Contents lists available at ScienceDirect

Journal of Responsible Technology

journal homepage: www.sciencedirect.com/journal/journal-of-responsible-technology

A critical professional ethical analysis of Non-Fungible Tokens (NFTs)

Dr Catherine Flick *

De Montfort University, The Gateway, Leicester LE1 9BH, United Kingdom

ARTICLE INFO

Keywords:
Ethics
Blockchain
Non-fungible tokens
NFTs

ABSTRACT

Non-Fungible Tokens (NFTs) have quickly become an important part of the blockchain economy, theoretically representing ownership of a digital asset registered on a public blockchain such as Ethereum. While several applications of this technology exist, the key underlying factor in NFTs' success is in their potential for investment – buying, selling, and trading the digital assets such as artwork or video game items using cryptocurrency. The rise and mid-2022 crash of NFT and associated crypto markets have shown the volatility of the sector, and questions have been raised around the sustainability, environmental impact, and exploitative practices within this space – and whether there are, in fact, any possible socially responsible use cases for NFTs. This paper aims to fill a gap in the literature surrounding NFTs, primarily through a thorough ethical analysis of the technology and its implementation, deployment, and sustainability. To do this, it uses the Association of Computing Machinery's Code of Ethics and Professional Conduct as a framework for analysis and, following this analysis, makes some recommendations for those wishing to investigate and/or implement NFTs in an ethically responsible manner. The key message is that unless there is absolutely no other way to solve a problem other than using NFTs, then they should not be implemented, as there is currently no ethical use case or means of implementation of NFTs.

Introduction

Non-Fungible Tokens (NFTs) have skyrocketed into the public eye in the last couple of years: one of the more visible transactions was when digital artist Beeple sold an artwork through auction house Christie's for USD$69 million at their first ever NFT auction sale (Kastrenakes, 2021a). Prior to this, most NFT sales had been of Internet "memes" such as "Nyan Cat" (NyanCat, 2021) and the "deal with it" sunglasses meme. These had sold for large amounts of money within a space mostly populated by meme-loving tech people, but the legitimisation that Christie's gave the sale of Beeple's work propelled the discussion directly from niche technological spaces into the mainstream art world and general media. According to Erskine (2022), there are USD$10–20 m worth of NFTs sold on the blockchain each week, with most NFTs selling for under $300. This valuation is volatile, however, as the value of the underlying cryptocurrency the NFTs are sold for can fluctuate significantly between making the sale on the blockchain and cashing out the cryptocurrency into fiat. Regardless, increasing numbers of NFT "drops" (sales of new collections) are being published to markets such as OpenSea,[1] and being promoted by celebrities such as Paris Hilton, Jimmy Fallon, and more (Morse, 2022). NFTs are also seen to be one of the key building blocks of "Web3", the blockchain-enabled decentralised vision of what might be a next generation World Wide Web (Edelman, 2021).

The interest in NFTs has also boosted interest in cryptocurrencies. In particular, the cryptocurrency ETH, on the Ethereum blockchain, is the key facilitator of most NFT sales. Limitations of the Ethereum blockchain (discussed below) have given rise to a number of alternatives, in the form of "side chains" such as Polygon,[2] or separate blockchains such as Solana.[3] Proponents argue that NFTs are a reasonable investment opportunity, much like the physical art market, and one that allows artists to reap royalties from future sales of their art. Critics argue that "ownership" of crypto art is relatively meaningless as the "owner" does not hold the copyright, and anyone can still look at, download, print off or otherwise see and interact with the art; thus what is being bought is bragging rights, or membership of a community (Hertzmann, 2021). Others argue that NFT artists are being ripped off, with many being sourced from low-income countries and paid a minimal fee in a new "gig

* Corresponding author.
E-mail address: cflick@dmu.ac.uk.

[1] https://opensea.io/ (Accessed 25/02/2022)

[2] https://polygon.technology/ (Accessed 25/02/2022)

[3] https://solana.com/ (Accessed 25/02/2022)

https://doi.org/10.1016/j.jrt.2022.100054

Available online 26 October 2022

economy" (Stokel-Walker, 2022). One of the highest selling NFT collections, the Bored Ape Yacht Club, barely even acknowledges the original artists involved in creating the collection; lead designer Seneca now "urges aspiring creators to make sure they understand NFTs" (Hissong, 2022) and to ask for royalties – something she did not. NFTs have also been the subject of high profile scams, fraud claims, "rug pulls", wash trading, insider trading, and other questionable behaviour – as documented by sites such as Molly White's "Web3 is going just great" website which charts the "enormous grift" in blockchain related technologies (White, 2022a). Meanwhile, the underlying cryptocurrencies are also heavily promoted and criticised – proponents leaning on the decentralised, trustless nature of the system allowing for easy payments outside of traditional institutions such as banks (Farrington, 2021); critics pointing out the lack of regulation, lack of recourse for theft or fraud, and concerns around the "pyramid" style system required to ensure capital flow through the systems (Kelly, 2021).

Other concerns around NFTs concern the high environmental costs. Up until Ethereum's 2.0 release ("the Merge") in September 2022 (Ethereum.org, 2022), a single Ethereum transaction consumed more than 238.22 kWh (Statista, 2022). The annual Ethereum energy use was comparable to the power consumption of The Netherlands (de Vries, 2022), and was only set to increase, but due to the Merge, it has pivoted to a lower energy-consuming approach, explained below. As this change only happened during the review process, much of the discussion of environmental concerns below apply to the pre-Merge version of Ethereum. Since there have also been discussions amongst Ethereum miners post-Merge about creating a new Ethereum or another NFT-hosting blockchain using the old approach, this paper will retain the discussion around the environmental impact of NFTs on Proof-of-Work blockchains (Harper, 2022).

Meanwhile, the promotion of NFTs and their associated cryptocurrencies continues to increase, regardless of the criticisms over the social, ethical, and environmental impact of these technologies. This paper adds to this discourse by examining NFT technologies against the Association for Computing Machinery's (ACM) Code of Ethics; a code of ethics and professional conduct for computing professionals, rewritten in 2018 by Gotterbarn et al. (2018). The ACM is the largest and oldest professional organisation in the computing and technology field, and has a longstanding commitment to ethical conduct (Association for Computing Machinery, 2022). It is likely that some, if not many, practitioners in the area of blockchain technologies are members of the ACM, therefore they are subject to this ethical code; regardless, it provides a reasonable benchmark and set of considerations for ethical behaviour within the field (as discussed in the Analysis Framework section).

This paper firstly explains the technology behind NFTs; critically analyses the social and ethical impact of blockchain technology and cryptocurrencies and NFTs against the ACM's Code of Ethics; finally it provides some recommendations for policy-makers, potential investors, and others wishing to get involved in NFTs. It is worth noting that the crypto space (blockchain, cryptocurrencies, NFTs, and other blockchain technologies) is still a rapidly emerging set of technologies, subject to volatility in development, spending, and uptake. Thus, while academic papers have been referenced to wherever possible, a lot of the cutting edge work in both development and criticism of these technologies is largely in the non-peer-reviewed "grey literature" and commercial media such as blogs, online newspaper articles, and whitepapers.

Background

To understand the social and ethical impacts of NFTs, it is firstly important to understand the infrastructure upon which NFTs are created, bought, and sold.

Blockchain and cryptocurrency

A blockchain is a distributed ledger that records all transactions made. It is publicly available, and duplicated across multiple computers (peers) which validate the transactions made in order to prevent fraudulent updates of the ledger. To a large degree, it is essentially an immutable public, distributed database with verified entries that cannot be updated or removed, just added to. The block is an entry (with some data and a unique hash assigned to it); the chain is the way these blocks are linked together – each block contains the hash from the previous block (Nakamoto, 2008). This provides the security mechanism to know that no errant entries have been made into the blockchain and the trustworthiness associated with that (Sriman et al., 2021).

There are different types of blockchains, differentiated mainly on how the entries are validated. Validation occurs through peer consensus. One peer will act as the validator, and the others will double check the validation action; if correct, the validator will receive a reward of cryptocurrency specific to that chain; if incorrect (e.g. attempting to insert false data), the validator will lose their reward and whatever they have put toward validating (this depends on which kind of chain it is). How the peers are chosen to be validators, and what they put up to become the validator are the distinguishing factors between different types of blockchains. For example, in Proof-of-Work (PoW) chains such as Bitcoin and pre-Merge Ethereum, peers compete with one another to solve increasingly complex mathematical puzzles for a cryptocurrency reward (Ethereum.org 2022a; Nakamoto, 2008). Since the hardware to solve these puzzles uses a lot of energy, there is an incentive both in the reward and in the cost of that energy use to not falsify the answer; the increase in difficulty of these puzzles and thus the energy cost to solve them is a built in feature of the blockchain, aimed at restricting inflation (Sriman et al., 2021). Pre-Merge, energy costs for a single Ethereum transaction stood at 238.22 kWh, compared with 148.63 kWh for 100, 000 VISA transactions (de Best, 2022a); Bitcoin is even worse at 2258.49 kWh per transaction (de Best, 2022b). For Bitcoin, and other Proof-of-Work blockchains, these numbers will only continue to rise as well, given the requirement for the puzzles to increase in difficulty over time.

For Proof-of-Stake (PoS) chains such as Tezos,[4] Cardano,[5] Solana,[6] and the recent Ethereum 2.0 PoS implementation[7] instead of using computing power to compete for validation claims, peers put forward an amount of the native cryptocurrency for the blockchain (the 'stake') and an algorithm chooses from the list of stakers in proportion to the value of their cryptocurrency holdings (this exact decision-making algorithm can change slightly depending on the blockchain) (Tasca & Tessone, 2019). For example, in Ethereum's post-Merge PoS implementation, validators have to stake 32 ETH (Ethereum's cryptocurrency), or become part of a staking pool that can make up the 32 ETH from multiple participants. A random staker is awarded the task of validating the transaction, so the more entries of 32 ETH stakes a single person puts forward, the more likely they are to be picked. Other peers then double check the work of the validator; the validator receives their stake back along with a reward of more ETH if the validation is approved. If there are problems with the validation of the transaction, for example, if the validator tries to manipulate the result, that staker will lose their ETH stake. This provides a high level of security without needing the specialist hardware required for validating Proof-of-Work blockchains (Ethereum.org 2022b).

Security concerns still exist for both PoS and PoW blockchains, mostly through consolidation of mining (PoW) or staking (PoS) by a small number of people. If a particular pool of miners or stakers takes over more than 51% of the cryptocurrency there is an opening for them to reverse or halt transactions, or to double-spend coins (Frankenfield, 2021). However, in PoS blockchains, this is considered to be more risky than in PoW, as it would be very expensive to execute, and would also

[4] https://tezos.com/ (Accessed 3/3/2022)

[5] https://cardano.org/ (Accessed 3/3/2022)

[6] https://solana.com/ (Accessed 3/3/2022)

[7] https://ethereum.org/en/upgrades/ (Accessed 3/3/2022)

likely cause the value of the cryptocurrency to drop. Indeed, in an instance where this opportunity opened in Bitcoin, the miners instead co-operated altruistically rather than take advantage of this exploit (Blackburn et al., 2022). However, this altruism was not replicated in newer PoW blockchains: because mining is linked to hardware requirements and there are significant chip shortages (Sweney, 2021), the hardware requirements of PoW could prevent competitive mining pools from emerging at all. This has already happened with several PoW-based blockchains, including Bitcoin SV (Bambrough, 2021).

These underlying blockchain ledgers theoretically allow for safe and secure transactions of the native cryptocurrencies and other blockchain entities (including NFTs) involved without the need for those transferring to trust the party at the other end of the transfer. Cryptocurrencies can be bought and sold without parties needing to take part in the validation exercises; due to the unregulated nature of the blockchain and the fact that cryptocurrencies have no intrinsic value, they are inherently speculative in value, in that the value is determined by the supply of cryptocurrency available for sale and the demand for that cryptocurrency (Lapin, 2021). This attracts investors who are not interested in using the cryptocurrency as an actual currency, but to “use it as a hedge against inflation, or as an investment vehicle” (Lapin, 2021). This effect is so pronounced in cryptocurrency that Elon Musk’s tweets about Bitcoin and Dogecoin significantly affected the price of both these coins on multiple occasions (Bambrough, 2022; Molla, 2021). Significant crashes of cryptocurrencies in mid-2022 caused high losses amongst those less savvy in the most effective way to play the crypto “game”, and particularly later investors that might have been inspired by media hype and celebrity endorsement (Yaffe-Bellany et al., 2022). Despite this volatility, eager investors continue to jump on – or hold on to – the cryptocurrency bandwagon, hoping to make it big, to catch the next big coin at an early stage (Alzahrani & Daim, 2019), or to recoup losses made in large crashes (Binder, 2022a).

Critique of blockchain technology (Dierksmeier & Seele, 2020; Golumbia, 2016, 2020; Tang et al., 2019; Walch, 2015) and researching the blockchain (DuPont, 2021) have so far primarily focused on cryptocurrencies and underlying blockchain technology rather than NFTs specifically, or do not stem from an ethical-philosophical framework (as identified by Hyrynsalmi at al., (2020)) hence the focus of this paper on an ethical critique of NFTs.

Non-Fungible Tokens

Non-Fungible Tokens (NFTs) are a record of digital ownership of a unique item. They come in the form of a token placed on a blockchain that records that ownership and some other information. These properties are encapsulated by the term “non-fungible” which means that the token is unique and can only be owned by one person. In contrast, fungible tokens are those which are interchangeable with other tokens, such as physical coins or cryptocurrency (Ethereum.org 2022c). Items that can be represented by NFTs include digital items such as artworks, collectibles, and music; other items that might, for example, come with a certificate or proof of ownership can also theoretically be “tokenised”, such as property or vehicle title deeds, tickets to events, etc. (Wilson et al., 2021). Other proposals for NFTs include them being used for health records (Kostick-Quenet et al., 2022), signatures (Smart Token Labs, 2022), and other personal data (Uribe & Waters, 2020).

Due to the distributed nature of the blockchain (and its increasing size over time), only a small amount of data can actually reside on the ledger: for Proof-of-Work blockchains like pre-Merge Ethereum, the larger the NFT, the more expensive it becomes to “mint” (create and log it on the blockchain). Minting charges (“gas” on Ethereum) are directly linked to the amount of work required to process the NFT; Proof-of-Stake blockchains like Polygon can offer a “gas-free” minting charge as the energy use is negligible. Post-Merge Ethereum will still charge gas fees, as the number of transactions per second is a limiting factor and the fees operate as a way to distribute the transactions away from peak times. However, they have remained much lower post-Merge (Redman, 2022). As a result of the limitations on size, NFTs are usually a combination of data about the item (for example, a link to an image) and a smart contract (which contains some code that can be used to govern what happens when the transaction occurs). The data about the item is usually a link to the asset, or information about the asset, or similar. While some NFT minters also use distributed blockchain-based file storage, for the most part most NFTs still rely on third parties to host files. This is likely to cause problems with the longevity of the NFT as the links need to be maintained; the immutability of the blockchain means that links cannot be updated (Kastrenakes, 2021b), and artists who have been finding their works lifted and minted as NFTs without their permission and no payment for their work have fought back by launching copyright claims against the file hosts (Beckett, 2022). Smart contracts usually have some information about how the fee paid for the transfer of the NFT is distributed (for example, if the author maintains a royalty agreement). Smart contracts have the potential to be quite powerful, but they are also unable to be tested prior to being rolled out onto the blockchain, which, due to the immutability of the blockchain, means that they can’t be updated should a bug be found. This has led to several problematic instances of smart contract bugs being exploited (Orcutt, 2018a). Similarly, specific smart contracts have been constructed that would steal money or NFTs from wallets if the NFT they are attached to is interacted with – NFTs can simply be sent to any wallet without the requirement of the owner to agree to the transaction. Due to the open nature of the blockchain, anyone can see where transactions of high value NFTs and cryptocurrencies are placed, and those wallets can become targets. To protect against these attacks, marketplaces such as OpenSea have had to change how their wallets work by hiding “gifted NFTs from an account’s page by default if they’re from unverified collections” (Clark, 2021).

It is important to note that purchasing a NFT of an asset like a piece of artwork does not convey any copyright or other special rights to the holder of the NFT unless it is agreed as part of the smart contract. This caused a lot of consternation amongst early NFT holders of collections such as the Bored Ape Yacht Club who claimed they owned the intellectual property of the art and were mocked by people making copies of the digital artworks and reposting them (Morse, 2021). In fact, the copyright issues are far more complex and by default would likely only protect the rights of the creator of the asset in the NFT; not the minter, purchaser, or seller (unless they are also the creator) (Fisher, 2019). Many of the implications of “ownership” of NFTs are still working their way through the legal systems in different countries; as yet this is still a cutting edge area of law. For example, the Bored Ape owner and actor Seth Green was making a TV show based on the Ape that he owned: in early May 2022 that NFT was stolen and it is now in a legal grey area where Green may no longer be able to use the character in the series due to the licence for the IP remaining with the current holder, regardless of how that holder came to acquire it (Binder, 2022b).

NFTs are one of the primary parts of the “Web 3″ movement, which aims to move away from centralised internet services to a blockchain-based decentralised world wide web; initial ventures that have been realised include video games that feature trading of NFTs as a key aspect of play. Games such as CryptoKitties[8] and Axie Infinity[9] (and their many derivatives) allow players to “play to earn” by collecting, buying, selling, and minting new NFT characters within the game. This has been a controversial move within the video game industry, with issues around the balance of the economy between play to earn players and pay to play players (Friedman, 2022), potential gambling relation (Scholten et al., 2019; Serada, 2020), accessibility of the games to those without much initial capital (and exploitation of those who come in under “sponsorship” methods) (Elafros, 2021; Friedman, 2022), and, overall, what the nature of games should be – should they ultimately be purely

[8] https://www.cryptokitties.co/ (Accessed 9/3/2022)

[9] https://axieinfinity.com/ (Accessed 9/3/2022)

entertainment or offer some people the opportunity to have a game be a (frequently stressful) job? On the other hand, proponents would argue that play-to-earn games can provide low income workers with alternative revenue streams and ways for dedicated gamers to be extrinsically rewarded for their time spent in-game, and bring "digital identity, assets, and ownership into players' hands" (Brambilla Hall & Baier-Lentz, 2021).

NFTs have been the focus of many discussions around fraud and theft, some of which have been mentioned previously. This is largely due to the speculative nature of NFT "investments" in which people buy NFTs not because of their intrinsic artistic (or other) value but in terms of what the NFT might be worth in the future. In terms of fraud, "rug pulls" are frequent occurrences where a group that aims to mint a large collection of NFTs will hype up what these NFTs will be used for – for example, as assets for a forthcoming video game, tickets to concerts, claim tickets for cars and other physical goods, and even access to celebrities (Princess, 2022). Once they have convinced enough people to buy into the scheme, they take the cryptocurrency generated by the sales of the NFTs and cash out, leaving the participants with nothing but the initial NFT that was bought, which is likely to be worth a lot less than what they purchased it for. Rug pulls are so frequent that an entire section of the "Web 3 is going just great" website is devoted to them with billions of dollars of cryptocurrency associated with rug pull scams alone (White, 2022a). Wash trading is another common issue in NFT sales, wherein minters will create artificial demand by buying and selling between different wallets they have set up themselves. One such high profile case was Melania Trump's NFT collection (Pearson, 2022); the LooksRare marketplace has reportedly generated over USD$8bn due to wash trading (Hayward, 2022), this is due largely to the marketplace offering rewards in its own cryptocurrency for high frequency traders. "Whitelisting" is another problematic insider aspect of NFT sales, wherein a select group of investors is chosen by the sellers to buy in at a reduced price before the main release of the sale with the ability to reap significant rewards by re-selling at the peak of the sale. Whitelisted users who sell their NFTs in this way gain a profit around 75% of the time, compared with 21% for non-whitelisted users (Ossinger, 2021).

One of the key components of the NFT ecosystem is hype, which drives trading (Sarkar, 2022). Much of the hype around NFTs is fuelled by "fear of missing out" (Financial Conduct Authority, 2022) on potential futures: increase in value, or utility. Key utility claims include as tokens to allow entrance to or interact with Web 3 implementations (e.g. items in video games), for interacting with the real world (through giveaways, as tickets to events, etc.), or to govern real world entity interactions (e.g. monitoring wildlife, carbon credits, planting trees, title deeds to properties, identity tokens, etc.). Key value claims are based on the relationship with the underlying cryptocurrency, i.e. that the value of the NFT will increase such that the owner will be able to sell it at a profit, or on the bragging rights that come with the exclusivity of ownership of a NFT within a limited collection (for example, those that might have others owned by celebrities and high-profile people (e.g. with the Bored Ape Yacht Club and similar series)). Celebrity connection bragging rights aside, NFT value claims are often hypothetical and frequently based on fictional projections in order to drive sales that serve to inflate the value of the NFT, the NFT collection and/or the underlying cryptocurrency (Dash, 2021). Most of the utility claims are already feasible with existing technology (Lielacher, 2022); one of the key challenges to NFTs currently is the lack of use cases that are only possible or are improved in implementation using NFT technology rather than using already-existing methods. There could well be some utility to NFTs that help prevent fraudulent asset transfer (e.g. concert tickets or similar), but as of writing, these use cases are still future promises rather than current reality (Moore, 2022; Plant, 2022), and require significant infrastructure and buy-in for them to displace existing methods for fraud prevention.

There are other emerging uses for blockchain technology that are linked with NFTs and cryptocurrencies; for example, Decentralised Autonomous Organisations (DAOs), which assign voting tokens to members based on how much cryptocurrency they have invested and use this method to decentralise ownership of the organisation to the members which then govern the direction of the DAO (Ethereum.org 2022d). These are outside the scope of this paper.

Research questions

Based on the background and motivation above, the key research question this paper addresses is:

RQ1: Are Non-Fungible Tokens (NFTs) ethical technologies?

Secondary questions that derive from this are:

RQ2: What ethical issues do NFTs raise, according to professional ethics standards?

RQ3: How might Non-Fungible Tokens (NFTs) be implemented in such a way as to mitigate any ethical concerns?

Analysis framework

This section will introduce and contextualise the framework that will be used for the analysis of blockchain and cryptocurrency technology as they relate to Non-Fungible Tokens: the Association for Computing Machinery Code of Ethics and Professional Practice.

ACM code of ethics

The Association for Computing Machinery was founded in 1947 and is the largest computing society for computing professionals with over 100,000 members (Association for Computing Machinery, 2022). By "computing professionals" the ACM attempts to draw in as broad a range of people who use computers in a meaningful way as part of their job, including education and research. The ACM Code of Ethics and Professional Conduct (known as "the Code") (Gotterbarn et al., 2018), was last updated in July 2018, in response to the changes in industry and society since the previous version from 1992, using a large-scale, international approach to capture both member and non-member understandings of professional practice within the computing sector (Brinkman et al., 2017; Gotterbarn et al., 2017). In the words of the ACM, the Code "identifies the elements of every member's commitment to ethical professional conduct. It outlines fundamental considerations that contribute to society and human well-being and those that specifically relate to professional responsibilities, organisational imperatives, and compliance with the Code" (Association for Computing Machinery, 2022). This ethical framework was chosen for this research due to a) its relatively recent renewal; b) the broad range of disciplines that it covers within the computing sector; and c) because there is a high likelihood that some members are engaged in research, education, or professional development or deployment of blockchain technologies including NFTs. The ACM Code has also been adopted or endorsed by national and international organisations for computing professionals such as the International Federation of Information Processing (IFIP, 2020; Kreps, 2020) which makes it widely accepted across the international computing field. Codes of Ethics and other similar documents such as the IEEE Code of Ethics (IEEE, 2020), a "technologist's Hippocratic Oath", such as in Abbas et al., (2019), or similar organisational approaches are either too vague or too specialised in a particular subfield of technology, such as health technologies (UK Department of Health & Social Care, 2021) or software engineering (Gotterbarn et al., 1997) for the purposes of this analysis. Although the less specific ones could be useful for analysis, the ACM Code provides the best balance of specificity and generalisability that would allow for an emergent technology to be analysed. Given the variety of backgrounds, professions, and educational levels of actors within the NFT sector, it could be questioned why a professional society's code of ethics is the at all appropriate to use. The ACM Code was specifically designed to encompass all types of industry – small, medium, and large; research and teaching at all levels; aspiring computing professionals (e.g. students of all types); and those working in voluntary roles such as on open source projects or hobbyists (Brinkman et al., 2017). It was designed to reflect "the diversity of the activities computing professionals are involved in" (Gotterbarn et al., 2017): for example, closed-source, open source, Free software, for-profit, and not-for-profit projects, teaching, learning, research, development, etc. Therefore, as a framework for the development of any technology, the ACM Code is well-suited for use for analysis as the technology developed is likely to (or should) have professionals (whether established or aspiring) involved in the creation of it, and as a reflection of the conscience of that profession (Gotterbarn et al., 2017), these professionals should be able to use it as a basis for ethical interrogation of the technology they are developing.

It is important to note that within the cryptosphere there are frequent claims about the future potential of NFTs and blockchain technologies. For example, claims about future environmental impact (for example solving carbon credit mismanagement), or future benefits to society. This paper will address some of these arguments throughout the analysis, but not every argument about potential future benefits of NFTs will be entertained because these usually involve significant changes away from the status quo that are far from being implemented. I am more interested in the current state of NFTs and how they fare under the ACM Code of Ethics than potential future implementations. A series of recommendations will be set forth in the final section of the paper, based on the analysis within; those wishing to implement NFTs will likely benefit from considering these prior to implementation. Some of these recommendations may also align with proponents' arguments about future potential; however, they may not be implementable unless significant other changes are made. This does not mean that NFTs should be implemented in the meantime. Indeed, one of the key requirements in technology ethics is to be able to decide *not* to implement a technology on ethical grounds. Therefore an ethically and socially-conscious professional asked or wishing to become involved in implementation of NFTs should very carefully consider this analysis and these recommendations prior to becoming involved in the project. Finally, this analysis stems from a critical perspective – while there is much literature on the potential benefits of blockchain technologies (including NFTs), there is a lack of academic critical analyses (Hyrynsalmi et al., 2020). Thus this paper takes on a critical ethical perspective using the ACM Code as its framework for analysis.

The Code itself comprises 4 sections – general ethical principles, professional responsibilities, professional leadership principles, and compliance with the Code. For the purposes of this analysis, the first three sections will be the ones focused on; the fourth is primarily for dealing with the compliance aspects of a Code of Ethics – promotion of the Code and reporting of violations. The third section, professional leadership principles, will be dealt with as a whole; this section tends to be more company/project organisational in nature in terms of management, so the aspects of the Code that apply to NFT projects in particular will be treated as a whole. This paper will focus on a general analysis of the issues surrounding NFTs and their ecosystem according to these principles.

Analysis

This analysis makes use of the ACM's Code of Ethics and Professional Conduct ("the Code" or "the ACM Code" henceforth) (Gotterbarn et al., 2018). The Code will be used for a general theoretical analysis around the ethics of the NFT landscape on an ethical principle-by-principle basis.

Ethical analysis - ACM code of ethics

As the preamble to the Code states, it "is not an algorithm for solving ethical problems; rather it serves as a basis for ethical decision-making. When thinking through a particular issue, a computing professional may find that multiple principles should be taken into account, and that different principles will have different relevance to the issue". With this in mind, the analysis will step through each principle in the first and second sections and assess its relevance to the NFT ecosystem and what, if any, ethical issues (both positive and negative) arise in the context of that principle. Not all principles may be so relevant, and some may raise more concerns than others; similarly, several issues are cross-cutting through several principles and are likely to be more detailed in the earlier principles than later ones: this may mean that in the following analysis, some principles might appear to be more discussed than others. This is as intended. The third section, as discussed above, will be treated holistically, given its more organisational leadership angle, and the final section will not be discussed at all as it pertains to ACM membership and enforcement of the Code.

Section 1: general ethical principles

This section will be dealt with principle by principle.

Principle 1.1: contribute to society and to human well-being, acknowledging that all people are stakeholders in computing

The first principle of the ACM Code puts societal good and human well-being at the centre of any computing technology. In the NFT space, this is questionable: there appears to be little to be gained in terms of human well-being other than through gains in capital, and that is generally at someone else's loss. This would also be in direct violation of the clause that states that "the needs of those less advantaged should be given increased attention and priority" when interests of different groups conflict – those who have power in these systems are those who already have high levels of capital to work with; those more vulnerable are more likely to be left in debt following fraud, a rug pull, or even simple volatility in the system that causes big (or insider) traders to cash out (Horowitz, 2021; Kale, 2021). This risk was considered so problematic in the UK, that the Financial Conduct Authority sent out a warning to consumers about the high risks involved, advising that consumers "should be prepared to lose all their money" (Financial Conduct Authority, 2021).

Proponents generally argue that cryptocurrencies and crypto-assets are in their infancy (Gailey & Haar, 2022), and will provide significant future benefits to society, for example, encouraging development of green energy sources, providing financial services to those without (often termed "banking the unbanked"), providing accountability to service providers (for example, carbon offsets, trade, etc.), and other future potential societal good. The Crypto Altruism website[10] has listings of projects that aim to provide social good through cryptocurrencies, "crypto philanthropy" and crypto-assets. Indeed, there are successful efforts in these spaces, largely with permissioned (private) blockchains, for example through IBM (2022). However, the underlying technological reliance on speculative cryptocurrencies, the environmental impact of the largest blockchains (discussed below), and the social inequalities promoted by public blockchains have undermined the socially beneficial aspects of these efforts, and make it difficult to evaluate the potential of these projects. For example, the World Wildlife Foundation NFT effort (discussed earlier) hid the reality of the environmental impact of its offering; efforts to "bank the unbanked" through cryptocurrencies such as stablecoins have left vulnerable people suffering significant losses during the mid-2022 crash (Binder, 2022a); and many crypto philanthropic efforts undermine the causes they claim to support (see below). A NFT-based play-to-earn fitness app called StepN that styles itself as a "Web3 lifestyle app", which could be argued to be socially beneficial, requires the purchase of NFT "sneakers" that wear out over time.[11] Purchasing "sneakers" adds a low level "earning"

[10] https://www.cryptoaltruism.org/ (Accessed 23/07/2022)

[11] https://stepn.com/ (Accessed 23/07/2022)

capacity which relies on a constant influx of new players, causing it to be likened to a Ponzi scheme (Hernandez, 2022). Many of these efforts could be created without blockchain technologies underlying them, and indeed, most of the examples on the Crypto Altruism website are copies of existing technology that has some sort of appeal to earning cryptocurrency (either through speculative purchases or play to earn) added to it. Monetary incentives to get fit or set up an alternative financial system might work for some people to engage in good faith, but they also cause an inequality amongst those who do engage – as was seen in Axie Infinity with the two classes of players, the exploited and exploiters – and this assumes that the monetary incentive is legitimate, which, as we often see in this space, it is not. Even with the arguments about decentralisation of the financial markets or appeals to returning control of data to individuals that we saw earlier, given that this utopia has not eventuated in over a decade and is unlikely to eventuate given the technical and societal problems inherent to blockchain technologies, it is only a very generous reading that would state that public blockchain technologies such as NFTs could possibly be used to be primarily beneficial to society and human well-being, rather than to increase one's monetary investments (with perhaps a social or ethics-washing effort through philanthropic cuts of sales or profit).

There are also concerns about the mental health of cryptocurrency and NFT traders, with traders experiencing anxiety and stress as a result of the volatility of the sector (Sharma, 2022). While some NFTs purport to support mental health causes (Erickson, 2021; MoonWhips, 2021), they are still reliant on speculative trading on the NFTs themselves (in fact, MoonWhips, whose NFT project donates 10% of revenue per sale to mental health charities, claims their NFTs will "drive you to the 📈 [emoji chart going up] 🌕 [emoji moon]", cryptosphere slang for making a lot of money). This, coupled with the trading of the underlying cryptocurrency used to power the blockchain they are minted on, could perpetuate or exacerbate the stress and/or anxiety of those who are involved even while handing proceeds to charities that support people in this situation.

Finally, the digital divide between those with knowledge of how to use crypto-based technologies and those without is problematic for arguments for inclusion of "all people [as] stakeholders" (Kelly, 2021b).

Alongside human well-being, this principle also presents specific requirements of computing professionals to protect the environment and "promote environmental sustainability". As discussed in the Background section, there are significant energy use issues with the implementations of blockchain technologies that work on a Proof-of-Work validation model. While the move to Proof-of-Stake and other lower-energy cost validation methods is within the ethical obligation of the Code, side-chains and other methods that reduce the environmental impact of PoW-based blockchains, such as Polygon has been to pre-Merge Ethereum, are likely not sufficient responses given their reliance on the perpetuation of PoW-based blockchains. Now that Ethereum has moved to a PoS-based blockchain implementation, this aspect is far less problematic, but PoW-based NFT-supporting blockchains still exist (forks of pre-Merge Ethereum, for example). To a lesser degree, the normalisation of blockchain technology and integration of it in places where existing technology (e.g. databases, peer-to-peer networks) is already sufficient could also potentially increase this negative impact if that normalisation leads to more uptake of PoW-based blockchain technologies. Blockchain technology proponents make the argument that the uptake of cryptocurrency and crypto-assets on PoW-based blockchains will fuel an increase in development of renewable energy sources and efficiency. While there are significant PoW mining operations around the world that use renewable energy sources, the outpacing of available renewable sources by the increased energy requirements for mining has, over time, led to a decrease in renewable energy use as a total percentage of energy sources for PoW mining (Schinckus, 2021), with non-renewable sources of energy being reactivated or increased to fuel the energy requirements of mining. The banning of mining in China and the energy crisis of 2022 have also caused more pressure on sources of renewable energy (Hinsdale, 2022), with "dirty" energy sources now coming back online in the US and other parts of the world to fuel the demand. The increase in demand for energy that is built into the PoW blockchains and the lack of regulation on what sources are used to drive them are key issues for the technology underlying NFTs when it comes to their obligations under this principle of the Code.

Principle 1.2 Avoid harm

Harm, according to the ACM Code, means "negative consequences, especially when those consequences are significant and unjust". It includes "unjustified physical or mental injury […] and unjustified damage to property, reputation and the environment". The energy cost of PoW-based blockchains has already been well discussed in the Background and in Principle 1.1; it is well-established that in order to reduce the effects of climate change it is necessary to reduce the carbon footprint of human activity (Ivanova et al., 2020). Given the differences between energy requirements for traditional transactions and PoW-based blockchains, there is no real justification for increased use of energy for these, especially when lower-energy versions exist. Thus, using existing PoW chains (or side-chains that require the existence and proliferation of PoW chains) would be in violation of this principle.

Similarly to Principle 1.1, this principle raises the issue of mental harm; the fundamental nature of investing in cryptocurrency and other blockchain-enabled investments is the volatility of it and this would be difficult to change. Donations to mental health charities is one way to potentially off-set these issues, but if the offering also feeds into the hype cycle that causes the harm in the first place, it is essentially charity-washing a problem caused by itself.

Finally, harm can be caused by taking advantage of vulnerable people's desperation and taking their money without returning on the promises made. This has already been discussed in terms of "rug pulls" and other forms of fraud that are frequent within the cryptosphere, but increasingly in other blockchain-using technologies such as "play to earn" games we are seeing manipulation of the market and hacks that are also leaving vulnerable people, particularly in developing countries, without the income they require to live. An example of this has been seen recently in the Axie Infinity hack, where over $600 m worth of cryptocurrency was drained from the reserves required for people playing to earn in the game to cash out into fiat currency (White, 2022b). Sky Mavis, creators of Axie Infinity, have promised to reimburse their players (Servando & Lagerkranser, 2022), but aren't regulated to be required to have insurance or to repay any lost funds. There is little chance of retrieving the stolen funds as well, so Sky Mavis will need to raise external funding to fulfil their promise. Meanwhile, the play to earn players, mostly from low socio-economic-status countries such as the Philippines, are without their source of income due to there being no way to cash out their earnings from the game (McGregor & Gordon, 2022; Servando et al., 2022). Heavier regulation of such games would mitigate this potential harm, though it would also likely remove the motivation to play, which is based around seeing growth in investments over time which supports and requires the market volatility that causes other harms in the first place.

Principle 1.3 Be honest and trustworthy

Blockchain technology was developed to be trustless, meaning that "it does not require the participants of the network to trust each other" (Pandey & Litoriya, 2021). However, this does not mean that developers who implement these technologies or who build systems on top of them can avoid the requirements for their own honesty and trustworthiness. Principle 1.3 states that "a computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties". This is regularly violated by blockchain-enabled technologies like NFTs, with the drive to hype up new projects in order for there to be significant initial uptake so that investors make money from them a large part of the sales pitch for the NFT “drop”. For example, as discussed in the background section above, investors in NFT projects regularly have no idea what they have bought (Morse, 2021), and those being contracted for their labour often do not understand the ramifications (Hissong, 2022). While this is not required by the technology itself, it is part of bringing a collection of NFTs to market in order to gain the best return on investment for these initial investors, rather than to ensure sustainability of the project in the long term. This gain for initial investors is not usually disclosed to later investors, who might assume from the initial high sale prices that their purchases will hold their value or increase, thus the transparency and limitations requirements of the Code are not adhered to.

Smart contracts within NFTs are limited in that they cannot be changed once registered on the blockchain, which can bring security risks due to poor programming (Halaburda et al., 2022). This is especially problematic because smart contracts are “difficult to agree upon and design”, and “require unambiguous digital input […] thereby limiting the scope of situations they can handle” (Halaburda et al., 2022). Thus, “edge cases” or mitigating circumstances would be hard to deal with; something about which developers implementing these algorithms within NFTs should be transparent. Instead, the jargon used in discussing cryptocurrencies and NFT technologies is often used as a gatekeeping mechanism to identify members of in-groups and out-groups within the community (Davis, 2021; Kale, 2022), obscure techno-jargon is also used to disguise the reality of intentional fraud or impossible claims about the capabilities of the technology (Sharma et al., 2022). Such lack of transparency in terms of limitations or obscuring claims would be in violation of this principle.

This principle also requires computing professionals to be “forthright about any circumstances that might lead to either real or perceived conflicts of interest or otherwise tend to undermine the independence of their judgement”. The reliance of NFTs on cryptocurrency-based blockchains means that developers usually have a vested interest in promoting the cryptocurrency and blockchain as well as the NFT sale itself in order for them to reap as large a reward as possible from the sale. This constitutes a significant conflict of interest, especially when techniques such as wash trading (sales between accounts held by the same person at increasingly high prices to falsely increase the perceived value of the NFT) are used so frequently (for example, with Melania Trump’s series of NFTs (Pearson, 2022)). Such behaviour to artificially inflate the value of the NFT or its underlying cryptocurrency token would be in violation of this principle.

Finally, a strong statement from the Code in this principle requires that “commitments should be honoured”. The lack of regulation within the NFT space and the cryptosphere along with the way that blockchain technology is built (while transfers are validated, they are only validated cryptographically, rather than checked to ensure that the transfer was intended) means that there is no recourse for those who lose their funds or assets through theft or fraud. As mentioned previously, the UK financial regulator has issued warnings to this effect (Financial Conduct Authority, 2021) though people are still losing investments and those responsible are avoiding liability. As seen in the Axie Infinity hack in the previous principle, although Sky Mavis wants to refund their players, there is (as yet) no obligation to do so and no recourse for those whose funds have been lost. Similarly, with fraudulent or “rug pull” scams, those in charge of the projects are not adhering to this principle of the Code – many NFT projects have overly ambitious roadmaps that are not realistically achievable, for example, promising video games despite not having a team capable of delivering one (for example, (White, 2022c, 2022d)). Once again, this sort of activity is in violation of the Code.

Principle 1.4 Be fair and take action not to discriminate

Amongst other values, fairness, equality and justice are the keys to this principle. Crypto proponents like to think that blockchain technologies promote fairness and equality through decentralisation and a free market economy. The libertarian, crypto-anarchic ideology (Ludlow, 2001) behind the development of cryptocurrencies such as Bitcoin (Nakamoto, 2008) certainly persuaded those with similar attitudes toward traditional financial systems to invest with promises of economic freedom. The “wild west” of the cryptosphere today continue to benefit from this unregulated environment. However, it is increasingly apparent that the desired aim of decentralisation and the free market has a) not happened, in that new centralised systems have sprung up to respond to inherent problems within the technology (such as usability), and b) has caused significant problems in terms of inequality. As discussed in previous principles, a result of this is that justice is not easy to come by in terms of recourse, which is specifically required in this principle: “fairness requires that […] processes provide some avenue for redress of grievances”.

In terms of fairness, this principle promotes the “fair participation of all people, including those of underrepresented groups”. In NFT-based systems such as play to earn video games, however, although there is participation of underrepresented groups, it is largely those with significant capital who benefit. In Axie Infinity, for example, there is a two-tier system whereby rich players “loan out” Axies to those who can’t afford the startup fee, then take a cut from their labour within the game (these are called “scholarships” in game). In fact, this is the way these players “play” the game – they earn through the labour of those they have employed without doing much themselves. For those who are the labourers, in Axie Infinity’s case largely poor people in developing countries (McGregor & Gordon, 2022), they are essentially doing meaningless busy-work to improve the investment portfolio of those who employ them. They are certainly not playing “for fun”, which might be expected for a game, nor are they playing to earn in the same way as those with large amounts of capital. Worse still, the game requires constant streams of new capital to come into the game, these largely come from the lower tier of players with higher tier players generally overselling the profits that could be made from playing as part of their “scholarship” in order to convince them to join up as part of their group. This style of recruitment and its reliance on “community” and hyping up of potential profits has drawn commentary as to the similarities between play to earn games and pyramid schemes, or multi-level marketing schemes (Armughanuddin, 2021; Keller, 2021).

Finally, it is in this principle that harassment and bullying are addressed, in that they “[limit] fair access to the virtual and physical spaces where […] harassment takes place”. Unfortunately for blockchain technologies, they are potentially very effective spaces within which bullying and harassment can take place. Public blockchains store every piece of information sent to them for as long as the blockchain continues, including images, messages, and information about transactions. These entries are immutable, meaning that they can’t be removed from the blockchain once they are listed. Even though cryptocurrency wallet addresses can be kept private, they would need to be given up to pay for goods and services, and movement of cryptocurrency around different wallets can still be followed. Significant technical acumen is required to obscure movement of funds once a wallet address is known (White, 2022e). In terms of NFTs, once a wallet address is known, an abuser could use this knowledge to “airdrop” NFT images or video into the wallet, because there are no restrictions on who can send crypto assets to other wallets. There are no ways to block senders in the cryptosphere. And once a NFT is created on the blockchain there is no way to remove it, and with certain blockchain-based file servers (e.g. IPFS[12]), there is no way to remove the file that NFT might point to (Ravenscraft, 2022a). We have already seen messages sent to hackers pleading with them to return cryptocurrencies (Quiroz-Gutierrez, 2022), child abuse images uploaded to the blockchain (BBC BBC News, 2019), NFTs with restrictive smart contracts (Ravenscraft, 2022a) and harmful NFTs airdropped into peoples’ wallets (Clark, 2021), so these possibilities are very real.

[12] https://ipfs.io/ (Accessed 08/07/2022)

Principle 1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts

This principle revolves around the idea that "those who expend […] effort should expect to gain value for this work". As mentioned in the introduction, there is widescale exploitation of artists within this space, despite the fact that NFTs were originally intended to free artists from exploitation and allow them to continue to receive royalties beyond the initial sale of their works. Indeed, Anil Dash, one of the joint creators of the first NFT, reflects: "Technology *should* be enabling artists to exercise control over their work, to more easily sell it, to more strongly protect against others appropriating it without permission. […] But nothing went the way it was supposed to" (Dash, 2021). Some artists have, indeed, benefited from NFT sales, such as Beeple (Kastrenakes, 2021a), but these tend to be exceptions rather than rules, with most artists who do control their own collections only making small amounts of money after fees (if any at all) (Kinsella, 2021). The shortcut that Dash and artist Kevin McCoy took with the first NFT – to not actually include the artwork as part of the information uploaded to the blockchain, and instead to simply include the link to an external hosting site – became the default, and this causes the main problem with NFTs as they stand: reliance on an external site that is likely to disappear within the decade, and the re-centralisation of authority over verification of ownership of that artwork (Dash, 2021). While file systems such as IPFS are offering distributed storage that theoretically works with this, many NFT services cannot resolve IPFS links natively (IPFS, 2022), so still rely on external HTTP URLs to serve the gateway information, so if the provider disappears, the link may also disappear or be manipulated (Wareing, 2021).

Another problem with art in the NFT space has been rampant copyright infringement, with sites such as DeviantArt being scraped for artwork that unscrupulous NFT minters used to create sets of artworks to sell to unknowing buyers (Williams, 2021). However, the protections DeviantArt implemented are minimal – they simply alert artists when their art has been found on large platforms. It is then up to the artist to file takedown notices, relying on the goodwill of the market platforms to regulate their users and comply with takedown notices (Kelly, 2021c) (thus recentralising what should be a decentralised platform once again). This also requires technical skills on the part of the artist, many of whom get caught up by the complex jargon and difficult usability of the multiple different strands of the cryptosphere. A similar lack of technical understanding allows artists engaged to work with NFT projects to be left out of royalties for future sales and other potential returns on their work: royalty payments are not in NFTs by default (Ravenscraft, 2022b). The complex programming required for smart contracts that are needed to implement these policies means that artists who want to check the actual status of the contract that has been entered needs to have good programming skills as well.

Principle 1.6 Respect privacy

The blockchain is, by design, not a privacy-preserving technology. With all transactions publicly recorded on the ledger, while participants might be able to remain pseudonymous, they are not ever truly anonymous and can often be traced due to the nature of the transactions they make and publication of wallet addresses for transaction purposes (Roberts, 2022). Public facing accounts attached to wallets such as on OpenSea, which display ownership of a collection of NFTs, might also link to social media accounts or provide more information about the person who owns the wallet. If this is extended to include personal information such as health data, ownership of "real world" assets such as houses or cars, or other such proposed use for NFTs, this could become very problematic from a privacy perspective. The immutability of the blockchain amplifies these issues, given the personal nature of this data, and is likely to violate various privacy laws around the world such as the GDPR and the UK Data Protection Act.

Even encrypting the data prior to putting it on the blockchain has a limited shelf life (Roberts, 2022). Encrypted data accessible to the public is more easily attacked than when it has other levels of security protecting it. Once again, immutability means that once that data is put on the blockchain, there is no removing it, even if it is or is likely to be compromised. Some companies, such as Aleo[13] attempt to resolve this using "zero-knowledge proofs" (ZK). Instead of the data itself being shared on the blockchain for verification purposes with another entity, proof of verification is shared – "a way to prove something to someone without revealing any of the information that goes into that proof" (Sirer, in Orcutt, 2017). However, this is only useful for certain situations, mostly verifying the validity of transactions, rather than, for example, smart contracts or storage of assets on the chain.

Given the above, blockchain technologies including NFTs are likely to violate this privacy principle in the Code because the data cannot be modified or deleted, could potentially violate privacy with merging of datasets (or transaction sets), and might be more vulnerable to compromise even if theoretically secured. Some potential solutions might help with certain kinds of data on the blockchain, but these are not widely taken up yet and do not suit all kinds of data.

Principle 1.7 Honour confidentiality

This principle specifically pertains to computing professionals and confidential information. It is unlikely that blockchain technology would be used to specifically store confidential information, but it is important to point out, once again, that the immutability of the blockchain means that if confidential information is (accidentally or otherwise) lodged onto it, or if encrypted confidential information on the blockchain is compromised, there is no way for it to be removed.

Confidentiality comes up in discussions around NFTs in other ways, however, specifically in terms of insider trading and "whitelisting". In USA vs. Nathanial Chastain, the defendant allegedly took advantage of his position in the trading marketplace OpenSea to take advantage of confidential insider information and benefit himself (United States Department of Justice, 2022). This misuse of confidential information would be a significant breach of the Code of Ethics. Whitelisting, although not illegal like insider trading, is not far from insider trading in its concept. NFT projects will often invite known "VIP" people to mint NFTs early on, or before a general release. This then allows those whitelisted people to make more of a profit in the general release if the project does well. There are guides on how to join whitelists, such as in Khan (2022). Thus, those with time, money, and connections within the NFT world are likely to profit more at the expense of those who only come in at the general release. This creates an inequity in the creation and sales of the NFTs and arguably can amount to misuse of confidential information depending on how easy it is to become part of a whitelist group.

Section 2: professional responsibilities

This section will be dealt with principle by principle, as it concerns individual professional responsibilities when working on NFT projects.

Principle 2.1 Strive to achieve high quality in both the processes and products of professional work

The first of the Professional Responsibilities principles requires that computing professionals "insist on and support high quality work from themselves and colleagues". This has been frequently seen to not happen within the NFT ecosystem: the poorly programmed smart contracts have been exploited for theft and fraud; poor quality software running the marketplaces and exchanges hacked or exploited; shoddy design of games and game economies causing significant problems for vulnerable people who use them have all been discussed previously. Even the art itself that is depicted in NFTs is often very poor quality – Wikipedia refused to include NFT art in their lists of "most expensive artworks by living artists" (Francombe, 2022). The lack of quality of the products in

[13] https://www.aleo.org (Accessed 08/07/2022)

the cryptosphere is largely due to the "gold rush" type effect that has been seen in the space – companies rushing to get their NFTs out (some examples amongst many include (Craig, 2022; James, 2021; Neal, 2022)), or to turn around a product to meet venture capital funding goals or to scale it up to meet demand (Volpicelli, 2022).

NFT minting problems are intensified by the lack of ability to fix any bugs due to the immutability of the blockchain. One game, "Wolf Game", could not patch an exploit they discovered, so instead had to recreate the whole game from scratch (Adams, 2021). The lack of ability to fix bugs should impose a greater responsibility on the programmers of the smart contracts; however countless examples continue to show that speed is prioritised over testing and evaluation of short and long term impacts of the smart contract and other blockchain-related code (White, 2022f).

Principle 2.2 Maintain high standards of professional competence, conduct, and ethical practice

The key issue to highlight from this principle is "Professional competence […] requires skill in communication, in reflective analysis, and in recognizing and navigating ethical challenges". From many of the examples shown so far, we can see that this is frequently not the case in the cryptosphere. Over-technical jargon, designed to obscure the reality behind blockchain technology and act as a gate-keeping exercise or hype enabler (White, 2022g), is frequently deployed. For example, pre-Ethereum Merge, the Polygon blockchain website[14] was not at all geared toward those who do not understand blockchain technologies, and they capitalised on this to convince charities that they are a low-carbon, "green" blockchain despite requiring the PoW-based Ethereum blockchain to function, resulting in social media backlash that caused the charities to cancel their plans for NFTs (Extinction Rebellion, 2022; Seabrook, 2022). The way the whole blockchain system works precludes reflective analysis, simply because once established, there are very few ways to roll back the systems or change their course (other than all participants agreeing to stop using/perpetuating the chain). The exceptions, unfortunately, tend to involve fraud or other scams such as rug pulls, and thus show the lack of ability to navigate ethical challenges. Those who proactively take on the challenge issued in this principle tend to steer clear of blockchain technologies (for example, those who responded to prominent computer scientist Jorge Stolfi's viral tweet (2022)), due to the technical and social issues associated with them. Employees and user-bases push back against their companies adopting NFT approaches, such as in the case of Ubisoft (Schreier, 2022); a partial list of other video game companies withdrawing their NFT approaches is detailed in Franzese (2022). Thus we are more likely to see adherence to this principle from employees in the context of NFTs.

Principle 2.3 Know and respect existing rules pertaining to professional work

Principle 2.3′s key focus is on understanding how ethical reflection fits in with the law and regulations, as well as "policies and procedures of the organizations to which the professional belongs". It advocates challenging unethical rules, but taking responsibility for any violation if challenging is not successful in changing the rule.

In some countries where there is a large population without bank accounts, local currency is devaluing, or where foreign currency restrictions exist yet remittances from their diasporas are frequent, cryptocurrencies have flourished due to their comparative ease of access, cost to use, and stability compared with traditional banking. In cryptosphere parlance, this is termed "banking the unbanked". Nigeria, for example, had a significant crypto economy before it banned bank transfers to and from cryptocurrency exchanges and launched its own digital currency (not a cryptocurrency), the eNaira (Salami, 2021). The obvious concern to countries around the regulation of currency and ability to control inflation and other economic aspects through a central banking service has led to other countries looking to crack down on the use of more decentralised cryptocurrency and provide their own e-currency solutions as well, such as China (Kharpal, 2022) and the UK (Ashvil, 2022). However, despite official sanctions, cryptocurrency trade continues. There is also a significant movement to bring NFTs to these countries through emerging artists (Ndukwe, 2022) and play-to-earn games such as Axie Infinity, mentioned previously. If this principle were to be implemented directly by those who develop NFTs, they would avoid targeting countries where trade of cryptocurrency is prohibited. However, this is difficult given the nature of the blockchain. Many who work in blockchain technology argue that cryptocurrencies and other blockchain technologies are actually liberating populations that are under repressive financial regimes, and thus this violation of this particular principle would be ethically justified. Certainly some of the efforts put forward by crypto companies, such as microfinance loans, tracking of water, biodiversity, and other environmental impacts, and digitising real world assets may have some benefits to local communities (Pinto, 2019). However, these can all be done without blockchain technologies – and the disadvantages of blockchain, particularly the speculative investment requirements of the underlying cryptocurrencies, could significantly offset these benefits (particularly the environmental ones that rely on PoW blockchains). Thus, any company wishing to employ blockchain within developing countries needs to consider the broader impacts, and not just the benefits of "banking the unbanked" or challenging unethical law. These can also be done in ways that don't require blockchain technologies, e.g. through well-established mechanisms such as M-Pesa[15] for "banking the unbanked" and don't subject vulnerable populations to highly volatile cryptocurrencies.

Another example in this area is the flourishing of parts of the cryptosphere that take advantage of the lack of regulation in the area, as has been detailed previously with regard to things like insider trading, fraud, advertising high returns, and other problematic aspects of NFTs and cryptocurrencies. While regulation is starting to catch up (United States Department of Justice, 2022), these examples illustrate that it is important to not just follow the literal text of these principles but also the spirit of them – NFT assets that act like securities should be managed in the same way as other securities, if they were to be handled responsibly, even if they are not specifically classified as such (Benson, 2022) – for example, as the law is likely to catch up.

Overall, this principle is likely to be quite contentious within the cryptosphere, with advocates claiming that challenging existing financial regulation and institutional law is morally acceptable, and those opposed pointing out the broader harms of blockchain technologies that do not offset the benefits of implementation. What is important here is not only looking at this from a pure perspective of blockchain but whether there are alternatives to investigate that also challenge unethical rules that don't have the same negative impacts that blockchain technologies have. If a scenario arises where there is recognisable harm being done and blockchain technology is the only way to avoid this harm, then it might be ethical to deploy it. However, such situations are yet to arise, despite the hype surrounding the possibilities of blockchain technologies such as NFTs.

Principle 2.4 Accept and provide appropriate professional review

This principle calls for peer and stakeholder review of technologies that are to be developed and/or deployed. Like with testing, review once a NFT project is live can be difficult to act upon. However, more fundamentally, critical review can occur in general – this paper forms a type of critical review of the ethics of this technology, for example. Companies are pulling out of blockchain technologies following stakeholder review as well (as detailed previously). There is some tension between the "crypto sceptics" and those developing the technologies,

[14] https://polygon.technology/ (Accessed 08/07/2022)

[15] https://www.safaricom.co.ke/personal/m-pesa (Accessed 08/07/2022)

with the former claiming the latter is ignoring the problems inherent to the technology in order to make money (Zeitchik, 2022). This sort of review may be difficult for those who develop the technology to engage with, but it is important that they do – if only to ensure that their technology develops in such a way that prevents the problems raised.

Principle 2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks

A key component of this principle is that "computing professionals should strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives". As discussed throughout this paper, we see a general trend within the NFT ecosystem to specifically ignore alternatives, not describe the systems in easy-to-understand language, and to have explicit conflicts of interest when it comes to objectivity in evaluation of NFT systems due to stakes in the underlying cryptocurrencies used on their blockchains. Specific examples of lack of adherence to this principle include the previously mentioned Polygon chain convincing the World Wildlife Fund and Extinction Rebellion charities to produce series of NFTs despite the environmental damage caused by the Ethereum blockchain (Extinction Rebellion, 2022; Seabrook, 2022). Similarly, general misleading advertising of returns on investment in NFTs combined with a lack of accessible technical explanations and social media influencer promotions of NFTs have meant that many people buying them do not understand what it is that they have bought, leading to unreasonable expectations of ownership (Morse, 2021) and general misconceptions of how much money they might make in the future (Hughes, 2022). New laws are coming in to regulate misleading advertising in the crypto-sphere, but, for example in the UK, NFTs are harder to more generally regulate than cryptocurrency or other "crypto-assets" (BBC BBC News, 2022). However, even in the UK sales of NFTs that promote a specific return on investment are starting to be investigated by the Advertising Standards Authority, such as in the case of an English footballer promising "my NFTs will be the first ever that can't lose their initial value", which was deemed to be misleading to consumers (BBC BBC Sport, 2022). This, of course, links back to Principle 2.3 as well.

Principle 2.6 Perform work only in areas of competence

At the height of the NFT boom, NFT drops were announced often with roadmaps for the things the NFTs would be useful for, for example, video games, tickets to exclusive events, and other things. However, it soon became clear that apart from the art for the initial NFT minting process, many companies advertising NFTs did not have the expertise required to deliver on their roadmaps. One such example is Pixelmon,[16] which raised cryptocurrency equivalents of USD$70 m on the promises made by the team. The NFTs were supposed to be part of a Pokemon-style open world game, with holders of the NFTs able to claim land, set up shops, design and build houses, and other virtual world activities. However, when the NFT minting process began, it was clear that the company did not have the ability to deliver on their promises (Boom, 2022; White, 2022d). After the backlash, they promised to spend money on improving the art and delivering on their roadmap, but the results of this are yet to be seen. Generally speaking, NFT-based games have largely been very poorly implemented in terms of actual gameplay – when the market for Axie Infinity crashed, there were very few players only playing for fun, rather than to make money. Similarly, newer games like Grit have been lambasted in the gaming community for its poor gameplay and art (Switzer, 2022), despite being backed by a major video game company (Epic). This has mirrored a trend of game developers shunning the idea of crypto in games, and subsequently refusing to take jobs in the area out of principle. According to GDC's State of the Game Industry survey, 70% of game developers said they and their studio were not interested in NFTs (GDC, 2022). Thus there is only a small pool of developers who want to become involved in the NFT game space, leading to less experience available to the many NFT projects that promise games. NFT companies planning on including a video game as part of their roadmap should ensure they are capable of delivering on their roadmaps and able to hire the required people for them. If they do not have people competent to deliver the roadmap, they should remove that aspect of the roadmap prior to the minting process.

Similarly with smart contract programming, as discussed earlier, poor programming of these can lead to significant issues further down the line. If a team does not have the skill or capacity to implement these accurately, tested as much as is possible, and monitored for potential compromise, then they should not do so.

Principle 2.7 Foster public awareness and understanding of computing, related technologies, and their consequences

Alongside a requirement for general encouragement of "understanding of computing", this principle requires sharing of technical knowledge in a "clear, respectful, and welcoming" way with the general public, including limitations, vulnerabilities, and opportunities (Gotterbarn et al., 2018). We have seen a lot of focus from NFT projects on the opportunities, but little on the limitations or vulnerabilities. We have also seen the lack of accessibility of information in terms of the jargon involved, often deliberately obscuring poor quality implementations of the technology. The outcomes of this poor communication and focus on opportunities over limitations and vulnerabilities are captured by the impact of the mid-2022 crash on amateur investors (Kale, 2022) who bought into the jargon and hype, assuming that those building these platforms were professionals and knew what they were doing. Indeed, the computer scientists and other professionals who pushed back against this technology (in keeping with the final statement in this principle, that professionals should "respectfully address inaccurate or misleading information related to computing") were denigrated as not knowing what they were talking about, or similar negative responses, such as in the crypto-asset community's responses to Stolfi's tweet stating that "Every computer scientist should be able to see that cryptocurrencies are totally disfunctional [sic] payment systems, and that "blockchain technology" (including "smart constracts [sic]") is a technological fraud. Would they please say that out loud?" (Stolfi, 2022). For example, a NFT avatar project creator, cory.eth, wrote in response, "@JorgeStolfi I guess we're all listing our degrees under this thread. So my math and computer science degree says you're an idiot. But really the argument you're an idiot isn't based in computer science or math. It's based on economics and markets" (cory.eth, 2022). This is one of many examples of similar responses from NFT and related cryptocurrency and crypto-asset creators' responses to the tweet from Stolfi and similar critical responses and quote tweets of Stolfi's tweet by other computer scientists and computing professionals. As this Code shows, being able to be critical of a technology prior to, during and after deployment is essential to ensure that it will serve the public good. Responses such as name-calling or casting aspersions on the professionalism or credentials of those who criticise are not conducive to achieving this aim.

Principle 2.8 Access computing and communication resources only when authorized or when compelled by the public good

This principle isn't so relevant to the NFT sphere, although the airdropping of NFTs with malware in their smart contracts or as a vehicle for harassment or abuse (as discussed in Principle 1.4) into a public wallet would constitute a breach of this principle. The key responsibilities related to NFT projects in this area are better dealt with in Principle 2.9, which follows.

Principle 2.9 Design and implement systems that are robustly and usably secure

Blockchain security is complex but operates on several levels – the cryptographic, the infrastructural, and the socio-technical. At the cryptographic level, it uses well-known algorithms that are currently best

[16] https://pixelmon.club/ (Accessed 08/07/2022)

practice in security. However, at the infrastructural level, there are more complex pathways that are required to ensure protection from malicious actors, such as Sybil attacks, 51% attacks, and other network-level attacks (Aggarwal et al., 2021; Orcutt, 2018b)). While these are well known potential problems for blockchain, the solutions to them are generally where discussions about security in blockchain ends (Orcutt, 2018b). The lock of usability of blockchain, as discussed several times before, precludes usable security as required by this principle, which has led to problems involving smart contracts, bridges between blockchains, wallet implementations, and other efforts at developing the blockchain beyond its simplest form. Much of this development has recentralised the socio-technical systems and brought with them opportunities for exploitation of the speed at which these implementations have been built (to keep up with the hype), the lack of expertise involved (see Principle 2.6), and the ignorance of the userbase as to the underlying technological implications (see, e.g. the misunderstandings over the smart contracts discussed previously in several sections). Nabben (2021) argues that there are “trust and security shortcomings at the micro and meso-organisational levels” in blockchain and that the “code is law” approach is insufficient to provide the appropriate level of security for most users. While security issues at all levels are often addressed, with the immutability of the blockchain technology, sometimes this requires more complex solutions than an upgrade or bug fix – for example, “hard forks” or complete withdrawals of NFT projects (as discussed earlier in Principle 2.1). Similarly, all too often, the damage is already done, as was seen in the Axie Infinity hack, and users have little recourse to claim damages or reimbursement of funds (Kale, 2021, 2022). It is clear here that adherence to this principle is poorly thought through at a socio-technical level, and often implemented after significant harms are already done.

The final statement of Principle 2.9 is that “in cases where misuse or harm are predictable or unavoidable, the best option may be to not implement the system”. Many of the examples throughout this analysis would fit into this category; though some could be better mitigated by more thoughtful implementation of security and harm avoidance. With the fallout from the mid-2022 crypto crash playing out as of writing, and the numbers of hacks registered on the “Web3 is going just great” website (White, 2022a), it is clear to see that many of these systems do not adequately adhere to this principle.

Section 3: professional leadership principles

This section will be dealt with holistically, as it mostly concerns higher level responsibilities that leaders bear within their organisations and may not apply to all professionals within the NFT development space.

As with Principle 1.1, the key message within this set of principles is to ensure that people are always the central concern within computing. Section three (3.1) reiterates this requirement in terms of ensuring that projects keep the public good as a key consideration when “evaluating tasks associated with research, requirements analysis, design, implementation, testing, validation, deployment, maintenance, retirement, and disposal” (Gotterbarn et al., 2018). It is clear from the previous analysis that, for the most part, this does not happen within the NFT space. NFT projects are largely driven by the desire to make money before anything else, often with over-exaggerated returns on investment and other exploitative practices engaged in to develop hype and encourage investors. We have seen how the nature of the blockchain prevents adequate testing and validation, causing problems for deployment; similarly so with maintenance and retirement of blockchain-based technologies – the immutability of the blockchain means that it is very hard to practically implement these vital aspects of ethical technology development and deployment in a fair and equitable way; the alternative is, for most blockchains, the hard shut down of the blockchain involved or the blocking of trade on that blockchain by exchanges.

The leadership principles also encourage projects to be transparent and of high quality (3.2) – the pseudonymity largely employed by teams developing NFT projects is encouraged by the platforms and part of the “decentralised” ethos and original goal for anonymity of the underlying cryptocurrency projects precludes full transparency. The unmasking of the founders of the Bored Ape Yacht Club caused much consternation within the NFT world; but the ability to do due diligence prior to investing large amounts of money is a fairly standard requirement for trust and accountability (Notopoulos, 2022) – though crypto project founders such as Soona Amhaz suggest that pseudonymous companies that use blockchain technologies are more transparent than most companies as all transactions are published on the blockchain (Notopoulos, 2022). While this might be helpful for companies that have only ever used blockchain, it doesn’t solve the issue of the founders themselves or companies that have operated prior to blockchain technologies. Other issues to do with transparency discussed earlier include the issues of misrepresentation (e.g. in Principle 2.2) of blockchains such as Polygon as being environmentally friendly, when in reality they relied on the energy-intensive pre-Merge PoW Ethereum chain. NFT projects that charity-wash the underlying problems that exacerbate poor investment decision making by ignorant and/or vulnerable people also violate these requirements for transparency (as discussed in Principle 1.1).

Systems modification and retirement has a special section in this set of principles as well (3.6) – the “rug pulls” and other scams that have left people wondering where their investments have gone are notably problematic in this regard. However, in the mid-2022 market crashes, we have also seen problems for entire blockchains and platforms such as stablecoins (e.g. Terra/Luna (Song, 2022)) or crypto exchanges and investment platforms (e.g. Voyager (Shubber, 2022)) – where graceful migration for users have not been thought about, let alone implemented. The assumption that the blockchain will continue forever is presupposed by most initiators of blockchains; no contingencies have been made for owners of NFTs should the blockchains carrying these be shut down. This is problematic because if those blockchains start to hold information more important than ownership of art or other collectibles, then it could lead to the loss of that data. Similar problems emerge if usable NFTs stop being supported by the companies that implemented the utility of them, especially if these assets were touted as being “portable”. With portability a key selling point, it is key to examine the claims made: while there is no implicit ethical issue with being able to take assets from one game to another, there are significant technical issues that appear to be largely hand-waved over by crypto enthusiasts. So far, there are no games that successfully implement portability between companies, let alone with assets from different game engines; and this is even before dealing with the intellectual property rights involved. And “traditional” gamers are not enthusiastic about NFTs: for example, in Ubisoft’s Ghost Recon Breakpoint, cosmetic assets sold through their Quartz NFT market (based on the Tezos blockchain) or earned through gameplay was a complete flop – with almost no interest (Tassi, 2021). Ubisoft stopped supporting the NFTs and developing the game further, leaving those players with the much hyped collectibles without any demand for them. This, however, strikingly illustrates the key issue with NFT assets in games – portability, even for simple cosmetic items, requires a lot of overheads by game developers, including legal and intellectual property agreements, translation into different art styles (if not engines), and other implementation complications that is likely to be a barrier to this desired portability. Additionally, functional assets such as weapons etc. would need to be balanced appropriately in games other than the ones they were developed for. Finally, when thinking about the end of life of NFT assets, the ACM Code states that developers should “investigate viable alternatives to removing support for a legacy system. If these alternatives are unacceptably risky or impractical, the developer should assist stakeholders’ graceful migration from the system to an alternative” (Gotterbarn et al., 2018). Understanding what this means for those who spent time and/or money gaining desirable assets is complex. Multiplayer games such as action games/looter-shooters etc. rely on "seasons" or expansions which render players' previously earned gear largely obsolete. How does this work for NFT assets that are supposedly earned and worth money? As with the non-game NFT market, the "greater fool" left holding the asset will likely be upset with having spent money prior to a planned obsolescence of that asset (which also, don't forget, cannot be updated once it is on the blockchain due to immutability of NFT smart contracts). This ultimately links in with the issues surrounding Dishonesty as discussed above. Promising portability, usefulness, etc. of items (whether cosmetic or functional) is likely to end up being problematic for both developer and player.

Finally, with the push toward basing the next iteration of internet user experiences on blockchain and NFTs (Web 3.0 or metaverse, depending on who is talking about it), it is vital that companies involved in this transition (if it happens) take note particularly of Principle 3.7 "Recognize and take special care of systems that become integrated into the infrastructure of society". So far we have not seen much to be confident that companies have the public good as their key interests in moving toward this potential future; this will need to change rapidly as "as the level of adoption changes, the ethical responsibilities of the organization or group are likely to change as well", and particularly focusing on access to systems "for those who may have been excluded" (Gotterbarn et al., 2018). This includes financial exclusion as well as technical; with the potential for transactional-based forms of service provision excluding those without the capital to establish themselves within the service (or who might need to "buy in" through other means, e.g. giving away personal information, labour, etc. as was done in Axie Infinity).

Ultimately, if NFT markets settle down and the companies involved become more established beyond the initial hype, a great deal more work is needed for them to become ethically responsible in their work toward the public good. Arguably, with an initial set up that relied on exploiting vulnerable people (through investment or labour or otherwise), this is largely impossible, but there may be a second generation of companies that wish to avoid these issues, in which case their leaders must take on these principles responsibly and ensure that their offerings remain open, fair, transparent, and well-planned rather than jumping on a hype-led bandwagon that only offers hypothetical futures.

Recommendations and conclusion

This paper has examined the background, implementation, and multiple examples of NFT development, deployment, and use across different application vectors, according to a professional ethics framework – the ACM Code of Ethics (RQ2). The ethical issues that arise are summarised in the recommendations below, where mitigating factors are suggested, but include issues of harm, well-being, discrimination, fairness, intellectual property rights, privacy, quality of work, competence of those involved, legal issues, the ability to give and receive critical review, lack of education for users, personal gain over public good, security, maintenance and end-of-life for NFT ecosystems, and ensuring the public good is the key concern when developing, deploying, and maintaining NFTs. Further research should monitor the future claims of NFT proponents, particularly when it comes to the environmental impact of post-Merge Ethereum based NFTs, the privacy and security aspects of NFT-based infrastructure, and future solutions to some of the problem raised above that have been mooted but remain unimplemented or currently impossible given existing technology.

In terms of RQ1, whether NFTs are ethical technologies, ultimately, it is recommended that NFTs are avoided. Instead, traditional technologies should be used to create the experiences desired, which are likely to result in no significant loss to the average user (other than those who want to speculate using the cryptocurrency underlying the NFT). However, should a company find a use case that has absolutely no other technical method for implementation other than NFTs, some key recommendations (RQ3) emerge from the analysis and discussion above, with links to some of the relevant principles included.

These key recommendations are, to respond to RQ3:

1) If NFTs must be used, and there is no other technical way to deliver the desired experience, avoid public blockchains that rely on environmentally destructive methods for validations (Principles 1.1, 1.2, 2.3, 2.5).
2) If NFTs must be used, have a plan for long-term support of any NFTs, whether aesthetic or functional, and/or have a way for players to exit ownership gracefully in a fair and equitable way (Principles 1.4, 3.6, 3.7).
3) If NFTs must be used, have a plan in place for potential for regulation of this space. We are already seeing NFTs being regarded as investment securities and other financial assets that are more heavily regulated than traditional collectibles. Be realistic, open, and transparent about the potential for returns on investment, and respect the spirit of regulation and existing laws as well as their word (Principles 1.3, 1.5, 2.3, 3.2, 3.7).
4) If NFTs must be used, ensure that smart contracts and platforms are developed to an extremely high quality, and have test spaces that allow for appropriate testing (whether this is possible may be a stopping point for the project). Be realistic and transparent with potential users with roadmap deliverables and timelines and consult with experts in milestones prior to planning (Principles 1.1, 1.3, 2.1, 2.2, 2.4, 2.6, 2.7, 3.1, 3.2, 3.6, 3.7).
5) If making a NFT game or application that is advertised as "play to earn" or "play and earn", ensure that the most vulnerable players are not exploited by other players, that they are protected from fraud, hacks, and volatility of the underlying cryptocurrency, and that any other potential risks are appropriately consented to (and not just disclosed). Similarly, if your platform requires some kind of "buy in" to engage with it, ensure that those who might be left out have some other means of entry that does not involve them being exploited (Principles 1.1, 1.2, 1.3, 1.4, 2.7, 3.2, 3.6, 3.7).
6) Be wary of storing personal, confidential, and other sensitive data on a public blockchain, even if encrypted. Consider the worst-case scenario if that encryption were to be broken or keys stolen, and whether that data may need to be updated or deleted (and not just appended to) in the future. Also be wary of "link rot" for hyperlinks stored in NFTs, of the potential impact of poor smart contract programming, and of the potential of your NFT project to be used for harassment purposes or illegal material (Principles 1.6, 1.7, 2.8, 2.9, 3.1, 3.7).
7) Consider the risks to your company of engaging with the NFT space: alienation of the user and developer base, changing what it means to engage in your company's product – e.g. for playing games, removing the "fun" aspect, especially for vulnerable people, or turning it into a vector for exploitation by those with capital, potential for hacking and fraud, and other risk factors such as IP rights, regulation of crypto-assets, etc. (all Principles).

Reflection using an approach such as the ACM's Code of Ethics should be a key part of engaging in the setup and planning of any NFT project. Inability to fulfil any of the above recommendations or a more in-depth analysis may well make the project impossible. Developing a responsible, ethical approach to the project requires the flexibility to *not* engage in development of an NFT-based project should it become impossible to find a way to solve or mitigate the ethical responsibility. Reflection at too late a stage will likely lead to financial or momentum pressure on continuing with the project. Therefore, this should be an initial step and engage with a wide variety of stakeholders in order to ensure that pre-existing biases can be exposed and mitigated along the way. Finally, as stated at the beginning of the ACM Code, the above recommendations are not a replacement for specific ethical reflection on a project, but as a starting point: "when thinking through a particular issue, a computing professional may find that multiple principles should be taken into account, and that different principles will have different relevance to the issue. Questions related to these kinds of issues can best be answered by thoughtful consideration of the fundamental ethical principles, understanding that the public good is the paramount consideration" (Gotterbarn et al., 2018). Only through an honest analysis of the specific project, with the public good (rather than the deployment of the project) kept at the forefront, will there be a possibility for an ethical NFT project.

Funding

This work was supported by the Tides Foundation on the recommendation of Unity Charitable Fund [grant number TF2201-105180].

Declaration of Competing Interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

The author was involved in the rewriting of the ACM's Code of Ethics and Professional Conduct. The author is a member of the ACM's Committee on Professional Ethics.

The author received funding for this project from the Tides Foundation on the recommendation of Unity Charitable Fund [grant number TF2201-105180].

Acknowledgements

Thanks to David Zendle and Anders Drachen for proof reading and thoughtful discussions of the issues.

References

Abbas, A. E., Senges, M., & Howard, R. A. (2019). A hippocratic oath for technologists. In A. E. Abbas (Ed.), *Next-Generation ethics* (pp. 71–80). Cambridge: Cambridge University Press.

Adams, R. N. (2021). *Wolf game highlights the challenges of nft game development [WWW document]*. TechRaptor. URL https://techraptor.net/gaming/news/wolf-game-highlights-challenges-of-nft-game-development (accessed 6.10.22).

Aggarwal, S., & Kumar, N. (2021). Chapter twenty - attacks on blockchain☆☆working model. In S. Aggarwal, N. Kumar, & P. Raj (Eds.), *Advances in computers, the blockchain technology for secure and smart applications across industry verticals* (Eds., pp. 399–410). Elsevier. https://doi.org/10.1016/bs.adcom.2020.08.020.

Alzahrani, S., & Daim, T. U. (2019). Analysis of the cryptocurrency adoption decision: literature review. In *2019 Portland International Conference on Management of Engineering and Technology (PICMET). Presented at the 2019 Portland International Conference on Management of Engineering and Technology (PICMET)* (pp. 1–11). IEEE. https://doi.org/10.23919/PICMET.2019.8893819.

Armughanuddin, M. (2021). *Play to earn nft games like axie spark pyramid scheme debate [WWW document]*. DualShockers. URL https://www.dualshockers.com/play-to-earn-nft-games-like-axie-spark-pyramid-scheme-debate/ (accessed 4.1.22).

Ashvil, Z. (2022). *Britcoin is coming. the treasury is woefully underprepared [WWW document]*. Wired UK. URL https://www.wired.co.uk/article/britcoin-treasury-currency (accessed 3.25.22).

Association for Computing Machinery, (2022). About the ACM organization [WWW Document]. URL https://www.acm.org/about-acm/about-the-acm-organization (accessed 3.15.22).

Bambrough, B. (2021). *Bitcoin fork suffers 'Massive' 51% attack in attempt to 'Destroy' the cryptocurrency, sending its price sharply lower [WWW document]*. Forbes. URL https://www.forbes.com/sites/billybambrough/2021/08/04/bitcoin-fork-suffers-massive-51-attack-in-attempt-to-destroy-the-cryptocurrency-sending-its-price-sharply-lower/ (accessed 3.3.22).

Bambrough, B. (2022). *Still has 'Potential as a currency'—Elon musk gives surprise dogecoin signal after huge bitcoin, ethereum and crypto price crash [WWW document]*. Forbes. URL https://www.forbes.com/sites/billybambrough/2022/05/13/still-has-potential-as-a-currency-elon-musk-gives-surprise-dogecoin-signal-after-huge-bitcoin-ethereum-and-crypto-price-crash/ (accessed 5.31.22).

BBC News. (2019). *Child abuse images hidden in crypto-currency blockchain [WWW document]*. BBC News. URL https://www.bbc.com/news/technology-47130268 (accessed 4.6.22).

BBC News. (2022). *New laws to tackle misleading crypto-asset adverts [WWW document]*. BBC News. URL https://www.bbc.com/news/technology-60032743 (accessed 6.22.22).

BBC Sport. (2022). *Owen nft tweet deleted after contact by authorities [WWW document]*. BBC Sport. URL https://www.bbc.com/sport/football/61751366 (accessed 6.22.22).

Beckett, L. (2022). *'Huge mess of theft and fraud:' artists sound alarm as nft crime proliferates*. The Guardian. URL https://www.theguardian.com/global/2022/jan/29/huge-mess-of-theft-artists-sound-alarm-theft-nfts-proliferates (accessed 3.9.22).

Benson, J. (2022). *SEC targets nft creators, marketplaces over ICO-Like sales: Report [WWW document]*. Decrypt. URL https://decrypt.co/94268/sec-targets-nft-creators-marketplaces-ico-sales-report (accessed 6.21.22).

Binder, M. (2022a). *After crashing the crypto market, terra returns with luna 2.0. it's already tanking again. [WWW document]*. Mashable. URL https://mashable.com/article/terra-luna-2-0-airdrop-plunge (accessed 5.30.22).

Binder, M. (2022b). *Seth green's bored ape was stolen. now he can't make his nft show. [WWW document]*. Mashable. URL https://mashable.com/article/seth-green-stolen-bored-ape-nft-show (accessed 5.30.22).

Blackburn, A., Huber, C., Eliaz, Y., Shamim, M. S., Weisz, D., Seshadri, G., & Aiden, E. L. (2022). *Cooperation among an anonymous group protected bitcoin during failures of decentralization (No. arXiv:2206.02871)*. arXiv. https://doi.org/10.48550/arXiv.2206.02871

Boom, D. V. (2022). *People spent $9K on pixelmon NFTs. then they saw the art [WWW document]*. CNET. URL https://www.cnet.com/personal-finance/people-spent-9k-on-pixelmon-nfts-then-they-saw-the-art/ (accessed 6.22.22).

Brambilla Hall, S., & Baier-Lentz, M. (2021). *What play-to-earn games mean for the economy - and metaverse [WWW document]*. World Economic Forum. URL https://www.weforum.org/agenda/2021/11/what-play-to-earn-games-mean-for-the-economy-and-metaverse/ (accessed 3.9.22).

Brinkman, B., Flick, C., Gotterbarn, D., Miller, K., Vazansky, K., & Wolf, M. J. (2017). Listening to professional voices: Draft 2 of the ACM code of ethics and professional conduct. *Communications of the ACM, 60*, 105–111. https://doi.org/10.1145/3072528

Clark, M. (2021). *OpenSea fixes vulnerabilities that could let hackers steal crypto with malicious NFTs [WWW document]*. The Verge. URL https://www.theverge.com/2021/10/13/22723092/opensea-nft-vulnerability-gift-security-researchers-wallet-hack (accessed 3.9.22).

cory.eth, (2022). @JorgeStolfi i guess we're all listing our degrees under this thread. so my math and computer science degree says you're an idiot. but really the argument you're an idiot isn't based in computer science or math. it's based on economics and markets. Twitter. https://twitter.com/cory_eth/status/1522873012432760832 Date: 2022-05-07 Accessed 2022-07-14.

Craig, T. (2022). *Yuga labs botches nft drop with bad code, blames ethereum*. Crypto Briefing. URL https://cryptobriefing.com/yuga-labs-botches-nft-drop-with-bad-code-blames-ethereum/ (accessed 6.10.22).

Dash, A. (2021). *NFTs weren't supposed to end like this [WWW document]*. The Atlantic. URL https://www.theatlantic.com/ideas/archive/2021/04/nfts-werent-supposed-end-like/618488/ (accessed 4.6.22).

Davis, B. (2021). Inside the NFT rush: entrepreneurs promise NFTs will destroy the gatekeepers. *While jockeying to become the new gatekeepers [WWW document]*. Artnet News. URL https://news.artnet.com/opinion/nft-rush-part-2-2039452 (accessed 4.1.22).

de Best, R. (2022a). *Ethereum energy consumption 2022 [WWW document]*. Statista. URL https://www.statista.com/statistics/1265891/ethereum-energy-consumption-transaction-comparison-visa/ (accessed 3.28.22).

de Best, R. (2022b). *Bitcoin energy consumption 2022 [WWW document]*. Statista. URL https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/ (accessed 3.28.22).

de Vries, A. (2022). *Ethereum energy consumption index [WWW document]*. Digiconomist. URL https://digiconomist.net/ethereum-energy-consumption/ (accessed 2.25.22).

Dierksmeier, C., & Seele, P. (2020). Blockchain and business ethics. *Business Ethics: A European Review, 29*, 348–359. https://doi.org/10.1111/beer.12259

DuPont, Q. (2021). *Guiding principles for ethical cryptocurrency, blockchain, and dlt research*. Cryptoeconomic Systems 0. https://doi.org/10.21428/58320208.a8364373

Edelman, G. (2021). What is web3, anyway? Wired. https://www.wired.com/story/web3-gavin-wood-interview/ Date: 2021-11-29.

Elafros, B. (2021). *Axie infinity scholarships: How does it work and how to join one? [WWW document]*. NFT Gaming, esports event consulting & Agile Project Management. URL https://www.billelafros.com/axie-scholarships-how-does-it-work-and-how-to-join-one/ (accessed 3.9.22).

Erickson, K. (2021). *Medical student creates, auctions NFTs to promote mental health awareness [WWW document]*. Medical School - University of Minnesota. URL. https://med.umn.edu/news-events/medical-student-creates-auctions-nfts-promote-mental-health-awareness (accessed 3.18.22).

Erskine, M. (2022). *Uncertainty in the valuation of non-fungible tokens [WWW document]*. Forbes. URL https://www.forbes.com/sites/matthewerskine/2022/02/02/uncertainty-in-the-valuation-of-non-fungible-tokens/ (accessed 2.25.22).

Ethereum.org. (2022). *The merge [WWW document]*. ethereum.org. URL https://ethereum.org (accessed 9.22.22).

Ethereum.org. (2022a). *Ethereum whitepaper [WWW document]*. ethereum.org. URL https://ethereum.org (accessed 3.3.22).

Ethereum.org. (2022b). *Ethereum staking [WWW document]*. ethereum.org. URL https://ethereum.org (accessed 3.3.22).

Ethereum.org. (2022c). *Non-fungible tokens (NFT) [WWW document]*. ethereum.org. URL https://ethereum.org (accessed 3.7.22).

Ethereum.org. (2022d). *Decentralized autonomous organizations (DAOs) [WWW document]*. ethereum.org. URL https://ethereum.org (accessed 3.9.22).

Extinction Rebellion. (2022). *Extinction rebellion nft project | grants [WWW document]*. Extinction Rebellion NFT Project Cancelled. URL https://gitcoin.co/grants/4905/extinction-rebellion-nfts (accessed 6.20.22).

Farrington, R. (2021). *Crypto is everywhere, but should you invest? [WWW document]*. Forbes. URL https://www.forbes.com/sites/robertfarrington/2021/01/18/crypto-is-everywhere-but-should-you-invest/ (accessed 2.25.22).

Financial Conduct Authority. (2021). *FCA warns consumers of the risks of investments advertising high returns based on cryptoassets [WWW document]*. FCA. URL https://www.fca.org.uk/news/news-stories/fca-warns-consumers-risks-investments-advertising-high-returns-based-cryptoassets (accessed 3.18.22).

Financial Conduct Authority. (2022). *Hype – spot the signs and manage your fomo [WWW document]*. FCA. URL https://www.fca.org.uk/investsmart/hype-spot-signs-manage-your-fomo (accessed 10.5.22).

Fisher, K. (2019). Once upon a Time in NFT: Blockchain, Copyright, and the Right of First Sale Doctrine 2019 AELJ Spring Symposium: Digital Art & Blockchain. *Cardozo Arts & Entertainment Law Journal, 37*, 629–634.

Francombe, A. (2022). *Why does nft art look so bad?* Vice. URL https://www.vice.com/en/article/qjbz5m/why-does-nft-art-look-so-bad (accessed 6.10.22).

Frankenfield, J. (2021). *What is a 51% attack? [WWW document]*. Investopedia. URL https://www.investopedia.com/terms/1/51-attack.asp (accessed 3.3.22).

Franzese, T. (2022). *Every canceled video game nft project (so far) [WWW document]*. Digital Trends. URL https://www.digitaltrends.com/gaming/canceled-gaming-nft-2022-2021/ (accessed 6.20.22).

Friedman, D. (2022). *The biggest nft video game's economy is collapsing because nft games don't work*. Reason.com. URL https://reason.com/2022/02/01/the-biggest-nft-video-games-economy-is-collapsing-because-nft-games-dont-work/ (accessed 3.9.22).

Gailey, A., & Haar, R. (2022). *The future of cryptocurrency: 8 experts share predictions for the second half of 2022*. Time.

GDC, (2022). State of the Game Industry 2022 [WWW Document]. URL https://reg.gdconf.com/state-of-game-industry-2022?BLG_GDC (accessed 6.23.22).

Golumbia, D. (2016). *The politics of bitcoin: Software as right-wing extremism*. Minneapolis: University of Minnesota Press. University of Minnesota Press.

Golumbia, D. (2020). *Cryptocurrency is garbage*. So Is Blockchain. https://doi.org/10.2139/ssrn.3628519

Gotterbarn, D., Bruckman, A., Flick, C., Miller, K., & Wolf, M. J. (2017). ACM code of ethics: A guide for positive action. *Communications of the ACM, 61*, 121–128. https://doi.org/10.1145/3173016

Gotterbarn, D., Miller, K., & Rogerson, S. (1997). Software engineering code of ethics. *Communications of the ACM, 40*, 110–118. https://doi.org/10.1145/265684.265699

Gotterbarn, D. W., Brinkman, B., Flick, C., Kirkpatrick, M. S., Miller, K., Vazansky, K., et al. (2018). *ACM code of ethics and professional conduct [WWW document]*. ACM Code of Ethics and Professional Conduct. URL https://www.acm.org/code-of-ethics (accessed 10.19.22).

Halaburda, H., Sarvary, M., & Haeringer, G. (2022). Smart contracts and blockchain. In H. Halaburda, M. Sarvary, & G. Haeringer (Eds.), *Beyond bitcoin: Economics of digital currencies and blockchain technologies* (Eds., pp. 135–178). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-88931-9_6.

Harper, C. (2022). *Ethereum miners will have few good options after the merge [WWW document]*. Forbes. URL https://www.forbes.com/sites/colinharper/2022/08/21/ethereum-miners-will-have-few-good-options-after-the-merge/ (accessed 9.22.22).

Hayward, D./A. (2022). *LooksRare has reportedly generated $8B in ethereum nft wash trading [WWW document]*. Decrypt. URL https://decrypt.co/91510/looksrare-has-reportedly-generated-8b-ethereum-nft-wash-trading (accessed 3.9.22).

Hernandez, O. (2022). *Stepn founder wants to promote healthy body and mind, but skeptics question the app's sustainability [WWW document]*. Blockworks. URL https://blockworks.co/stepn-founder-wants-to-promote-healthy-body-and-mind-but-skeptics-question-the-apps-sustainability/ (accessed 7.23.22).

Hertzmann, A. (2021). *Why would anyone buy crypto art – let alone spend millions on what's essentially a link to a jpeg file? [WWW document]*. The Conversation. URL http://theconversation.com/why-would-anyone-buy-crypto-art-let-alone-spend-millions-on-whats-essentially-a-link-to-a-jpeg-file-157115 (accessed 2.25.22).

Hinsdale, J. (2022). *Cryptocurrency's dirty secret: Energy consumption*. State of the Planet. URL https://news.climate.columbia.edu/2022/05/04/cryptocurrency-energy/ (accessed 7.21.22).

Hissong, S. (2022). *The nft art world wouldn't be the same without this woman's "Wide-Awake hallucinations."*. Rolling Stone. URL https://www.rollingstone.com/culture/culture-features/seneca-bored-ape-yacht-club-digital-art-nfts-1280341/ (accessed 2.25.22).

Horowitz, J. (2021). *Crashing crypto prices spooked some new investors. others are doubling down [WWW document]*. CNN. URL https://www.cnn.com/2021/06/05/investing/cryptocurrency-investing-crash/index.html (accessed 3.18.22).

Hughes, A. (2022). *Are social media influencers misleading their followers about NFTS? [WWW document]*. BBC Science Focus Magazine. URL https://www.sciencefocus.com/future-technology/are-social-media-influencers-misleading-their-followers-about-nfts/ (accessed 6.22.22).

Hyrynsalmi, S., Hyrynsalmi, S. M., & Kimppa, K. K. (2020). Blockchain ethics: a systematic literature review of blockchain research. In M. Cacace, R. Halonen, H. Li, T. P. Orrensalo, C. Li, G. Widén, & R. Suomi (Eds.), *Well-Being in the information society. fruits of respect, communications in computer and information science* (Eds., pp. 145–155). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-57847-3_10.

IBM, (2022). What is blockchain for social good? [WWW Document]. URL https://www.ibm.com/uk-en/topics/blockchain-for-good (accessed 7.23.22).

IEEE, (2020). IEEE code of ethics [WWW Document]. URL https://www.ieee.org/about/corporate/governance/p7-8.html (accessed 3.15.22).

IFIP, (2020). IFIP code of ethics – IFIP International Professional Practice Partnership (IP3). URL https://www.ipthree.org/ifip-code-of-ethics/(accessed 3.17.22).

IPFS, (2022). Best Practices for Storing NFT Data using IPFS | IPFS Docs [WWW Document]. URL https://docs.ipfs.io/how-to/best-practices-for-nft-data/#types-of-ipfs-links-and-when-to-use-them. (accessed 4.6.22).

Ivanova, D., Barrett, J., Wiedenhofer, D., Macura, B., Callaghan, M., & Creutzig, F. (2020). Quantifying the potential for climate change mitigation of consumption options. *Frontiers of Computer Science, 15*, Article 093001. https://doi.org/10.1088/1748-9326/ab8589

James, D. (2021). *There's a html error in the $5.43M NFT representing the internet's source code [WWW document]*. PC Gamer. URL https://www.pcgamer.com/nft-internet-source-code-error/ (accessed 6.10.22).

Kale, S. (2021). *'I put my life savings in crypto': How a generation of amateurs got hooked on high-risk trading*. The Guardian. URL https://www.theguardian.com/lifeandstyle/2021/jun/19/life-savings-in-crypto-generation-of-amateurs-hooked-on-high-risk-trading (accessed 3.18.22).

Kale, S. (2022). *'They couldn't even scream any more. they were just sobbing': The amateur investors ruined by the crypto crash [WWW document]*. The Guardian. URL https://www.theguardian.com/technology/2022/jul/12/they-couldnt-even-scream-any-more-they-were-just-sobbing-the-amateur-investors-ruined-by-the-crypto-crash (accessed 7.14.22).

Kastrenakes, J. (2021a). *Beeple sold an nft for $69 million [WWW document]*. The Verge. URL https://www.theverge.com/2021/3/11/22325054/beeple-christies-nft-sale-cost-everydays-69-million (accessed 2.22.22).

Kastrenakes, J. (2021b). Your million-dollar NFT can break tomorrow if you're not careful [WWW Document]. The Verge. URL https://www.theverge.com/2021/3/25/22349242/nft-metadata-explained-art-crypto-urls-links-ipfs (accessed 3.9.22).

Keller, L. (2021). *Can axie infinity go the distance? [WWW document]*. Forkast. URL https://forkast.news/axie-infinity-play-to-earn-model/ (accessed 4.1.22).

Kelly, J. (2021a). *Crypto: Definitely not a pyramid scheme*. Financial Times. URL https://www.ft.com/content/025ea33f-7351-4d86-a1ca-b6c268f5b042 (accessed 2.25.22).

Kelly, L. (2021b). *What would a global switch to cryptocurrency mean for vulnerable people? [WWW document]*. The Big Issue. URL https://www.bigissue.com/life/money/how-would-a-world-run-on-cryptocurrency-impact-vulnerable-people/ (accessed 3.18.22).

Kelly, Z. (2021). NFT Theft is Still Plaguing DeviantArt, Despite Fraud Detection Tool [WWW Document]. Gizmodo Australia. URL https://www.gizmodo.com.au/2021/12/deviantart-nft-theft/(accessed 4.6.22).

Khan, M. (2022). Whitelists are the golden ticket to buy NFTs for cheap. Here's how to get on one [WWW Document]. Fortune. URL https://fortune.com/2022/02/28/what-are-nft-whitelists-and-how-to-get-on-one/.(accessed 6.10.22).

Kharpal, A. (2022). China launches app for its own digital currency as it looks to expand usage [WWW Document]. CNBC. URL https://www.cnbc.com/2022/01/04/china-launches-digital-currency-app-to-expand-usage.html (accessed 3.25.22).

Kinsella, E. (2021). Think Everyone Is Getting Rich Off NFTs? Most Sales Are Actually $200 or Less, According to One Report [WWW Document]. Artnet News. URL https://news.artnet.com/market/think-artists-are-getting-rich-off-nfts-think-again-1962752 (accessed 7.23.22).

Kostick-Quenet, K., Mandl, K. D., Minssen, T., Cohen, I. G., Gasser, U., Kohane, I., et al. (2022). How NFTs could transform health information exchange. *Science (New York, N.Y.), 375*, 500–502. https://doi.org/10.1126/science.abm2004

Kreps, D. (2020). IFIP Code of Ethics – David Kreps. URL http://kreps.org/academic/ifip-code-of-ethics/(accessed 3.17.22).

Lapin, N. (2021). Explaining Crypto's Volatility [WWW Document]. Forbes. URL https://www.forbes.com/sites/nicolelapin/2021/12/23/explaining-cryptos-volatility/ (accessed 3.3.22).

Lielacher, A. (2022). 6 NFT Use Cases That Will (Probably) Remain After the Hype Dies Down [WWW Document]. URL https://cryptonews.com/exclusives/6-nft-use-cases-that-will-probably-remain-after-hype-dies-down.htm (accessed 10.1.22).

Ludlow, P. (2001). *Crypto anarchy, cyberstates, and pirate utopias, digital communication* (Ed.). Cambridge, Mass: MIT Press.

McGregor, G., & Gordon, N. (2022). *Millions of players in poor countries earned real money on axie infinity. then came an economic crisis and a $620 million hack [WWW document]*. Fortune. URL https://fortune.com/2022/03/31/axie-infinity-hack-coin-price-crypto-crisis/ (accessed 4.1.22).

Molla, R. (2021). *When Elon Musk tweets, crypto prices move [WWW document]*. Vox. URL https://www.vox.com/recode/2021/5/18/22441831/elon-musk-bitcoin-dogecoin-crypto-prices-tesla (accessed 3.3.22).

MoonWhips. (2021). *MoonWhips is all about mental health in the NFT space [WWW document]*. GlobeNewswire News Room. URL https://www.globenewswire.com/news-release/2021/11/09/2329864/0/en/MoonWhips-is-all-about-Mental-Health-in-the-NFT-space.html (accessed 3.18.22).

Moore, S. (2022). *NFTs join crypto in the race to zero*. Medium. URL https://stephenmoore.medium.com/nfts-join-crypto-in-the-race-to-zero-b2dff19e1ced (accessed 10.5.22).

Morse, J. (2021). *NFT owners insist they're totally not owned by "right-click savers" [WWW document]*. Mashable. URL https://mashable.com/article/non-fungible-tokens-nfts-right-click-save (accessed 3.9.22).

Morse, J. (2022). *Jimmy fallon and paris hilton pumping their NFTs is beyond cringe [WWW document]*. Mashable. URL https://mashable.com/video/jimmy-fallon-paris-hilton-pump-bored-apes-nft (accessed 2.25.22).

Nabben, K. (2021). Blockchain security as "people security": Applying sociotechnical security to blockchain technology. *Frontiers of Computer Science, 2*, Article 599406. https://doi.org/10.3389/fcomp.2020.599406

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Ndukwe, I. (2022). *Nigerian nft artist osinachi: The work created by using a word processor [WWW document]*. BBC News. URL https://www.bbc.com/news/world-africa-59703123 (accessed 6.21.22).

Neal, J. (2022). *Did akutar nft just rug pull themselves? $34M Lost to bad coding*. NFT Evening. URL https://nftevening.com/did-akutar-nft-just-rug-pull-themselves-34m-lost-to-bad-coding/ (accessed 6.10.22).

Notopoulos, K. (2022). *We found the real names of bored ape yacht club's pseudonymous founders [WWW document]*. BuzzFeed News. URL https://www.buzzfeednews.com/article/katienotopoulos/bored-ape-nft-founder-identity (accessed 7.5.22).

NyanCat. (2021). *Nyan cat [WWW document]*. Foundation. URL https://foundation.app/@NyanCat/foundation/219 (accessed 2.22.22).

Orcutt, M. (2017). A Mind-Bending Cryptographic Trick Promises to Take Blockchains Mainstream [WWW Document]. MIT Technology Review. URL https://www.technologyreview.com/2017/11/09/3857/a-mind-bending-cryptographic-trick-promises-to-take-blockchains-mainstream/(accessed 6.10.22).

Orcutt, M. (2018a). *Ethereum's smart contracts are full of holes [WWW document]*. MIT Technology Review. URL https://www.technologyreview.com/2018/03/01/144962/ethereums-smart-contracts-are-full-of-holes/ (accessed 3.9.22).

Orcutt, M. (2018b). *How secure is blockchain really? [WWW document]*. MIT Technology Review. URL https://www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/ (accessed 7.14.22).

Ossinger, J. (2021). NFT Gains Mostly Go to Small Group of Whitelisted Investors: Study - Bloomberg [WWW Document]. Bloomberg. URL https://www.bloomberg.com/news/articles/2021-12-06/small-group-is-reaping-most-of-the-gains-on-nfts-study-shows?sref=HQB7G2wY (accessed 3.25.22).

Pandey, P., & Litoriya, R. (2021). Promoting trustless computation through blockchain technology. *National Academy Science Letters, 44*, 225–231. https://doi.org/10.1007/s40009-020-00978-0

Pearson, J. (2022). Analyzing the Very Bizarre Sale of Melania Trump's \$170,000 NFT. Vice. URL https://www.vice.com/en/article/m7vpx8/analyzing-the-very-bizarre-sale-of-melania-trumps-dollar170000-nft (accessed 3.9.22).

Pinto, A. (2019). Unbanked to big banks: How crypto facilitates financial inclusion IBM Supply Chain and Blockchain Blog [WWW Document]. IBM Supply Chain and Blockchain Blog. URL https://www.ibm.com/blogs/blockchain/2019/04/unbanked-to-big-banks-how-crypto-facilitates-financial-inclusion/(accessed 6.21.22).

Plant, L. (2022). The technological case against Bitcoin and blockchain [WWW Document]. Luke Plant's home page. URL https://lukeplant.me.uk/blog/posts/the-technological-case-against-bitcoin-and-blockchain/(accessed 6.20.22).

Princess, (2022). Crypto Twitter Outraged By "Cash-Grab" Tai Lopez NFT Collection. NFT Evening. URL https://nftevening.com/crypto-twitter-outraged-by-cash-grab-tai-lopez-nft-collection/(accessed 3.9.22).

Quiroz-Gutierrez, M. (2022). 'Crypto Robin Hood' stole \$50 million before experiencing a change of heart. Now he's asking victims to apply to get their money back [WWW Document]. Fortune. URL https://fortune.com/2022/03/31/crypto-robin-hood-50-million-theft-apply-and-get-a-refund-hacker-cashio/(accessed 4.6.22).

Ravenscraft, E. (2022a). NFTs Are a Privacy and Security Nightmare [WWW Document]. Wired. URL https://www.wired.com/story/nfts-privacy-security-nightmare/(accessed 4.6.22).

Ravenscraft, E. (2022b). NFTs Don't Work the Way You Might Think They Do [WWW Document]. Wired. URL https://www.wired.com/story/nfts-dont-work-the-way-you-think-they-do/(accessed 4.6.22).

Redman, J. (2022). Ethereum's Post-Merge Transfer Fees Remain Low, Since Mid-May High-Priority ETH Fees Are 93% Cheaper – Bitcoin News [WWW Document]. Bitcoin.com News. URL https://news.bitcoin.com/ethereums-post-merge-transfer-fees-remain-low-since-mid-may-high-priority-eth-fees-are-93-cheaper/(accessed 9.23.22).

Roberts, S. (2022). How 'Trustless' Is Bitcoin, Really? [WWW Document]. The New York Times. URL https://www.nytimes.com/2022/06/06/science/bitcoin-nakamoto-blackburn-crypto.html (accessed 6.10.22).

Salami, I. (2021). Nigeria's digital currency: What the eNaira is for and why it's not perfect [WWW Document]. The Conversation. URL http://theconversation.com/nigerias-digital-currency-what-the-enaira-is-for-and-why-its-not-perfect-171323 (accessed 3.25.22).

Sarkar, A. (2022). Beyond the NFT hype: The need for reimagining digital art's value proposition [WWW Document]. Cointelegraph. URL https://cointelegraph.com/news/beyond-the-nft-hype-the-need-for-reimagining-digital-art-s-value-proposition (accessed 10.5.22).

Schinckus, C. (2021). Proof-of-work based blockchain technology and anthropocene: An undermined situation? *Renewable and Sustainable Energy Reviews, 152*, Article 111682. https://doi.org/10.1016/j.rser.2021.111682

Scholten, O. J., Hughes, N. G. J., Deterding, S., Drachen, A., Walker, J. A., & Zendle, D. (2019). Ethereum crypto-games: mechanics, prevalence, and gambling similarities. In *Proceedings of the Annual Symposium on Computer-Human Interaction in Play. Presented at the CHI PLAY '19: The Annual Symposium on Computer-Human Interaction in Play, ACM* (pp. 379–389). https://doi.org/10.1145/3311350.3347178

Schreier, J. (2022). Ubisoft employees push back hard on blockchain initiative. Bloomberg.com.https://www.bloomberg.com/news/articles/2022-02-11/ubisoft-employees-push-back-hard-on-blockchain-initiative Date: 2022-06-18, Last accessed 2022-06-20.

Seabrook, V. (2022). WWF UK faces backlash over "destructive" plans to sell "eco-friendly" NFTs [WWW Document]. Sky News. URL https://news.sky.com/story/wwf-uk-faces-backlash-over-destructive-plans-to-sell-eco-friendly-nfts-12531042 (accessed 6.20.22).

Serada, A. (2020). Why is cryptoKitties (Not) gambling?. In *in: International Conference on the Foundations of Digital Games. Presented at the FDG '20: International Conference on the Foundations of Digital Games* (pp. 1–4). ACM, Bugibba Malta. https://doi.org/10.1145/3402942.3402985.

Servando, K., & Lagerkranser, P. (2022). Axie infinity owner 'fully committed' to reimbursing players after hack. Bloomberg.com. URL https://www.bloomberg.com/news/articles/2022-03-30/axie-owner-fully-committed-to-reimbursing-players-after-hack (accessed 4.1.22).

Servando, K., Nicolle, E., & Tran, J. (2022). Who Hurts most in \$600 million axie heist? 'Not the venture capitalists' [WWW Document]. Bloomberg.com. URL https://www.bloomberg.com/news/articles/2022-04-02/who-loses-more-in-600-miilion-axie-crypto-heist-not-venture-capitalists (accessed 4.6.22).

Sharma, R. (2022). 'Crypto ruined my life': the mental health crisis hitting bitcoin investors. Vice. URL https://www.vice.com/en/article/akvn8z/crypto-bad-for-mental-health (accessed 3.18.22).

Sharma, T., Zhou, Z., Huang, Y., & Wang, Y. (2022). It's A Blessing and A Curse. *Unpacking creators' practices with non-fungible tokens (NFTs) and their communities.* arXiv:2201.13233 [cs].

Shubber, K. (2022). Voyager digital shares crash after warning of three arrows crypto loss [WWW Document]. Financial Times. URL https://www.ft.com/content/d75801c9-b9dd-4f90-b012-6948cca680d0.

Smart Token Labs, (2022). AutographNFT - get your NFT autographed by famous people [WWW Document]. URL https://autographnft.io/(accessed 3.9.22).

Song, J. (2022). *South korea launches investigations into company behind luna crypto crash [WWW document]*. Financial Times. URL https://www.ft.com/content/a8319c03-3d49-4923-a51a-fc403dcce58a.

Sriman, B., Ganesh Kumar, S., & Shamili, P. (2021). Blockchain technology: Consensus protocol proof of work and proof of stake, in: S. S. Dash, S., Das., & B.K., Panigrahi (Eds.)., Intelligent computing and applications, advances in intelligent systems and computing. Springer Singapore, Singapore, pp. 395–406. https://doi.org/10.1007/978-981-15-5566-4_34.

Statista, (2022). Ethereum energy consumption 2022 [WWW Document]. Statista. URL https://www.statista.com/statistics/1265891/ethereum-energy-consumption-transaction-comparison-visa/(accessed 2.25.22).

Stokel-Walker, C. (2022). An NFT Bubble Is Taking Over the Gig Economy [WWW Document]. Wired UK. URL https://www.wired.co.uk/article/nfts-gig-economy (accessed 2.25.22).

Stolfi, J. (2022). Every computer scientist should be able to see that cryptocurrencies are totally disfunctional payment systems, and that "blockchain technology" (including "smart constracts") is a technological fraud. Would they please say that out loud? Twitter.https://twitter.com/JorgeStolfi/status/1522011168604409856 Date: 2022-05-05, Accessed 2022-06-20.

Sweney, M. (2021). Global shortage in computer chips "reaches crisis point." The Guardian. URL https://www.theguardian.com/business/2021/mar/21/global-shortage-in-computer-chips-reaches-crisis-point (accessed 3.3.22).

Switzer, E. (2022). We Should All Be Grateful That Blockchain Games Are So Embarrassingly Bad [WWW Document]. TheGamer. URL https://www.thegamer.com/new-article-we-should-all-be-grateful-that-blockchain-games-are-so-embarrassingly-bad/(accessed 6.23.22).

Tang, Y., Xiong, J., Becerril-Arreola, R., & Iyer, L. (2019). Blockchain ethics research: a conceptual model. In *Proceedings of the 2019 on Computers and People Research Conference. Presented at the SIGMIS-CPR '19: 2019 Computers and People Research Conference* (pp. 43–49). ACM. https://doi.org/10.1145/3322385.3322397.

Tasca, P., & Tessone, C. J. (2019). *A taxonomy of blockchain technologies: Principles of identification and classification* (p. 4). ledger. https://doi.org/10.5195/ledger.2019.140

Tassi, P. (2021). Ubisoft Quartz's Ghost Recon NFTs Appear To Have Made Just \$400 Total [WWW Document]. Forbes. URL https://www.forbes.com/sites/paultassi/2021/12/20/ubisoft-quartzs-ghost-recon-nfts-appear-to-have-made-just-400-total/ (accessed 6.27.22).

UK Department of Health & Social Care, (2021). A guide to good practice for digital and data-driven health technologies [WWW Document]. GOV.UK. URL https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology (accessed 3.17.22).

United States Department of Justice, (2022). Former Employee Of NFT marketplace charged in first ever digital asset insider trading scheme [WWW Document]. URL https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-charged-first-ever-digital-asset-insider-trading-scheme (accessed 6.10.22).

Uribe, D., & Waters, G. (2020). Privacy laws, non-fungible tokens, and genomics. *The JBBA, 3*, 1–10. https://doi.org/10.31585/jbba-3-2-(5)2020

Volpicelli, G.M. (.2022). Why opensea's nft marketplace can't win [WWW Document]. Wired. URL https://www.wired.com/story/opensea-nfts-twitter/(accessed 6.10.22).

Walch, A. (2015). Why Bitcoin fails as money: an operational risk analysis. https://doi.org/10.2139/ssrn.3864612.

Wareing, J.(2021). [@jonty],"WELL actually you just pin the file to your own ipfs node": You absolutely can! but the metadata file generally points to a specific http ipfs gateway url - NOT the ipfs hash. this means when the gateway operator goes bust i can buy the domain and start serving cat pictures. Twitter. https://twitter.com/jonty/status/1372206059151052803 accessed: 2022-06-04.

White, M. (2022a). Web3 is going just great [WWW Document]. URL https://web3isgoinggreat.com/(accessed 2.25.22).

White, M. (2022b). The Axie Infinity hack, what happened, and why people keep talking about bridges [WWW Document]. Molly White. URL https://blog.mollywhite.net/axie-hack/(accessed 4.1.22).

White, M. (2022c). BattleCatsArena apparently rug pulls several weeks after launch [WWW Document]. URL https://web3isgoinggreat.com/?id=2022-03-05-0 (accessed 4.1.22).

White, M. (2022d). Pixelmon raises \$70 million only to reveal hilariously bad NFTs [WWW Document]. URL https://web3isgoinggreat.com/?id=2022-02-25-3 (accessed 4.1.22).

White, M. (2022e). Abuse and harassment on the blockchain [WWW Document]. Molly White. URL https://blog.mollywhite.net/abuse-and-harassment-on-the-blockchain/ (accessed 4.6.22).

White, M. (2022f). Web3 Is Going Just Great - Bug [WWW Document]. URL https://web3isgoinggreat.com/?theme=bug (accessed 6.20.22).

White, M. 2022g. Cryptocurrency's Robinhood effect [WWW Document]. Molly White. URL https://blog.mollywhite.net/cryptocurrencys-robinhood-effect/(accessed 6.20.22).

Williams, L.J. (.2021). DeviantArt is using AI to alert artists when their work is stolen for NFTs [WWW Document]. Gizmodo Australia. URL https://www.gizmodo.com.au/2021/09/deviantart-ai-stolen-nfts-artists/(accessed 4.6.22).

Wilson, K. B., Karg, A., & Ghaderi, H. (2021). Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity. *Business Horizons S0007681321002019*. https://doi.org/10.1016/j.bushor.2021.10.007

Yaffe-Bellany, D., Griffith, E., & Livni, E. (2022). Cryptocurrencies melt down in a 'perfect storm' of fear and panic [WWW Document]. The New York Times. URL https://www.nytimes.com/2022/05/12/technology/cryptocurrencies-crash-bitcoin.html (accessed 5.30.22).

Zeitchik, S. (2022). *The crypto-skeptics' voices are getting louder [WWW document]*. Washington Post. URL https://www.washingtonpost.com/business/2022/06/03/crypto-skeptics-growing/ (accessed 6.21.22).