NFTs: a failure of their counterfeit-proof and trusty objective?

ELIAS NEOCLEOUS & Co LLC

Non-Fungible Tokens (NFTs) have gained significant popularity and success in the last several years, generating billions of dollars in revenue due to their growing notoriety.

The NFT success story is one based on the element of uniqueness. Each NFT has its own combination of tokenID[1] and an address code of a smart contract[2] which are stored on a blockchain[3] like Ethereum, EOS, Bitcoin Cash to name a few. The combination of both codes is unique, making the NFT "non-fungible", thereby adding value to it. Once the NFT is created, the digital asset can be offered for sale to buyers who can purchase it on platforms such as OpenSea, Mintable, and Rarible, using cryptocurrencies.

CHALLENGES AND RISKS ASSOCIATED WITH NFTS

Lack of regulation

One of the issues that arises in the sale of an NFT is the way in which the NFT market operates. Whoever inserts an NFT on the Blockchain is presumed to be the author and can sell it, thus collecting profits that in fact are owed to the real digital copyright holder. Further, the minting of an NFT is available to anyone with access to the blockchain network, but with NFTs still largely unregulated, this creates a paradise for scammers and counterfeiters.

Scams and Intellectual Property infringements

To date, there are still repeated thefts of NFTs, copyright infringements, as well as intricate rug pull scams involving such tokens, where scammers and hackers exploit the blurriness surrounding the topic for profit. Rug pull scams are essentially based on "pumping up" a new project (either by two individuals buying and rebuying the same NFT, adding value to it and creating the sentiment of demand; or by other similar means) in order to collect money and then disappear with the profits, leaving the purchasers of NFTs with worthless investments. In other words, instead of being trustworthy, NFTs are sadly becoming an easier way to scam people.

1. https://walt.id/white-paper/nfts-for-identity#:~:text=Token%20IDs%20are%20used%20to,key%20infrastructure)%20and%20to%20metadata.
2. https://www.realvision.com/blog/smart-contracts-for-nfts#:~:text=Therefore%2C%20a%20smart%20contract%20NFT,and%20creators%20millions%20of%20dollars.
3. https://www.investopedia.com/terms/b/blockchain.asp

LOSS OF MILLIONS OF DOLLARS IN NFT RELATED SCAMS

A number of different scams have duped crypto art collectors over the last few years, either via social media, Ethereum transactions, or by other electronic means, leading to large losses of money.

Bored Ape Yacht Club

The hack of the Bored Ape Yacht Club Instagram account saw followers tricked into clicking on a post, enabling the attacker to steal the assets held in the wallets of the victims, amounting to approximately $3 million of benefit to the hacker[4].

The case of emoji NFTs

Another recent incident saw an unknown user put up 8000 NFTs for sale which supposedly depicted 3D versions of popular artworks. The series quickly sold out but instead of receiving the artwork they paid for, horrified buyers instead received a collection of emojis. The scammer disappeared with the profits[5].

"Metabirkins" NFTs not protected speech

A recent case of the "Metabirkins" NFTs involved the globally renowned brand Hermès, whereby a creator designed NFTs[6] representing the infamous Hermès Birkin bags, without the brand's consent. Hermès went on to sue the creator where it was found that the Metabirkins NFTs violated the trademark of the luxury brand. The jury awarded Hermès $133,000, stating also that the NFTs were not First Amendment protected speech.

Fake Bansky NFT

Bansky is an elusive graffiti artist whose identity remains unknown, but whose works have appeared all over the world, and sold for millions at different auctions. Bansky's official website was thought to have been hacked when an advertisement appeared on the site, redirecting the user to OpenSea where an auction of an NFT called "Great Redistribution of the Climate Change Disaster" was taking place. The auction was soon revealed to be a scam and, due to public outcry, the scammer issued a full refund to the buyer of the fake NFT[7].

4. https://www.theguardian.com/technology/2022/apr/26/bored-ape-yacht-club-nft-hack-theft-art-simian-oblivion
5. https://nftevening.com/explained-the-iconics-rugpull-that-left-holders-with-emoji-nfts/
6. https://www.theverge.com/2023/2/8/23591000/metabirkins-nft-mason-rothschild-hermes-birkin-bag-lawsuit-outcome
7. https://www.bbc.com/news/technology-58399338

Teddy bears and NFTs

More recently in France, some 770 individuals spent a combined total of around €1.5 million on NFTs of teddy bears which were supposed to make them co-producers in an animated film called Plush, featuring comedian Kev Adams. Buyers were also led to believe that they would make 6 to 7 times their investment in a 24 month period. French newspaper Mediapart has however reported that the Plush NFTs no longer exist on the project's website and that its Twitter account has been inactive since September 2022[8], much to the disappointment of the investors.

WEB 3'S ANONYMITY AND THE PROBLEM OF IMPUNITY

NFT scams and copyright infringements bring to light many other issues, in particular, how to hold scammers and copyright infringers accountable in the sphere of Web3?

NFTs operate on Web3 which is based on privacy, anonymity, and pseudonymity. It's where users can participate incognito in the blockchain, under a pseudonym, with the ability to use obscure Ethereum name service addresses.

The Web3 network is built on a peer-to-peer, decentralized system, meaning users don't require intermediaries, enabling communication and transactions between third parties. Unlike Web2 networks which are typically centralized, with legislation in place to enforce the disclosure of necessary information to identify and convict perpetrators of cybercrimes; the Web3 network makes it considerably more difficult if not nearly impossible to identify and locate the bad actors, and to hold them accountable for their actions.

"In Web2 the big influencers benefit from everything they do know about us. In Web3, the big (anonymous) influencers benefit from everything we do not know about them." — NFT Ethics (@NFTethics), January 17, 2022

Conclusion

To conclude, in the current framework of legislation and technology, anonymity and impunity seem to be guaranteed in the crypto space. For years, comparative private international law specialists have tried to find a uniform solution to the questions of jurisdiction and applicable law in the presence of a tort situation generated in a digital environment.

The problem in this case is that the infringing crypto asset is everywhere at once, which is equivalent to essentially nowhere in private international law. The traditional rules of conflict of jurisdictions offer several solutions but none of them seem to be truly adequate. As anonymity in financial transactions is already being used to further all manner of criminal activity, the need for the adoption of legislation to mitigate the risks incurred through unregulated NFT transactions and Web3 usage is thus becoming critical.

Author: Iosifina Koutsonikola
Lawyer Trainee
Elias Neocleous & Co LLC

8. -https://www.mediapart.fr/journal/france/230423nounours-et-cryptomonnaies-dubai-le-mauvais-film-de-kev-adams