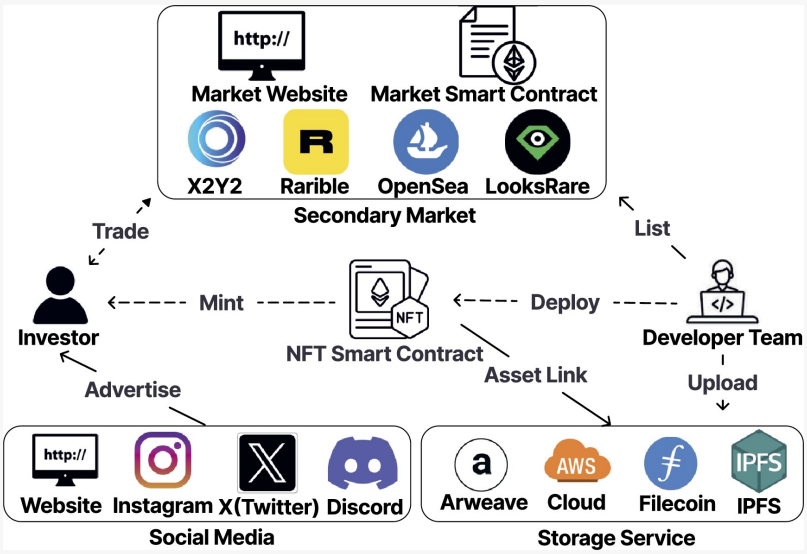
Mapping the minefield: first comprehensive security review of NFTs reveals widespread vulnerabilities

GA, UNITED STATES, July 19, 2025 /EINPresswire.com/ -- Non-Fungible Tokens (NFTs) have captivated the digital world with their unique ability to certify ownership of art, collectibles, and assets. But as the market surged to $69 billion, it also became a target-rich environment for hackers and fraudsters. In the first comprehensive review of its kind, researchers mapped 176 real-world NFT security incidents, classifying them into 12 threat categories and uncovering critical vulnerabilities across platforms and protocols. Their findings not only expose the hidden cracks in the NFT ecosystem but also offer a structured roadmap of defense strategies to make digital ownership more secure and trustworthy.



Non-Fungible Token (NFT) life cycle. It shows the various stages of an NFT and the people taking part. The dashed lines stand for actions recorded on the blockchain, and the solid lines represent off-chain activities not recorded on the chain.

Non-Fungible Tokens (NFTs) have transformed digital ownership by enabling the trade of unique assets through blockchain technology. From art and music to virtual real estate, these tokens have become central to the Web3 economy. Yet, this rapid innovation has outpaced security measures, leaving users vulnerable to sophisticated scams, technical exploits, and project failures. As NFTs grow in popularity and financial value, the consequences of security breaches have become increasingly severe. Due to these concerns, there is a critical need to systematically study the full scope of NFT security risks and create practical defenses against emerging threats.

In a new study published on June 25, 2025, in Blockchain: Research and Applications, researchers from Huazhong University of Science and Technology and Peking University unveil the first systematization of knowledge (SoK) on NFT security. By analyzing 248 security reports and 35

academic publications, the team identified and classified 176 NFT-related security incidents. Their work culminates in a multilayered NFT security reference framework that pinpoints the most common vulnerabilities, assesses detection challenges, and proposes a clear path forward for safeguarding the Web3 ecosystem.

The researchers constructed a three-tier security model encompassing the contract layer, market layer, and auxiliary service layer. Within this framework, they uncovered 12 core types of threats—including smart contract bugs like reentrancy flaws and access control lapses, market manipulations such as wash trading and rug pulls, and infrastructure attacks like phishing, fake interfaces, and website exploits. These findings are grounded in real incidents, including high-profile cases where attackers stole millions by exploiting minting functions or deceived users through counterfeit tokens tied to celebrity names.

The team also developed practical detection tools, such as transaction trace analysis for identifying reentrancy loops and symbolic execution to test logic vulnerabilities in minting functions. Alarmingly, they found that many real-world incidents—especially those involving phishing and front-end manipulation—remain underexplored in academic research. Their open-source dataset and security taxonomy now provide a foundational reference for future research, policy guidance, and secure development practices.

"Despite the explosive growth of NFTs, the community has lacked a comprehensive understanding of where and how these systems fail," said Dr. Haoyu Wang, senior author of the study. "Our work bridges this knowledge gap by not only exposing the root causes of major attacks but also offering developers and researchers the tools to detect and prevent them. This is a call to action—for academia and industry alike—to take NFT security seriously."

This pioneering research lays the groundwork for a more secure and resilient NFT ecosystem. Developers can now reference the proposed framework to preemptively address common vulnerabilities in smart contracts and marketplaces. Investors and collectors gain a better understanding of the warning signs associated with fraudulent projects. Perhaps most importantly, the study advocates for greater collaboration between cybersecurity researchers and blockchain practitioners to stay ahead of evolving threats. As NFTs continue to expand into finance, gaming, and identity, securing their foundations is essential to sustain innovation and build long-term public trust.

References
DOI
10.1016/j.bcra.2024.100268

Original Source URL
https://doi.org/10.1016/j.bcra.2024.100268

Funding information

This work was partly supported by the Knowledge Innovation Program of Wuhan-Basic Research, Key R&D Program of Hubei Province (Nos. 2023BAB017 and 2023BAB079), and HUSTCSE-Hongxin Joint Research Center for Network Security.

Lucy Wang
BioDesign Research
email us here