Scams, Frauds, and Crimes in the Nonfungible Token Market

Nir Kshetri, University of North Carolina at Greensboro

This article delves into scams, frauds, and deceits in the nonfungible token (NFT) market. It also proposes a typology of cyberattacks and other malicious behaviors in the NFT space.

The nonfungible token (NFT) market is growing rapidly. According to Lithuania-based data acquisition and analysis company DappRadar, which tracks decentralized applications across multiple blockchains, the NFT market exceeded US$23 billion in 2021 compared to less than US$100 million in 2020.[1] The U.S. multinational investment bank and financial services company Morgan Stanley estimates that the NFT market could reach US$240 billion in 2030.[2] This rapid growth in the NFT market has offered a wide variety of opportunities for scammers, fraudsters, and cybercriminals. The targets of such acts are creators and owners as well as consumers and buyers of NFTs. Investors in NFT projects have also been defrauded. Some perpetrators use techniques such as hacking and malware that are intended to gain unlawful access to victims' digital wallets that store NFTs and other cryptoassets. Others rely on novel but simple social engineering scams to convince victims to invest in fake schemes involving NFTs and to divulge sensitive information that can be used to breach cryptoaccounts.

Instances of other abusive practices such as insider trading have also been reported. In September 2021, the world's largest NFT marketplace, OpenSea, admitted that its product head was engaged in an insider trading scam. The scheme involved buying an NFT before it was advertised. When buyers' interest in the NFT increased, the asset would be sold at a higher price.[3] In one trade, a digital artwork was bought for US$822 and sold for US$4,000.[4] In this article, I discuss how NFTs are vulnerable to breaches, bugs, and attacks as well as other types of scams, frauds, and deceits. The article delves into cyberattacks and other malicious behaviors in the NFT space.

Digital Object Identifier 10.1109/MC.2022.3144763
Date of current version: 8 April 2022

0018-9162/22©2022IEEE

EDITOR **NIR KSHETRI**
University of North Carolina at Greensboro;
nbkshetr@uncg.edu

CYBERATTACKS AND OTHER MALICIOUS BEHAVIORS IN THE NFT SPACE

Cryptoassets, such as cryptocurrencies and NFTs, are vulnerable to cyberattacks at various levels. First, NFTs face risks related to the platform on which smart contracts run.[5] That is, the blockchain behind the NFTs themselves could be vulnerable to hacking. For instance, Ethereum was hacked in 2016 by exploiting vulnerabilities in the code of the decentralized autonomous organization (DAO). Note that the DAO was launched by a group of Ethereum developers, who are run through smart contracts and do not need centralized management and the direct control of self-interested institutions. At the next level, exchanges that facilitate the trading of NFTs (for example, OpenSea) have their own vulnerabilities. Finally, cybercriminals can hack wallets that are used to store NFTs.

Cyberattacks targeting NFTs mainly include actions against NFT exchanges and wallets. While NFTs are based on blockchain, exchanges and marketplaces such as OpenSea and Rarible, function in a centralized manner.[6] Thus, they cannot seize the benefits of decentralized technologies, such as peer review systems to identify and fix bugs. Consequently, they are vulnerable to breaches, bugs, and attacks. In September 2021, a bug in the OpenSea token market led to the disappearance of 42 NFTs that were valued at more than US$100,000.[7]

There are two types of wallets: hot ones (for example, accounts in an exchange/website-based wallets) and cold ones (for instance, those based on hardware or paper). NFTs that are stored in hot wallets are under the control of the wallet provider. For instance, custom protocols are used for accounts in cryptoexchanges, which are often based on a nonblockchain system.[8] The majority of attacks involving NFTs have been carried out against hot wallets.

Social engineering, which involves emotional appeals, such as fear, pity, and excitement, to victimize targets, has been a major modus operandi of most NFT fraudsters. Those parties establish interpersonal relationships and create a feeling of trust and commitment to achieve their goals. Social engineering tricks are used to gain access to victims' private keys to accounts associated with NFTs. In other cases, victims may be lured to click malicious links and download files containing malware.

In addition to cybercrimes, many other unlawful and malicious behaviors occur in the NFT space. Perpetrators are taking advantage of the relative newness of the NFT market and potential victims' lack of understanding of such assets. Other key challenges include underdeveloped regulations around cryptoasset intellectual property rights, copyright theft, unauthorized replication of NFT artwork, and the creation of phony NFT artwork.[5] For instance, scammers are creating and selling NFTs without the knowledge and consent of the owners of the assets that the NFTs represent.

Some NFT platforms have facilitated fraudulent practices by allowing transactions without proper due process and verification. Twinci, which describes itself as the first NFT social marketplace, permits anyone to open an account and start creating and collecting NFTs. A user can connect cryptocurrency wallets such as Metamask and imToken, and automatically set up a profile for them. Note, too, that wallets such as imToken do not require email addresses or any other personal information to set up an account. Once a user connects on Twinci, he or she can upload an image of an artwork. Twinci mints a token of the image, and the NFT is ready to go to the marketplace. Twinci accountholders can name their price in a chosen cryptocurrency.

SCAMS, FRAUDS, AND CRIMES INVOLVING NFTs: A TYPOLOGY

Table 1 presents a typology of cyberattacks and other malicious behaviors in the NFT space. The vertical axis represents fraudsters' modi operandi. The horizontal axis shows the targets of the schemes. In this section, we discuss the nature of the crimes in each cell.

Cell 1

As mentioned, cybercriminals increasingly target digital wallets of NFT owners. In June 2021, an NFT artist, Fvckrender, reported that he was tricked into opening a file containing a virus delivered to his social media account,[9] which enabled a criminal to access his digital wallets. He reported that the hacker stole 40,000 Axie Infinity tokens valued at US$4 million within minutes.[10] In a similar incident, in December 2021, an art curator and NFT collector reported the theft of 16 NFT tokens in a phishing attack. NFTs worth about US$2.2 million were stolen from the collector's hot wallet.[11]

Cell 2

As noted, NFT platforms face protocol risks such as hacking. Israeli cybersecurity company Check Point reported that it found vulnerabilities in OpenSea that could have enabled cybercriminals to sell malicious NFTs or trojanized digital art. Check Point researchers said that a security flaw in OpenSea made it possible for hackers to offer a malware-infected image file as an NFT. For instance, a user could be lured with a free NFT. When he or she opened the NFT file, a series of malicious pop-ups pretending to be from OpenSea would deploy. One of them would request the user to connect his or her digital wallet. When the user did so, the hackers would steal funds. OpenSea patched the flaw when it was brought to the company's attention.[12]

Another category of scams involves giveaways and airdrops, in which

fraudsters lure victims by offering free NFTs. In such a scheme, a fake account sends a message to users on social media, such as Twitter, telling them that they have won an NFT. Users are given a link to a fake website, which asks them to connect their digital wallet and enter their seed phrase.[13] The criminals then steal NFTs and digital currencies and tokens in the wallet.[14]

Cell 3

Some scammers use fake customer service pages to trick NFT owners into divulging sensitive information. When creative producer and director Jeff Nicholas was trying to get help for a royalty issue from OpenSea in August 2021, a group of criminals masquerading as company employees scammed him. They invited Nicholas into a channel of the voice over Internet Protocol instant messaging and digital distribution platform Discord, called *OpenSea Support Server*. After hours of interaction, they convinced him to share his screen. When he did, they took a picture of the QR code synced to his private key, or seed phrase, which enabled them to gain full access to his cryptoassets. They stole 150 ether (ETH) valued at about US$480,000.[15]

Fraudsters also take advantage of the lack of clear regulations regarding the ownership of an NFT versus the ownership of the physical or digital object represented by the NFT.[5] A distinct category of NFT scam involves creating and selling NFTs of works by high-profile artists without their knowledge and permission. Serbian artist Milos Rajkovic, who created video loops in which human faces and landscapes transform in strange ways (http://sholim.com/biography.html), was not involved with NFTs. In July 2021, he found that 122 of his works were for sale on OpenSea. While the first fakes were removed, another account posted the same works. Fraudsters exploit NFTs because many artists and collectors do not know about crypto. This makes the market an attractive target.[16] To cite another example, a scammer listed the Chinese artist Qing Han's (known as Qinni) popular artwork *Bird Cage* on Twinci. The platform deleted the NFT and banned the account when the fraud was reported. However, other Twinci accounts had five listings connected to NFTs of Qing's work. Some were listed for as much 500 TWIN (Twinci's cryptocoin) (1 TWIN = US$0.54 on 25 November 2021).[17]

Scammers are also reported to be creating and selling NFTs in the metaverse that falsely appear to be created by luxury brands. This has raised questions around ownership and legality. For instance, there is no clear answer to whether sales of branded digital items are legal if the brand did not participate in creating the products. In the metaverse and gaming platform Roblox, brands such as Gucci, Stella McCartney, and Nike have sold digital items. Users can also buy items that appear to be related to Burberry, Chanel, Prada, Dior, and Louis Vuitton despite the fact that these brands may not have been involved.[18] Finally, scammers are said to approach artists to deceive them into paying money and cryptocurrencies, such as ETH, to have NFTs made from their work. The fraudsters then run off with the money.[19]

Cell 4

NFT investment scams have also proliferated. One example is the popular NFT project Evolved Apes, which is described on OpenSea as "a collection of 10,000 unique NFTs trapped inside a lawless land."[27] Scammers took 798 ETH from the project's funds in multiple transfers. The funds were derived from the initial public sale of NFTs and commissions on the secondary market and meant for project-related expenses.[20] More than 4,000 NFTs in the Evolved Apes offering were sold in a week.[21] The artist who created the images was not paid. A social media competition was launched to create buzz. The winners did not receive the promised NFT prizes.[20] Cash giveaways were not delivered, and expenses for activities such as marketing and developing game and rarity tools,

TABLE 1. A typology of NFT scams.

Victim/target ⇨ Main element of the victimization strategy	Creators/owners of NFTs or the actual assets that NFTs represent	Consumers/buyers of NFTs or investors in NFT projects
Technology attacks, such as malware and hacking (mostly in combination with social engineering)	Cell 1 • Attacks targeting digital wallets of NFT creators/owners	Cell 2 • Exploiting security flaws in NFT platforms • Giveaway scams
Purely social engineering and other nontechnological attacks	Cell 3 • Creating fake NFT customer service pages to lure NFT creators/owners • Creating and selling NFTs without the knowledge and consent of the owner of the actual assets that NFTs represent • Tricking artists into paying to mint NFTs of their assets	Cell 4 • Investment scams • Tricking consumers into buying fake NFTs

The U.S. multinational investment bank and financial services company Morgan Stanley estimates that the NFT market could reach US$240 billion in 2030.

which are used by brands and creators to list NFT projects for a fee,[22] were not paid. Scammers also trick consumers into buying fake NFTs. They copy social media accounts of reputable companies and create fake pages that closely resemble the originals. Using the accounts, they sell bogus NFTs.[13]

PROTECTING AGAINST NFT SCAMS

Creators and owners of NFTs, owners of assets that are potentially attractive for creating high-value NFTs, and consumers, buyers, and investors need to be aware of a wide variety of crimes and scams taking place in NFT marketplaces and exercise security precautions. Owners of NFTs and assets that can be minted into NFTs must be vigilant and take measures to ensure that their assets are not misused. Consumers should understand that buying an NFT is different from buying things on e-commerce websites. There is little recourse for victims of NFT scams. There are often no refunds and few protections.

In addition, for Ethereum-based NFTs, volatility and gas fees could increase the costs to execute smart contracts.[23] There are also gas fees to transfer NFTs from marketplaces into personal cryptocurrency wallets. For example, in September 2021, *Time* magazine announced the sale of NFTs that consisted of 4,676 tokens tied to digital artwork. Each token was priced at 0.1 ETH (around US$310 based on the price then of ETH). All tokens were immediately sold, which clogged the Ethereum blockchain network. The fees also increased drastically. Buyers spent about four times as much on transaction fees as they did on the NFTs.[24]

It is also critical to understand NFT functions such as the storage of content and metadata. In most cases, an NFT is only a smart contract. Content and metadata are stored separately mainly because their files could be too large to hold on the Ethereum blockchain. Thus, while a contract may exist, the data can disappear. NFT markets such as OpenSea, Rarible, Foundation, and Nifty Gateway do not store images. They display only a media file linked with a code on the blockchain. If the media file is deleted from the actual source or the uniform resource locator to that source gets changed or breaks, a buyer may not be able to access an NFT from his or her digital wallet. For instance, online digital art NFT auction platform Nifty Gateway stores data with Cloudinary, a software-as-a-service company providing cloud-based image and video management. If Cloudinary shuts down, NFTs sold by Nifty Gateway may disappear.

Some argue that storing an asset as an interplanetary file system hash is better. The hash acts as an immutable fingerprint. Even in this case, a file can become unavailable if the only node storing it is disconnected from the network.[25] An Australian artist and programmer found that most of the images associated with NFTs were hosted in web 2.0 storage, which may lead to the "404: File not found" error, which means that a page does not exist.[26] An NFT can also be removed at the source if a platform's terms of service, such as those related to copyrights, are violated.[28]

In light of the proliferation of NFT-related investment scams, it is important to undertake due diligence of investment schemes. For instance, investors can use the Discord platform to understand the community behind an NFT and get a feel for the project. They should interact with other members and follow topics of conversation. It is important to ask the creators questions about the project's technical aspects. A lack of substance in the discussion can raise a red flag. If the creators have a presence on Discord and respond with details, the project is more likely to be genuine. People associated with fake projects may try to create distractions. It is also important to check if a project creator has an inflated social media following with a high number of fake Twitter followers. For instance, Followeraudit.com (https://www.followeraudit.com/?ref=alternativeassets.club) can be used to track the number of active, inactive, and fake followers of a project.

NFTs have provided a number of avenues for criminals, and thus there is a wide range of fraudulent acts in the NFT market. While some scams require technical skills, such as malware and hacking, only social engineering is sufficient to victimize targets in other schemes. The potential problem of storage failure is also an important issue that needs NFT buyers' attention. Likewise, transaction fees may increase the amount buyers need to pay to get their NFTs. Because of the lack of a clear regulatory framework around the ownership of an NFT versus the physical or digital object being represented, some scammers are also creating and selling NFTs without the knowledge or permission of the owners.

REFERENCE

1. P. Herrera, "Dapp industry report," DappRadar, Dec. 17, 2021. https://dappradar.com/blog/2021-dapp-industry-report
2. I. Lee, "Budweiser is getting in on the NFT craze with its 'Key to the Budverse' line of ethereum-based collectibles," Markets Insider, Nov. 29, 2021. https://markets.businessinsider.com/news/currencies/budweiser-budverse-nft-1936-gold-rare-core-token-collection-beer-2021-11
3. A. Gupta, "OpenSea bans insider trading after employee defrauds buyers," Jumpstart, Sep. 20, 2021. https://www.jumpstartmag.com/opensea-bans-insider-trading-after-employee-defrauds-buyers/
4. A. Herena, "NFT trader OpenSea bans insider trading after employee rakes in profit," *The Guardian*, Sep. 16, 2021. [Online]. Available: https://www.theguardian.com/technology/2021/sep/16/nft-trader-opensea-bans-insider-trading-after-employee-rakes-in-profit
5. M. Fox, "The NFT market is now worth more than $7 billion, but legal issues facing the nascent sector could hinder its growth, JPMorgan says," Markets Insider, Nov. 19, 2021. https://markets.businessinsider.com/news/currencies/nft

-market-worth-7-billion-legal-issues-could-hinder-growth-2021-11
6. L. Keller, "Does content moderation on platforms like OpenSea amount to censorship?" Forkast, Dec. 17, 2021. https://forkast.news/does-opensea-censor-nft-content/
7. "$100,000 worth of NFTs disappear forever, thanks to OpenSea bug," Investing, Sep. 09, 2021. https://www.investing.com/news/cryptocurrency-news/100000-worth-of-nfts-disappear-forever-thanks-to-opensea-bug-2611477
8. I. Novikov, "The three layers of cryptocurrency security," *Forbes*, May 3, 2018. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2018/05/03/the-three-layers-of-cryptocurrency-security/?sh=12e0ec3e29aa
9. K. Crow, "NFT art the latest target for online fraudsters," *Financial News*, Aug. 26, 2021. [Online]. Available: https://www.fnlondon.com/articles/nft-art-the-latest-target-for-fraudsters-20210826
10. S. Millare, "Four tips for NFT artists to protect themselves from hacking and online theft," BitPinas, Jul. 2, 2021. https://bitpinas.com/feature/four-tips-for-nft-artists-to-protect-themselves-from-hacking-and-online-theft/
11. V. Chawla, "Bored Ape NFT collector loses $2.2M in phishing scam," Crypto Briefing, Dec. 31, 2021. https://cryptobriefing.com/bored-ape-nft-collector-loses-2-2m-in-phishing-scam/
12. L. Ropek, "Gullible OpenSea users were vulnerable to 'malicious NFT' attacks, researchers say," Gizmodo, Mar. 28, 2021. https://gizmodo.com/gullible-opensea-users-were-vulnerable-to-malicious-nft-1847850437
13. K. Rees, "The 5 biggest NFT scams and how to avoid them," MakeUseOf, Oct. 21, 2021. https://www.makeuseof.com/biggest-nft-scams-how-to-avoid/
14. L. Alex, "Evaluating NFTs: How to know whether an NFT project is legit," Cryptonews, Oct. 9, 2021. https://cryptonews.com/exclusives/evaluating-nfts-how-to-know-whether-an-nft-project-is-legit.htm
15. A. Wang, "The NFT scammers are here," The Verge, Sep. 21, 2021. https://www.theverge.com/22683766/nft-scams-theft-social-engineering-opensea-community-recovery
16. "Scammers turn their attention to NFTs as the crypto subsector sees multimillion dollar mania," Coin News, Aug. 27, 2021. https://thecoin.news/post/35827
17. J. Kwan, "An artist died. Then thieves made NFTs of her work," *Wired U.K.*, Jul. 28, 2021. [Online]. Available: https://www.wired.co.uk/article/nft-fraud-qinni-art
18. M. Mcdowell, "The 'Baby Birkin' NFT and the legal scrutiny on digital fashion," *Vogue Business*, Jun. 15, 2021. [Online]. Available: https://www.voguebusiness.com/technology/the-baby-birkin-nft-and-the-legal-scrutiny-on-digital-fashion
19. "Scammers target Sacramento artists through crypto currency: A first-hand account of going down the rabbit hole," *Sacramento News & Review*, Nov. 10, 2021. [Online]. Available: https://sacramento.newsreview.com/2021/08/20/scammers-target-sacramento-artists-through-crypto-currency-a-first-hand-account-of-going-down-the-rabbit-hole/
20. E. Gen, "Investors spent millions on 'evolved apes' NFTs. Then they got scammed," *Vice*, Oct. 5, 2021. [Online]. Available: https://www.vice.com/en/article/y3dyem/investors-spent-millions-on-evolved-apes-nfts-then-they-got-scammed
21. "NFT buyers scammed as 'creator' bails, who could possibly have seen this coming?" Kotaku, Oct. 5, 2021. https://kotaku.com/nft-buyers-scammed-as-creator-bails-who-could-possibly-1847806528
22. "Top 7 NFT tools to find the best NFTs," BeInCrypto, Nov. 1, 2021. https://beincrypto.com/learn/nft-tools/
23. L. Daryanani, "Everything you need to know about the 5 categories of risk associated with DeFi," AMBCrypto, May 13, 2021. https://ambcrypto.com/everything-you-need-to-know-about-the-5-categories-of-risk-associated-with-defi/
24. W. Gottsegen, "Time's NFT launch sends gas fees spiraling: Keith Grossman, the magazine's president, admits the rollout was 'not ideal,'" CoinDesk, Sep. 24, 2021. https://www.coindesk.com/business/2021/09/23/chaotic-time-magazine-nft-launch-sends-gas-fees-spiraling/
25. J. Benson, "Yes, Your NFTs Can Go Missing—Here's What You Can Do About It Most NFTs don't really permanently live on a blockchain. That's potentially a huge problem when it comes to storing them," Decrypt, Mar. 19, 2021. https://decrypt.co/62037/missing-or-stolen-nfts-how-to-protect
26. I. Walker, "Someone right-clicked every NFT in the heist of the century," Kotaku, Nov. 18, 2021. https://kotaku.com/someone-right-clicked-every-nft-in-the-heist-of-the-cen-1848084379
27. Unnamed Creator, "Evolved Apes Inc." OpenSea. https://opensea.io/collection/evolved-apes-inc (Accessed: Jan. 25, 2022).
28. R. Brahambhatt, "NFTs are mysterious disappearing, here's how." Interesting Engineering. https://interestingengineering.com/nfts-are-mysteriously-disappearing-heres-how (Accessed: Jan. 25, 2022).

NIR KSHETRI is the "Computing's Economics" column editor and a professor in the Bryan School of Business and Economics, University of North Carolina at Greensboro, Greensboro, North Carolina, 27412, USA. Contact him at nbkshetr@uncg.edu.