Cybercrime in the Crypto-Art Market – Types of Crimes Committed Against NFT’s Creators and Owners

Introduction

On the Internet, crimes against works of art have been present for a long time. It is either the sale of artifacts dug out of illegal archaeological sites or illicitly traded, forgeries of works of art sold in online auctions, or the exchange of information regarding criminal activity. However, new types of cybercrimes have emerged with the increasing popularity of cryptocurrency and pieces of art existing only as digital files. For the last three years, the art market has been dominated by non-fungible tokens (hereafter as: NFTs). A non-fungible token is a unique digital identifier recorded on a blockchain protected by a security key. In other words, it is a database containing information on a file and all its transactions, neither of which can be modified without leaving a trace. Tokens are financial instruments for selling digital files. NFTs became a phenomenon in the art market after a record-breaking sale of Mike ‘Beeple’ Winkelmann’s work ‘Everydays: The First 5000 Days’ at Christie’s auction in 2021. Since then, the NFT market (or crypto art market) has snowballed and now represents 5% of the art market worldwide. The opportunity for significant financial gain has caught the attention of cybercriminals, leading to rapid growth in the number of crimes committed against creators of NFTs and their owners.

1 Olivia Rybak-Karkosz, PhD — Faculty of Law and Administration at the University of Silesia in Katowice. Contact the author via the editor.
2 In other words, they are digital assets that are equivalents either of physical goods or other digital goods. Electronic source: https://www.politykabezpieczenstwa.pl/pl/a/tokenizacja-czy-to-jest-bezpieczne, accessed: 26.09.2023.
How to secure the authenticity of digital artworks

NFTs play a crucial role in the art market and might be the next step in the art authentication and provenance research revolution. Digital art, similar to ‘traditional’ plastic art, is prone to falsification. The higher the demand, the more forgeries appear, and frauds are committed, which creates problems with object attribution. In digital art, the creation of unauthorised reproductions is an additional problem. It is a typical issue with easily copied digital files, which has been known for years in the cinema and music industries. However, unlike with video and music files, the owner of the piece of digital art wants a guarantee of being this file’s sole owner, *i.e.*, to block the possibility of it being reproduced. However, it needs to be stressed that this does not mean this will be the only piece of the artwork, as it is possible to publish an edition of numbered pieces with each file numbered, similar to edition proof of prints. The owner of the digital work also wants assurance and evidence of attribution and authenticity.

There are a few methods to ensure the owner’s rights and the file’s authenticity. Firstly, there are Certificates of Authenticity, known in the ‘traditional’ art market. These are issued on paper or digitally, proving that the set file is the only authentic one, despite many other unauthorised copies. This solution, however, raises the question of which is more valuable – the piece of art (file) or the COA itself. As a result, the forgers sometimes add forged authenticity documents (expertise, collections stamps, etc.) to already forged objects. Another option for securing digital artwork is watermarks. They can be inserted either on the image or in the properties of a file. However, this solution is also far from satisfactory. The first type of watermark can be easily deleted in image editor software. The latter can be copied with the image itself, therefore, cannot be used as an authenticator.

These are the reasons why a blockchain is currently considered the best way to secure a digital file. The information chain placed in the NFT supports adding metadata, such as change of ownership, token rights, description, and image. It also represents the history of the object (which provides its provenance). The non-fungibility of the token proves the object’s authenticity – it cannot be destroyed, lost, or modified without a trace. Secure ownership on a blockchain makes it possible to minimise the risk of the copyright and intellectual property infringement that are typical for images of digitalised objects provided via open access. A token saved on a blockchain proves that its owner is also the owner of the

---


5 Such was the case with Keith Haring’s oil painting – the forger attempted to create a false print of it. He scanned its reproduction from the album with Harring’s works and printed it on good-quality paper. He then added a fake version of Harring’s signature, number of proofs, and forged a COA supposedly issued by a Spanish art expert. A comparative analysis revealed that Harring never used that type of signature and that the pixels could be seen on the image.
piece of artwork to which that token was dedicated and that both are authentic.\textsuperscript{6} Co więcej, łańcuch bloków ma być nie do podrobowienia, ponieważ według szacunków, do jego złamania potrzebna byłaby moc obliczeniowa równa połowie internetu\textsuperscript{7}. However, the NFT system’s most significant advantage, non-fungibility, might be its flaw. There are already NFTs considered forgeries or copyright or intellectual property infringement. And since it is impossible to provide any improvements and raise the security level, users’ satisfaction and trust in NFT decreases.\textsuperscript{8} Moreover, dynamic growth in the popularity of NFTs and the system’s complex form causes many legal problems, and countries’ legislations cannot respond as quickly with appropriate legal protections for investors.

**Copyright and Property Intellectual Right breaches**

A non-fungible token is a proof of ownership in the virtual world, but this does not necessarily mean it will be respected by countries’ jurisdictions in the ‘real’ world, which is a crucial problem in seeking protection due to copyright and/or intellectual property infringement. Minting\textsuperscript{9} an NFT does not require its creator to prove he or she holds the relevant copyright. This means such an NFT could be minted without the consent or even knowledge of the artwork’s author.\textsuperscript{10} There are already many examples of such infringements, which are still growing.\textsuperscript{11} As a result, digital creators and artists fail to identify and combat them. This was the issue for many of them; for example, Lois van Baarle and Shepard Fairey reported that their artworks were minted into NFTs without their consent and authorisation and uploaded to marketplaces such as OpenSea (the largest NFT marketplace) and Rarible. For some creators, the losses are enormous, and any attempt to block the sale might last a few weeks, such as with Aja Trier’s van Gogh-inspired images being minted into 86,000 NFTs without her knowledge. This was possible due to ‘lazy minting’, a technique that allows anyone to create and offer NFTs for sale without saving them on the blockchain. The seller bears the costs only after the

\textsuperscript{9} ‘It is one of the steps in creating an NFT. It is converting digital data into crypto collections or digital assets recorded on the blockchain. Because of this, the digital products or files will be stored in a distributed ledger or decentralised database and cannot be edited, modified, or deleted’. *Electronic source*: https://www.binance.com/pl/blog/all/mint-nft--co-to-znaczy-421499824684903997, *accessed*: 26.09.2023.
\textsuperscript{10} Mackenzie S, Berzina D, *op. cit.*, p. 535.
sale, risking the theft of unsecured tokens. OpenSea admitted that 80% of
NFTs forged or plagiarised were ‘lazy minted’.12

Other copyright infringements and frauds occur when perpetrators cre-
ate fake accounts using the original creators’ names, copy their digital
pieces, and upload them on other platforms. Then they mint the files into
NFTs and, posing as their creator, sell them as ‘original pieces’. Such
was the modus operandi of perpetrators connected with platform the-To-
enized Tweets, where it was possible to mint a random person’s tweet
into an NFT. Digital creators often upload reproductions of their artworks
as tweets and using Tokenized Tweets to fraudulently mint them into
NFTs is a copyright infringement.13

So, the question becomes how to secure the authenticity and owner-
ship of a digital file during the minting process. An NFT on a blockchain
becomes a valuable source of provenance, but it might be problematic
to prove who minted the NFT and if it was the piece’s rightful owner, or
rather, the owner of all rights to the set piece.14 The Terms of Service for
crypto platforms such as OpenSea may also obstruct legal protection pro-
ceedings. They do not collect data on most clients due to their policy as ‘a
“self-serve” gateway to a loosely regulated market’.15 This means to be a
manifestation of a utopian version of the ‘new Internet’ (Web 3.0) managed
by common users instead of giant corporations.16

An intellectual property (IP) service managed by artificial intelligence
is supposed to provide a solution. In the MarqVision software, bots will
analyse new offers uploaded on platforms once a week and report those
that might be forgeries. Another one, Protect, is image recognition soft-
ware that will inform its users of copyright infringement. Sniffl
esNFT uses
image recognition as well, plus when a case of copyright infringement is
confirmed, the software sends a request to block the image in question on
behalf of the creator.17 Some creators secure their interests by limiting the
rights of NFT buyers. The terms of the agreements state that tokenised
artworks can only be exhibited in online galleries, with the rest of the
creative and IP rights remaining with the artist.18

12 Jacobs H, The counterfeit NFT problem is only getting worse. Electronic source:
https://www.theverge.com/22905295/counterfeit-nft-artist-ripoffs-opensea-deviantart,

13 Munster B, People Are Stealing Art and Turning It Into NFTs. Electronic source:
https://www.vice.com/en/article/n7vxe7/people-are-stealing-art-and-turning-it-into-nfts,


15 Electronic source: https://www.nytimes.com/2022/06/06/technology/nft-opensea-

16 Yaffe-Bellany D, Thefts, Fraud and Lawsuits at the World’s Biggest NFT Market-
place. Electronic source: https://www.nytimes.com/2022/06/06/technology/nft-opensea-

17 Batycka D, Counterfeit NFTs are creating major problems for digital platforms –
but new tools to spot fakes are on the rise. Electronic source: https://www.theartnews-
paper.com/2022/04/01/how-counterfeit-create-problems-for-nft-platforms, accessed:
10.10.2022.

18 Wong J, NFTs explained: Coveted by Chamath, Vaynerchuk, Cuban, and regular
people, too; but what the heck are they? Electronic source: https://www.businessofbusi-
IP rights infringements are also often a result of a lack of legal protection or different interpretations of existing ones. The Hermitage announced it was taking legal action due to a misuse of the museum’s name and artworks in its collection, created as NFTs by Rammstein’s leading singer. He allegedly breached the terms of an agreement when, after making a music video in Hermitage space, he minted it into NFTs.\(^\text{19}\) In another case, a settlement was reached in a dispute between Miramax and Quentin Tarantino over minting NFTs to ‘Pulp Fiction’. The director created a series of tokens containing a secret message about the movie. He claimed to be the copyright owner of the script and, therefore, could mint the NFTs. Miramax, however, disagreed, pointing out that the director’s rights do not apply to the creation of NFTs based on a movie that is an IP of the studio.\(^\text{20}\)

**Forgeries of NFTs**

One prominent example of NFT forgery concerned Banksy. A user called Pest Supply\(^\text{21}\) uploaded NFTs similar to Banksy’s works to OpenSea and Rarible. Some resembled his famous series of prints, ‘I can’t believe you morons actually buy this shit’, and his paintings, ‘Crude Oils’. The NFTs reached a very high value instantly. However, Pest Control quickly denied Banksy’s involvement in the project.\(^\text{22}\)

Another issue with the authenticity of an NFT appears when it is minted from a piece of art with disputed attribution. The question is how to describe the NFT and what its value would be if the piece’s attribution is denied. The issue appeared when da Vinci’s ‘La Bella Principessa’ was minted into an NFT.\(^\text{23}\) Its creators described it as the ‘first token of a verified da Vinci piece’, adding several indicators that they believe confirm its attribution: minting with the drawing’s current owner’s approval and self-authentication of one of the creators, who is a former Sotheby’s Old Masters expert.\(^\text{24}\) Since both of these arguments are hardly scientific, maybe


\(^\text{21}\) The name is similar to Pest Control, the firm confirming the authenticity of Banky’s works.

\(^\text{22}\) Shaw A, Banksy-style NFTs have sold for $900,000—but are they the real deal and does it even matter? Electronic source: https://www.theartnewspaper.com/2021/02/22/banksy-style-nfts-have-sold-for-dollar900000but-are-they-the-real-deal-and-does-it-even-matter, accessed: 10.10.2022.


the authenticity of the NFT should instead be described as a confirmation of minting from a particular piece.

**Frauds and thefts of NFTs**

Fraud with the intent to steal an NFT is, next to copyright infringement, the most often reported crime. There are a few different ways of committing it, including by using a vulnerability or weakness in a system – this is how someone was able to fraudulently buy a token from the ‘Bored Ape’ series for a third of its price on OpenSea. When Nifty Gateway, one of the biggest NFT platforms, was hacked, NFTs were stolen and sold from users who were not using Two Factor Authentication. In the next step, funds from credit cards connected with the account were used to buy and sell another token. Luckily for the users, the thefts were quickly noted, and because the perpetrators used the same platform for the sale, it was possible to block it and recover the stolen goods.

NFTs are also stolen through the installation of malware. In June 2021, an attack was carried out that was aimed specifically at NFT creators, intending to steal cryptocurrency from their digital wallets. Perpetrators posing as an NFT creators contacted other artists via Twitter with a collaboration proposal. The victims installed software hidden in a .SCR file (Windows screensaver) containing malware that stole confidential user information.

Phishing attacks are nowadays one of the biggest threats on the Internet, and the level of this crime is increasing every year. At the beginning of 2022, OpenSea confirmed that 254 high-value tokens were stolen through a phishing attack on their platform. Perpetrators’ modus operandi is often to take control of artists’ and NFTs creators’ social media accounts to commit extortion. A link is posted on the hacked account that opens a page demanding a wallet connection to finalise a transfer and recover the NFT, but in reality, opening the wallet results in the theft of NFTs and other tokens. This happened, for example, to Mike ‘Beeple’ Winkelmann’s account and the Yuga Labs team, the creators behind the famous ‘Bore Ape Yacht Club’ project (the total amount of stolen NFTs is estimated at almost 3 million dollars).

---

25 One of the most expensive NFTs on the crypto-art market.
27 NFT transfer outside of the platform means it is lost since all transactions on the blockchain are irreversible.
Other types of frauds on the NFT crypto-art market are crimes known from stock exchanges, such as the ‘pump and dump’ and ‘rug pull’. In the first one, the financial instrument is manipulated by inflating the product’s price by publishing false information about the positive value of the product and selling it when it reaches the highest value. The latter is based on the artificial pumping of the value of the project, obtaining funds from potential investors, and then dumping it and returning worthless tokens to the victims. For example, the influencer Blue Kirby organised such a fraud in cyberspace in the ‘OFF BLUE’ project.

NFT owner – the weakest security link

NFT investors are prone to cybercrime as they often lack knowledge of cyber threats and the possible measures they can take to protect their digital assets. The owner of the NFT is often the weakest link in its security. This makes educational campaigns on cybersecurity of utmost importance. It is necessary for the most prominent platforms storing NFTs to improve the internal and external security of their users and collectors. Due to users’ criticism, OpenSea changed its policy on stolen tokens. The firm will require proof of a police report to confirm the user’s report of NFT theft. The platform believes this will prevent false statements of theft and disable stolen NFTs from being bought or sold using OpenSea’s services. However, it might be problematic in Poland since this is not legally considered theft, as described in Article 278 of the Polish Criminal Code of June 6, 1997. Accordingly, whoever takes someone else’s movable item with the purpose of appropriating it is subject to the penalty of deprivation of liberty for between 3 months and 5 years. Since tokens are digital files, qualifying them as movable items would be impossible. The criminal proceeding would be discontinued because this act would not fulfil the required criteria of a prohibited act. Depending on the modus operandi of the perpetrators, it would be qualified as either: gaining illegal access to information by breaching or bypassing computer protection (article 267 par. 1 of the P.C.C.); gaining unlawful access to a computer system (article 267 par. 2 of the P.C.C.); gaining unauthorised access to information (article 267 par. 3 of the P.C.C.); disrupting the operation of a computer system (article 269a of the P.C.C.); or as a computer fraud described in article 287 of the P.C.C. However, in these cases, the act that preceded the

35 Consolidated text, DzU, 2022, item 1138.
theft will be penalised, not the theft itself. What’s more, the transnational aspect of these crimes obstructs the efficient working of law enforcement, and their international cooperation is inadequate. Legal regulations are still in the initial stage of shaping, hence the difficulties in criminalising such acts. So far, the victims can only take civil action. Sometimes the users themselves are helpful. When art dealer Todd Kramer lost his valuable tokens due to theft, he asked for users’ help on Twitter to locate the NFTs and perpetrators. The information provided helped to retrieve some of the tokens.  

The main communication channel for NFT creators and their clients is Discord, which can be a helpful source of information and evidence.

Where an NFT is stored might also be risky and lead to theft. The simplest tool is a ‘custodial’ wallet. The owner, however, shares control over the wallet and assets with another party, so there is a risk of losing them if the set party is hacked or is dishonest and steals the assets.  

So, to minimise the risk of attack or malware installation, an NFT should be stored on a wallet disconnected from the network. Since it is an offline tool, the owner has to remember the security key to access it.

Conclusions

The blockchain contains information regarding only this chain, such as the order of transactions and metadata linking an NFT with an artwork. Only this information is solid and non-fungible. The authenticity of an artwork is a separate issue. So, the question is whether the token’s creator was the artwork’s copyright owner. This cannot be implied because the NFT is stored on a blockchain. It requires a legal regulation that would allow the verification of the NFT and grant the protection of creators and buyers. Crimes against NFTs are not exclusive to thefts or data extortion directed to single victims. They are used to finance crimes on a large scale, such as money laundering, drug smuggling, and human trafficking.

As a final remark, another problem connected with NFTs and cyber art is worth noting. The carbon footprint emitted by participants in the art market was high even before the rise in popularity of NFTs. Transfers of artworks and other activities have already increased environmental pollution. But minting NFTs, maintaining the platforms, and other activities requires a significant amount of energy. To compare, one of the biggest NFT art platforms, ‘Ethereum’, used as much energy as Qatar, and its carbon footprint was equal to Sudan’s. A single online transaction used the same amount of energy as a single household in 2.8 days, and the carbon

---


footprint was equivalent to 6.5 hours of watching videos on YouTube\textsuperscript{38}. With the increasing social awareness of protecting the natural environment, decreasing energy consumption and the carbon footprint should be a priority,\textsuperscript{39} especially now with the growth of the NFT market and the rise in minting and owning NFTs.

**References**


\textsuperscript{39} In September 2022, Ethereum announced that it finalised the work on software allowing the switch from the Proof-of-Work mining cryptocurrency method, which required powerful computer power, to Proof-of-Stake, which will work on lower power. In the platform’s opinion, it will reduce energy consumption by 99.998% and carbon footprint by 99.982%. Jhala, K, Ethereum, the NFT market’s blockchain of choice, cuts its CO2 output by 99%. *Electronic source*: https://www.theartnewspaper.com/2022/09/15/nft-blockchain-ethereum-cuts-climate-impact, accessed: 10.10.2022.


29. Shaw A, Banksy-style NFTs have sold for $900,000—but are they the real deal and does it even matter? Electronic source: https://www.theartnewspaper.com/2021/02/22/banksy-style-nfts-have-sold-for-dollar900000but-are-they-the-real-deal-and-does-it-even-matter.


DOI: 10.5604/01.3001.0053.9747
http://dx.doi.org/ 10.5604/01.3001.0053.9747

Keywords: NFT, non-fungible token, cybercrime, crypto-art market, NFT theft

Summary: In this paper, the author aims to analyse the types of crimes committed in cyberspace against creators and owners of NFTs. Non-fungible tokens have been favoured by the art world (also known as the crypto-art market) for a few years now. They attract numerous digital art creators and cryptocurrency investors. The tokens are recorded in a blockchain and are used to certify authenticity and ownership, which had made the art world particularly interested in this solution. However, as practice shows, the NFT system isn’t flawless, and cybercriminals exploit its flaws. Using methods known from typical cybercrimes, they modify their modus operandi according to the crypto-art market practice. In this paper, the author describes examples of breaches of copyright and intellectual property law, as well as examples of the forgery of NFTs. Other crimes, such as fraud and theft of NFTs, are also described, including bypassing security systems, phishing, installing malware.
**Palabras clave:** NFT, token no fungible, ciberdelincuencia, mercado de criptoarte, robo de un NFT

**Resumen:** El objetivo de este documento es analizar las formas de delitos cometidos en el ciberespacio contra los creadores y propietarios de los NFTs. Los tokens no fungibles gozan de gran popularidad en el mercado del arte (también conocido como mercado del criptoarte) desde hace varios años y han atraído a un gran número de creadores de arte digital e inversores en criptodivisas. La colocación del token en la blockchain, que está protegida por una clave de seguridad, proporciona la confirmación de la autenticidad y la propiedad del archivo relacionado con él. Esta es la razón por la que el mundo del arte, siempre en busca de nuevos métodos para confirmar la autenticidad y la procedencia, está especialmente interesado en esta cuestión. Sin embargo, como demuestra el ejemplo de los NFT, este sistema no carece de defectos, que los delincuentes que operan en el espacio digital aprovechan con éxito. Mediante unos métodos conocidos de la ciberdelincuencia típica, modifican su modus operandi para adaptarlo a las especificidades del mercado del criptoarte. El artículo describe ejemplos de violaciones de la legislación sobre derechos de autor y propiedad intelectual contra creadores de los NFTs, así como ejemplos de falsificación de los mismos. También se analizan las formas de cometer fraudes y robos de los NFTs (p. ej. burlando las medidas de seguridad, ataques de phishing, o instalación de programas maliciosos).