toward improving the relevance of information systems research to practice: The role of applicability checks, *MIS Quarterly,* 32, 1(2008), 1-22.

Regner, F., Urbach, N., and Schweizer, A. (2019). "N.F.Ts in Practice–Non-Fungible Tokens as Core Component of a Blockchain-Based Event Ticketing Application," *ICIS 2019 Proceedings* (0:0), pp 1 - 17.

Smith BT. Understanding shoplifting of fast-moving consumer goods: an application of the CRAVED model. Security Journal. 2018 Apr;31:428-50.

Statista.(2022). "N.F.T.: Industries & Markets." from https://www.statista.com/topics/8513/nft/#dossierKeyfigures

Sundararajan, A. (2004). "Nonlinear Pricing of Information Goods," *Management science* (50:12), pp 1660 -1673.

Tschorsch, F., and Scheuermann, B. (2016). "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Communications Surveys & Tutorials* (18:3), pp 2084-2123.

Wang, Q., Li, R., Wang, Q. and Chen, S., 2021. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. *arXiv preprint arXiv:2105.07447.*

White, B., Mahanti, A., and Passi, K. (2022). "Characterizing the Opensea Nft Marketplace," in: *Companion Proceedings of the Web Conference 2022*. Lyon, France: ACM, pp. 1 - 9.

Yoder, M. (2022). "An "Opensea" of Infringement: The Intellectual Property Implications of Nfts," *The University of Cincinnati Intellectual Property and Computer Law Journal* (6:2), pp 1 - 14.