 ***DOI:*** *https://doij.org/10.10000/IJLMH.115343*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

**[ISSN 2581-5369]**

**Volume 6 | Issue 4**

**2023**

# Unveiling the Cyber Crime Shadows: Exploring the Dark Side of NFTs and the Logan Paul Cryptozoo Scam

AMISHA MITTAL[1] AND SHUBHI AGRAWAL[2]

## ABSTRACT

*In the vast digital landscape, Non-Fungible Tokens (NFTs) have emerged as unique assets representing ownership of digital content, revolutionizing the world of art, music, and collectibles. However, the dazzling rise of NFTs has also paved the way for cybercriminals seeking to exploit vulnerabilities in this new and booming market. This article delves into the intriguing world of NFT-related cybercrime, using the infamous Logan Paul CryptoZoo scam as a case study.*

*Drawing upon the Logan Paul incident, the article explores the various financial crimes that plague the NFT space. The article also presents an in-depth analysis of the financial crime theories applicable to NFTs. These frameworks help unravel the motivations and modus operandi of cybercriminals, explaining how they exploit the unique characteristics of NFTs and the anonymity of the digital realm. Moreover, this case study underscores the pressing need for regulations in the NFT and cryptocurrency ecosystems, as well as the importance of education and due diligence for prospective NFT investors. It highlights the risks associated with celebrity endorsements and the imperative of cautious evaluation, regardless of the involvement of famous personalities. The article concludes by emphasizing the multifaceted implications of financial crimes on victims, extending beyond monetary losses to reputational damage and emotional distress.*

*As the NFT market continues to thrive, it becomes paramount to address the growing cybercrime risks and develop effective strategies for detection, prevention, and mitigation. By shedding light on the Logan Paul CryptoZoo scam, this article serves as a wake-up call for the industry, urging stakeholders to protect the interests of NFT market participants and foster a secure and trustworthy digital marketplace and to do so, it also makes brief mention to various crypto regulatory regulations across the world.*

***Keywords:*** *Non-fungible tokens, financial crime, cyber-crime, in-ecosystem tokens, game tokens, cryptocurrency scams.*

[1] Author is a student at Jindal Global Law School, Haryana, India.
[2] Author is a student at Jindal Global Law School, Haryana, India.

 [ISSN 2581-5369]

# I. INTRODUCTION

Non-fungible tokens (hereinafter referred as NFTs) have gained significant attention in recent years as a new form of digital asset that can represent ownership of unique digital content, such as artwork, music, and collectibles.[3]

The emergence of NFTs has opened up new opportunities for creators, investors, and collectors in the digital market. In the current era, these digital assets are being bought, sold, and traded for millions of dollars. However, with the rapid growth of NFTs, there are also increasing concerns about the potential risks and vulnerabilities associated with them especially when it comes to the discourse of their vulnerability to cybercrime.

The purpose of this piece is to examine the growing cybercrime risk associated with NFTs, using the alleged Logan Paul CryptoZoo scam as a premise. The Logan Paul scam, which occurred in 2021 in the jurisdiction of the United States, involved the popular YouTuber Logan Paul and his team promoting and selling a game called 'CryptoZoo'[4] through which his fans and investors could earn by investing in the NFTs and cryptocurrency associated to the game. The entire project turned out to be a scam and resulted in financial losses to the victims' raising questions about the security and legitimacy of NFT transactions. By analysing this case, this piece aims to provide insights into the types of financial crimes associated with NFTs, the theoretical premise of NFT scams, and the detection, analysis, and recommendations for addressing NFT-related cybercrime risks.

## (A) Definition of NFTs and their Emergence in the Digital Market

In essence, NFTs are "unique digital assets" that are imprinted on the Blockchain, a digital ledger or register that keeps track of all the pertinent information and transactions pertaining to a particular digital asset. NFTs are linked to real-world tangible and intangible items like artwork, music albums, memes, photographs, in-game items, real estate, any cloth, or furniture, etc. Anything that can be represented digitally can be turned into an NFT.[5] They essentially demonstrate the ownership and reliability of the said asset and facilitate its trade on digital marketplaces through cryptocurrencies. Since data entered on a blockchain cannot be changed once it is there, NFTs are claimed to have a higher level of validity. It is crucial to remember

[3] Aleksandra Jordanoska, The exciting world of NFTs: a consideration of regulatory and financial crime risks, *Butterworths Journal of International Banking and Financial Law*, Vol. *10*, pp. 716

[4] Andrew R. Chow, How Logan Paul's Crypto Empire Fell Apart, TIME (February 2, 2023), https://time.com/6252093/logan-paul-cryptozoo-liquid-marketplace/.

[5] **ANDRES GUADAMUZ,** NON-FUNGIBLE TOKENS (NFTS) AND COPYRIGHT, WIPO (DECEMBER, 2021), HTTPS://WWW.WIPO.INT/WIPO_MAGAZINE/EN/2021/04/ARTICLE_0007.HTML.

that the NFT only serves to digitally represent the underlying work or asset and is not the asset itself.[6]

These tokens are non-fungible; that is, they are distinct and cannot be exchanged. Each NFT has a unique identification because they are each coded in such a way that their algorithm has distinctive data pertaining to their creation and transaction history that sets them apart from other similar NFTs in existence and makes them non-interchangeable. This contrasts with an asset like money or cryptocurrency, which are homogeneous and can be exchanged. One asset can nevertheless be linked to many NFTs; in this case, the uniqueness and non-fungibility of the resulting NFT are unaffected. Demand and supply, just like with any other good or service, determine the price of NFTs.

### (B) Growing Popularity and Adoption of NFTs and the Importance of Studying the associated Cybercrime Risk

NFTs have gained significant popularity and adoption in recent years, with notable sales and endorsements from celebrities, artists, musicians, and athletes. NFT marketplaces, such as Open Sea, Rarible, and Foundation, have emerged as platforms for buying, selling, and trading NFTs. NFTs have been used to tokenize various digital assets, including digital art, music, real estate, virtual goods, and collectibles. NFTs can represent anything and everything on the face of this earth, to a real estate building to a meme or a GIF. The unique characteristics of NFTs, such as scarcity, provenance, and transferability, have been touted as advantages that offer value and investment opportunities in the digital realm.

However, this rapid growth has also attracted cybercriminals who exploit vulnerabilities in the NFT ecosystem. The digital nature of NFTs, the lack of regulations for this substantially new and evolving Form of asset, and the anonymity of transactions present opportunities for cybercriminals to perpetrate various financial crimes. Victims of NFT related cybercrimes may suffer financial losses, reputational damage, and emotional distress. Therefore, it is crucial to study and understand the cybercrime risks associated with NFTs to develop effective detection, prevention, and mitigation strategies to protect the interests of NFT and crypto market participants.[7]

[6] Supra note 2.
[7] Al Shamsi, M., Smith, D. and Gleason, K., Space transition and the vulnerabilities of the NFT market to financial crime, Journal of Financial Crime.

## II. FINANCIAL CRIMES ASSOCIATED WITH NFTS

NFTs are vulnerable to several types of financial crimes due to the unique characteristics of digital assets and the decentralized nature of blockchain technology. From the creation of fake NFTs and pump-and-dump schemes to insider trading and money laundering, cybercriminals have found ingenious ways to deceive and defraud unsuspecting investors. The scam orchestrated by Logan Paul and his team reveals the dark underbelly of the NFT market, shedding light on the consequences faced by victims and the broader community.[8]

Cybercriminals may create and promote fake NFTs, misrepresenting them as genuine and valuable digital assets, and tricking buyers into purchasing them. NFT scams may involve impersonating legitimate artists, celebrities, or influencers, creating fake NFT marketplaces, or using phishing techniques to steal private keys or wallet credentials from NFT holders. In order to do this, cybercriminals may use techniques like celebrity endorsement, social media manipulation and phishing to gain trust of the victims and leverage off that to conduct cyber financial crime.[9]

Another way to conduct such a crime may include schemes like Pump and Dump schemes wherein such criminals artificially inflate prices of NFTs through bulk buys, manipulation, creating a fake hype around them in order to coerce the buyers into buying worthless NFTs for a significant price. Manipulation of the market is also done through insider trading by using non-public information to trade NFTs and gain unfair advantages over other market participants.[10]

Further, NFTs may also be used for money laundering, where cybercriminals may transfer illicit funds through NFT transactions to disguise the origin and ownership of the funds.

## III. THE LOGAN PAUL CASE

The Logan Paul CryptoZoo scam serves as a relevant case study to analyse the financial crime aspects of NFT related scams. Logan Paul, a popular YouTuber, and social media influencer announced the launch of his NFT game called 'CryptoZoo' in April 2021. He marketed CryptoZoo as a game that involved limited-edition collection of digital animal-themed cards

[8] Dupuis, Daniel and Gleason, Kimberly C., Old Frauds with a New Sauce: Digital Coins and Behavioral Paradigms, SSRN Electronic Journal.
[9] SEC Statement Urging Caution Around Celebrity Backed ICOs, U.S. SECURITIES AND EXCHANGE COMMISSION (November 1, 2017), https://www.sec.gov/news/public-statement/statement-potentially-unlawful-promotion-icos.
[10] Supra note 7.

 [ISSN 2581-5369]

with unique attributes and values.

This game that Logan Paul described as one of his biggest projects involved buying a crypto token called "Zoo" using in-game currency in the game. With Zoo coins, players could buy NFTs in the form of eggs, which could be hatched to become animals. These animals could then be bred to create hybrid animals, such as a Gorilla and a Kitten breeding to create a "Gorkitten." The rarity of the bred animal decided the rarity of the NFTs which determined the daily yield of Zoo tokens that the animal earned, creating a passive income for players. Players could choose to burn their animal income to earn back the Zoo tokens they earned, which could then be reinvested in buying more eggs or cash out their income.

Logan Paul claimed that what set his game apart from other similar games which worked on the play-to-earn model was that the animals in his game were just not randomly generated assets but instead feature hand-made art created by 10 different artists he had consulted with. The game players and investors were promised 'handmade unique art' in the form of animals they could trade with the in game crypto currency and NFTs. The game had gained support from famous influencers worldwide, making it an enticing prospect for players interested in the play-to-earn model.

However, the scam unfolded when it was revealed that the CryptoZoo NFTs were a sham, with the project lacking the promised features and functionality. The handmade animal art that was promised as one of the USPs of the game was actually found to be nothing but edited stock photos of different animals. By the time information regarding the game had been revealed, several people had already spent millions on buying 'Zoo' coins and game NFTs in the hope to receive great passive income on the final hatch day of their 'eggs.' Before the actual launch of the game itself, during pre-sale, the game had garnered more than 2.5 million Dollars of investment. The Logan Paul team themselves engaged in huge pump and dump schemes, insider trading and celebrity endorsement to create the hype around his game for increased investment and price manipulation. However, it was later found out that, the game had never finished being programmed because Logan Paul had not been paying his head developers and the money invested by investors was nothing but a waste due to the internal politics and sabotaging in the whole team which lead to the abandonment of the project by Logan Paul after appropriating millions of investment money.[11]

Earlier this year, in February 2023, a class action suit[12] against Logan Paul was also filled in

[11] Supra note 3.

[12] Ciaran Lyons, Logan Paul and CryptoZoo hit with lawsuit as investors take action, COIN TELEGRAPH

 [ISSN 2581-5369]

the United States District Court for his role in Crypto Zoo along with Jeff Levin, Crypto king, Eddie Ibanez and more people on his team against the mis representation and other financial crimes committed by them against numerous people who entrusted their money in investing in the game. The NFTs and eggs that several buyers bought from the game were actually worthless to them, leaving them with utmost disappointment and huge financial losses.

The case study of the Logan Paul CryptoZoo scam showcases various financial crime aspects, including fraudulent misrepresentation, as Logan Paul misled buyers with false promises and misrepresented the value of the NFTs. Additionally, the scam involved theft, as buyers paid substantial amounts for worthless NFTs that lacked the promised attributes. The case study also highlights the impact of the scam on the victims and the broader NFT community, with many buyers losing money and trust in the NFT market. This scam serves as a cautionary example of the risks and challenges associated with financial crimes in the NFT space.

Unfortunately, Logan Paul's involvement of failed cryptocurrency projects is not limited to CryptoZoo. Paul has spent a significant amount of effort over the past two years in creating a larger-than-life crypto empire by founding numerous enterprises and encouraging his millions of followers to put money into the upcoming cryptocurrency trend. However, all his projects showcase a consistent pattern that thrives on irresponsible behaviour and negligence. He advocates for one or another crypto project in a chronological order and then when things go haywire, he abandons the project to erase his name from it. For instance, blockchain evidence in the case of the meme coin Dink Doink reveals that Paul greatly benefited from a token he advocated to his followers while concealing his own involvement in the business to earn huge money through this misrepresentation.[13]

## IV. ASSOCIATED FINANCIAL CRIME THEORIES

The theoretical frameworks[14] and concepts relevant to NFTs and financial crimes can include various crime theories, such as rational choice theory, differential association theory, utility theory, space transition theory and fraud theory.

Differential Association theory suggests that criminal behaviour is often learnt through one's close circle of friends through interaction with people who posses' criminal traits. In the Logan Paul Case itself, the financial crime was systematically organized through a set of people working collaboratively which could explain their association to this theory. The crime

(February 3, 2023), https://cointelegraph.com/news/logan-paul-and-cryptozoo-sued-in-class-action-lawsuit.
[13] Supra note 3.
[14] Petter Gottschalk, Theories of financial crime, Journal of Financial Crime.

committed also involved a balance of weighs to ascertain the utility through this act and the certainty of not getting caught for it. This shows the interplay of utility theory in the action.

Rational choice theory suggests that individuals engage in criminal activities after weighing the risks and rewards. The rational choice theory posits that individuals engage in criminal behaviour when the benefits outweigh the risks and costs of the crime. In the case of the Logan Paul CryptoZoo scam, the cybercriminals made a rational choice to perpetrate the scam by leveraging Logan Paul's popularity and the hype around NFTs to lure unsuspecting buyers into purchasing fake NFTs, with the expectation of financial gain.

Another theory that could be related to the Logan Paul CryptoZoo scam is the Fraud Triangle Theory. This theory suggests that fraud occurs when three elements are present: opportunity, incentive, and rationalization. In the case of the Logan Paul CryptoZoo scam, the cybercriminals had the opportunity to create and promote fake game to earn investment money, they had the incentive of financial gain through the sale of fake NFTs, and they rationalized their actions by exploiting the lack of regulations and the anonymity of NFT and crypto transactions and by using techniques like avoiding presale of tokens to manipulate the market so that it does not catch attention from securities regulatory board and instead opt for trade in liquidity pool when a token is released without official announcement and investors bulk buy the token in cheap prices to manipulate the market and earn huge profits. Such techniques are in practice nothing but misappropriating lacunas in law.[15]

Further, it is an established notion that, people with a very naturalistic behaviour tend to display their criminal or socially deferred behaviour when they transition from a physical space to a virtual space. This is called the space transition theory[16] of cyber-crime and it explains why some people might commit cyber-crime when they physically have a very law-abiding behaviour. It is essentially because online setting offers dissociative anonymity, an escape from the physical reality of the world, it offers people to hide behind an online entity and creates an image of being more likely to evade any law.

Applying these theoretical frameworks to the emergence of NFT related scams, it can be argued that the motivation for cybercriminals is influenced by the potential high financial gains and the perceived low risks associated with NFTs. They may observe and imitate successful scams,

[15] TIANHAO CHEN, BLOCKCHAIN AND ACCOUNTING FRAUD PREVENTION: A CASE STUDY ON LUCKIN COFFEE, ATLANTIS PRESS (APRIL 29, 2022), HTTPS://WWW.ATLANTIS-PRESS.COM/PROCEEDINGS/ICSSED-22/125973833.
[16] Al Shamsi, M., Smith, D. and Gleason, K., Space transition and the vulnerabilities of the NFT market to financial crime, Journal of Financial Crime.

 [ISSN 2581-5369]

targeting vulnerable victims who lack knowledge or experience in the NFT ecosystem.

## V. WHY IS A SCAM LIKE THE LOGAN PAUL CRYPTOZOO SCAM RELEVANT IN FINANCIAL CRIME STUDIES

The Logan Paul Crypto NFT scam serves as a relevant case to highlight the growing cybercrime risk associated with NFTs for several reasons.

Celebrity endorsements and the associated trust with it fall under a major part of why cybercriminals are able to benefit off this trust to engage in different financial crimes. This scam highlights the vulnerability of NFT investors to celebrity endorsements, and the need for cautious evaluation of investments regardless of celebrity involvement.[17]

Further, the case study also underscores the lack of regulations in the cyber and crypto ecosystem, which provides opportunities for cybercriminals to exploit vulnerabilities and perpetrate financial crimes. This demonstrates the necessity of regulatory frameworks to safeguard the interests of NFT market participants and stop cybercrime by utilizing the technically advanced cybercrime techniques utilized in such frauds. The case study also emphasizes the large monetary losses suffered by scam victims, who may also suffer reputational harm and emotional suffering and may not be able to take legal action due to the absence of relevant regulations in the NFT and cryptocurrency ecosystems in many jurisdictions. This demonstrates the need for enhanced education among prospective NFT investors regarding the dangers of cybercrime and the need of due diligence before any investment.

Any financial crime does not only have a financial implication, but it is also often associated with various emotional and health distress which severely affect the quality of life on a victim.[18]

## VI. THE WAY AHEAD

Financial crimes using NFTs, and cryptocurrencies need to be identified and prevented, and this calls for a multi-layered strategy that includes technological solutions, regulatory measures, and market participant knowledge.

One way in which NFT marketplaces, games and other platforms could detect suspicious activities is through installation of enhanced KYC and AML Procedures and Real Time

[17] Sam Gilbert, Crypto, web3, and the Metaverse, BENNETT INSTITUTE OF PUBLIC POLICY CAMBRIDGE (March 2022), https://www.bennettinstitute.cam.ac.uk/publications/crypto-web3-metaverse/.
[18] Jacobs, J. A., Review of Other People's Money. A Study in the Social Psychology of Embezzlement, by D. R. Cressey, The Journal of Criminal Law, Criminology, and Police Science, Vol. *45*, Issue.4, pp. 464–465.

 [ISSN 2581-5369]

Monitoring. Robust Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures could be installed to verify the identities of buyers and sellers, and to detect suspicious transactions that may be indicative of financial crimes.[19] Further, in order to detect patterns of suspected behaviour Real-time monitoring and analysis of transactions and market activities and the use of AI (Artificial Intelligence) Algorithms could be bought to practice detecting activities like sudden price spikes, unusual trading volumes, and irregularities in transaction patterns, which may indicate pump-and-dump tactics or insider trading. Security measures like multi-factor authentication, encryption, and transaction monitoring should also be adopted by such platforms to safeguard against criminals and unauthorized access.[20]

Further, knowledge and prevention through due diligence serves as the best practice one could do at an individual level. Along with that, regulatory bodies should also prioritize education and awareness campaigns and reports to educate potential investors about the risks associated with cybercrime, including tactics like social media campaigning, celebrity endorsements and tricks like highlighting the urgency of investment through providing a time constrained deadline. Investors should be encouraged to conduct thorough **due diligence** before investing in NFTs and to report any suspicious activities. Any financial crime cannot be limited without proper regulations to prohibit it. While there exists a framework to limit cyber and financial crimes, with technologies increasing by the day, it is important for policy considerations and changes to be implemented in order to increase the scope of these regulatory compliances. Regulatory bodies must establish clear guidelines for NFT and crypto markets which may include registration requirements, disclosure obligations, and penalties for non-compliance along with providing a mechanism for legal recourse for victims of financial crimes.

At present, there exists a major need for legislations and amendments that address the growing needs of globalised economies and innovative technologies like NFTs that bring about a pool of threats. The class action suit that is filed against Logan Paul is being argues currently by the petitioners under the Texas's Deceptive Trade Practices Act[21] and other contractual principles that are essentially covered under law of contracts. While such laws could address the concerns surrounding innovative technologies like NFTs, clear legislations and rules are the need of the hour. The Logan Paul scam happened in the US. The US does not have a comprehensive

[19] Regner, Ferdinand; Urbach, Nils; and Schweizer, André, NFTs in Practice – Non-Fungible Tokens as Core Component of a Blockchain-based Event Ticketing Application, ICIS 2019 PROCEEDINGS (2019), https://core.ac.uk/reader/301384284.
[20] Supra note 2.
[21] **The Deceptive Trade Practices Act,** BUSINESS AND COMMERCE CODE (USA)

framework that deals with in-ecosystem tokens like zoo-tokens in the CryptoZoo game The European Union has been primarily active with respect to addressing innovative technologies and the challenges posed by them by proposing new legislations by the day. The Digital Markets Act[22] and the Market in Crypto-Assets Regulation (MiCA)[23] that were instituted recently are just some examples of it. Certainly! The US Congress could enact a new legislation to regulate cryptocurrencies, similar to the European Union (EU) regulations implemented in 2022. The EU's regulatory framework, known as the Market in Crypto-Assets Regulation (MiCA), aims to address the risks associated with crypto-assets and ensure their value and integrity. MiCA recognizes the benefits of crypto assets for capital raising, innovation, and economic growth, but also acknowledges the lack of regulation in many markets. To tackle these issues, MiCA establishes comprehensive rules for crypto assets, requiring issuers, traders, and exchanges to be authorized and adhere to disclosure requirements. It also categorizes crypto assets into different types and excludes certain unique assets like digital art from regulation. In contrast, the current crypto-asset legislation in the United States, such as the Responsible Financial Innovation Act (RFIA)[24], falls short of the EU's approach. While the RFIA aims to create a regulatory framework for digital assets, it lacks comprehensive coverage for non-fungible tokens (NFTs) and in-ecosystem tokens. This means that there are no new enforcement powers, consumer protections, or requirements for these types of tokens.

To improve the US legislation, it may be a better approach that Congress adopts a similar approach to the EU by defining NFTs narrowly and considering their primary use and issuer's intent when determining regulatory requirements. This would ensure that potential risks associated with NFTs, and in-ecosystem tokens are addressed adequately.

## VII. Conclusion

Significant potential for creators and collectors has resulted from the development of NFTs, but it has also raised the possibility of financial crime. The case of the Logan Paul CryptoZoo fraud demonstrates the elements of financial crime associated with NFT-related scams as well as the difficulties in identifying and pursuing such crimes. Understanding the risks of financial crime linked with NFTs is essential in order to take preventative actions to safeguard investors, customers, and the credibility of the NFT sector as a whole.

*****

[22] Digital Markets Act, 2022 (European Union).
[23] Market in Crypto-Assets Regulation (MiCA), 2023 (European Union)
[24] Lummis-Gillibrand Responsible Financial Innovation Act, 2022 (USA)

 [ISSN 2581-5369]