A Review of the Non-Fungible Tokens (NFT): Challenges and Opportunities

Mwrwan Abubakar[1](✉), Nilupulee A. Gunathilake[1], William J. Buchanan[1], and Brian O'Reilly[2]

[1] Blockpass Identity Lab (BIL), School of Computing, Engineering and the Built Environment, Edinburgh Napier University, Edinburgh, UK
{m.abubakar,n.gunathilake,b.buchanan}@napier.ac.uk

[2] TreeGreen Ltd. trading as EGG Lighting, Glasgow, UK
brian@egglighting.com

Abstract. Non-Fungible Token (NFT) is an emerging blockchain-based technology. These tokens can represent digital assets, as it has proof of ownership built in. NFTs have the potential to hugely influence both the decentralised markets that exist now and the commercial possibilities that will arise in the future. While there is a wealth of information about NFTs accessible, NFTs are still in an early stage, and some potential obstacles need to be properly addressed. Therefore, in this study, we aim to present a comprehensive review of NFTs and an in-depth study of their underlying fundamental technologies, the current state of their technology roadmap and the potential they present. The paper focuses on the most significant obstacles that must be overcome to use NFT technology from the points of view of security, confidentiality, ownership, administration and property ownership. By doing so, we want to bring attention to these concerns since they have been noticed. Additionally, we go over some of the solutions that can be put into action to avoid some of the challenges that may appear.

Keywords: Blockchain · Non-Fungible Token (NFT) · Cryptography

1 Introduction

Before blockchain-based technology was widely used, the processes for validating digital asset ownership commodities and, consequently, the means of securing them were vulnerable to manipulation, resulting in substantial losses. This is because fast technology breakthroughs and their expansion come in tandem with greater security problems, especially those related to legitimacy [1]. On the other hand, the development of blockchain and distributed ledger technologies led to the creation of a new kind of token known as Non-Fungible Token (NFT) [2]. These tokens indicate digital assets and have integrated evidence of ownership.

This research is Partially funded by the Scottish Funding Council under SFC Innovation Voucher Scheme Agreement.

Z. Tan et al. (Eds.): BDTA 2023, LNICST 555, pp. 171–190, 2024.
https://doi.org/10.1007/978-3-031-52265-9_12

The fact that each token has a new quality that makes it one of a kind and distinguishable from others has strengthened the safety of resources and enhanced the concept of unique ownership. Figure 1 shows differences among fungible, semi-fungible and non-fungible tokens. As more and more uses for NFTs are discovered, interest in this cutting-edge technology grows and attracts a wider audience. By incorporating a digital certificate of the owner into each token, the non-fungibility and uniqueness of NFTs make it possible to easily determine an asset's owner [3]. While this does not completely solve the issue of validity and counterfeit money, it dramatically reduces its severity and makes it much easier to identify.

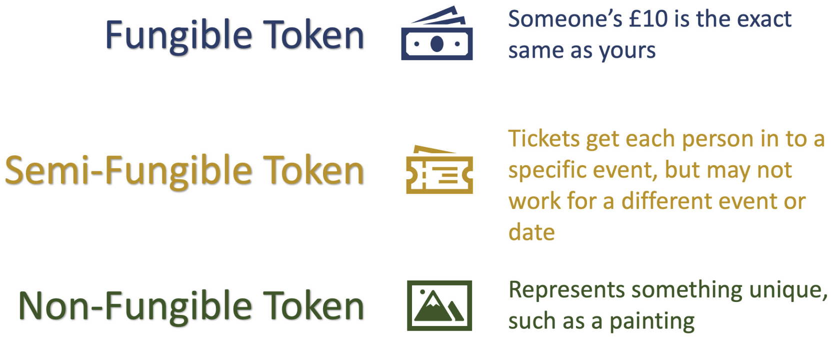
Fungible Token
Someone's £10 is the exact same as yours
Semi-Fungible Token
Tickets get each person in to a specific event, but may not work for a different event or date
Non-Fungible Token
Represents something unique, such as a painting

Fig. 1. Token classification

In addition, it solves the issue of consumers being misled into purchasing counterfeit items, such as tickets or artwork. This is a problem that has been affecting businesses for years. It is simple for purchasers to track down the proprietors of the products that are up for sale, which ensures that they are making a legal investment. Moreover, the emergence of NFTs is opening up new possibilities for creative firms, which have struggled to build online marketplaces in an age controlled by internet-based corporations owing to the absence of exclusive ownership. The introduction of NFTs alleviated this difficulty. By associating a single piece of one-of-a-kind data with a single digital asset on a blockchain, NFTs provide enhanced mechanisms for confirming the authenticity and legality of asset ownership. Customers of NFTs are capitalising on the benefits of NFTs to boost the efficiency and safety of selling their own unique works, therefore increasing their potential for financial gain [3].

Although NFT is a relatively new technology, there is a significant amount of enthusiasm behind it in the scientific community. NFT is not restricted to digital assets, and many other use cases have surfaced recently. According to the study in [4] data collected over the day, shows that the NFT market sees an average trading volume of $4,592,146,914.50, while the cryptocurrency industry as whole notices a volume of $341,017,000.00. In such a short time, NFT-related solutions have contributed 1.3% of the whole Bitcoin market's liquidity. Unique digital artefacts can bring in thousands of times more money for early investors. As of May 2021, the market for NFT-related products and services had expanded significantly from May 2020. More specifically, there were a total of 25,729 sales, and those sales generated $34,530,649,86 in U.S. currency. Some have even labelled NFT "the future of digital assets" because of its sudden surge in popularity. In addition to the data presented above, many people have also expressed curiosity about other types of NFTs. They take part in gaming and trading involving NFTs with equal fervour. More than 10,000 collectable punks (6,039 men and 3,840 women) were created thanks to CryptoPunks [5], one of the earliest NFTs developed on Ethereum, which also contributed to the broad adoption of the ERC-721 standard. By making the process of breeding virtual pets into a game in 2017, CryptoKitties [5] informally drew attention to NFTs and introduced them to the market.

1.1 Problem Statement

As a result of the many beneficial results that have arisen from this merging, NFT technology has attracted an extraordinary amount of interest from the scientific and industrial community. Although NFT technologies show promise, they are still in their development, and several possible obstacles must be properly addressed. For example, concerns about users' privacy and security are among the most significant threats posed by the many applications for NFTs already in existence. Since all transactions take place online, any details of such deals are open to abuse by anybody with access to the internet [6]. However, with technologies such as Zero-Knowledge Proof (ZKP), these issues can be solved. ZKP is a cryptographic system that enables one party to demonstrate specified qualities to another without releasing those attributes [7]. One example would be demonstrating the subject's age without giving the real age.

In addition, users' growing interest in cryptocurrencies such as bitcoin and Ethereum has given rise to a variety of new platforms, one of which is web wallets. Even though blockchain technology is the backbone of web wallets, accounts can still be compromised by hackers using means such as phishing, malware, or Distributed Denial of Service (DDoS) attacks. For this reason, it is suggested that collectors and traders who retain significant quantities of NFTs utilise more than simply an online wallet to store their assets. The most reliable methods of keeping your bitcoin secure in the long run are hardware wallets like Trezor [8] that guarantee the encryption keys never leave the device. Increasing the number of people using these wallets might lessen the likelihood of security breaches and hacking attempts. Binance and Coinbase are two types of non-browser wallets. These services have advanced security teams and support Two-Factor Authentication (2FA) [8].

1.2 Our Contribution

Although a wealth of information regarding NFTs is readily available, the NFT technologies are in a very early stage and some potential obstacles need to be properly addressed. Throw this study we provided a comprehensive review of NFT and their underlying foundational technologies, with the intention of enhancing understanding and awareness of this emerging technological innovation. Our main contribution to this paper can be summarised as follow:

- Provided in-depth study of NFTs and their fundamental components, the current state of their technological roadmap, and the potential they present.
- Analysis of the business cases for tokenization and discussed various markets for purchasing and selling NFTs in various industries.
- Analysis of the most significant obstacles that must be overcome to use NFT technology and outline the existing technical and business risks involved in the tokenization process and discussed some solutions that are now available.
- Finally, provided an investigation into the possible security concerns, and suggested some defensive measures that are necessary to solve these concerns.

The remainder of this paper is organised as follows. We first started with a background overview of blockchain technology in Sect. 2. Then in Sect. 3, we provided an in-depth study of the NFT and its fundamental components, protocols and standards, discussed various markets of the NFTs, and discussed its desired properties. In Sect. 4, we discussed the NFT challenges and summarised the most significant obstacles that need to be overcome. Section 5, presented a security analysis of the NFT technology and investigated the possible security concerns and suggested some defensive measures that are necessary to solve these concerns. Finally, we concluded the paper in Sect. 6.

2 Background Overview of Blockchain Technology

Blockchain is a decentralised digital ledger that preserves all of the transactions that take place across the blockchain network. Because it is distributed, it does not need a centralised authority to perform its functions. In 2008, [9] Nakamoto made the first suggestion that would become known as blockchain technology. Transaction process in blockchain is as in Fig. 2. The term ‘blockchain’ refers to a decentralised database that stores a list of data records and keeps these records connected and secure via cryptographic protocols. The Byzantine problem has been there for a long time, but blockchain technology has found a solution. This solution has been agreed upon by a broad network of players who cannot be trusted. Once the majority of the distributed nodes have validated the data being shared on the blockchain, the data becomes immutable. This is because any modifications made to the data that is being stored would render all future data invalid.

Nodes are an essential component of the blockchain system. They are used to represent customers’ personal computers or other devices that have associated with the blockchain network. Nodes have been used to accomplish various activities, including mining, routing and acting as a wallet by holding a copy of the blockchain data. Additionally, the nodes’ responsibility is to locate the peers

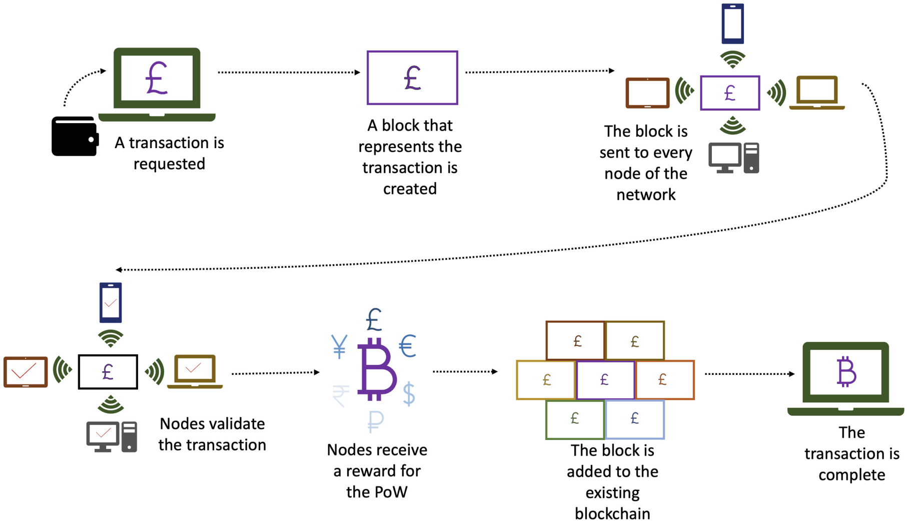
£
A transaction is requested
£
A block that represents the transaction is created
£
The block is sent to every node of the network
£
Nodes validate the transaction
£
¥
€
₹
$
₽
Nodes receive a reward for the PoW
£
£
£
£
£
£
£
The block is added to the existing blockchain
₿
The transaction is complete

Fig. 2. Transcation process in blockchain

directly linked to the blockchain network. In addition to this, it is the responsibility of each node to establish and keep a relationship with its peers that have been found [9]. Every single node contributes to verifying transactions and spreading them further. Additionally, nodes function as a distributed network by keeping copies of the blockchain, which includes details about all the activities that have been preserved in the blockchain system, thereby displacing the need for centralised servers to store the transaction data in favour of a decentralised and distributed ledger. In conclusion, nodes have the potential to also act as miners, a role in which they might be rewarded with cryptocurrency for their efforts in verifying and confirming previous transactions carried out over the blockchain [9].

Cryptographic codes are used to permanently record blockchain transactions, and the network can verify the integrity of individual blocks. This idea guarantees that the blockchain will remain secure. Because of the one-of-a-kind nature of the hash values, it is possible to identify fraudulent activity since any changes made to a block in the chain instantly result in a new hash value. All transactions may be examined in full transparency thanks to the decentralised nature of the blockchain's structure [9]. However, the technology can be used in many scenarios and is the subject of study in various disciplines. As a result, the idea has piqued the interest of other efforts coming from various sectors, such as banking, public and welfare care, privacy and security smart contracts and the Internet of Things (IoT). Despite this, the financial sector is generally considered the most significant user. It seems that the reason for this is that it is often impossible to determine an item's actual owner.

2.1 Ethereum

Ethereum is a distributed ledger technology that incorporates a Turing-complete programming language. A configurable ownership model, transaction format and state transition mechanisms are all user-definable due to their abstract layer. To this end, decentralised applications are used, which are a set of cryptographic rules executed only when certain conditions are met [10]. Furthermore, such a network provides the backbone for the Ethereum blockchain's virtual currency, Ether. Ether can be considered the fuel that powers Ethereum's decentralised apps. Payments can be made using this currency to other accounts or machines performing a certain activity. Therefore, you can use Ether to make conventional P2P payments, launch decentralised applications, create tokens and create smart contracts. Ether can also be used to build smart contracts. The Ethereum network agrees on the state of a central computer (the Ethereum Virtual Machine, or EVM) in all Ethereum blockchain systems. Every computer that is part of the Ethereum network, also known as an Ethereum node, stores a copy of the current state of this particular machine. In addition, every member can broadcast a request for this machine to carry out any computation they want. The calculation is checked, validated and executed by other participants in the network whenever a request of this kind is broadcast. Because of this execution, the EVM will enter a new state, which will then be committed and broadcast over the whole network [10].

2.2 Smart Contract

Nick Szabo was the first person to use this terminology, 'smart contracts', which was coined in 1994 [11], before using the decentralised ledger to host them. This was proposed as an idea for a technology that could monitor and ensure compliance with the conditions of an agreement that had been negotiated online. Smart contracts have been used to facilitate the movement of Bitcoin from one user to another when specific requirements are met [9]. However, this is restricted to the realm of digital money. On the other hand, Ethereum treats the smart contract as an item in its own right, complete with a separate account and a unique address. In addition to facilitating communication between contracts, this account may also be used to store data, receive digital currency and make payments. Ethereum replaced the difficult language used by Bitcoin with a language known as solidity, which is a Turing complete language. This change was made so that developers could create their own smart contracts [10]. Smart contracts allow unknown parties and decentralised players to carry out fair trades without needing a trustworthy third party. In addition, they provide a uniform mechanism that can be used to construct apps for various business sectors. Every person involved can see the states that include the requirements and directions, guaranteeing that everyone can see how the rules are followed. To guarantee the sequence-dependent execution of their procedures, most NFT solutions [12] rely on blockchain platforms that are based on smart contracts.

3 Non-Fungible Token (NFT)

NFT is an abbreviation for 'Non-Fungible Tokens', which refers to digital assets reflective of physical and digital creative labour or Intellectual Property (IP). Some examples of NFT include gifs, music, games, digital art, video clips, and other media types. Because each token in an NFT system cannot be exchanged for another token, the term 'nonfungible' refers to the fact that each token is an independent entity that stands in for a particular thing. The NFTs are a component of blockchains in general and the Ethereum blockchain in particular. However, they are distinct from Ethereum cryptocurrencies, which are fungible, meaning that they may be traded for other assets of a similar kind. This is because NFT is an Ethereum smart contract-based coin. It was first suggested in Ethereum Improvement Proposals (EIP)-721 [13], and further work was carried out in EIP-1155 [14].

NFT is not the same as other cryptocurrencies similar to Bitcoin in terms of the features built into it. Bitcoin is a conventional coin, meaning that all of the coins are comparable and cannot be differentiated from one another. In comparison, NFT cannot be imitated and traded, making it an ideal choice for describing something or someone in a unique way. A developer may use NFTs on digital currencies to prove the presence of digital goods like movies, photos, artwork, theater tickets, and other tangible assets. These digital assets can take the shape of movies, images, art, etc. Applications in NFT can be recognised as indicated in Fig. 3. Additionally, the inventor can earn royalties whenever a successful deal occurs on any NFT marketplace or via peer-to-peer trading. Because of its full-history commodities, deep volatility, and simple compatibility, NFT can be an efficient mechanism for preserving IP. This is because NFT is a distributed ledger that many parties can use. In this section, we will investigate the possibilities presented by NFTs and talk about a few common areas that can profit from using NFTs [4].

3.1 Protecting Digital Collectibles

Digital assets may include everything from collectibles and wine to digital photos and movies, digital property investment, domain names, and even jewels and crypto passports. For our example today, let us go to the artistic world. Traditional artists are limited in where they may show their work. Due to inattention, the prices do not fairly reflect the value of the works. Unfortunately, platforms and advertisements have eaten into their profits from sharing their work online. NFTs are liable for creating digital copies of their work that incorporate credentials. Artists are not required to sign up for ownership of their work or material for distribution services. The financial benefits to them are substantial. Artists seldom stand to gain royalties on later sales of their works [15]. An NFT may be designed such that the artist receives a predetermined royalty payment whenever an NFT based on his digital work is sold, such as SuperRare [16], MakersPlace [17], VIV3 [18]. These platforms might be used to efficiently manage and secure digital artworks. Furthermore, numerous sites like Mintable [19] and Mintbase

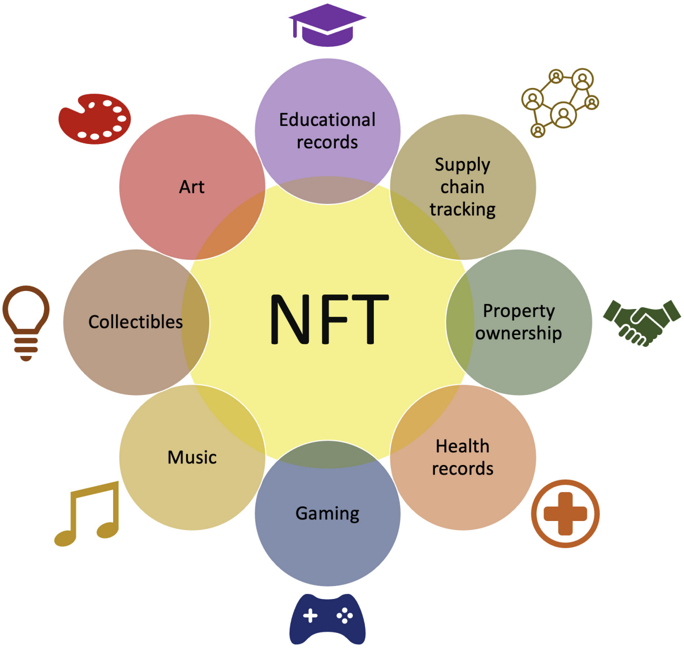

Fig. 3. NFT applications

[20] have made it easy for ordinary people to create their own NFT works by providing them with pre-made templates and other templates and tools to work from.

3.2 Boosting Gaming Industry

There are many unrealised possibilities for NFT in the gaming industry. Numerous past crypto-themed video games have been published, including CryptpoKitties [21], Cryptocats [22], CryptoPunks [23], Meebits [24], etc. A novel and engaging feature of these games is the 'breeding' system. Users have the option of taking care of their own pets and spending considerable time in the breeding of new springs. They may even buy rare or limited edition digital pets to flip for a profit. With the bonus, many investors are eager to get in on the action, which has boosted NFTs' appeal. The NFT serves many fascinating functions, like establishing a chain of titles for virtual things in games and encouraging the economic marking of ecological hotspots. Producers of games and players alike stand to gain from such endeavours. Game developers who are also NFT publishers of features, such as guns and skins may be eligible for royalties on every instance of their creations being resold on the international market. In this case, everyone becomes victorious. The gamers may obtain unique and personalised gaming gear. Because of this, a business model will emerge that is mutually beneficial for NFT players and developers. After that, the blockchain community further broadens NFTs to include many additional forms of digital assets.

3.3 Tokenised Stock

Tokenised stocks are essentially the same as shares of stock in an openly listed firm, such as those traded on the Nasdaq or the S&P 500. These indexes measure the performance of 500 of the largest publicly traded companies in the United States. On the other hand, tokenised equities are represented by digital tokens rather than traditional stock certificates. When an investor purchases a conventional stock on an exchange or during an Initial Public Offering (IPO), their shares will normally appear in their brokerage account shortly after the transaction is completed. The methodology for tokenised equities is the same, with one significant modification being required. Since the shares are based on a blockchain, they can be purchased and traded on a cryptocurrency exchange just like any other cryptocurrency. When generating a tokenised stock, the procedure often involves the participation of a custodian and an investing institution. The institution purchases the underlying stock, which is deposited with the custodian. Tokens are distributed over a blockchain and are denominated in shares held in reserve by the custodian. The value of the underlying shares is used to determine the price of each token. After that, the tokens might be posted on a crypto exchange, where they would function similarly to other cryptocurrencies in terms of being able to be purchased and exchanged. Those who own stock tokens are granted the same exposure to the underlying stock as if they held the shares themselves, including the right to receive dividend payments if appropriate. However, they do not hold any shares in the company. They own an asset that is a derivative backed by real company shares [25].

To raise cash, which is the primary objective of the majority of firms, tokenising equity is being done by many businesses for the same reason that they issue shares of stock. Instead of issuing extra shares or going public via the more conventional route of having an IPO, there might be significant benefits to be gained by releasing digital tokens to increase a company's capital [26]. Tokenised equity is putting the securities and exchange regularities in a position where it has no choice but to regulate cryptocurrencies like Bitcoin and others. However, the federal government has been somewhat slow to decide how or if they want to handle Bitcoin regulations and other cryptocurrencies. Tokens are considered securities since they have the same qualities and functions as stocks and are thus issued by firms in place of shares. This indicates they must register with the appropriate authorities and submit the required paperwork. Because of this, Security Token Offerings (STOs) came into existence. STOs are comparable to Initial Coin Offerings (ICOs), which are essentially the same as ICOs except for the additional stipulation that the company that issues the tokens admits that the token symbolises fairness and is, therefore, security [26].

3.4 Protocols

The development of an NFT calls for using an underlying distributed ledger to keep records and the execution of tradable transactions across a peer-to-peer network. In most of its coverage, this paper considers the distributed ledger to be a specialised database that holds NFT data. In particular, we are working on the assumption that the ledger has the qualities of fundamental security, integrity, and accessibility. In addition to this, two other responsibilities make up an NFT system. These are the NFT owner and the NFT buyer. The step-by-step procedure can be found below:

- **NFT digitisation**: The owner of an NFT makes sure that all of the details included in the lease, including the title and description, are correct. After that, he or she converts the raw data into the appropriate digital format using a computer.
- **NFT store**: An owner of NFTs often places raw information in a database that is not part of the blockchain. It is important to note that they are permitted to save the raw data inside of a blockchain, although this procedure requires a significant amount of gas.
- **NFT signing**: A transaction is signed by the NFT owner and sent to a smart contract along with a hash of the NFT data.
- **NFT mint and trade**: Once the smart contract has received the transactions with the NFT data, the minting and trading procedure may commence. The reasoning behind the Token Standards is the primary mechanism that supports NFTs.
- **NFT confirmation**: The minting process is considered finished after verifying that the transaction took place. With this method, NFTs will indefinitely connect to a specific blockchain address, which will prove their persistence.

Each block in a blockchain-based system has a certain amount of storage space available. When the storage space in one block is exceeded, more transactions will be added to a subsequent block connected to the initial data block [27]. In the end, all interconnected bricks have produced a history that covers a lengthy period of time and is unchangeable. The NFT system may be considered an application that uses blockchain technology. In order to activate the smart contract, a fresh transaction has to be sent each time an NFT is created or sold. Following the confirmation of the transaction, the information about the NFT and the ownership information is appended to a new block. This operation ensures that the history of the NFT is not altered and that ownership is maintained.

3.5 Standards

ERC-20. Tokens are increasingly being created using the ERC-20 [28] standard. It introduces the concept of fungible tokens that may be built atop Ethereum if certain requirements are fulfilled. Tokens are made interchangeable because of the standard (in terms of type and value). An arbitrary token will always have the same value as each and every other token. This has contributed to the mania around ICOs since 2015 and continues to do so today. This is how many public chains and several blockchain-based DApps get enough initial investment for their projects.

ERC-721. ERC-721 [29] introduces a new token standard that is not interchangeable with existing tokens. This token type is distinct from those already in circulation. To be more specific, each NFT has a contract address and a corresponding uint256 variable called tokenId that provide a globally unique identifier. Additionally, the tokenId could be entered into a system to generate random, one-of-a-kind identifiers, like zombie or cartoon figure images.

ERC-1155. To further increase the description of both fungible and non-fungible tokens, there is a specification described as ERC-1155 (multi-token standard) [14]. A graphical user interface is provided regardless of the number of tokens being represented. According to the previous norms, each tokenId in contact may only include a single token type. With ERC-20, for instance, any currency type may be used with a dedicated smart contract. The ERC-721 standard also centralises the distribution of NFTs in a single contract with standard parameters. ERC-1155, on the other hand, is an extension of the capabilities of tokenId, and each of its components may separately represent a distinct adjustable token type. Metadata, lock times, dates, supplies, and other individualised qualities may all be stored in this field. We have provided an image for your consideration to further illustrate the aforementioned structural distinctions between the two.

3.6 Desired Properties

NFT schemes are fundamentally decentralised applications, and as a result, they use the advantages and features provided by the public ledgers upon which they are built. The following is a summary of the most important characteristics:

- **Verifiability**: The NFT, together with the token information and ownership, may be independently confirmed by the public.
- **Transparent execution**: All transactions involving NFTs, from creation through exchange and purchase, are transparent.
- **Availability**: There is never an outage in the NFT system. On the other hand, all tokens and NFTs issued are always open for purchase and sale.
- **Tamper resistance**: Once a deal has been validated, the associated NFT metadata and trade records are unchangeable.
- **Usability**: The most recent ownership information is displayed simply and easily on each NFT.
- **Atomicity**: Trading NFTs can be done in a single transaction that is simultaneous, consistent, segregated, and permanent. The NFTs can share the same execution state.
- **Tradability**: Every non-fiat currency and the things that correspond to it may be traded and exchanged with complete freedom.

4 NFT Challenges

As with any developing technology, many hurdles must be cleared before the NFT, as mentioned above, applications may be developed. We address both the system-level concerns generated by blockchain-based platforms and human elements such as governance, legislation, and society as we explore some common obstacles from accessibility, safety, democratic accountability, and extensibility [6].

4.1 Usability Challenges

Testing a product or design for usability is evaluating how well it performs for the intended audience in terms of their time, effort, and overall happiness. Most NFT techniques are developed using Ethereum as their base layer. As a result, it should not surprise that the primary issues with Ethereum were inherited. In this article, we will explore two significant difficulties that directly affect the user's experience.

4.2 Slow Confirmation

The transactions related to NFTs are often sent to the smart contract to accomplish dependable and transparent administration (such as mining, selling, and exchange). Current NFT systems, on the other hand, are inextricably linked to the public blockchains on which they are based, which causes them to have poor efficiency. Bitcoin reaches merely 7 Transactions Per Second (TPS) [30] while Ethereum does only 30 TPS. This ultimately leads to the validation of NFTs taking an incredibly long time. In order to resolve this problem, either the topology of the blockchain has to be redesigned, the structure needs to be optimised [31], or the consensus procedures need to be improved [32].

4.3 High Gas-Prices

When it comes to the minting of NFTs at a big scale, which entails uploading the information to the blockchain network, high gas costs have become a serious concern for NFT markets. This is particularly true when gas prices are taken into consideration. Because smart processing contracts require computing resources and storage space, the fees associated with NFT-related transactions are always higher than those associated with simpler transfer operations. As of the time, this article was written, mining one NFT coin may cost up to $150 USD or more [33]. The expense of doing a simple NFT trade might range from $60 USD to $100 USD for each transaction. The widespread adoption of this technology is severely hampered by the high costs associated with its complicated operations and heavy congestion.

4.4 Data Inaccessibility

A cryptographic “hash” is used in the more popular NFT projects. To reduce the amount of gas needed, the identifier, which will serve in place of a copy of the file, will be tagged with the token before being added to the blockchain. Since the original file might be deleted or corrupted, this raises scepticism about the NFT among users. Many NFT projects have combined their infrastructure with a dedicated file-sharing platform such as IPFS [34]. If users know an IPFS address and are connected to the IPFS network, they may access the content in inquiry. This integration allows users to discover content more easily.

Nevertheless, these kinds of systems are unavoidable. When users “upload” their files to the server, When you transfer metadata to IPFS nodes, there is no assurance that the data will be duplicated across all nodes. The data might become inaccessible if a property is kept on IPFS and that node loses network connectivity. DECRYPT.IO and CHECKMYNFT.COM have identified and reported this problem. There is also the possibility that an NFT may refer to an incorrect file address. In such a situation, it would be difficult for a user to demonstrate that they are the rightful owner of the NFT. It is risky to build an NFT system around storage provided by an external system because of the potential for data loss [35].

4.5 Anonymity and Privacy

Currently, there is a lack of research on the security and confidentiality of NFTs. The Ethereum network, upon which most accounting entries of NFTs are conducted, provides only pseudo-anonymity rather than full invisibility or privacy. Users can hide some facets of their identity, despite the fact that the general public is informed of the links between their real names and their associated email addresses. Users’ activity associated with the exposed address may be seen in any other case [36]. Due to the complexity of the cryptographic primitives and confidentiality requirements, existing privacy-preserving methods, such as ring signatures, encryption algorithm, zero-knowledge verification, and multiparty computation have been introduced as a solution for privacy issues in NFTs [37]. Reducing the high cost of computing is essential for implementing privacy-promised methods in blockchain-based systems as in other distributed ledgers. In addition, the information collected from users is the primary focus of any system. However, there is always a chance that the data (kept off-chain but related to tags on-chain) will become unconnected or misused.

4.6 Governance Consideration

NFTs, much like the scenarios that most cryptocurrencies find themselves in, are met with obstacles such as stringent management from the governance. On the other hand, figuring out how to appropriately manage this young technology and the market it corresponds to is another difficulty. Two concerns that are common on both sides are discussed below.

Legal Dilemmas. In many fields, including law and politics, NFTs confront obstacles. Potential danger zones include commodity markets, foreign exchange, Know Your Customer (KYC) information, and more. It is necessary to be thoroughly aware of the regulatory oversight and problems linked with the issue before moving further into the NFT tracks. Some countries, like China and India, may have strict regulations on the buying and selling of NFTs and cryptocurrencies. In order to successfully exchange, trade, sell, or purchase NFTs, one must first overcome the hurdles management provides. In accordance with the law, users are only permitted to engage in derivatives trading on regulated exchanges (like those for stocks and commodities), or they must trade tokens directly with another individual [38]. Many nations, such as Malta and France, are working on enacting appropriate regulations to control the market for digital assets and related services [39]. In other places, problems are handled using the laws already in place. They demand that purchasers adhere to conditions that are difficult to understand and are often even contradictory. This means that thorough research must be conducted before putting any real money into NFTs.

Property Taxation Concerns. According to the regulations now in place, goods associated with IP, such as books, artworks, and domain names, among other things are considered taxable. Contrarily, this does not include applicable to NFT-based transactions. Even while only a small number of countries, such as the US (via the Internal Revenue Service, or known as IRS), tax cryptocurrency as ownership, the vast majority of governments and regions throughout the world have not yet pondered doing so; this might lead to a surge in the amount of fraudulent financial activities disguised as NFT trading. Many governments worldwide have expressed an interest in determining consistent tax consequences for the distribution of NFTs [40]. In particular, tax liabilities arising from investment income on NFT investments must be the responsibility of the relevant individuals. It is also necessary to impose taxes on exchanges of NFT for NFT, NFT for IP, and Ether for NFT (or vice versa). Also, high-yield commodities, such as rare books and art, need a more lenient tax rate. Following such in-depth deliberation, it has been suggested that NFT-related transactions seek out the advice of a specialised tax department for additional help.

4.7 Intellectual Property (IP) Right

This includes information regarding IP to help compensate for the next major factor on the list of dangers and roadblocks posed by NFTs. It is essential to analyse a person's ownership rights regarding a particular NFT. Before completing a purchase, it is essential to ascertain whether or not the vendor holds the NFT in question. There have been documented cases of individuals photographing non-circulating tax receipts (NFTs) or minting replicas of NFTs. Therefore, when an NFT is acquired, the purchaser receives the rights to use it but not the rights to its IP. The terms and conditions necessary to acquire ownership of an NFT are stored in the metadata of the underlying smart contract [41].

It should come as no surprise that applications for NFT can provide significant income possibilities. They are, nevertheless, confronted with a great number of challenges. NFTs are experiencing a big market hype bubble due to the support they receive from notable public figures. The fact that the volume of trading in NFTs has increased more than once in only one year indicates that they have a lot of untapped potential. The exchange of NFTs, on the other hand, is not subject to any particular regulations or guidelines.

5 Security Analysis

The blockchain, storage, and web application that make up an NFT system are the three components that make up a combined technology known as an NFT system. It is difficult to do a security assessment on the NFT system because each component can become an attacking interface, which leaves the whole system very exposed to the attacker. As a result, we have chosen to implement the threat and risk assessment, which considers all elements of a system's security, including its authenticity, integrity, non-reliability, availability, and access control. We do an investigation into the possible security concerns, and we suggest a few of the defensive measures that are necessary to solve these concerns.

5.1 Cybersecurity

The development of the digital world and an increase in the volume of NFTs transactions have led to a major rise in the danger of cybercrime and fraudulent activity. Criminals with malicious intent can impersonate well-known NFT tokens and sell fake NFTs using their identities. Theft of copyright, piracy of popular NFTs, and the distribution of free NFTs are some of the other key dangers and difficulties that NFT tokens face in terms of cybersecurity and fraud. The recent instances of hackers stealing NFTs from users of Nifty Gateway are one of the most current illustrations of the cybersecurity risk associated with NFTs [36]. Although the development of technology makes it possible to conduct transactions involving digital assets with increased efficacy but also presents risks, most notably in the cyber security domain.

5.2 Spoofing

Spoofing is the capacity to pretend to be something else, such as another user or machine on the system. A hostile attacker might exploit identification flaws or steal a user's private key while minting or selling interactions with NFTs, allowing the attacker to unlawfully transfer ownership of the NFTs. Because of this, we strongly advise establishing a formal verification for the NFT smart contract and using a cold wallet to prevent private key information leaks.

5.3 Tampering

The term 'tampering' refers to the act of deliberately modifying NFT data, which is a violation of the system's integrity. Assume that the blockchain is a secure public transaction ledger and that the hash method is both preimage and second preimage resistant. Once a transaction has been validated, the metadata and possession of NFTs cannot be deliberately altered beyond that point. Nevertheless, the data held outside of the blockchain is susceptible to manipulation. When trading or exchanging NFT-related assets, we strongly advise our customers to give the original data in addition to the hash data to the NFT buyer. This is because the hash data is used to verify the authenticity of the original data [42].

5.4 Smart Contracts Security

From the perspective of the NFT environment, one of the most pressing challenges is creating and protecting smart contracts. Poly Network, a well-known protocol for Decentralised Finance (DeFi) that allows cross-chain interoperability, was recently the victim of an attack by hackers. The theft of almost $600 million worth of NFTs draws attention to severe problems in the security of smart contracts [43]. One of the primary factors that might result in weaknesses in smart contracts is the absence of certain security standards that have been validated throughout the industry. This issue pertains to the Solidity programming language. Because both the transactions and the code in a smart contract are immutable, the developers must make certain that both the code and each transaction are secure. On the other hand, there are no clearly established standard methods for constructing smart contracts that programmers should adhere to across all projects. Developers do not have access to the tools that would simplify the process of creating, testing, verifying, and auditing smart contracts. More significantly, developers do not have access to the tools that would allow them to work together.

5.5 Repudiation

The term "non-repudiation" refers to the scenario in which a statement's creator cannot refute it. Those involved in blockchain transactions cannot deny the transaction's legitimacy or their behaviour. A non-repudiation service aims to ensure the authenticity of transmitted data by amassing and delivering irrefutable proof of message delivery. Therefore, it is impossible to refute that one user sent NFT to another [44]. Cryptography, such as digital signatures, is used to accomplish nonrepudiation, which also includes services for authentication, auditing, and recording. Digital signatures in blockchain ensure that a party cannot subsequently dispute delivering information or repudiate the authenticity of its signature. A malicious attacker might intercept the hash data or cause it to bind with the attacker's address. Since a multi-signature contract requires confirmation from more than one party before it can legally bind, we think it can help alleviate some of the severity of the problem. In addition, the attackers can easily take advantage of the connection between the hash and the transaction. As a result, we advise that developers of NFTs employ privacy-preserving smart contracts rather than standard smart contracts to safeguard their users' personal information.

5.6 DoS

DoS attacks breach the availability of the NFT service and bring it to a halt, although unauthorised users may use it. To users' great relief, blockchain technology ensures that their transactions will always be highly available. Users authorised to do so may access the necessary information whenever required, and there will be no loss of data resources as a result of unintended mistakes. DoS attacks may also be launched against non-blockchain-based resources, such as centralised web apps or raw data, which can disrupt NFT operations. The decentralised autonomous organisation and parity wallet hacks of 2016 and 2017, respectively, demonstrated the critical flaws in Ethereum smart contracts. Ethereum's fundamental flaws were uncovered in the 2016 Decentralised Autonomous Organisation (DAO) and 2017 parity wallet hacks. The approach given in [45] employs two Artificial Intelligence (AI) techniques-Random Forest (RF) and XGBoost that grant complete independence to decision-making skills within the proposed security framework. Second, an interplanetary file system is proposed enabling data load balancing and distributed file storage of IoT data. They also suggested a distributed system based on cloud and fog computing for monitoring smart contracts for DDoS attacks. The detection system's efficacy is measured against a real-world IoT dataset called BoT-IoT. As smart contracts control the distribution of sales permits in the NFT system. Once again, a weak smart contract's design can cause NFTs to lose their desirable qualities. Another technique was described in [46] as a potential sort of attack that can be launched against the memory pools (mempools) of blockchain-based cryptocurrencies. This study examined the implications of such an assault on the Bitcoin mempool on the transaction fees paid by normal users. Additionally, the study offered methods to prevent such an assault. The countermeasures consist of fee-based as well as age-based designs that maximise the size of the mempool and assist in mitigating the consequences of DDoS attacks. Then, they simulated their designs and assessed their utility under various attack conditions. The findings can be applied to other blockchain-based apps that cache network events using memory pools.

6 Conclusion

This study provided a comprehensive review of NFTs and an in-depth study of their underlying fundamental technologies, illustrated their technical framework, and unique characteristics, and analysed the business cases, and the possible roadblocks that may arise. The paper started with a background on blockchain technology and its decentralised structures, the Ethereum blockchain and discussed the role of smart contracts in the development of tokenization. In addition, the paper provided an in-depth study of the NFT and its fundamental components, protocols and standards, discussed various markets of the NFTs, and discussed its desired properties. However, the ever-increasing prevalence of the usage of NFTs is accompanied by many obstacles. So, therefore, the paper outlined the existing technical and business risks involved in the tokenization process, discussed the NFT challenges and summarised the most significant obstacles that need to be overcome, such as the absence of industry-wide security standards for smart contracts, the lack of clarity about intellectual property rights, the potential for fraud as a result of artist impersonation, transparency that breaches the user's security and privacy, and the severe negative impacts on the environment caused by the high amount of energy consumption. The paper goes further and presented a security analysis of the NFT technology and investigated the possible security concerns and suggested some defensive measures that are necessary to solve these concerns. Finally, we hope that the findings of this study provide a point of reference and motivation for future research efforts in this domain.

References

1. Catalini, C., Gans, J.S.: Some simple economics of the blockchain. Commun. ACM **63**(7), 80–90 (2020)
2. Steinwold, A.: The History of Non-Fungible Tokens (NFTs) (2019). Retrieved from Medium: https://medium.com/@Andrew.Steinwold/the-history-of-non-fungible-tokens-nftsf362ca57ae10
3. Raman, R., Raj, B.E.: The world of NFTs (non-fungible tokens): the future of blockchain and asset ownership. In: Enabling Blockchain Technology for Secure Networking and Communications, pp. 89–108. IGI Global (2021)
4. Wang, Q., Li, R., Wang, Q., Chen, S.: Non-fungible token (NFT): overview, evaluation, opportunities and challenges. arXiv preprint arXiv:2105.07447 (2021)
5. Plachimowicz, E., Wójcik, P.: What makes Punks worthy? Valuation of Non-Fungible Tokens based on the CryptoPunks collection using the hedonic pricing method. No. 2022–27 (2022)
6. Rehman, W., e Zainab, H., Imran, J., Bawany, N.Z.: NFTs: applications and challenges. In: 2021 22nd International Arab Conference on Information Technology (ACIT), pp. 1–7. IEEE (2021)
7. Hasan, J.: Overview and Applications of Zero Knowledge Proof (ZKP). Nanjing University of Posts and Telecommunications, Nanjing (2019)
8. Khan, A.G., et al.: Security of cryptocurrency using hardware wallet and QR code. In: 2019 International Conference on Innovative Computing (ICIC). IEEE (2019)
9. Nakamoto, S., Bitcoin, A.: A peer-to-peer electronic cash system (2008). Bitcoin https://bitcoin.org/bitcoin.pdf4.2
10. Buterin, V.: A next-generation smart contract and decentralized application platform 2014 (2019). https://github.com/ethereum/wiki/wiki/White-Paper
11. Szabo, N.: Smart Contracts (1994). https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

12. Arora, A., Kanisk, K.S.: Smart Contracts and NFTs: non-fungible tokens as a core component of blockchain to be used as collectibles. In: Khanna, K., Estrela, V.V., Rodrigues, J.J.P.C. (eds.) Cyber Security and Digital Forensics. LNDECT, vol. 73, pp. 401–422. Springer, Singapore (2022). https://doi.org/10.1007/978-981-16-3961-6_34
13. Entriken, W., Shirley, D., Evans, J., Sachs, N.: EIP-721: ERC-721 non-fungible token standard. Ethereum Improvement Proposals 721 (2018)
14. Radomski, W., Cooke, A., Castonguay, P., Therien, J., Binet, E., Sandford, R.: EIP 1155: ERC-1155 multi token standard. Ethereum, Standard (2018)
15. Ali, M., Bagui, S.: Introduction to NFTs: the future of digital collectibles. Int. J. Adv. Comput. Sci. Appl. **12**(10), 50–56 (2021)
16. Tran, K.C.: What is SuperRare? 26 March 2020. https://decrypt.co/resources/what-is-superrare-3-minute-guide-explained-art-collectible
17. Makersplace: Rare, Authentic & Curated Digital Art. https://makersplace.com/
18. VIV3: WELCOME TO VIV3 - Explore the Marketspace. https://viv3.com/
19. Mintable: MoonPay — MINTABLE - Revolutionizing WEB3 Payments. https://mintable.app/
20. Mintbase: What can I do with Mintbase? https://docs.mintbase.io/
21. CryptoKitties: CryptoKitties. https://www.cryptokitties.co/
22. CryptoCat NFT: CRYPTOCATS, Collectible 8-bit Cats on Ethereum Blockchain. https://cryptocats.thetwentysix.io/
23. CryptoPunks V1. https://v1punks.io/. Accessed 02 Mar 2023
24. Larva Labs: What are the Meebits? https://meebits.app/. Accessed 02 Mar 2023
25. Bhandarkar, V.V., Bhandarkar, A.A., Shiva, A.: Digital stocks using blockchain technology the possible future of stocks? Int. J. Manage. (IJM) **10**(3) (2019)
26. Roth, J., Schär, F., Schöpfer, A.: The Tokenization of assets: using blockchains for equity crowdfunding. In: Theories of Change: Change Leadership Tools, Models and Applications for Investing in Sustainable Development, pp. 329–350 (2021)
27. Antonopoulos, A.M.: Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, Inc., Sebastopol (2014)
28. Vogelsteller, F., Buterin, V.: ERC-20 token standard (2015). https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20-token-standard.md (2018)
29. Entriken, W., Shirley, D., Evans, J., Sachs, N.: ERC-721 non-fungible token standard (2018). Ethereum Foundation-https://eips.ethereum.org/EIPS/eip-721
30. Croman, K., et al.: On scaling decentralized blockchains. In: Clark, J., Meiklejohn, S., Ryan, P.Y.A., Wallach, D., Brenner, M., Rohloff, K. (eds.) FC 2016. LNCS, vol. 9604, pp. 106–125. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53357-4_8
31. Abubakar, M., Jarocheh, Z., Al-Dubai, A., Liu, X.: A survey on the integration of blockchain and IoT: challenges and opportunities. In: Jiang, R., et al. (eds.) Big Data Privacy and Security in Smart Cities. Advanced Sciences and Technologies for Security Applications, pp. 197–221. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-04424-3_11
32. Abubakar, M., Jaroucheh, Z., Al-Dubai, A., Buchanan, B.: PoNW: a secure and scalable proof-of-notarized-work based consensus mechanism. In: Proceedings of the 2020 4th International Conference on Vision, Image and Signal Processing, pp. 1–8 (2020)
33. Baldwin, A.: How Much Does It Cost to Mint an NFT? The Answer (2022). https://www.cryptopolitan.com/how-much-does-nft-minting-cost/
34. Ossa, P.: Evaluating decentralized storage services for storing NFT related data (2021)

35. Ali, O., Momin, M., Shrestha, A., Das, R., Alhajj, F., Dwivedi, Y.K.: A review of the key challenges of non-fungible tokens. Technol. Forecast. Soc. Chang. **187**, 122248 (2023)
36. Das, D., Bose, P., Ruaro, N., Kruegel, C., Vigna, G.: Understanding security issues in the NFT ecosystem. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, pp. 667–681 (2022)
37. Salleras, X., Rovira, S., Daza, V.: FORT: right-proving and attribute-blinding self-sovereign authentication. Mathematics **10**(4), 617 (2022)
38. Uribe, D., Waters, G.: Privacy laws, genomic data and non-fungible tokens. J. Br. Blockchain Assoc. (2020)
39. Blemus, S.: Law and blockchain: a legal perspective on current regulatory trends worldwide. Revue Trimestrielle de Droit Financier (Corporate Finance and Capital Markets Law Review) RTDF 4–2017 (2017)
40. Nguyen, A.Q.: The mysteries of NFT taxation and the problem of crypto asset tax evasion. SMU Sci. Technol. Law Rev. **25**(2), 323 (2022)
41. Okonkwo, I.E.: NFT, copyright and intellectual property commercialization. Int. J. Law Inf. Technol. **29**(4), 296–304 (2021)
42. Kshetri, N.: Scams, frauds, and crimes in the nonfungible token market. Computer **55**(4), 60–64 (2022)
43. Wright, T.: Hackers stole at least $600 M in Poly exploit across three chains (2021)
44. Hasan, H.R., et al.: Incorporating registration, reputation, and incentivization into the NFT ecosystem. IEEE Access **10**, 76416–76433 (2022)
45. Kumar, R., Kumar, P., Tripathi, R., Gupta, G.P., Garg, S., Hassan, M.M.: A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. J. Parallel Distrib. Comput. **164**, 55–68 (2022)
46. Saad, M., Njilla, L., Kamhoua, C., Kim, J., Nyang, D., Mohaisen, A.: Mempool optimization for defending against DDoS attacks in PoW-based blockchain systems. In: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 285–292. IEEE (2019)