Assessing non-fungible tokens (NFTs): A resource guide for fraud practitioners

Commissioned by ACFE UK Chapter

Dr Janice Goldstraw-White
Prof Martin Gill

June 2023

Perpetuity Research & Consultancy International (PRCI) Ltd
11a High Street · Tunbridge Wells · TN1 1UL · United Kingdom
www.perpetuityresearch.com
prci@perpetuityresearch.com
Tel: +44 (0)1892 538690

Copyright

Acknowledgements

We would like to thank the ACFE UK Chapter for commissioning this piece of research. In particular, Tim Harvey for acting as our advisor and providing helpful insights whenever called upon.

Furthermore, we extend our thanks to the experts in the fields of blockchain, cryptocurrencies and NFTs whom we had the privilege of consulting throughout our research. Additionally, we are indebted to the anonymous contributors from the ACFE UK Chapter, who gave their time to participating in our survey and providing valuable insights. Although their identities must remain undisclosed by necessity and agreement, we acknowledge and appreciate their significant contribution in this context.

Finally, thanks to our colleague Charlotte Howell for help with the data analysis.

Table of Contents

Foreword

The ACFE UK Chapter is delighted to endorse this small-scale study, focusing on an area that is gaining significant importance but has received limited research attention thus far. By engaging Janice and Martin to undertake this, the ACFE UK Chapter aims to contribute to the existing knowledge base on fraud risks in the cryptoasset market. This study provides valuable insights into the specific risks and vulnerabilities associated with NFTs, helping to inform economic crime professionals, organisations, and policymakers on how to better mitigate and address these risks.

The increasing interest in the cryptoasset market is undeniable; however, the adequacy of regulations to keep up with these advancements is not as evident. Consequently, it is vital for counter fraud professionals to be aware of the potential risks that this emerging phenomenon poses. Through this assessment our aim is to improve understanding of this subject and contribute to raising awareness about the potential risks associated with NFTs.

Timothy Harvey
ACFE UK Chapter

June 2023

Executive Summary

Overview

The purpose of this report is to enhance the anti-fraud community's understanding of the benefits and risks associated with Non Fungible Tokens (NFTs). This small-scale project consisted of two key approaches:

1. A literature review to explore the main concerns and risks associated with NFTs, cryptoassets, and the blockchain.
2. Interviews with professionals who have expertise in working with NFTs and other cryptoassets, either in a general capacity or specifically focused on fraud prevention.

Key Findings

- NFTs have been in existence for over 10 years but have witnessed a massive surge in popularity over the last couple of years.
- The sale of NFTs exceeded $25 billion in 2021 with predictions this figure could rise as high as $200 billion by 2030.
- Anything that can be stored digitally can be made into an NFT.
- To date, most NFTs relate to the art, collectibles or gaming markets.
- The most expensive NFT ever sold is "The Merge" which was bought for $91.8 million in December 2021.
- Most NFTs started out on the Ethereum blockchain but are now available on other blockchain platforms.
- NFTs offer a number of benefits, not least that they are a unique, permanent, immutable record on the blockchain that proves ownership.
- NFTs however also pose a number of issues and risks to both investors and society as a whole (such as usability, privacy concerns, environmental impact and legal issues).
- There are a multitude of reasons why people invest and collect NFTs including as a status symbol.
- New and old type frauds and scams have been associated with NFTs and they may help facilitate other crimes, like money laundering.
- The police are only just getting to grips with cryptocurrency and therefore, NFTs pose a new and additional challenge.
- Global regulation of NFTs is patchy and underdeveloped.

Section 1. Introduction

Aims and objectives

1.1 Non-fungible tokens (NFTs) are unique cryptographic tokens that reside on a blockchain representing a real-life or virtual asset. They cannot be duplicated; each NFT possesses an exclusive and irreplaceable identity (setting it apart from other tokens). Unlike cryptocurrencies, NFTs are distinct entities and cannot be interchangeably substituted. Utilising blockchain technology enhances their security, making them more difficult to hack, although not entirely immune to breaches.

1.2 Initially rooted in the concept of cryptocurrencies, NFTs have evolved into a market primarily focused on collectibles such as digital artwork, sports cards, personal memorabilia, and other rare items. However, their potential extends far beyond that as they have the capability to streamline processes, eliminate unnecessary intermediaries, whilst maintaining permanent records on the blockchain.

1.3 Despite their advantages, NFTs face some less publicised drawbacks such as those relating to their usability ; their governance; and regulatory concerns. Just like any emerging phenomenon, NFTs attract criminals, potentially leading to scams, frauds often facilitating further offending.

1.4 There is a real need to better understand the risks associated with the NFT market for both consumers and investors. Additionally, raising awareness among professionals in the fraud prevention and security sectors is crucial. Our survey conducted with ACFE UK members, albeit based on small numbers, at the start of this project indicated that the sector may lack a comprehensive understanding of the risks posed by NFTs, and showed a desire for more training on the subject. The lack of prior research encouraged this relatively small scale study to help inform the many knowledge gaps.

Benefits of this research

1.5 There are several benefits of this research, including:

- The rapid emergence of NFTs in our economy has occurred without sufficient regulation and oversight. This research has the potential to provide valuable information that can be used to develop a regulatory framework for NFTs.
- Limited guidance is currently available for individuals purchasing and investing in NFTs, particularly in the collectibles market where less financially experienced individuals may be involved. This research can contribute to the development of guidance and warnings regarding NFT investments.

- The creation, marketing and selling of NFTs renders them susceptible to both new and existing types of fraud, By shedding light on the types of fraud and scams perpetrated the research aims to generate insights to enhance fraud awareness and prevention efforts.

Structure of the report

1.6 Section 2: provides a foundation to the report tracing the historical evolution of NFTs. Section 3 discusses the common uses of NFTs while assessing their main characteristics and benefits and introduces the legal issues surrounding their use. Section 4 looks at the compelling reasons driving individuals to invest in NFTs, while also exploring the broader psychology of collecting. It investigates the specific circumstances that led to the sudden and significant surge of interest in NFTs in 2021. Section 5 reviews the crime recording process of NFT frauds. It moves on to discuss offender methodologies including real-life examples of scams and frauds committed. The role of NFTs as enablers of other criminal activities, particularly money laundering is discussed. Section 6 examines governance arrangements highlighting the inherent regulation challenges. Section reviews the evolving landscape of NFTs exploring potential use cases. The appendices contain essential supplementary information to support the findings of the report and include an overview of the research methodology; and also details of NFT frauds reported to Action Fraud.

Section 2. Background and history of NFTs

Introduction

2.1 NFTs have emerged as a ground-breaking innovation within the realm of digital assets, revolutionising the way we perceive ownership, authenticity, and value in the digital world. Unlike traditional cryptocurrencies such as Bitcoin or Ethereum, which are interchangeable and hold equal value, NFTs are unique and indivisible digital tokens that represent ownership of a specific item or piece of content. These items can range from digital art, music, videos, virtual real estate, collectibles, and even virtual goods in video games. With their potential to reshape industries and empower creators, NFTs have captured the attention of artists, investors, and enthusiasts worldwide, creating an industry that continues to evolve and push the boundaries of what is possible in the digital age.

2.2 NFTs have witnessed an astounding surge (see Table 1). In 2021 alone, total sales were estimated to have exceeded $25 billion (Howcroft, 2022), and this could rise as high as $200 billion dollars by 2030.[1] The reasons vary from a desire for buyers to own rare and exclusive digital collectibles, support favourite artists and creators, or even to speculate on potential future value appreciation.

Table 1 – Most expensive NFTs ever sold[2]

NFT	Cost
The Merge by Pak	$91.8 million
Everydays: The First 5000 Days by Beeple	$69.3 million
Clock by Pak	$52.7 million
Human One by Beeple	$28.9 million
CryptoPunk #5822	$11.7 million
CryptoPunk #7523	$10.5 million
TPunk #3442	$10.2 million
CryptoPunk #4156	$ 7.7 million
CryptoPunk #5577	$ 7.5 million
CryptoPunk #3100	$ 7.5 million
CryptoPunk #7804	$ 7.5 million

Key definitions

Cryptoassets

2.3 There is no single, widely agreed definition of a cryptoasset, but the UK Government defines them as “a digital representation of value, the

[1] https://news.bitcoin.com/nft-market-projected-to-reach-200-billion-in-2030/

[2] As at 14th April 2023 https://www.coindesk.com/learn/the-top-10-most-expensive-nfts-of-all-time/

ownership of which is cryptographically proven (using computer code)."[3] Cryptocurrency, specifically Bitcoin, was the first kind of cryptoasset and remains the best-known and predominant one. Unlike real life assets though, cryptoassets do not have an equivalent physical manifestation, with coins or tokens existing only notionally, and can be transferred, stored or traded electronically. Over time, the potential applications of cryptoassets have broadened and grown, incorporating new asset categories.

NFTs

2.4 Unlike cryptocurrencies, which are fungible and can be exchanged on a one-to-one basis, NFTs are unique and distinct and therefore cannot be exchanged on a like-for-like basis. The value of an NFT is derived from its scarcity, uniqueness, and demand from collectors and enthusiasts. NFTs can be bought, sold, and traded on various online marketplaces that specialize in the exchange of digital assets. Because they are created – or minted on a blockchain through a smart contract, they are impossible to change. They behave exactly as they are programmed through their smart contract (Gerard, 2021).

2.5 An NFT can be any digital asset that has utility attached, but to date they have mainly been used in the collectibles market. If something can be stored digitally then it can be made into an NFT including JPEGs, GIFs, tweets, videos, songs, video games and other collectible items. They are originals, not copies, with that authenticity attached to the digital token. When sold, ownership transfers to the buyer with their rights stipulated in the smart contract (Conti, 2022).

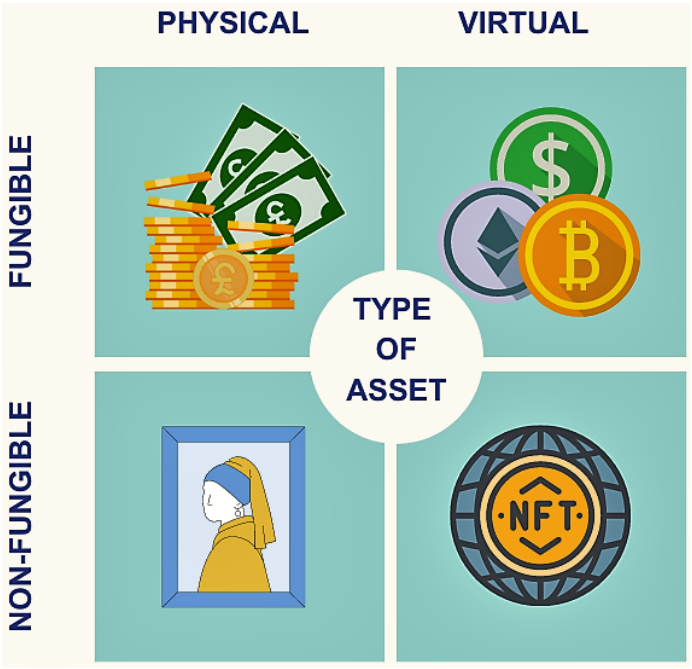
Fungibility and non-fungibility

2.6 In economic terms, fungibility denotes the ability of an asset to be seamlessly exchanged with another asset or item of equivalent value. In the context of cryptoassets, fungibility is expressed through a code script embedded in crypto tokens. This script ensures that each token is indistinguishable from others of the same type and carries the same value, allowing for effortless interchangeability. This characteristic of fungibility plays a crucial role in facilitating the smooth transfer and trade of cryptoassets on various blockchain networks.[4] Fungible assets are therefore divisible and interchangeable – for example when you buy an item at a supermarket, all things being equal you would not mind which specific item you choose from the shelf. Figure 1 demonstrates the different types of real life and digital assets that can be fungible or non-fungible.

[3] See Government Factsheet https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/fact-sheet-cryptoassets-technical

[4] https://cointelegraph.com/learn/fungible-vs-nonfungible-tokens-what-is-the-difference

Figure 1 – Asset classification



2.7 The most common example of a fungible asset is currency – whether crypto or fiat currency – one pound Sterling or one Bitcoin have the same value as another one pound Sterling or one Bitcoin. Such assets are divisible into small amounts and are non-unique (Rich, 2021). In contrast, non-fungible assets, such as NFTs are unique and cannot be divided or merged with another because of the digital signature assigned to each token on the blockchain (Voshmgir, 2018). They should be considered as a type or deed or title of ownership of a unique and irreplaceable item, such as a flight ticket, house, picture, or other one-of-a-kind asset. Table 2 highlights the key differences between fungible and non-fungible assets.

Table 2 – Fungible versus non-fungible assets

Fungible	Non-fungible
• Divisible • Non-unique • Interchangeable	• Indivisible • Unique • Irreplaceable

Tokens and standards

2.8 When NFTs were first created on the Ethereum blockchain, a set of standards were drawn up to legitimise the requirements attached to each unique token, whilst also allowing for critical variations such as value (Anderson, 2022: 45). Because NFTs were first created via the Ethereum blockchain, they set the standards, the most commonly used being ERC-721 and ERC-1155 (Musimih, 2022). ERC stands for Ethereum Request for Comment and starts life as an Ethereum Improvement Proposal (EIP) which is discussed and peer reviewed

before it may make its way into an official ERC (Elliptic, 2022). Standards are also usually numbered and can be freely transferred between EVM-compatible (Ethereum Virtual Machine) blockchains and execute smart contracts on Ethereum blockchains with a chain bridge enabled.

2.9 ERC-721 is a standard for representing ownership of non-fungible tokens. Each token is distinct, allows for the tracking of unique assets and has multiple optional extensions (Ali, 2023; Scharfman, 2023). Smart contracts underpinning NFTs must contain eight compulsory functions and two events to meet this standard (Ali, 2023). The ERC-1155 standard was approved six months after ERC-721 and improves performance by batching multiple non-fungible tokens into a single contract, thereby reducing transaction costs (Anderson, 2022: 45). This multi-token standard allows for any combination of fungible and non-fungible tokens to be managed in a single contract. ERC-1155 requires each token to have six functions that can be considered mandatory functions and four events (Ali, 2023). Other blockchains that are compatible with the Ethereum blockchain have their own standards, for example, Binance smart chain (BSC) has standards BEP-721 and BEP-1155; Stacks blockchain has SIP-009; and Tezos has FA-2.0, and each work differently depending on the technology used for each blockchain.

Blockchain

2.10 A blockchain is often described as a public distributed digital ledger that records various types of transactions on a decentralised network of computers operated by different parties in a continuous manner (Hughes et al, 2019; Li et al, 2018). As the name suggests, data is organised and stored in packages known as blocks, and the link between adjacent blocks is known as a chain (Twesige, 2015). These data blocks are immutable meaning they cannot be altered, just verified or added to, and as such blockchains are considered to be very secure. In addition, they are usually public so that transactions are transparent, therefore, in theory, can be viewed by anyone (Ali and Bagui, 2021).

2.11 Because distributed ledger technology is used, blockchains eliminate the need for a central organisation, such as a bank, to validate transactions and are therefore an attractive option for decentralised finance operations. In the past, a single person or organisation has had complete control over systems, including how data are stored and changed and this has facilitated fraud and errors. The technology is suitable for recording a wide range of operations, not just financial (Rehman et al, 2021).

Smart contracts

2.12 NFTs are unpinned by smart contracts and the metadata embedded in these clearly sates the terms and conditions of owning an NFT (Wood, 2014; Purtill, 2021). Put simply, a smart contract is a sales agreement on the blockchain – but also a software program that executes

automatically when a pre-defined set of requirements are fulfilled (Zheng et al, 2020). They are similar to traditional contracts and define the rules and penalties to an agreement. Because they are self-executing on the blockchain, automatically verifying that the terms of the contact have been met, human intervention is not required to approve or process transactions (Ellul and Revolidis, 2023).

2.13 Anything on a paper contract can now be recorded digitally on a smart contract and this is starting to happen with leases for house and land purchases. A recent Law Commission report[5] concluded that smart contracts are compatible with the existing principles of English law and are therefore capable of being legally binding. Benefits and limitations of smart contracts are detailed in Table 3.

Table 3 – Benefits and limitations of smart contracts

Benefits	Limitations
• Autonomy – no third party required • Transparent – immutable on blockchain • Cost – no intermediary • Fast – saves time on business processes • Application – wide range of uses in many sectors	• Difficult to change – almost impossible to update • Vague terms – difficult to handle • Scalability – can be slow transaction processing • Third parties – difficult to totally eliminate • Loopholes – hard to spot errors can be exploited

The history of NFTs

2.14 Although 2021 is often referred to as the year of the NFT, their origins can be traced back much earlier to 2012-13, with the introduction of "coloured coins" on the Bitcoin blockchain. These represented and managed various real-life assets (such as property, company shares, collectibles etc) with an added token to determine their use and make their ownership unique. The major flaw behind coloured coins was their inability to hold a fixed price and their limited functionality (Bamakan et al, 2022). This led to the creation of Counterparty, a platform built on the Bitcoin blockchain with an open-source protocol allowing anyone to engage in creating digital assets and exchanging them via a decentralised market. In 2015, the creators of the popular game Spells of Genesis began issuing in-game assets on the blockchain (Chen, 2021a).

2.15 In August 2016, Counterparty teamed up with the trading card game, Force of Will, a company with no previous cryptocurrency or blockchain presence, signalling an important development in this new type of technology. Memes started to be issued on the Bitcoin blockchain, the Pepe the Frog collection, known as Rare Pepes, was one of the most

[5] https://www.lawcom.gov.uk/project/smart-contracts/

well-known and attracted a large fan base. At the same time this new technology enabled artists to monetise their works (Steinwold, 2019).

2.16 In 2017, the Ethereum blockchain was increasingly being used to host artwork and collectibles and it was a popular choice because of its built-in scripting language. Matt Hall and John Watkinson, creators and owners of Larva Labs, generated a set of unique tokens on this blockchain with a project called CryptoPunks[6] featuring characters that were 100% unique and limited in number. This led to the creation of the Ethereum token ERC721, attracting further interest from artists, gamers and the collectibles market and leading to the release of CryptoKitties,[7] a blockchain-based virtual game enabling players to adopt, take care of, breed, and trade digital cats (Anderson, 2022).

2.17 Following these successes (with some people were making huge profits from trading virtual assets), NFT gaming and metaverse[8] interest exploded with Decentraland,[9] an online virtual world and also one of the first where users could buy virtual plots of land, build, collect items and undertake other real life activities within the game. The popularity of NFTs led to the creation of NFT marketplaces (see Table 4 for the most popular ones in 2023), such as Open Sea and SpareRare, with 100s of projects released on these from 2018. Soon others appeared on the scene and a significant addition was the formation of a company called Dapper Labs, who secured $15 million in funding from top investors as people realised the true power of NFTs (Steinwold, 2019).

Table 4 – Top NFT Marketplaces 2023[10]

Rank	Marketplace	Market Share
1	Blur	56.80%
2	OpenSea	36.70%
3	X2Y2	2.60%
4	Magic Eden	2.10%
5	LooksRare	1.00%
6	CryptoPunks	0.80%

2.18 Then a market explosion in NFTs in 2021 occurred for a number of reasons. One of the biggest factors was prestigious auction houses, such as Christie's and Sotheby's, started not only to take their auctions online, but also began selling NFT art. Christie's made headlines by selling Beeple's Everydays: the First 5000 Days NFT for a record-breaking $69 million. This landmark event created a ripple effect,

[6] https://www.larvalabs.com/cryptopunks
[7] https://www.cryptokitties.co/
[8] The metaverse is a hypothetical iteration of the Internet as a single, universal, and immersive virtual world that is facilitated by the use of virtual reality (VR) and augmented reality (AR) headsets (Mystakidis, 2022).
[9] https://decentraland.org/
[10] As at 2023 https://www.coingecko.com/research/publications/market-share-nft-marketplaces

prompting other blockchains beyond Ethereum, including Cardano, Solano, Tezos, and Flow, to actively engage with NFTs.

2.19 The pandemic played a part too. People found themselves in lockdown; many were bored; had a surplus of disposable income; and were accustomed to or already engrossed in online activities became engaged in "recreational investing" emerged. So much so it diverted funds away from traditional stocks and shares just as trust in conventional fiat currencies waned and cryptocurrencies were surging. Bitcoin and other digital currencies increased in price and NFTs were sought as an alternative. Additionally, the involvement of well-known celebrities promoting NFTs, in particular using them for their profile pictures, further fuelled curiosity and intrigue.

Section 3. Using NFTs – benefits, limitations and issues

Background

Despite the enormous potential NFTs can have on decentralised markets and future business opportunities, NFT technologies are still new (Wang et al, 2021). So far, their application has been predominantly observed in a handful of sectors, namely art, collectibles, and gaming markets (Nadini et al, 2021) (see Figure 2). It is worth exploring these.

Figure 2 – Current NFT uses

Current uses for NFTs

Artwork

3.1 The use of NFTs by artists has been the most publicised, and tokenised art can be anything from digital pictures, GIFs or short videos. In fact, the first ever NFT was posed at an art experiment in a hackathon portion of a New York-based conference in 2014, when artist Kevin McCoy registered a video clip as a monetised graphic and sold it to another hackathon partner for $4 USD (Ross et al, 2021). In the past, artists who have created digital artwork have faced a number of challenges –

proving authenticity, preventing copycat works and receiving royalties. Because NFT ownership is recorded on a blockchain and run via smart contracts, these issues can be overcome (Kietzmann et al, 2020).

3.2 For those NFTs that pay royalties there are some key benefits. The requirement is hard coded into the smart contract and dues are paid out automatically to the creator not only when they initially sell a piece of artwork, but whenever that artwork is sold on. Something that is frequently missed in the traditional artworld. There are benefits also for collectors. Unlike physical art, NFTs are easy to store and protect, and they are simple to transfer electronically between different platforms and devices (Kugler, 2021). NFTs have not only revolutionised the creation, purchase, and sale of art but have also transformed how it is perceived and exhibited. While certain art galleries continue to focus exclusively on traditional physical artworks, numerous others, including renowned establishments like the Uffizi, British Museum, Hermitage, MoMa, and Christie's, have embraced the changes (Valeonti et al, 2021)

Collectibles

3.3 NFT collectibles can be thought of as a crypto alternative to rare collectible cards, memes, tweets etc. and are particularly popular for sports (Fai, 2021); for example, those minted by the Bored Ape Yacht Club (BAYC); CryptoPunks; and NBA Top Shot.[11] As well as being collectible items, NFTs are often used as a digital avatar for a person's profile picture on social media sites, primarily on Twitter and some celebrities have paid very high prices for these digital assets.

Gaming/Virtual Reality

3.4 As there are estimated to be 3 billion gamers in the world,[12] the potential for harnessing NFT technology here is enormous. CryptoKitties was probably the first mainstream game created on an NFT platform and one of the added features of NFTs is extensibility or the ability to "breed", meaning that owners of two NFTs can create a new third entity from the original two. If those two are rare, then the ensuing third NFT will be even rarer and could possibly sold for an even higher price (Fowler and Pirker, 2021 Kugler, 2021).

3.5 Other uses for NFT in gaming include giving player access to certain games or levels, which may be exclusive, or they may be able to trade or sell this access through their NFTs with other players. One popular use of NFTs and games is the development of playing-to-earn (P2E) gaming models, especially in the metaverse, where users can play a game and earn rewards at the same time. Gamers can obtain two types of in-game assets either by collecting items with variable scarcity (such

[11] https://boredapeyachtclub.com/#/; https://www.larvalabs.com/cryptopunks; https://nbatopshot.com/

[12] https://earthweb.com/mobile-gaming-statistics/

as weapons or skins) or actually earning cryptocurrency or P2E (Vidal-Tomás, 2022). These games offer real value, ownership and incentives for gamers and instead of just accessing and using these assets in games, NFT gamers own these items (compared to previous ownership with remained with the game owner) and have the option to sell them for real money on NFT marketplaces (Muthe et al, 2020). Popular games incorporating NFT technology include Sandbox, Decentraland, and Axie Infinity.[13]

Tickets and exclusive membership

3.6 The use of NFT tickets can benefit both issuers and ticket holders. Secured on the blockchain, they are an immutable record providing details of attendance numbers and allowing the issuer to interact with the purchaser in a new and innovative way, both before and after the event. Ticket holders not only receive an immutable and often interactive digital asset that grants access to an event (real life or virtual), but also retain a permanent record of the experience which may also include exclusive access to other events only open to holders of similar NFT tickets (Wang et al, 2021).

3.7 A rising trend has emerged wherein NFTs are used to offer exclusive access to clubs or real-life events. This includes granting membership privileges to exclusive restaurants, clubs, or private meeting spaces through the utilisation of NFTs. (Elliptic, 2022). For example, the Flyfish Club[14] is the world's first NFT members only private dining club where token-holders can gain access to their restaurant in New York, as well as various culinary, cultural and social experiences. In addition, the Crypto Travel Club[15] is the world's first travel platform where members holding NFTs can get access to a range of benefits, including exclusive deals on hotels, flights, and private jets (Regner et al, 2019).

3.8 What this is enabling, is for the leisure industry, sports teams, musicians and other brands to connect with their fan base in a new and different way, offering perks such as VIP, celebrity meet and greets, and access to exclusive merchandise. Sports events, such as the American NFL are selling game highlights as NFTs, and musicians who have released music NFTs include Kings of Leon, Ringo Starr, Snoop Dog and Eminem (Rauman, 2021).

Fundraising

3.9 NFTs have considerable potential to enhance fundraising including donations from those profiteering in the NFT marketplace. For example, owners of the Bored Ape Yacht Club have reportedly donated over

[13] https://www.sandbox.game/en/; https://decentraland.org/; https://axieinfinity.com/
[14] https://www.flyfishclub.com/
[15] https://cryptotravelclub.io/

$200,000 to orangutan outreach centres in Borneo and Sumatra[16] and $1 million to Ukraine to support the country after the Russian invasion.[17] Indeed, NFTs have featured widely in charitable donations to the Ukrainian crisis, and in February 2022, the crypto fundraising campaign UkraineDAO sold an NFT of the Ukrainian flag for $6.75 million, becoming the 10th most expensive NFT sale at the time.[18]

3.10 There are many other examples of the ways in which fundraising and giving have been enhanced through NFTs and use of a blockchain. The Giving Block[19] is a platform helping non-profit organisations to fundraise. It provides tools and resources for organisations to help them set up and manage cryptocurrency donation campaigns, including NFTs. DoinGud[20] is an NFT platform set up to allow NFT creators to allocate a minimum of 5% on every sale to a chosen social impact organisation. Finally, Maxity,[21] launched in early 2022, was the first NFT marketplace created exclusively for charities and philanthropy-minded NFT projects.

Fashion

3.11 To-date the fashion industry has engaged with NFTs in a number of ways and there is still much untapped potential in this market (Umer and Kishan, 2021). Designers such as Dolce & Gabbana and Tommy Hilfiger, have released virtual garments as NFTs which customers can try on or wear in virtual environments through augmented reality, or purchase for their avatars for use in a metaverse platform (Joy et al, 2022). Others have released digital content that owners can interact with. One popular use however has been the "twinning" of the physical and virtual worlds to create a phygital experience; fashion brands and retailers like Nike have capitalised on this (Periyasami and Periyasamy, 2022).

Noteworthy NFTs

- Everydays: The First 5000 Days by Beeple was sold in 2021 for $69.3 million by the art auction house, Christie's. The image consists of 5,000 artworks made by Beeple over 5,000 days.
- Jack Dorsey, founder of Twitter, sold an NFT of the first-ever tweet for $2.9 million USD.
- In 2021, an artist created an NFT of a stick called "Twig" for dogs for $1,200. Price included a real-life stick in a presentation box, from a West Village sidewalk in New York attractive to dogs.
- Canadian musician Grimes sold 10 pieces depicting her digital avatar War Nymph for $6 million.

[16] https://news.bitcoin.com/troop-of-bored-ape-nfts-rises-above-the-competition-bayc-donates-200k-in-eth-to-orangutan-outreach/
[17] https://decrypt.co/94660/bored-ape-yacht-club-donates-1-million-ethereum-ukraine
[18] https://cointelegraph.com/news/ukraine-dao-raises-over-6m-via-nft-sale-to-aid-ukrainian-citizens
[19] https://thegivingblock.com/
[20] https://doingud.com/
[21] https://maxity.io/

- In February 2022, a digital version of handwritten notes for the Beatles' hit single Hey Jude has sold at auction for nearly £60,000.
- In February 2021, Charmin, the toilet-paper manufacturer produced a series of NFTs for charity, at the time costing around $3,500 each.
- Look Labs sold its "Cyber Eau de Parfum", the first digital-only fragrance in 2021 as an NFT for $18,000.

Main characteristics and benefits of NFTs

3.12 There are many benefits of NFTs a number of which are inherited from the key features of the blockchain on which they reside (Musamih et al, 2022). From literature reviews and talking to experts in NFT technology, detailed below are some of the main characteristics and benefits of NFTs secured on the blockchain.[22]

Ownership

3.13 Whoever creates or mints an NFT has ownership and control over it. This is recorded on a blockchain proving provenance and ownership. Creators are able to determine how the NFT is used in the future, with the rights of future owners stipulated and built into the underlying smart contract. Artists and creators can collect royalties from the initial and any future sales of their NFTs and these are executed automatically when contract conditions are met and verified by the blockchain (Chohan and Paschen, 2021).

Uniqueness

3.14 The primary characteristic of NFTs lies in their digital uniqueness, ensuring that each NFT is distinct and unlike any other. This concept of scarcity plays a significant role as users and collectors strive to gain a competitive edge over others, driving up the value and desirability of NFTs. (Sharma and Alter, 2012). Because of the uniqueness and immutable records on the blockchain this avoids easy counterfeiting of NFT tokens once minted (Bhujel and Rahulamathavan, 2022).

Verifiability

3.15 The process of authenticating transaction is one of the underlying features of blockchain technology. This means that cryptoassets, such as NFTs are traceable within the public ledger and all historical data is registered and stored within blocks, which are connected to each other in a chain (Popescu, 2021). These blocks contain transaction data and include timestamps, thereby allowing the ownership of any asset to be traced back to the original creator/owner (Anderson, 2022).

[22] Based on the findings of Anderson (2022); Anjum and Rehami (2022); and Wang et al (2021)

Tamperproof

3.16 NFTs, once secured on the blockchain, cannot be altered or manipulated in any way and therefore, are deemed secure and tamperproof (Bhujel and Rahulamathavan, 2022). The technology behind NFTs and the blockchain makes records immutable and all the metadata stored in smart contracts cannot be replicated, removed or destroyed (Popescu, 2021).

Transparency

3.17 Activities relating to NFTs (minting, selling, and purchasing) are all recorded on the blockchain which is public[23] and permissionless. Because all transactions are recorded there, this gives end-to-end transparency and anyone can access it if they wish. This allows users and individuals to check ownership and transaction histories without requiring permission (Bhujel and Rahulamathavan, 2022)

Availability

3.18 The availability of NFTs holds great significance for both creators and buyers. The blockchain and its affiliated platforms remain continuously accessible, ensuring that tokens and created NFTs are constantly available for sale and purchase. Moreover, creators and sellers are not constrained by physical distribution factors like geographic boundaries, delivery expenses, and packaging, enabling them to reach a global audience without limitations (Chohan and Paschen, 2021).

Limitations and issues with NFTs

Practical use and usability

3.19 A number of concerns have been raised about the practicality and usability of NFTs, specifically as they involve the use of a blockchain and almost certainly cryptocurrency. Whereas at present it is estimated that there are just over 5 billion Internet users, (equating to around 65% of the world's population),[24] it is thought that only approximately 0.5% of the population use the blockchain. Clearly, there is a reluctance to embrace blockchain-based technology; the vast majority of people still favour more traditional alternatives. This hesitant adoption stands in stark contrast to the rapid uptake observed when the Internet was initially introduced (Dash, 2021).

[23] Private and hybrid blockchains exist as well as public chains, but NFTs are usually on the public blockchain.

[24] https://datareportal.com/global-digital-overview

3.20 The relatively slow adoption can be attributed, in part, to the requirement of having a crypto wallet. These digital counterparts of physical wallets serve as repositories for proof of ownership of digital currency and other digital assets. Additionally, they provide a digital signature that validates all transactions. When a user creates a wallet, they receive a private key and a recovery "seed" phrase, both of which must be safeguarded and kept confidential. These components are essential for accessing wallets and accounts, and if lost or shared, users risk losing access to all their assets, including NFTs.

3.21 Wallets fall into one of two categories – either hot wallets or cold wallets. Hot wallets are connected to the Internet all the time, whereas cold wallets are offline. Hot wallets are more friendly but pose more security risks than cold wallets.[25] Users have noted the fear of losing their “private key” or access to their wallets. There is the potential of losing all that is contained in them; unlike with traditional banks there is no third party to help remedy the situation (Meyns, 2022).

3.22 A further usability issue relates to the speed of confirmation for NFT transactions which typically involves sending information via the smart contract and the underlying blockchain. This has put NFT popular blockchains, such as Ethereum and Solana networks, under considerable stress and at times leads to data congestion resulting in slow confirmation of transactions. Blockchains were not originally designed to handle virtual assets such as NFTs and many are now redesigning technology to handle these better. In addition, users who pay higher fees can have their transactions confirmed faster (Wang et al, 2021).

3.23 Although NFTs were initially found on the Ethereum blockchain, other blockchain networks have evolved their systems to handle NFTs. Unfortunately, the technology behind each of these often works very differently and consequently, do not communicate well with each other. This means that NFTs cannot be traded or moved across different blockchains and this lack of interoperability severely limits the development and scalability of NFTs and other virtual assets (such as cryptocurrency) (Hardjono, 2021). To get over this, blockchain bridges (or cross-chain bridges) have been developed which connect two blockchains and enables users to transfer assets and data between different blockchain networks. Although these have been a notable development in decentralised finance (DeFi) they can be expensive to use and their design often leaves room for vulnerabilities, which can be exploited (Lee et al, 2022).

[25] For further information about crypto wallets see https://www.nerdwallet.com/article/investing/hot-wallet-vs-cold-wallet

Storage of virtual assets

3.24 NFTs have only ever been the token representation of an asset and the associated asset might be stored 'on-' or 'off-' chain, with the token being the "pointer" to that object. Storing an NFT on-chain means that the entire NFT asset, the media/asset and all its metadata exist on the blockchain. Whereas off-chain storage means that the token and smart contracts are stored on the blockchain, the actual media/asset they represent are stored on other servers, such as Dropbox, Google Drive, or iCloud (Ross et al, 2021).

3.25 On-chain storage has the advantage that users are then able to verify all facets of the NFT, however, this creates storage and cost issues as these assets tend to contain a lot of data and hence take up a lot of storage. Therefore, most NFT projects are stored off-line on centralised servers, particularly as some of these digital collections can run into tens of thousands of images (such as with CryptoPunks or BAYC for example) (Kostick-Quenet et al, 2022). One implication of this is that if there is an issue with the off-chain network, the associated link becomes obsolete, rendering the asset inaccessible to its owner. This problem, often referred to as "link rot," is a widely recognised issue within the realm of NFTs. It entails the occurrence of broken or disappearing links, leading to the loss of access to the NFT (Idelberger and Mezei, 2022; Mackensie and Brenzia, 2021). The InterPlanetary File System (IPFS) is a decentralized peer-to-peer file storage protocol which addresses certain security concerns but has experienced security issues of its own. (Prünster et al, 2022).

Environmental issues

3.26 The increase in use of cryptoassets (NFTs and cryptocurrency) has created a massive increase in energy consumption and various concerns have been raised about the impact this is having on our already fragile environment (Meyns, 2022; Weijers and Turton, 2021; Valeonti et al 2021). One study suggests that Bitcoin emissions alone could increase global warming by 2°C (Mora et al, 2018) and crypto miners have also been held responsible for power shortages in Iran (Bamakan, 2021). The reason for the high energy use of NFTs relates to the digitally labour-intensive process of confirming transactions on the blockchain, called Proof-of-Work (PoW).[26]

3.27 As there is no centralized authority, such as a bank, to govern blockchain transactions, the responsibility falls upon users or "miners" who earn rewards by competing to solve complex algorithmic puzzles using powerful computers concurrently. However, this process is highly energy inefficient, resulting in significant electricity consumption by major blockchains like Ethereum, comparable to that of an entire small country.

[26] Proof-of-Work (POW) is the consensus mechanism used where miners compete to validate a blockchain transaction in order to receive the blockchain reward.

Furthermore, prominent blockchain mining operations are often situated in countries reliant on environmentally harmful energy sources, further increasing carbon emissions (Calma, 2021 and Ross et al, 2021).

3.28 Many blockchains have recognised this issue and the Ethereum blockchain, for example, changed its PoW system to a Proof-of-Stake (PoS) one, called the Merge, reducing the energy consumption by an eyewatering 99.95%.[27] They initially ran two blockchains in parallel, one using PoW and the other PoS, and then merged them using PoS.[28] PoS has several advantages over PoW systems including being more energy efficient in mining blocks and the validators can use technology which is less energy hungry (Zhang and Chan, 2020). Besides moving to PoS systems NFT transactions are being made more sustainable by using clean energy (like wind, water, solar or zero nuclear) to mine blockchain transactions and batching transactions together for processing. Unfortunately, environmental responsibility is frequently disregarded and is considered an afterthought, potentially jeopardising profits (Dash, 2021).

Investment risks

3.29 Investing in NFTs entails a considerably higher level of risk compared to cryptocurrency, which is comparatively more mature. The primary reason behind this heightened risk is the issue of liquidity. Cryptocurrency owners generally have the flexibility to sell their holdings to other buyers at different price points within a relatively short span of time. In contrast, NFTs pose a challenge in terms of matching sellers with buyers due to their uniqueness, making the process of buying and selling more intricate (Ghosh et al, 2023). Furthermore, similar to other cryptoassets, the value of NFTs is highly volatile, making it challenging to forecast their future worth (Jordanoska, 2021). Unlike traditional investment assets like stocks or shares, NFTs do not generate income. Investors rely solely on the appreciation of the asset to earn a profit. This implies that investors could face significant losses if an NFT fails to maintain its value (Howie, 2023). Additionally, these markets are susceptible to manipulation through social media hype, which can artificially inflate or deflate prices.

3.30 That many NFT marketplaces do not undertake significant checks on their users' identities, nor carry out any type of due diligence (although improvements are being made), which combined with an overarching anonymity surrounding NFT trading, creates additional risks for potential investors compared to alternatives (Jordanoska, 2021). To aid potential investors in making informed decisions, regulatory bodies such as the Financial Conduct Authority (FCA) have recently issued guidance on

[27] https://ethereum.org/en/roadmap/merge/

[28] Instead of miners producing valid blocks for the blockchain via PoW processes, PoS validators are responsible for processing the validity of all transactions and proposing new blocks on the chain.

crypto investments, but this refers to cryptocurrency only and does not mention NFTs.[29]

Security concerns

3.31 The growth of the digital world, including cryptoasset transactions has resulted in a significant increase in cyber security and fraud risk (Rehman et al, 2021). As noted, blockchain technology is usually extremely secure as any changes made are immediately flagged to all users creating a secure and permanent record. Blockchains work on a "consensus model" such that if one actor behaves badly or is compromised, a consensus is needed amongst those users or miners verifying the blockchain to arrive at a "correct" version (Guo and Yu, 2022).

3.32 However, not all blockchains are as secure as the major ones, and where blockchain miners are able to gain control of over 50% of the computational power of the network, known as a "51% attack", they can potentially manipulate transactions on the ledger and double-spend coins.[30] However, the more prevalent risks rests on the vulnerabilities of the associated off-chain programs. These programs are susceptible to typical cybersecurity threats, including malware attacks, phishing, Denial of Service (DoS) attacks, spoofing, and tampering. It is crucial to address and mitigate these threats in order to safeguard the integrity and security of the overall system (Rehman, et al, 2021).

Legal issues associated with NFTs

3.33 As NFTs have gained substantial popularity in recent years, they have also brought to the forefront a range of legal issues that require attention. Lawmakers and regulators are currently grappling with numerous policy concerns associated with them (see Section 6 for more detail), encompassing financial regulations, intellectual property rights, consumer protection, energy consumption, privacy, and content moderation. The decentralised nature of blockchain technology and its associated systems further exacerbate many of these legal challenges. This section will explore some of the legal complexities surrounding NFTs and consider how these affect those who are involved with them (Di Angelo and Salzer, 2021 and Pravdiuk, 2021).

Defining NFTs as assets

3.34 The legal status of NFTs is a hotly debated topic, including exactly what constitutes the asset, who owns it, and exactly what they own. In March 2022, the UK High Court made a landmark ruling recognising NFTs as legal property. This resulted from a court case where a proprietary freezing order had been applied for after stolen NFTs were traced to

[29] https://www.fca.org.uk/investsmart

[30] Double-spending is when a user is able to spend the same tokens in their wallet more than once.

another wallet. Although courts had previously viewed cryptocurrencies as such assets, this was the first time that NFTs had been treated in the same way. In paving the way for recognising NFTs as property it also enabled them access to legal protections.[31]

3.35 Under UK property law, an asset's location generally determines which laws apply to it. However, as already pointed out, often the NFT and the asset it represents will be stored in different locations and possibly in different countries. This creates cross border issues and raises the question of which legal system should govern a particular NFT should the owner or investor experience any legal difficulties, or who is responsible if one of these systems is attacked or hacked (such as a marketplace or crypto wallet site) (Wang et al, 2021). Such concerns are already being addressed by those countries currently using and trading cryptoassets, however, in many countries there is a lack of clarity.

Intellectual property (IP) issues

3.36 The issue of IP rights (including copyright, trademarks, patents and designs) with NFTs is another, often misunderstood legal area. When an NFT is bought, this does not mean that the copyright ownership of the digital or physical items associated with the NFTs transfers with the sale. It doesn't, unless explicitly stated elsewhere in external terms and conditions or contracts (Yoder, 2022; Rehman et al, 2021). The authors or creators initially own the copyright of their work unless the sale includes a transfer of copyright in the underlying assets, which is not the case by default. Therefore, any unauthorised reproduction or communication of an NFT would be classed as an infringement of the sale agreement (Klein and Selz, 2021).

3.37 There are no authenticated industry-wide statistics on the volume or proportion of NFTs that violate copyright laws, but in 2022 the marketplace OpenSea tweeted that it found that 80% of its NFTs "were plagiarised works, fake collections, and spam," (though the site later recanted this figure) (Scheck, 2022), and Dune Analytics data reported in March 2023 that it believed over 42% of its traffic was fake.[32]

3.38 NFT sellers and IP rights owners can grant a licence for personal and/non-commercial use for the IP rights in the underlying asset to purchasers for certain process. In some instances, NFTs do not provide any information on how or whether the underlying digital or physical item may be used, but the lack of this information does not mean that IP rights are included. In some instances, NFT marketplaces may have misleading advertisements or terms of service that lead consumers to believe they are purchasing "true ownership" or copyright of digital or physical items associated with the NFTs' metadata. Such claims of

[31] *Osbourne v (1) Persons Unknown and (2) Ozone Networks Inc trading as Opensea* [2022] EWHC 1021 (Comm)

[32] Reported in https://cointelegraph.com/magazine/4-out-of-10-nft-sales-are-fake-learn-to-spot-the-signs-of-wash-trading/

authenticity are often made based on links to an item, even when no legal connection between an item and NFT token is established (Moringiello and Odinet, 2022).

3.39 More reputable marketplaces and NFT sites are thus favoured. For example, CryptoKitties[33] outlines its terms of use, including licence conditions on their website.[34] This allows NFT owners to make commercial use of their "kitties" providing this does not result in earning more than $100,000 in gross revenue each year. Whereas NBA Top Shop grants owners highlight video clips called "moments", a non-exclusive licence to use, copy and display the moment solely for personal and non-commercial use.[35] (Klein and Selz, 2021).

3.40 Trademark law appears to work in the digital world, as it does in real life, albeit a relatively new and evolving area. Trademark infringement may arise where an unauthorised party mints an NFT for sale linked to an underlying asset they do not own, or where the same or similar mark takes advantage of the reputation of the asset owner's registered trademark (Muraca, 2022). One of the first cases addressing these issues was brought to a New York federal court by the French fashion house Hermès, against the artist Mason Rothschild, for unauthorised use of the Hermès Birkin bags.[36] He produced an NFT collection, he digitally covered the bags in fur and called them "MetaBirkins" which he sold for over $1 million. Hermès won the trademark infringement case and were awarded damages (Yoder, 2022).

3.41 In the UK, although not an official lawsuit, John Terry's promotion of his "Ape Kids Club", was a high-profile NFT trademark case. His tweets contained cartoons of baby apes, some of which included football trophies or badges which are protected under trademark laws by organisations such as the Premier League, UEFA and Chelsea Football Club. Permission for their use had not been sought and no licencing agreement existed. The trademarks and badges have since been removed and are no longer available for purchase as NFTs. Both the International Trademark Association (INTA) and the UK Intellectual Property Office (UKIPO)[37] have recently provided guidance on how to deal with trademarks in the metaverse and for NFTs.

NFTs and privacy

3.42 NFTs raise a couple of privacy matters that regulators need to address but are currently still understudied (Wang et al, 2021). First, there is the issue of the level of anonymity associated with the use of a publicly

[33] CryptoKitties is a blockchain collectible game built on the Ethereum blockchain where players can breed, collect and sell virtual cats or "kitties".
[34] https://www.cryptokitties.co/terms-of-use
[35] https://nbatopshot.com/terms
[36] Hermès International v. Mason Rothschild – February 2023, 1:22-cv-00384 (SDNY)
[37] https://www.gov.uk/government/publications/practice-amendment-notice-223/pan-223-the-classification-of-non-fungible-tokens-nfts-virtual-goods-and-services-provided-in-the-metaverse

accessible blockchain where transactions can be viewed by anyone (Arcenegui et al., 2021). Blockchains tend to only provide pseudo-anonymity rather than complete anonymity. In other words, users can hide their identify to some extent but this can be revealed (intentionally or unintentionally) with links to other addresses associated with NFTs or the blockchain (Agarwal et al, 2022). Not only might this reveal personal information but also other sensitive information, such as locality, if for example an NFT had been used as a ticket for an event (Castro, 2023). Second, because some data protection laws give individuals the right to erase their data, NFTs can conflict with these laws because of the immutable nature of blockchain technology, meaning that things cannot be changed. This means that NFTs that contain personal information may violate data protection laws (Rehman et al 2021).

Taxation and NFTs

3.43 Because NFTs are a fairly new recent phenomena, most global tax organisations have not yet issued specific guidance on these. However, in light of the rise of cryptocurrency earlier, many have outlined the tax implications relating to these digital assets, and the principles of these taxation rules are likely to apply for NFTs, if the tax office has not specifically said this. The tax implications relating to NFTs will depend on a variety of factors: whether you are an individual or an organisation; whether you are a creator seller or buyer; and the definition of cryptoassets adopted by the relevant government (Budak and Yilmaz, 2022).

3.44 In the UK, the HM Revenue and Customs (HMRC) issued a Cryptoasset Manual[38] detailing the taxable events relating to cryptoassets (see Table 5 for summary). If an NFT is bought as an investment and disposed of, capital gains tax is due on any profit made. The HMRC does not consider theft or other loss of a cryptoasset as a capital loss, but a negligible value claim may be made in specific circumstance. Buying cryptoassets with crypto currency (as opposed to a fiat currency) is also classed as a taxable event and is subject to capital gains tax. Likewise, gifting cryptoassets attracts capital gains tax unless this gift is to a spouse/civil partner. Donating a cryptoasset to a registered charity is tax free in the UK.

Table 5 – Summary of taxable events for NFTs[39]

- Buying an NFT with a fiat currency: Not taxable
- Buying an NFT with cryptocurrency: Capital Gains Tax
- Selling an NFT for crypto or fiat currency: Capital Gains Tax
- Swapping an NFT for another NFT: Capital Gains Tax
- Minting an NFT: Not taxable
- Farming NFTs: Could be subject to Capital Gains Tax or Income Tax

[38] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual
[39] https://koinly.io/blog/what-is-an-nft-and-how-is-it-taxed/

- Gifting an NFT: Capital Gains Tax (unless to your spouse, which is tax free)

3.45 Individuals trading in cryptoassets will also be subject to income tax on that activity. However, "day trade" individuals are unlikely to meet the HMRC definition of a "trader", [40] and therefore more likely to be taxed on the capital gains tax regime. However, if a company's activity involves NFTs and is considered a trading activity, then any profits made will be subject to corporation tax. If a company acquired NFTs as an investment, then their value needs to be reflected in the balance sheet as an intangible asset and any disposal will likely fall within the Corporation Tax Intangible Asset Regime. Value Added Tax (VAT) would be due on any goods and services sold in exchange for NFTs and likewise, the value of the supply of goods or services on which VAT is due will be the sterling value of the NFTs.

NFTs and consumer protection

3.46 NFT marketplaces should logically adhere to local consumer protection laws to ensure that sellers accurately describe the NFTs they are selling and enable buyers to be aware of their rights and any recourse of action, should something go wrong. Smart contracts should offer the same level of protection as real-life contracts. Although this sounds straightforward, the anonymity that the blockchain and associated programs afford complicates the process; consumer protection is minimised when it is not evident from who to seek relief and whom to make a claim against (Kooleen, 2022).

Securities and Regulatory Compliance for NFTs

3.47 In certain cases, and in particular jurisdictions, NFTs may be considered securities under applicable laws, providing an NFT meets the legal definition of a security in that particular country. If it does, and this may depend on how it is structured, marketed and sold, that could trigger securities regulations, including registration requirements, investor disclosures, and compliance with anti-fraud provisions (Workie and Jain, 2017). In the United States, the determination of whether an NFT is a security is primarily determined via the "Howey Test",[41] which is used to identify investment contracts. No such equivalent exists in the UK and the regulatory framework for securities is primarily governed by the Financial Services and Markets Act 2000 (FSMA) and overseen by the Financial Conduct Authority (FCA). However, a recent report on regulating cryptoassets strongly recommends that the Government regulates retail trading and investment activity in unbacked cryptoassets

[40] To fall into the definition of 'trading', an individual would need to buy and sell cryptoassets with such intention, sophistication, frequency and level or organisation that the activity amounts to a financial trade.

[41] The Howey test is a legal test used in the United States to determine whether a transaction qualifies as an investment contract

as gambling rather than as a financial service (House of Commons, 2023, para 52).

Legal issues with smart contracts

3.48 In addition to legal issues relating to NFTs, smart contracts, which underpin them, also pose some issues, mainly in two areas. First, because a smart contract consists of a number of lines of code built into the metadata of the NFT secured on the blockchain, not everything can be coded into this format. Therefore, sellers may want to introduce additional terms and conditions into their sales agreements. Second, for smart contracts to be legally enforceable, they need to comply with the legal requirements of more traditional paper-based written contracts (Aksoy and Uner, 2021).

3.49 In 2021 the Law Commission published advice about smart contracts and concluded that they are legally binding and that the current legal framework of England and Wales is able to support and facilitate their use.[42] They did, however, acknowledge that they pose some unique jurisdictional challenges - given the blockchain is a distributed ledger - and they recommended that parties involved should include appropriate jurisdictional and governing law clauses to mitigate legal uncertainty. Building on this report, the Law Commission has published a consultation on digital assets, which closed in November 2022, the final report with law reform recommendations due later in 2023.

3.50 The rapid emergence and popularity of NFTs has outpaced the development of specific legal frameworks and regulations in many jurisdictions, including the UK. As a result, the benefits of investors and collectors conducting due diligence when engaging in NFT transactions are highlighted. Further discussion on regulatory frameworks is discussed in Section 6.

[42] https://www.lawcom.gov.uk/project/smart-contracts/

Section 4. Why people invest in NFTs

Background

4.1 There are various (often hidden) reasons behind purchasing NFTs, but they generally fall into two categories. First, individuals may seek to generate profits by engaging in short-term buying and re-selling, commonly known as "flipping," to generate quick financial gains. Alternatively, they may view NFTs as a long-term investment, holding onto them in anticipation of future value appreciation. Abundant information is available on the Internet to assist individuals in pursuing either strategy.

4.2 According to Rich (2021), there are two types of individuals currently investing in NFTs. “Collectors” are driven by the desire to acquire unique and one-of-a-kind items, while “hagglers” aim to make swift profits. Rich notes that the profitability of NFTs currently relies on their novelty and the limited regulatory oversight, and he cautions that as these circumstances evolve, investment opportunities may diminish.

4.3 However, given that much of the rapid rise in NFTs to date has been closely associated with the collectibles markets, it is worth considering why people collect items in the first place. This is summarised below:

- Collecting is not a new phenomenon, it goes back at least as far as the Middle Ages and thought to be more widespread in western post-industrial societies (Apostolou, 2011).
- Collecting has been defined as “the process of actively, selectively, and passionately acquiring and possessing things removed from ordinary use and perceived as part of a set of non-identical objects or experiences” (Belk, 1995: 67).
- It is often confused with hoarding, but collecting tends to be more organised (Aristides, 1988: 330).
- In the past there have been other collecting crazes such as sports cards, Furbies, Beanie Babies, Pokémon cards etc.
- Various theories have been put forward to explain collecting behaviour, ranging from consumerism and materialism (Spaid, 2018 and Rykwert, 2001), to more biological and psychological theories, (Nordsletten et al, 2012 and Baron-Cohen, 2004).
- Social status plays an integral role in explaining the popularity of NFTs and can be seen as the new virtual luxury item (D’Agnostino, 2022).
- A high number of celebrities have bought NFTs for large amounts of money and have used them as their profile pictures or avatars (see Table 6).

Table 6 - The most expensive NFTs bought by celebrities[43]

- US rapper Snoop Dogg bought Right Click & Save As Guy for $7,088,229
- Serial entrepreneur Gary Vee bought CryptoPunk #2140 for $3,953,216
- Pop music icon Justin Bieber bought BAYC #3001 for $1,301,550
- American DJ Steve Aoki bought Doodle #2238 for $862,056
- YouTube personality Logan Paul bought K4M-1 #03 for $624,669
- Brazilian football player Neymar Jr. bought BAYC #5269 for $569,531
- Electronic music producer Marshmello bought CryptoPunk #8274 for $504,069)
- Pop legend Madonna bought BAYC #4988 for $466,461
- US rapper Eminem bought BAYC #9055 for $453,776
- NFL Veteran Tom Brady bought BAYC #3667 for $453,062

Why was there a sudden boom in 2020-21?

4.4 Although NFTs have been in existence for over 10 years, there was a sudden boom between 2020 and 2021, and undoubtedly the Covid pandemic influenced this. More people were working from home, everything seemed to be carried out online, and people saved money from not being able to go out. Studies have found out that the cryptocurrency market liquidity increased significantly after the WHO's identification of a worldwide pandemic, and this included "recreational" investments in NFTs (Corbet et al. 2022).

4.5 The significant decrease in global market interest rates over the last decade also attracted investors to cryptoasset markets, coupled with a general distrust of fiat currencies (Aharon and Demir 2021; Sarkodie et al. 2022). The increased demand caused a rise in prices of Bitcoin and other cryptocurrencies, making investment in NFTs more attractive and possibly explaining the disinterest in initial coin offerings[44] (Dowling, 2021; Chalmers, 2022; and De Andrés, 2022).

4.6 A further reason for the recent interest in NFTs is that they are just a product of a continuing technological world, specifically supported by the younger generation (Valez, 2022). As the move to more decentralised finance (DeFi) system continues, with the aim of providing financial services using automated protocols on blockchains without intermediaries (Aramonte et al, 2021), NFTs with their smart contracts seem attractive. Of course, substantial profits have been made from NFTs, they are not subject to inflation and cannot be divided, so they are always worth more than the cryptocurrency they are bought with.

[43] From Benzinga https://www.benzinga.com/markets/cryptocurrency/22/10/29295291/the-10-most-expensive-nfts-bought-by-celebrities

[44] Initial Coin Offerings (ICOs) are a fundraising mechanism used by cryptocurrency and blockchain-based projects to raise capital.

Section 5. Fraud and other crimes involving NFTs

Background

5.1 As noted, the relative lack of robust regulation, or in some cases the absence of regulation altogether, exacerbates the vulnerabilities inherent in NFTs and provides a conducive environment for unscrupulous individuals to exploit the market.

5.2 The incidence of NFT fraud has been steadily increasing although official statistics likely underestimate the actual extent and consequences of scams. Moreover, apart from offences directly linked to NFTs, there is a belief that NFTs enable other illicit activities, including money laundering (Jordanoska, 2021). This section of the report will look at the reported levels of NFT fraud to Action Fraud, examining various types of frauds and scams commonly associated with NFTs, as well as those crimes that NFTs have been said to facilitate.

Levels of reported NFT fraud

5.3 As with the introduction of any new product, it is likely that risks will increase which need to be addressed, and our survey of ACFE UK members confirmed that this was likely to be true for NFTs, in terms of causing more frauds and scams, as well as enabling other crimes to be committed. Following a Freedom of Information request submitted to all 43 police forces in England to request information for the reporting levels of frauds relating to NFTs most police forces did provide this information as it was not seen "in the public interest". However, the City of London police and National Fraud Information Bureau (NFIB) did do so (see Table 7 and further details and methodology for collecting the data is detailed in Appendix 1). From November 2020 to March 2023, there were 112 instances of NFT fraud reported with verified losses amounting to nearly £5 million.

Table 7 – NFT frauds reported to Action Fraud[45]

Year	Report Volume	Verified Loss (£)
2020	2	3,177.69
2021	17	788,815.51
2022	80	4,072,132.51
2023	13	53,765.00
Total	**112**	**£4,917,890.65**

[45] From November 2020 to March 2023

Types of NFT frauds and scams

5.4 A review of the common frauds and scams associated with NFTs shows that while many of these fraudulent schemes are variations of scams that have been witnessed in the past, there are some unique elements. Understanding these is key to improving prevention.

5.5 A typology of different types of NFT frauds and scams has been developed by Kshetri (2022) (see Table 8) which shows attacks against two main groups – first, creators or owners of NFTs (or assets they represent), and second consumers, buyers or investors of NFTs. Different types of frauds and scams are then classified via these two groups by the modus operandi of the attack – being either a technology attack or one through social engineering. Sometimes frauds and scams involve more than one type of attack and therefore, there is some overlap between the four cells shown.

Table 8 – Different types of NFT frauds and scams[46]

Target	Creators or Owners of NFTs (or assets they represent)	Consumers, Buyers or Investors of NFTs
Technology attacks	**Cell 1** • Theft of NFTs from wallets • Malware and virus attacks on wallets	**Cell 2** • Exploiting security flaws in NFT platforms • Airdrop scams
Social engineering and other attacks	**Cell 3** • Counterfeit minting and selling of NFTs • Theft of artwork • Selling fake wallets • NFT customer service scams • Phoney job offers	**Cell 4** • Selling fake/non-existent NFTs • Phishing scams • Investment scams (rug-pulls, pump and dump schemes) • Technical support scams • Market manipulation/wash trading • Bidding scams • Website scams

Theft from and attacks on cryptocurrency wallets

5.6 Attacks on crypto wallets are quite common, especially hot wallets which are held on provider websites (as opposed to cold wallets which, as noted earlier, are either held on hardware or are paper-based). Because these websites are not directly part of the blockchain, they are more vulnerable to malicious technology attacks, as well as users who may vulnerable to social engineering scams.

[46] Based on the Scam Typology developed by Kshetri (2022)

Crypto wallet attack examples

The NFT influencer who goes by the name of "NFT God" on Twitter, lost all his digital assets in a hack in January 2023 when he was trying to download some software from a sponsored Google link. His crypto wallet was emptied of a number of NFTs, including a Mutant Ape Yacht Club NFT whose market value was over $25,000 at the time, and cryptocurrency around $23,000.

Also, in January 2023, Kevin Rose, the co-founder of the NFT collection Moonbirds, fell victim to a phishing scam resulting in him losing more than $1.1 million worth of NFTs. It is understood that Rose's NFTs were drained after he approved a malicious signature that transferred a significant proportion of his NFT assets to the scammer. In addition, Luke Dashjr, one of Bitcoins early and core developers, revealed he had been hacked after his PGP key was compromised which he was unaware of how this happen. He lost around $3.6 million worth of Bitcoin.

Once fraudsters have access to crypto wallets they can empty the contents of any digital assets held there, including both NFTs and cryptocurrency. Some popular platforms[47] offer custodial wallets managing keys on behalf of users, and in so doing create a vulnerability; and creates problems should the link or organisation disappear or get compromised, as any assets would be lost (Valeonti et al, 2021). Some scammers avoid the hassle of hacking a wallet, instead they create fake wallets selling them to unsuspecting users and gaining access to anything stored in them. There have also been instances where fake paper-based wallets have been scattered in public areas designed to look like the real paper-based wallets. The intention here is to get the finder to scan the QR code[48] which will send them to a link claiming to contain cryptoassets which if accessed will compromise their security and personal details.

Attacks on NFT platforms and website scams

5.7 Although the blockchain is immutable and in general secure from cyberattacks, many of the programs associated with it for creating, minting, promoting and selling NFTs, as well as those hosting crypto wallets, are not. They are vulnerable to the usual phishing and cyber threats such as malware; denial-of-service (DoS) attacks; phishing; spoofing; code injection attacks to name but a few. In addition, some scammers create fake websites replicating the details and designs of the original hoping to scam users (Kshetri, 2022).

Attacks on NFT platforms and website scam examples

Lympo, a sport-based NFT platform suffered a hot wallet security breach in January 2022 and lost 165.2 million LMT tokens worth $18.7 million at the time of the hack.

[47] For example Binance https://www.binance.com/en/wallet-direct

[48] A QR code is a multi-dimensional bar code which can store information, often url link

In July 2022, NFT lending platform Omni had 1,300 ETH taken by an attacker who employed a flash loan[49] technique to withdraw funds from Omni's NFT lending contract and laundered the money through mixer site.[50]

In April 2022, BAYC's Instagram account was hacked and NFTs were stolen from multiple users, with the floor price at the time of nearly $14 million.

Also in April 2022, hackers stole over $2 million by creating a fake Shifters website to sell their NFTs after sending numerous messages to Discord members to trick them into buying these, taking payments via an illegitimate mint link.

NFTs valued at $2.23 million at the time stolen, were stolen from TopGoal in February 2022, TopGoal after a cyberattack and over 4.8 million TMT was transferred from the platform's hot wallet to the hacker's address.

In May 2021 Larva Labs Meebits NFT collection was hacked and NFTs worth $700,000 stolen. The hack effectively involved the attacker re-rolling the minting process for a Meebit until he received a rare valuable one.

Free airdrop giveaway scams and stealth drops

5.8 An airdrop refers to the distribution NFTs to a group of individuals for free or at a reduced cost and is a legitimate dispersal method to potential investors. However, scammers exploit these by tricking unsuspecting individuals into revealing personal information or sending funds. Such scams are usually carried using social media especially on popular sites such as Twitter, YouTube, TikTok, Discord and Telegram. The scam usually works by enticing participants to provide personal information, such as email addresses, wallet addresses, or private keys, which will be then stored on their sites and provide scammers full access to their cryptoassets. Scammers often cleverly time their fraudulent airdrops to coincide with genuine airdrops. Awareness of the risks is the starting point to reducing them (Scharfman, 2023).

Free airdrop scam examples

In July 2022, an airdrop of ApeCoins to holders of its various NFT projects including BAYC, Mutant Ape Yacht Club and Bored Ape Kennel Club was planned. Scammers saw this as an opportunity to fraudulent target users and started to create fake campaigns for scam airdrops by hacking and hijacking verified Twitter accounts and driving people to phishing sites.

In December 2021 the Discord channel of Fractal, a startup NFT marketplace, was hacked and led to a fake NFT airdrop scam that netted over $150,000 worth of Solara from 373 users.

Also, in 2021 scammers targeted NFT marketplace Rarible in a giveaway scam by promoting a fake a giveaway link on the social media, misleading users into spending 500 RARI cryptocurrency to receive five times the amount back. Participants received noting and fund instead went to the scammer.

[49] A flash loan is a loan which does not need collateral, where cryptoassets are borrowed and repaid immediately in a single, instantaneous transaction

[50] A mixer site blends the cryptocurrencies of many users together to obfuscate the origins and owners of the funds

Other sites and collections that are known to have been targeted include: Moonbirds NFTs, Bulls and Apes NFT project and Goblintown NFTs.

Investment scams and market manipulation

5.9 Investment scams and market manipulation occur across investment sectors and NFTs are no different. Being new and popular renders them particularly attractive to the would-be fraudster. Tactics adopted include rug-pulls, pump and dump schemes, fake mining and sleepminting.

5.10 Rug-pulls, commonly associated with cryptocurrency, are also increasingly being seen with NFT projects, and it has been estimated that they make up nearly 40% of all crypto scams costing users approximately $2.8 billion in 2022 (Chainalysis, 2022). A typical rug-pull scam will involve developers using social media to create a lot of hype around their NFT collections both to promote and build trust of potential investors, and boost the price of the collection, thereby attracting further attention and investment. The developers then shut down the project without any warning – usually when they feel that the price has peaked and they have drained investors funds – and disappear with the money. They are helped by the anonymity of the decentralised market. Worse still for victims, the price of the NFT collection plummets (Sharma et al, 2023).

5.11 There is very little individuals can do to if they are scammed by a rug-pull, therefore precautions such checking the social media profiles of developers; monitoring feedback from others; and checking past project collections are key to avoiding being one of the many repeated victims (Sharma et al, 2023)

Rug-pull examples

In March 2022, two 20-year-olds were arrested for their involvement in a NFT rug-pull. The pair promoted their Frosties NFT project and made several promises to investors including exclusive mint passes, giveaways and access to a metaverse game. However, after they netted over $1.3 million they shut down their website and social media accounts and transferred the money they had made to a number of external wallets, leaving investors with nothing.

The Animoon NFT project, which was based on recoloured Pokémon image was promoted as a play-to-earn NFT game, promising world travel, clothing giveaways, comics, and a project with Netflix. However, in June 2022 those behind it pulled the project and shutdown social media accounts stealing $6.3m worth of tokens

Around 770 people lost a total of $1.66m in a celebratory-backed French NFT rug-pull which offered them the chance to become “co-producers” in a movie called *Plush*.

5.12 Pump and dump scams are schemes designed to artificially drive up the demand and price of an NFT (in a typical shill bidding scam[51]) and then sell out at a higher price. To achieve this, the fraudster usually goes through three stages: obtaining a large amount of NFTs or collections at a low price; spreading false or exaggerated information to attract further buyers and investors (the pump); then at the price peak cash in, causing the price to collapse and leaving other investors with significant losses (the dump). A related activity is wash trading, which occurs when one or more individuals who collude with each other simultaneously buy and sell the same NFT or collection, thereby creating an illusion of higher trading activity and liquidity of a particular NFT or collection. This is carried out to make particular NFTs more attractive to potential investors and buyers than they actually are and create misleading and false market data (Leppla et al, 2022).

5.13 Both pump and dump and wash trading activities can be difficult to spot. Thought tricky to identify, unsolicited promotions, including exaggerated claims, and low value projects with a sudden spike in prices are an indication (Serneels, 2023). Celebrity endorsements can also play a significant role in promoting NFTs, and while most act responsibly, there have been instances where some individuals have been associated with scams or questionable projects, especially in the investment arena. Celebrities who have had law suits brought against them for this include Paris Hilton, Kim Kardashian, Madonna, Justin Bieber, and Snoop Dogg.[52]

5.14 Fake mints refer to fraudulent or deceptive practices where individuals or entities create and sell counterfeit or unauthorised NFTs. These are essentially counterfeit versions of legitimate NFTs. Scammers copy existing popular or valuable NFTs mimicking the original artwork, metadata or other characteristics to sell to unsuspecting buyers, often targeting deceased artists or the less technically-savvy (Mackenzie and Bērziņa, 2022).

5.15 In other cases, scammers may create NFTs that appear to be associated with well-known artists or projects, and by using similar names and branding make their counterfeits appear legitimate to the unsuspecting buyer. To counter this, some platforms and marketplaces, like OpenSea for example, show a “blue tick” next to the seller authenticating the seller’s legitimacy. However, many platforms do not require the verification of users (Ross et al, 2021). Finally, “sleepminting” occurs when an attacker takes advantage of vulnerabilities in smart contract data and impersonates the artist or creator to sell fakes to to unsuspecting buyers (Guidi and Michienzi, 2022).

[51] Shill bidding involves sellers or their accomplices placing bids to artificially drive up the price of an item.

[52] https://www.deseret.com/2023/1/31/23579681/celebrity-endorsers-named-crypto-nft-lawsuits-tom-brady-post-malone-ftx

Fake minting examples

In 2021, a hacker, known as "Monsieur Personne", created counterfeit copies of a number of famous NFTs, including Beeple's "Everydays: The First 5000 Days," which originally sold for $69 million, in order to highlight what that NFTs are not as unique or secure as they are made out to be, according to his blog. They did not just copy the artwork, but also engineered components of the NTF such as the token ID and transaction history in order to resemble the ones originally minted by Beeple.

In early 2021, the artist Derek Laufman found his artwork appearing on Rarible for sale as NFTs from a verified account, where someone had copied his work and minted NFTs and been through the platforms verification process management to impersonate him.

Other artists have found their work on NFT marketplaces including the Dutch artists Lois van Baarle and Rosa Menkman, concept artist and illustrator Anna Podedworna, retro-futuristic artist Simon Stålenhag.

Bidding scams

5.16 Bidding scams exploit individuals participating in NFT auctions. One of the most common examples is the currency swap scam. This occurs mostly in secondary markets when a scammer places a winning bid or agrees to purchase an NFT at a certain price using the accepted currency. After securing the NFT, the scammer attempts to swap the payment currency for a cheaper or less valuable cryptocurrency. By doing this the scammer aims to benefit from the price difference or potential arbitrage between the initial payment currency and the cheaper currency, resulting in a financial loss for the seller (Das et al, 2022).

5.17 Other bidding scams include scammers manipulating bidding processes by exploiting vulnerabilities or weaknesses in NFT marketplaces or platforms. For example, they use automated bidding bots or hacking tools to enable either the scammer to the win the bidding or manipulate the bidding process in their favour (Gupta and Kumar, 2022). Some scammers create entirely fake auctions, advertising rare or valuable NFTs that do not exist.

Phishing scams

5.18 Phishing scams are also not unique to NFTs and operate in a similar way by tricking people into revealing personal information. One of the most common in the NFT market space is the technical support scam. For these, NFT holders' contact details are usually found through popular social media sites and the scammer reaches out claiming to be from a genuine NFT technical support team requesting remote access or payment for services. They may install malware on users devices or steal funds and NFTs during the process. General advice to be cautious with personal information, to verify those offering help, and to only use official channels for support and assistance have a specific applicability here (Mooney et al, 2022).

Table 9 – General advice to avoid NFT scams and frauds

Protect personal information Do not share or reveal any login information with anyone else including your private key or seed phrase or any other passwords. Use two-factor authentication for all accounts. **Use a cold storage crypto wallet** A cold storage (or offline) wallet stores private crypto keys offline usually on a physical device, therefore, is protected from online attacks. **Ensure security on all devices** Ensure all your device have up to date anti-virus and anti-malware tools for protection against accidentally clocking on a malicious link. Using a virtual private network (VPN) for encryption will give added security. **Only use reputable platforms** Stick to established and reputable NFT marketplaces or platforms that have robust security measures in place. **Do not engage with suspicious messages** Do not interact with potential phishing and scam emails and texts and avoid clicking on any suspicious links you may receive. **Undertake background research** Before engaging with websites and seller carry out some background research to ensure you know who you are dealing with. Where possible use verified sellers and consider online reviews and feedback before making any investments. **Be sceptical of unrealistic prices or promises** If an NFT auction or bid seems too good to be true, it probably is. Be cautious of extremely low prices or sellers making grandiose claims.

Other crimes associated with NFTs

5.19 Being a new and generally unregulated area, NFTs (as well as other cryptoassets) are targets for money laundering. As the NFT process is quasi-anonymous and decentralised it is a very attractive option for criminals to “launder” and “clean funds”. In addition, the process of transferring these digital assets is relatively simple and cost effective, although some transactions fees may be incurred. There is no need to transfer a physical asset, pay shipping fees, insurance or custom taxes, and it can cross borders without considering geographic distance nearly instantaneously (Cancelli, 2020).

5.20 The traditional art market, which has also been used to launder money in the past, is regulated for anti-money laundering (AML) processes with individuals being required to provide identity documents to assist in validating ownership. In contrast, NFT marketplaces are not (yet) explicitly regulated by global regulatory regimes and many of them do not implement any Know your Customer (KYC) requirements to verify the identity of those using their services. This was not the case when NFTs were first introduced to the marketplace, meaning that many accounts are already operational that have little or no knowledge of customers. Additionally, because digital art is less likely to be affected by factors such as age or condition, the pricing of NFTs can be more

subjective – sometimes inflated, giving criminals an opportunity to launder their money through these markets without attracting suspicion (Mikkelsen and Olsen, 2022).

5.21 Although NFT marketplaces are ripe for laundering illicit gains, criminals are not so active, at least not compared to more traditional methods of money laundering (Chainalysis, 2022). That being said, we know that offenders are fast to identify new methods of criminality and adapt their modus operandi accordingly, and the Financial Action Task Force (FATF)[53] has recognised that NFTs create opportunities for money laundering and financing terrorism[54] and has called for further regulation (FATF, 2023). In fact, in 2022 an NFT named IS-NEWS #0 was found to have been created and shared by a terrorist sympathiser supporting Afghanistan-based Islamic militants, and in March of the same year, Israeli authorities seized 30 crypto wallets from 12 exchange accounts linked to Hamas, a militant group based in the Gaza Strip (Katte, 2022).

Police investigations of NFT frauds

5.22 As part of this research FOI request was made to all 43 national police forces in England and Wales and a small sample of police personnel were interviewed about the vulnerabilities of NFTs and the process of investigating irregularities.

5.23 The reporting of NFT crimes is still in its infancy and in some regions of the UK it is still notably very low. Pump and dump schemes are the most common scams reported to the police or Action Fraud. Usually, NFT and other crypto-related crimes are referred to the police Regional Economic Crime Units (ROCUs), unless they involve hacking, in which case they are referred to the Cyber Protect teams.

5.24 Although no police force reported having specific procedures for investigating NFTs, most said that they relied on those they had for generic crypto-asset. In addition, training is available on crypto-related crime through the National Cyber Security Centre (NCSC).

5.25 Although no officer or force was able to discuss individual cases, from open source references it is known that the HMRC were able, with the assistance of the South East Regional Organised Crime Unit (SEROCU), to seize three NFTs and some cryptocurrency as part of an investigation into a VAT fraud amounting to around £1.4 million early in 2022.[55] It is unclear how these NFTs featured in their offending. From 2022, other police forces around the globe started to seize NFTs for the

[53] The Financial Action Task Force (FATF) is the global money laundering and terrorist financing watchdog.
[54] https://cointelegraph.com/news/terror-groups-may-turn-to-nfts-to-raise-funds-and-spread-messages-wsj
[55] https://www.bbc.co.uk/news/business-60369879

first time.[56] For example, the Eastern Region Special Operation Unit (ERSOU) recently arrested an 18-year old on suspicion of a rug-pull fraud. In addition, the High Court of England and Wales allowed the serving of lawsuits via an NFT drop where people are not known but details of their crypto wallets are. This is a significant move showing the court's willingness to adapt to new technologies.[57]

[56] For example, https://www.brusselstimes.com/234830/nfts-seized-by-police-for-the-first-time-ever-in-belgium; https://protos.com/dutch-police-seize-first-ever-nfts-as-part-of-stolen-data-investigation/; and https://www.binance.com/pl/feed/post/148180

[57] https://www.coindesk.com/policy/2022/07/13/uk-court-allows-serving-of-suits-via-nfts/

Section 6. Regulation of NFTs

Background

6.1 Cryptoasset markets and technology, especially those relating to NFTs, have developed far faster than accompanying regulatory frameworks, and this is a global challenge. While many countries therefore are currently trying to play catchup, others are falling short in addressing the issues that these virtual assets raise in world economies and the security needed to protect their populations (Kostik and Quenet, 2022).

6.2 Often the level of regulation is influenced by whether individual countries encourage the use and trading of cryptoassets within their jurisdictions. For example, while some countries will create favourable environments that try to attract NFTs, other countries, like China for example, ban them outright. It is also likely that countries currently with or developing regulatory frameworks for cryptocurrency and initial coin offerings, will be faster introducing (or extending) specific NFT regulations (Chalmers et al, 2022).

Why cryptoassets are difficult to regulate

6.3 The very nature of cryptoassets, including NFTs, makes more difficult to regulate compared to more traditional, physical assets. The characteristics that make them attractive to users (such as the ease of transferring ownership, no geographical borders, and instantaneous transactions) render them difficult to regulate. Moreover, the decentralised environment they operate in, including blockchains and marketplaces (which all differ in size, structure, operations, due diligence protocols and ownership) adds to this challenge (Cornelius, 2021). Furthermore, existing regulatory and legal environments were not designed to accommodate these virtual assets (Doan et al, 2021).

6.4 One of the pivotal challenges of regulating NFTs extends beyond how they are classified to the different approaches adopted by jurisdictions as to how they are sold, held or traded (Elliptic, 2022). The need for clarification on this area has been recognised by the intergovernmental Financial Action Task Force (FATF), and in its recent guidance it has explained to regulators when and how they should identify and regulate NFT's as virtual assets. It states that NFTs should not be evaluated on a case-by-case basis and should be regulated as virtual assets when the use of them conforms to the definition of a virtual asset (FATF, 2023).

Regulation in the UK

6.5 In the UK, the Financial Conduct Authority (FCA) states in its Guidance on Cryptoassets (PS19/22)[58] that all cryptoassets can be divided into two main categories – regulated or unregulated tokens. Regulated tokens consist of e-money and security tokens, whereas unregulated tokens include exchange and utility tokens. They also stated that in general, unless they exhibit characteristics of e-money or security tokens in giving additional rights, most NFTs would fall in the category of unregulated tokens and therefore outside of the regulatory perimeter (Jordanoska, 2021).

6.6 That said, NFT trading platforms and businesses facilitating the exchange of NFTs could be subject to the UK's AML regime if the NFTs being traded are deemed to be cryptoassets. AML requirements for cryptoassets has been set by the European Union's Fifth Anti-Money Laundering Directive (AMLD5), and the UK law implements this via the Money Laundering and Terrorist Financing (Amendment) Regulations 2019. The regulations are expanded to include to providers of cryptoasset exchanges and custodian wallets. Therefore, any UK business which provides these services will be subject to the 2019 regulations and be regulated for AML purposes.

6.7 The rapid rise of NFTs over the last few years means that generally the law and other regulations have not yet fully caught up. But there is also those who feel that regulating this area is the antithesis of what a decentralised market is all about, going against the aim to move away from any central control and regulation, and by this view, creates barriers of entry to the market (Sharma, et al, 2022). However, they also fear that the lack of regulations could lead to misuses of NFTs, increasing fraud and scams and possibly money laundering and therefore the majority of countries around the world are expediting their legislation around cryptoassets (Hendrickson et al, 2016). Although the UK has abandoned its own plans for Royal Mint NFTs, the publication of The Treasury's Committee report on regulating crypto in May 2023 recommended that the crypto market should be regulated similarly to gambling.[59]

[58] https://www.fca.org.uk/publication/policy/ps19-22.pdf
[59] https://committees.parliament.uk/publications/39945/documents/194832/default/

Section 7. Discussion

7.1 NFTs have revolutionised the concept of ownership and value in the digital world and the marketplace has experienced exponential growth, with transactions reaching unprecedented heights with sales predicted to reach $200 billion by 2030. They have captured the attention of artists, investors, and enthusiasts worldwide and people are drawn to NFTs for various reasons, including owning rare collectibles, supporting favourite artists, and speculating on future value. They have transformed the way we perceive and interact with digital content, opening up new opportunities for creators and collectors and redefining the concept of value in the digital realm.

7.2 Looking ahead, it is highly probable that NFTs will continue to evolve both in terms of their technology and functionality, as well as their applications. Despite gaining considerable popularity in the art world, music industry, and gaming communities, there remains a vast untapped potential for further exploration. One notable avenue is the convergence of NFTs with Artificial Intelligence (AI), giving rise to a new category of tokens known as intelligent NFTs (iNFTs). Essentially, AI algorithms grant an AI-based personality upon the NFT, empowering it to analyse and collect data. This enables the NFT to learn, evolve and engage in real-time conservations based on the information it acquires. From a technical perspective, the AI algorithms enable the iNFT to store new metadata within its smart contract layer, which plays a pivotal role in shaping the iNFT's future interactions and personality. As a result, the iNFT evolves and grows more valuable with each interaction, accumulating experience along the way, undergoing emotional and mood changes over time.[60]

7.3 Some believe that in the future NFTs will be used to represent the ownership of a broader range of digital and physical assets and will be adopted in various other domains. This encompasses establishing a decentralised framework to register real estate ownership, employing NFTs for medical records and identification-related documents, like passports, thus granting individuals a lifelong identity connected to birth certificates through a blockchain. Additionally, NFTs could serve as evidence of original authorship or research ownership, protecting intellectual property rights and patents. Furthermore, academic credentials could be verified through NFTs, attesting to attendance and earned qualifications. Moreover, integrating NFTs into supply chains would safeguard products against tampering and enable companies to track their journey from manufacturing to shipping and delivery.

7.4 However, we have seen that there are already many frauds, scams and other NFT-enabled crimes being committed, not only because offenders are constantly looking for new avenues to commit their offences, but that

[60] https://payspacemagazine.com/blockchain-crypto/what-is-an-inft/

current regulation in this area is very limited. This is a situation which will grow without the appropriate attention from governments worldwide. Moreover, the broader adoption of NFTs in existing or emerging areas may be severely inhibited due to several onboarding factors. One major hindrance is the fact that most individuals do not possess a crypto wallet, and the overall crypto market remains unfamiliar and complex to many. Consequently, the next decade will be focused on education and technological advancements that simplify the transition to a more digital and decentralised market.

7.5 Whether one is in favour of NFTs or not, it appears that they have become a permanent fixture in the digital landscape, at least for the foreseeable future. While they may lose their status as the latest trend, or experience a decline in value for certain collections, the underlying principles of NFTs, particularly their security on a blockchain and reliance on smart contracts, make them an attractive asset for future applications. It remains to be seen whether these will facilitate an extension of their current uses, or new and yet-to-be-discovered possibilities. Consequently, professionals involved in tackling economic crime need to be aware that it is highly probable all organisations will be impacted in one way or another in the coming years. It is crucial experts familiarise themselves with these new type of digital assets, understand their capabilities, and recognise the potential fraud risks they may pose; after all criminals are already gearing up.

Bibliography

Agarwal, U., Singh, K., and Verma, R. (2022). An Overview of Non-Fungible Tokens (NFT). *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)* Volume 2, Issue 1.

Aharon, D. Y., and Demir, E. (2022). NFTs and asset class spillovers: Lessons from the period around the COVID-19 pandemic. *Finance Research Letters*, *47*, 102515.

Aksoy, P.C. Üner, Z.O. (2021). NFTs and copyright: challenges and opportunities. *Journal Of Intellectual Property Law and Practice* 16, no. 10 (2021): 1115-1126.

Ali, M., and Bagui, S. (2021). Introduction to NFTs: the future of digital collectibles. *International Journal of Advanced Computer Science and Applications*, *12*(10), 50-56.

Anderson, L.M. (2022). *The Ultimate Beginners Guide to Understanding NFTs: Learn How to Make Money by Creating, Buying and Selling with Non-Fungible Tokens (NFTs), Cryptoart and Blockchain Technology*. Amazon: Great Britain.

Anjum, N. A., and Rehmani, M. H. (2022). Non-Fungible Tokens in Business and Management--A Review. *arXiv preprint arXiv:2208.04836*.

Apostolou, M. (2011). Why men collect things? A case study of fossilised dinosaur eggs. *Journal of Economic Psychology*, *32*(3), 410-417.

Aramonte, S., Huang, W., and Schrimpf, A. (2021). DeFi risks and the decentralisation illusion. *Business Quarterly Review December 2021.*

Arcenegui, J., Arjona, R., Román, R., and Baturone, I. (2021). Secure combination of IoT and blockchain by physically binding IoT devices to smart non-fungible tokens using PUFs. *Sensors*, *21*(9), 3119.

Aristides, N. (1988) 'Calm and uncollected', *American Scholar* 57(3): 327–36.

Bamakan, S. M. H., Nezhadsistani, N., Bodaghi, O., and Qu, Q. (2022). Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. *Scientific Reports*, *12*(1), 1-13.

Baron-Cohen, S. (2004). *The essential difference*. Penguin: UK.

Belk, R. W. (1995). Collecting as luxury and consumption: Effects on individuals and households. Journal of Economic Psychology, 16, 477–490.

Belk, R. W. (2012). Collectors and collecting. In *Interpreting objects and collections* (pp. 329-338). Routledge.

Bhujel, S., and Rahulamathavan, Y. (2022). A Survey: Security, Transparency, and Scalability Issues of NFT's and Its Marketplaces. *Sensors*, *22*(22), 8833.

Budak, T., and Yilmaz, G. (2022). Taxation of Virtual/Cryptoassets/Currencies. *Sosyoekonomi*, *30*(52), 37-54.

Calma, J. (2021). The climate controversy swirling around NFTs. *The Verge*, *15*.

Cancelli, L. (2020). The Growing Crypto-assets Threat to Anti-money Laundering: How Institutions Are Coping with This Phenomenon. *Ca'Foscari University Venice: Venice, Italy*, 1-21.

Castro, D. (2023). *NFTs: US Policies and Priorities in 2023*. Information Technology and Innovation Foundation (ITIF). Retrieved from: https://www2.itif.org/2023-nft-policies-priorities.pdf [27th April 2023]

Chainalysis (2022). *The Chainalysis 2021 NFT Market Report*. https://go.chainalysis.com/nft-market-report.html [Accessed 6th May 2023]

Chalmers, D., Fisch, C., Matthews, R., Quinn, W., and Recker, J. (2022). Beyond the bubble: Will NFTs and digital proof of ownership empower creative industry entrepreneurs? *Journal of Business Venturing Insights*, *17*, e00309.

Chen, J.L, (2021a) *A brief history of cryptocurrencies and blockchain*. Great Britain: Amazon.

Chen, J. (2021b). *Scarcity Principle: Definition, Importance, and Example.* https://www.investopedia.com/terms/s/scarcity-principle.asp#:~:text=Scarcity%20Principle%20in%20Social%20Psychology,scarce%2C%20people%20want%20it%20more [Accessed 6th May 2023]

Chohan, R., and Paschen, J. (2021). What marketers need to know about non-fungible tokens (NFTs). *Business Horizons*.

Conti, R. (2022). What Is An NFT? Non-Fungible Tokens Explained. Forbes Advisor February 15th http://www.forbes.com/advisor/investing/nft-non-fungible-token [Accessed 6th May 2023]

Corbet, S., Hou, Y. G., Hu, Y., Larkin, C., Lucey, B., and Oxley, L. (2022). Cryptocurrency liquidity and volatility interrelationships during the COVID-19 pandemic. *Finance Research Letters*, *45*, 102137.

Cornelius, K. (2021). Betraying blockchain: accountability, transparency and document standards for non-fungible tokens (nfts). *Information*, 12(9), 358.

D'Agnostino, C. (2022). *NFT, the ultimate in dematerialised social status?* https://www.luxurytribune.com/en/nft-the-ultimate-in-dematerialised-social-status [Accessed 16th March 2023]

Dannefer, D. (1980). Rationality and passion in private experience: Modern consciousness and the social world of old-car collectors. *Social Problems*, *27*(4), 392-412.

Das, D., Bose, P., Ruaro, N., Kruegel, C., and Vigna, G. (2022). Understanding security issues in the NFT ecosystem. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* November (pp. 667-681).

Dash, A. (2021). NFTs weren't supposed to end like this. *The Atlantic*, *2*.

De Andrés, P., Arroyo, D., Correia, R., and Rezola, A. (2022). Challenges of the market for initial coin offerings. *International Review of Financial Analysis*, *79*, 101966.

Di Angelo, M., and G. Salzer. (2021) 'Identification of Token Contracts on Ethereum: Standard Compliance and Beyond'. *International Journal of Data Science and Analytics.*

Doan, A. P., Johnson, R. J., Rasmussen, M. W., Snyder, C. L., Sterling, J. B., and Yeargin, D. G. (2021). NFTs: Key US Legal Considerations for an Emerging Asset Class. *Journal of Taxation of Investments*, *38*(4).

Dowling, M. (2022). Is non-fungible token pricing driven by cryptocurrencies?. *Finance Research Letters*, *44*, 102097.

Elliptic, (2022). Elliptic NFT Report 2022 Edition: NFTs and Financial Crime Money Laundering, Market Manipulation, Scams and Sanctions Risks in Non-Fungible Tokens. Retrieved from: https://www.elliptic.co/hubfs/NFT%20Report%202022.pdf [13th April 2023]

Ellul, J., & Revolidis, I. (2023). Non-Fungible Tokens (NFTs), Smart Contracts and Contracts: The Need for Legal and Technology Assurances. *Smart Contracts and Contracts: The Need for Legal and Technology Assurances (January 16, 2023)*.

Fai, A. (2021). *Smart Collectibles: Unlocking The Value of Non-Fungible Tokens (NFTs)*.

Financial Action Task Force (FATF) (2023). *Money Laundering and Terrorist Financing in the Art and Antiquities Market, FATF*: Paris. https://www.fatf-gafi.org/publications/Methodsandtrends/Money-Laundering-Terrorist-Financing-ArtAntiquities-Market.html [Accessed 6th May 2023]

Fowler, A., and Pirker, J. (2021, October). Tokenfication-The potential of non-fungible tokens (NFT) for game development. In *Extended Abstracts of the 2021 Annual Symposium on Computer-Human Interaction in Play* (pp. 152-157).

Gelber, S. M. (1992). Free market metaphor: The historical dynamics of stamp collecting. Comparative Studies in Society and History, 34, 742–769.

Gerard D (2021) NFTs: crypto grifters try to scam artists, again. attack of the 50 Foot Blockchain https://davidgerard.co.uk/blockchain/2021/03/11/nfts-crypto-grifters-try-to-scam-artists-again/ [Accessed 6 September 2022]

Ghosh, B., Bouri, E., Wee, J. B., & Zulfiqar, N. (2023). Return and volatility properties: Stylized facts from the universe of cryptocurrencies and NFTs. *Research in International Business and Finance*, *65*, 101945.

Guidi, B., and Michienzi, A. (2022). Sleepminting, the brand new frontier of Non Fungible Tokens fraud. In *Proceedings of the 2022 ACM Conference on Information Technology for Social Good*. September 2022 (pp. 75-81).

Guo, H., and Yu, X. (2022). A Survey on Blockchain Technology and its security. *Blockchain: research and applications*, *3*(2), 100067.

Gupta, Y., and Kumar, J. (2022). Identifying security risks in NFT platforms. *arXiv preprint arXiv:2204.01487*.

Gutierrez, B. (2021). Why do we collect things? https://news.miami.edu/stories/2021/09/why-do-we-collect-things.html [Accessed 6th March 2023]

Hardjono, T. (2021). Blockchain gateways, bridges and delegated hash-locks. *arXiv preprint arXiv:2102.03933*.

Hendrickson, J. R., Hogan, T. L., and Luther, W. J. (2016). The political economy of bitcoin. *Economic Inquiry*, *54*(2), 925-939.

House of Commons (2023). *Regulating Crypto. Report by the Treasury Committee*. Fifteenth Report of Session 2022–23. https://committees.parliament.uk/publications/39945/documents/194832/default/ [Accessed 20th May 2023]

Howcroft, E. (2022). *NFT sales hit $25 billion in 2021, but growth shows signs of slowing*. Reuters.

Howie, L. (2023) The Benefits and Risks of NFT Investing. https://www.myartbroker.com/investing/articles/benefits-and-risks-of-nft-investing [Accessed 20th May 2023]

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., and Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management*, *49*, 114-129.

Idelberger, F., and Mezei, P. (2022). Non-fungible tokens. *Internet Policy Review*, *11*(2).

Jordanoska, A. (2021). The exciting world of NFTs: a consideration of regulatory and financial crime risks. *Butterworths Journal of International Banking and Financial Law, 10*, 716.

Joy, A., Zhu, Y., Peña, C., and Brouard, M. (2022). Digital future of luxury brands: Metaverse, digital fashion, and non-fungible tokens. *Strategic change*, *31*(3), 337-343.

Katte, S. (2022). Terror groups may turn to NFTs to raise funds and spread messages: WSJ. Cointelegraph https://cointelegraph.com/news/terror-groups-may-turn-to-nfts-to-raise-funds-and-spread-messages-wsj [Accessed 6th May 2023]

Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135e146.

Klein, F.K. and Selz, P.C. (2021) A Primer on NFTs and Intellectual Property *Lexology* https://www.lexology.com/library/detail.aspx?g=d96ed012-8789-4e87-bc1d-70ba76569c0f [Accessed 29th April 2023]

Koolen, C. (2022). 'Apes Gone', but What about Consumer Protection? Applying EU Consumer Law to the Transfer of NFTs. *Applying EU Consumer Law to the Transfer of NFTs (January 17, 2022)*.

Kostick-Quenet, Kristin, Kenneth D. Mandl, Timo Minssen, I. Glenn Cohen, Urs Gasser, Isaac Kohane, and Amy L. McGuire. "How NFTs could transform health information exchange." *Science* 375, no. 6580 (2022): 500-502.

Kshetri, N. (2022). Scams, Frauds, and Crimes in the Nonfungible Token Market. *Computer*, *55*(4), 60-64.

Kugler, L. (2021). Non-fungible tokens and the future of art. *Communications of the ACM*, *64*(9), 19-20.

Lee, S. S., Murashkin, A., Derka, M., and Gorzny, J. (2022). SoK: Not Quite Water Under the Bridge: Review of Cross-Chain Bridge Hacks. *arXiv preprint arXiv:2210.16209*.

Leppla, A., Olmos, J., and Lamba, J. (2022). Fraud Pattern Detection for NFT Markets. *SMU Data Science Review*, *6*(2), 21.

Li, Z., Barenji, A. V., & Huang, G. Q. (2018). Toward a blockchain cloud manufacturing system as a peer-to-peer distributed network platform. *Robotics and computer-integrated manufacturing*, *54*, 133-144.

Mackenzie, S., and Bērziņa, D. (2021). NFTs: Digital things and their criminal lives. *Crime, Media, Culture*, 17416590211039797.

Meyns, S. C. (2022). Happy, risky assets: Uncertainty and (mis) trust in non-fungible token (NFT) conversations on Twitter. Degree project for Linnaeus University, Sweden.

Mikkelsen, J., and Olsen, M. (2022). Non-fungible tokens (NFTs) How are NFTs valued, regulated, and can they help facilitate money laundering?. Master's thesis, Copenhagen Business School: Copenhagen.

Mooney, A., Ronald, Z., Zhang, X., & Crabtree, J. D. (2022). Understanding cybercrime: A three-generation approach. *Issues in Information Systems*, 23(3).

Mora, C., Rollins, R. L., Taladay, K., Kantar, M. B., Chock, M. K., Shimada, M., & Franklin, E. C. (2018). Bitcoin emissions alone could push global warming above 2 C. *Nature Climate Change*, *8*(11), 931-933.

Moringiello, J. M., and Odinet, C. K. (2022). The property law of tokens. *Fla. L. Rev.*, *74*, 607.

Mueller, S.M. (2019). *Inside the Head of a Collector: Neuropsychological Forces at Play*. *Además De. Revista on Line De Artes Decorativas Y diseño*, (6), 177-179.

Muraca, Caitlin, "The 'MetaBirkin' and the Beginning of Trademark Litigation in the NFT Space" (2022). *AELJ Blog. 308*. https://larc.cardozo.yu.edu/aelj-blog/308 [Accessed 30th April 2023]

Musamih, A., Salah, K., Jayaraman, R., Yaqoob, I., Puthal, D., and Ellahham, S. (2022). NFTs in Healthcare: Vision, Opportunities, and Challenges. *IEEE Consumer Electronics Magazine*.

Muthe, K.B., Sharma, K., and Sri, K.E. (2020). A Blockchain Based Decentralized Computing And NFT Infrastructure For Game Networks. *2020 Second International Conference on Blockchain Computing and Applications (BCCA)*, 73-77.

Mystakidis, S. (2022). Metaverse. *Encyclopedia*, *2*(1), 486-497.

Nadini, M., Alessandretti, L., Di Giacinto, F., Martino, M., Aiello, L. M., and Baronchelli, A. (2021). Mapping the NFT revolution: market trends, trade networks, and visual features. *Scientific reports*, *11*(1), 1-11.

Nordsletten, Ashley E.; Mataix-Cols, David (2012). Hoarding versus collecting: Where does pathology diverge from play?. *Clinical Psychology Review*. 32 (3): 165–176.

Olmstead, A. D. (1991). Collecting: leisure, investment or obsession?. *Journal of Social Behavior and Personality*, *6*(6), 287.

Periyasami, S., and Periyasamy, A. P. (2022). Metaverse as future promising platform business model: Case study on fashion value chain. *Businesses*, *2*(4), 527-545.

Popescu, A. D. (2021). Non-Fungible Tokens (NFT)–Innovation beyond the craze. In *5th International Conference on Innovation in Business, Economics and Marketing Research*.

Pravdiuk, M. (2021). International experience of cryptocurrency regulation. *Norwegian Journal of Development of the International Science*, (53-2), 31-37.

Prünster, B., Marsalek, A., and Zefferer, T. (2022). Total Eclipse of the Heart–Disrupting the {InterPlanetary} File System. In *31st USENIX Security Symposium (USENIX Security 22)* (pp. 3735-3752).

Purtill, J. (2021). *Artists report discovering their work is being stolen and sold as NFTs*." ABC Science. (March 15, 2021). https://www.abc.net.au/news/science/2021-03-16/nfts-artists-reporttheir-work-is-being-stolen-and-sold/13249408 [Accessed 21 May 2023]

Rauman, B. (2021). *The Budding Disruption of Blockchain Technology Upon the Current Structure of the Music Industry*. Senior Thesis University of South Carolina: Columbia.

Regner, F., Urbach, N., and Schweizer, A. (2019). NFTs in practice–non-fungible tokens as core component of a blockchain-based event ticketing application. *Proceedings of the 40th International Conference on Information Systems (ICIS).* - Munich, Germany , 2019

Rehman, W., e Zainab, H., Imran, J., and Bawany, N. Z. (2021). Nfts: Applications and challenges. In *2021 22nd International Arab Conference on Information Technology (ACIT)* (December) (pp. 1-7).

Rich, O.J. (2021). *NFTs for Beginners: Making Money with Non-Fungible Tokens*. Independent Publisher: Great Britain.

Ross, D., Cretu, E., and Lemieux, V. (2021). NFTs: Tulip Mania or Digital Renaissance?. In *2021 IEEE International Conference on Big Data (Big Data)* (pp. 2262-2272).

Rykwert, Joseph (December 2001). Why Collect?. *History Today*. 51 (12).

Sarkodie, Samuel Asumadu, Maruf Yakubu Ahmed, and Phebe Asantewaa Owusu. 2022. COVID-19 pandemic improves market signals of cryptocurrencies–evidence from Bitcoin, Bitcoin Cash, Ethereum, and Litecoin. *Finance Research Letters* 44: 102049

Scharfman, J. (2023). *The Cryptocurrency and Digital Asset Fraud Casebook*. Switzerland: Springer Nature.

Scheck, J. (2022). OpenSea's NFT Free-for-All. *Wall Street Journal.* https://www.wsj.com/articles/openseas-nft-free-for-all-11644642042 [Accessed 30th April 2023]

Serneels, S. (2023). Detecting wash trading for nonfungible tokens. *Finance Research Letters*, *52*, 103374.

Sharma, T., Agarwal, R., and Shukla, S. K. (2023). Understanding Rug-pulls: An In-Depth Behavioral Analysis of Fraudulent NFT Creators. *arXiv preprint arXiv:2304.07598*.

Sharma, E., and Alter, A. L. (2012). Financial deprivation prompts consumers to seek scarce goods. *Journal of Consumer Research*, 39(3).

Sharma, T., Zhou, Z., Huang, Y., and Wang, Y. (2022). " It's A Blessing and A Curse": Unpacking Creators' Practices with Non-Fungible Tokens (NFTs) and Their Communities. *arXiv preprint arXiv:2201.13233*.

Spaid, B. I. (2018). Exploring consumer collecting behavior: a conceptual model and research agenda. *Journal of Consumer Marketing*. Vol 35(6): 653–662.

Steinwold, A. (2019). *The History of Non-Fungible Tokens (NFTs).* https://medium.com/@Andrew.Steinwold/the-history-of-non-fungible-tokens-nfts-f362ca57ae10 [Accessed 17th April 2023]

Twesige, R (2015). *A simple explanation of Bitcoin and Block Chain technology*. Jan. 2015.

Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. *arXiv preprint arXiv:2105.07447*.

Umer, S. M., and Kishan, V. (2021). *Application of non-fungible tokens (NFTs) and the intersection with fashion luxury industry*. Politecnico: Milano.

Valeonti, F., Bikakis, A., Terras, M., Speed, C., Hudson-Smith, A., and Chalkias, K. (2021). Crypto collectibles, museum funding and OpenGLAM: challenges, opportunities and the potential of Non-Fungible Tokens (NFTs). *Applied Sciences*, *11*(21), 9931.

Valez, J., 2022. *The credit cycle turns: Key risks - Jorge Valez*, European Territorial Observation Network. Luxembourg.

Vidal-Tomás, D. (2022). The new crypto niche: NFTs, play-to-earn, and metaverse tokens. *Finance Research Letters*, 102742.

Voshmgir, S. (2018). *Fungible Tokens vs. Non-Fungible Tokens*. https://blockchainhub.net/blog/blog/nfts-fungible-tokens-vs-non-fungible-tokens/ [Accessed 6th September 2022]

Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. *arXiv preprint arXiv:2105.07447*.

Weijers, D. and H.J. Turton. (2021) 'Environmentally Smart Contracts for Artists Using Non-Fungible Tokens', 2021 IEEE International Symposium on Technology and Society (ISTAS), pp. 1-4.

Wolf, E.S. (1980) 'On the developmental line of selfobject relations', in A. Goldberg (ed.) Advances in Self Psychology, New York: International University Press.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1-32.

Workie, H., and Jain, K. (2017). Distributed ledger technology: Implications of blockchain for the securities industry. *Journal of Securities Operations & Custody*, *9*(4), 347-355.

Yoder, M. (2022). An "OpenSea" of Infringement: The Intellectual Property Implications of NFTs. *The University of Cincinnati Intellectual Property and Computer Law Journal*, *6*(2), 4.

Zhang, R., and Chan, W. K. V. (2020). Evaluation of energy consumption in block-chains with proof of work and proof of stake. In *Journal of Physics: Conference Series* (Vol. 1584, No. 1, p. 012023). IOP Publishing.

Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, *105*, 475-491.

Appendix 1 – Methodology

Background

This study involved using both quantitative and qualitative research methods as summarised below:

Evidence review

To gain a comprehensive understanding of the research context and to guide the interview schedule with experts, a literature review was conducted. The aim was to explore the main concerns and risks associated with NFTs, cryptoassets, and the blockchain. This review utilised a combination of broad and targeted searches, employing open-source research tools and academic library databases. The evidence arising from these searches was quality assessed prior to inclusion in the review.

Interviews with experts and other professionals

This study adopted an approach that involved actively engaging with professionals who have expertise in working with NFTs and other cryptoassets, either in a general capacity or specifically focused on fraud prevention. The engagement process encompassed both formal and informal methods and largely involved 'snowballing'. We reached out to individuals recommended to us by the ACFE UK Chapter, and in some instances, these individuals referred us to additional experts. We also leveraged personal contacts and their professional networks to further expand our reach and engage with relevant professionals.

The interviews typically lasted thirty minutes utilising semi-structured interview schedules. These schedules were designed based on the insights gathered from the literature review. One advantage of using a semi-structured approach is that it offers flexibility to the interviewers, enabling them to delve deeper into specific issues as they arise during the interview. The interviews were conducted with a typical duration of thirty minutes, utilizing semi-structured interview schedules.

Findings from the interviews were subjected to thematic analysis, by familiarising with the responses provided, coding the data according to emerging ideas and creating categories through comparison of the responses. The purpose of this approach was to identify the overall issues and themes apparent from the discussions and the report was then structured around these emerging themes.

We formally interviewed 10 experts and professionals.

Freedom of Information request from the police

We undertook a Freedom of Information request from the 43 police forces in England and Wales to find out what kinds of issues they were witnessing with NFTs and what training they were given to tackle these. We received responses from 35 of the forces.

Limitations of research

While every effort has been made to ensure the information presented in this report is up-to-date at the time of drafting, it is acknowledged that the subject matter is a rapidly evolving area and therefore subject to change.

Appendix 2 – NFT frauds reported to Action Fraud

Month	Report Volume	Verified Loss
2020		
Nov	2	£3,177.69
2021		
May	2	£35,509.62
June	1	£21,333.33
July	1	£26,666.67
August	1	£32,545.00
September	2	£301,800.00
November	5	£367,662.22
December	5	£3,298.67
2022		
January	11	£11,236.07
February	11	£86,280.52
March	8	£42,161.24
April	7	£16,806.00
May	6	£41,176.91
June	10	£30,242.22
July	4	£3,299,577.29
August	4	£228,699.20
September	5	£6,411.00
October	4	£246,887.00
November	3	£23,401.00
December	7	£39,254.00
2023		
January	3	£1,413.00
February	3	£30,000.00
March	7	£22,352.00

Statistics were derived from analysis of Action Fraud crime reports classified as one of the nine investment or pension fraud Home Office Crime Codes:

- NFIB1E - Recovery Fraud
- NFIB2A - Share Fraud or Boiler Room Fraud
- NFIB2B - Pyramid or Ponzi Schemes
- NFIB2C - Prime Bank Guarantee Fraud
- NFIB2D - Time shares and Holiday Club Fraud
- NFIB2E - Other Financial Investment Fraud
- NFIB16A - Pension Fraud Committed by Pensioners (or their estate)
- NFIB16B - Pension Fraud Committed on Pensioners
- NFIB16C - Pension Liberation Fraud

A series of keywords were then searched against the reports to identify instances where an NFT asset had been referred to:

- Non fungible token
- Non-fungible token
- NFT
- N-F-T
- N.F.T
- NFT's
- NFTs

About Perpetuity Research

Perpetuity Research is a leading research company with wide expertise in both quantitative and qualitative approaches. We have been extensively involved in studies relating to economic crime including the fraudsters' perspective, staff dishonesty, the links between fraud and organised crime, tackling fraud in the public sector, issues in respect of the reporting of fraud, and the police response to fraud. Our clients include businesses, national and local governments, associations and international organisations as well as charities and foundations. Our aim is to exceed their expectations and it speaks volumes that so many have chosen to work with us repeatedly over many years. We are passionate about our work, and we would welcome the opportunity to work with you. For more information visit: www.perpetuityresearch.com

Our Director, Martin Gill, founded the Tackling Economic Crime Awards (TECAs); an award scheme that recognises and rewards individuals, teams, initiatives and companies involved in tackling different areas of economic crime operating in the public, private and third sector. For more information visit https://thetecas.com/

About ACFE UK Chapter

The ACFE is the world's largest anti-fraud organization and premier provider of anti-fraud training and education. Together with nearly 90,000 members, the ACFE is reducing business fraud world-wide and inspiring public confidence in the integrity and objectivity within the profession.

The ACFE UK Chapter is one of nearly two hundred global Chapters whose objective is to provide training, education and to increase public awareness of fraud.

For more information visit: www.acfeuk.co.uk

About the authors

Doctor Janice Goldstraw-White

Janice is a criminologist who has worked with Perpetuity since 2010 and has expertise in the areas of crime, governance, audit, risk management and security. With more than 20 years' prior experience as an accountant, mainly in the public sector, she is particularly interested in crime in the workplace, fraudster behaviour and the role of women in white-collar crime. She has extensively researched in the area of white-collar crime both here and in Australia, with a focus on offender accounts of criminal behaviour. She has particular experience in interviewing within prisons and has undertaken over fifty interviews with incarcerated white-collar offenders.

She has managed and delivered on a range of projects including research on tackling fraud in local authorities; whether the reporting of fraud in the UK should be compulsory; fraud in the Middle East; the problems of using digital evidence; and improving the police response to victims of fraud and scams. Her research interests however are by no means confined to white-collar crime and other research includes why death rates for security officers from COVID-19 are so high; security for data centres and the use of AI in security. She is currently involved in a study developing KPIs for the security sector.

Janice's research skills cover the spectrum of qualitative research, including desk-based literature and policy reviews; analysis and mapping of practice and procedures; interviews with professionals and service users; and facilitating focus groups. She also has a good understanding of quantitative data collection methods and analysis.

Janice has published a number of articles and co-authored separate chapters in books on workplace crime and the motives of white-collar criminals. Her own book entitled 'White-Collar Crime: Accounts of Offending Behaviour' was published in October 2011.

Professor Martin Gill

Professor Martin Gill is a criminologist and Director of Perpetuity Research which started life as a spin out company from the University of Leicester. He holds honorary/visiting Chairs at the Universities of Leicester and London. Martin has been actively involved in a range of studies relating to different aspects of business crime with a special emphasis on fraud and dishonesty offences. For example, much of his work has been involved with better understanding the fraudsters' perspective and he has interviewed a variety of different types of fraudsters, including dishonest staff, insurance fraudsters and identity fraudsters. He has published 15 books including the third edition of the 'Handbook' of Security' which was published in 2022. He is the organiser and Chair of the Security Thought Leadership webinar series. Martin is a Fellow of The Security Institute, a member of the Company of Security Professionals (and a Freeman of the City of London). He is a Trustee of the ASIS Foundation. In 2002 the ASIS Security Foundation made a 'citation for distinguished service' in 'recognition of his significant contribution to the security profession'. In 2009 he was one of the country's top 5 most quoted criminologists. In 2010 he was recognised by the BSIA with a special award for 'outstanding service to the security sector'. In 2015 and 2016 he was nominated and shortlisted for the Imbert Prize at the Association of Security Consultants and in the latter he won. In 2016 ASIS International awarded him a Presidential Order of Merit for distinguished service. In annual IFSEC listings he is regularly recorded as one of the world's most influential fire and security expert. In 2022 he was recognised by *Security Magazine* as one of the 'Most Influential People in Security' and also received the Mervyn David Award from the ASIS UK Chapter 'for his significant contribution to the security profession'. In 2016 he was entered onto the Register of Chartered Security Professionals. Martin is

the Founder of the Outstanding Security Performance Awards (the OSPAs and Cyber OSPAs) and Tackling Economic Crime Awards (the TECAs).

Perpetuity Research & Consultancy International Ltd
11a High Street
Tunbridge Wells
TN1 1UL
United Kingdom
Tel: +44 (0)1892 538690
www.perpetuityresearch.com
prci@perpetuityresearch.com